T-CY (2023)4
Strasbourg, 12 décembre 2024

# Comité de la convention sur la cybercriminalité (T-CY)

## Évaluation de l'article 19 de la Convention de Budapest

## la perquisition et la saisie de données informatiques stockées :

## Rapport d'évaluation

Adoptée par la 31e plénière du T-CY le 12 décembre 2024

## Contenu

# Abréviations

| | |
|---|---|
| CC | Code pénal |
| CCP | Code de procédure pénale |
| CMA | Loi sur les mesures coercitives |
| CPC | Code de procédure pénale |
| CrimPC | Code de procédure pénale suisse |
| DCCP | Code de procédure pénale néerlandais |
| CEDH | Convention européenne des droits de l'homme |
| Par exemple | Par exemple |
| IPA | Loi sur les pouvoirs d'investigation |
| NCIS | National Criminal Investigation Service (Service national d'enquête criminelle) |
| RIPA 2000 | Loi sur la réglementation des pouvoirs d'investigation (Regulation of Investigatory Powers Act) 2000 |
| | Strafprozeßordnung (Code de procédure pénale) |
| TCA | Loi sur la cybercriminalité |
| TEI | Brouillage ciblé de l'équipement |

# 1 INTRODUCTION

Le Comité de la Convention sur la cybercriminalité (T-CY), lors de sa 26ème plénière session (10-11 mai 2022), a décidé, conformément à l'article 46 de la Convention et au Règlement intérieur du T-CY, de consacrer son 4ème cycle d'évaluations à l'article 19 de la Convention sur la cybercriminalité relatif à la perquisition et à la saisie de données informatiques stockées.

L'objectif de cette évaluation est de partager l'expérience et les bonnes pratiques sur la manière dont les Parties ont mis en œuvre cet article. L'évaluation de l'article 19 présente un intérêt pour un certain nombre de raisons, notamment :

- L'article 19 est un pouvoir procédural important dans le cadre de la Convention. Le partage d'informations et d'expériences sur les mesures législatives et autres, ainsi que sur les pratiques de mise en œuvre de l'article 19, faciliterait la poursuite des réformes dans les parties actuelles et futures, le cas échéant.

- La procédure interne de l'article 19.2 - qui exige que chaque partie adopte les mesures nécessaires pour garantir que lorsque ses autorités effectuent une perquisition ou accèdent à un système informatique sur son territoire, elles puissent rapidement étendre la perquisition ou l'accès similaire à un autre système informatique sur son territoire dans certaines conditions - peut être liée à la question de l'extension des perquisitions aux territoires d'autres parties qui reste d'intérêt pour le T-CY.

Un questionnaire, adopté par le T-CY lors de sa 27e session plénière des 29 et 30 novembre 2022, a été envoyé aux représentants du T-CY le 2 décembre 2022.

Les représentants du T-CY ont été invités à préparer des réponses consolidées à ce questionnaire en coopération avec leurs autorités nationales compétentes et à soumettre leurs réponses sous forme électronique et en anglais ou en français au secrétariat du T-CY avant le 1er mars 2023.

Le Bureau du T-CY a présenté la compilation des réponses reçues à ce stade avec les commentaires initiaux à la 28e plénière du T-CY les 27-28 juin 2023. Les parties qui n'ont pas encore fourni leurs réponses ont été invitées à les soumettre avant le 31 août 2023.[1]

Le Bureau du T-CY a présenté un projet de rapport d'évaluation - basé sur les contributions de 40 Parties reçues avant le 1er août 2023 - à la 29e Plénière du T-CY.

La 29e plénière (Bucarest, 11-12 décembre 2023) a décidé de "saluer le projet de rapport d'évaluation sur l'article 19 de la Convention et les exemples de mise en œuvre présentés au cours de la plénière". Elle a invité les Parties à soumettre les réponses en suspens au questionnaire et les observations sur le projet de rapport avant le 31 janvier 2024 afin de permettre au Secrétariat et au Bureau du T-CY de préparer et de partager une version complète du rapport en mai 2024 pour examen des observations par la 30e plénière du T-CY en juin 2024.

La 30e plénière (Strasbourg, 18-20 juin 2024) a décodé pour s'en féliciter la dernière version du projet de rapport d'évaluation et les exemples de mise en œuvre et de conclusions préliminaires présentés pendant la plénière, qui contenait l'évaluation de 58 Parties et invitait:

[1] https://rm.coe.int/t-cy-2023-10-plen28-rep-v3/1680abca03

- les parties qui n'ont pas encore soumis leurs réponses (1 partie) ou qui n'ont pas encore répondu aux demandes de clarification (8 parties) à le faire avant le 1er septembre 2024 ;

- les 7 États qui sont devenus Parties depuis le début de ce cycle d'évaluation à participer aux présentes évaluations et donc à soumettre leurs réponses au questionnaire avant le 1er septembre 2024 ;

- toute partie à présenter des observations sur le projet de rapport, le cas échéant, avant le 1er septembre 2024 ;

- le secrétariat et le bureau du T-CY à communiquer une version complète du projet de rapport d'évaluation aux parties d'ici début novembre 2024 pour observations et examen en vue de l'adoption par la 31e plénière du T-CY en décembre 2024.

La version finale du rapport a été adoptée par le T-CY lors de sa 31ème session plénière.

Le présent rapport est structuré comme suit :

- Le chapitre 2 présente une vue d'ensemble de l'article 19.

- Le chapitre 3 résume les réponses soumises par les Parties à la partie 1 du questionnaire, c'est-à-dire les informations sur la base juridique des perquisitions et des saisies.

- Les chapitres 4 à 8 traitent des paragraphes 1 à 5 de l'article 19, chacun comprenant une vue d'ensemble de la mise en œuvre et des exemples de pratiques, suivis d'une évaluation.

- Le chapitre 9 présente des conclusions et des recommandations ainsi qu'un résumé de la mise en œuvre de l'article 19 par les parties.

- Le chapitre 10 contient des annexes (1) sur les dispositions juridiques nationales et (2) une vue d'ensemble des réponses au questionnaire.

La matrice des réponses et les analyses individuelles des parties sont des résumés. Les membres de T-CY intéressés par les détails, le texte statutaire, etc., doivent consulter les soumissions des parties.

Les exemples fournis dans les différentes sections de ce rapport ont pour but d'illustrer l'éventail des approches adoptées par des Parties ayant des systèmes juridiques différents et dans différentes régions du monde lors de la mise en œuvre de l'article 19. Ils ne sont pas nécessairement destinés à indiquer les "meilleures pratiques" ou les "modèles" à adopter. Ces exemples peuvent attirer l'attention des Parties intéressées sur d'autres Parties auprès desquelles elles souhaiteraient obtenir des informations plus détaillées.

| **Réponses, mises à jour et clarifications reçues au plus tard le 8 décembre 2024** | |
|---|---|
| **Parti** | **Reçu** |
| 1. Albanie | 13 décembre 2023 |
| 2. Andorre | 8 mars 2023 |
| 3. Argentine[2] | 14 avril 2023 |
| 4. Arménie | 31 août 2023 |
| 5. Australie | 24 mars 2023 |
| 6. Autriche | 1er mars 2023 |
| 7. Azerbaïdjan | 13 avril 2024 |
| 8. Belgique | 9 mars 2023 |
| 9. Bénin | 27 septembre 2024 |
| 10. Bosnie et Herzégovine | 27 février 2023 |
| 11. Brésil | 27 mars 2023/20 juin 2023 (mise à jour) |
| 12. Bulgarie | 23 mars 2023 |
| 13. Cabo Verde | 30 janvier 2024 |
| 14. Cameroun | 2 septembre 2024 |
| 15. Canada | 5 septembre 2023 |
| 16. Chili | 11 août 2023 |
| 17. Colombie[3] | 27 mars 2023 |
| 18. Costa Rica | 23 février 2023 |
| 19. Croatie | 13 mars 2023 |
| 20. Chypre | 6 mars 2023 |
| 21. République tchèque | 7 mars 2023 |
| 22. Danemark | 1er mai 2023 |
| 23. République dominicaine | 3 février 2024 |
| 24. Estonie | 3 mai 2023 |
| 25. Fidji | 10 septembre 2024 |
| 26. Finlande | 1er mars 2023 |
| 27. France | 22 février 2023 |
| 28. Géorgie | 2 mars 2023 |
| 29. Allemagne | 2 mars 2023 |
| 30. Ghana | 27 mars 2024 |
| 31. Grèce | 5 septembre 2023 |
| 32. Grenade | 19 septembre 2024 |
| 33. Hongrie | 6 mars 2023 |
| 34. Islande | 20 mars 2023 |
| 35. Israël | 15 février 2023 |
| 36. Italie | 4 septembre 2023 |
| 37. Japon | 28 février 2023 |
| 38. Kiribati | 12 septembre 2024 |
| 39. Lettonie | 20 mars 2023 |
| 40. Liechtenstein | 28 février 2023 |
| 41. Lituanie | 24 février 2023 |
| 42. Luxembourg | 1er septembre 2023[4] /25 septembre 2023 (mise à jour) |
| 43. Malte | 30 août 2023 |
| 44. Maurice | 31 octobre 2023 |
| 45. Monaco | 27 mars 2024 |
| 46. Monténégro | 9 juin 2023 |

[2] Réponses de l'original espagnol traduites en anglais par un service de traduction automatique neuronale

[3] Réponses de l'original espagnol traduites en anglais par un service de traduction automatique neuronale

[4] Version préliminaire des réponses.

| Réponses, mises à jour et clarifications reçues au plus tard le 8 décembre 2024 | |
|---|---|
| **Parti** | **Reçu** |
| 47. Maroc [5] | 22 mai 2023 |
| 48. Pays-Bas | 14 mars 2023 |
| 49. Nigéria | 27 mars 2024 |
| 50. Macédoine du Nord | 23 août 2023 |
| 51. Norvège | 1er mars 2023 |
| 52. Panama[6] | 27 janvier 2023 |
| 53. Paraguay | 28 février 2023 |
| 54. Pérou | 03 mars 2023 |
| 55. Philippines | 29 août 2023 |
| 56. Pologne | 16 août 2023 |
| 57. Portugal | 18 avril 2023 |
| 58. République de Moldavie | 30 janvier 2024 |
| 59. Roumanie | 1er mars 2023 |
| 60. Saint-Marin | 30 août 2024 |
| 61. Sénégal | 19 mai 2024 |
| 62. Serbie | 22 août 2023 |
| 63. Sierra Leone | 12 septembre 2024 |
| 64. République slovaque | 2 mai 2023 |
| 65. Slovénie | 28 février 2023 |
| 66. Espagne | 24 février 2023 |
| 67. Sri Lanka | 11 décembre 2023 |
| 68. Suède | 20 mars 2023/ 7 septembre (mise à jour) |
| 69. Suisse | 17 mars 2023/26 juillet 2023 (mise à jour) |
| 70. Tonga | 31 janvier 2024 |
| 71. Tunisie[7] | 10 septembre 2024 (réponse partielle) |
| 72. Türkiye | 03 mars 2023 |
| 73. Ukraine | 31 août 2023 |
| 74. Royaume-Uni | 5 juin 2024 |
| 75. États-Unis d'Amérique | 27 mars 2023 |
| **Total** | **74/75 reçu** |

[5] Des amendements législatifs sont en cours concernant le Code de Procédure Pénale et ont pris leur processus de la voie législative. Ces amendements concernent plusieurs dispositions, y compris celles relatives à la cybercriminalité.

[6] Réponses de l'original espagnol traduites en anglais par un service de traduction automatique neuronale.

[7] Réponse partielle reçue. En conséquence, la Tunisie n'a pas pu être évaluée.

## 2 ARTICLE 19 - PERQUISITION ET SAISIE DE DONNEES INFORMATIQUES STOCKEES[8]

La plupart des lois nationales de procédure pénale prévoient des pouvoirs de perquisition et de saisie d'objets tangibles dans le cadre d'enquêtes ou de procédures pénales spécifiques. Nombre des caractéristiques des pouvoirs généraux ou "traditionnels" de perquisition et de saisie des preuves, y compris les conditions et garanties connexes, sont également applicables aux données et systèmes informatiques, comme l'indique le rapport explicatif de la Convention.

Il existe toutefois des différences importantes :[9]

- Les données informatiques sont intangibles. Les dispositions générales couvrant les objets ou les "choses" peuvent ne pas être applicables. Le droit national devrait couvrir les données informatiques.
- Si les données peuvent être lues à l'aide de systèmes informatiques, elles ne peuvent pas être saisies et emportées de la même manière que des documents papier ou d'autres objets. Le droit interne devrait prévoir un pouvoir, par exemple, de faire des copies ou de rendre les données inaccessibles.
- En raison de la connectivité des systèmes informatiques, les données peuvent ne pas être stockées dans le système informatique qui fait l'objet de la recherche, mais ces données peuvent être facilement accessibles à ce système par l'intermédiaire de réseaux de communication, tels que l'internet. Des dispositions supplémentaires ou complémentaires peuvent être nécessaires pour réglementer une telle extension des recherches.

En outre, la complexité croissante et l'évolution constante de la technologie et des dispositifs, ainsi que des techniques de masquage des données, telles que l'anonymisation ou le cryptage des données, posent sans cesse de nouveaux défis aux autorités de justice pénale qui ont besoin de rechercher et de saisir des données informatiques stockées aux fins d'enquêtes ou de procédures pénales spécifiques.

Les pouvoirs procéduraux de la Convention, y compris l'article 19, exigent que les Parties disposent de certaines capacités - perquisition et saisie, par exemple. L'évolution de la technologie implique les Parties doivent moderniser leur droit procédural interne là où il existe des lacunes, afin de garantir que les autorités de justice pénale disposent ou continuent de disposer de pouvoirs de perquisition et de saisie suffisants pour collecter des preuves électroniques. Comme d'autres dispositions de la Convention relatives au droit procédural, l'article 19 "garantit une capacité équivalente ou parallèle pour l'obtention ou la collecte de données informatiques à celle qui existe en vertu des pouvoirs et procédures traditionnels pour les données non électroniques. [10]

Par exemple, l'article 19, paragraphe 2, prévoit la possibilité d'effectuer une recherche dans un système informatique, dans un support de stockage, ainsi que dans un système informatique distinct qui est légalement disponible ou accessible à partir du système informatique initial. Cette dernière possibilité permet à l'autorité effectuant la recherche "d'étendre rapidement la recherche à un autre système" lorsque, au cours d'une recherche licite dans un système informatique spécifique ou une partie de celui-ci, l'autorité effectuant la recherche a des raisons de croire que les données recherchées sont stockées dans un autre système informatique sur son territoire.

---

[8] Le rapport explicatif de la Convention (paragraphes 184-204) fournit des explications supplémentaires sur l'article 19. Disponible à l'adresse suivante

[9] Voir le paragraphe 187 du rapport explicatif de la Convention.

[10] Paragraphe 141 du rapport explicatif de la Convention.

En outre, l'article 19 exige que les enquêteurs soient habilités à "saisir ou sécuriser de la même manière" les données informatiques auxquelles ils ont accès et permet aux autorités de justice pénale d'obliger toute personne (telle qu'un administrateur de système) à prêter son concours, dans la mesure du raisonnable, à l'exécution de la perquisition et de la saisie. Compte tenu des différentes manières de saisir des données informatiques, l'article 19 fournit une liste d'actions de base que les enquêteurs doivent être habilités à effectuer.

La perquisition et la saisie de données informatiques stockées est une mesure intrusive qui peut interférer avec les droits des individus. Il est donc essentiel que cette mesure soit soumise à des limitations, des conditions et des garanties afin d'assurer un équilibre approprié entre les intérêts de la justice et les droits fondamentaux des individus. Comme le prévoit l'article 15, le droit interne des Parties "assure la protection adéquate des droits de l'homme et des libertés", y compris les droits découlant des obligations que chaque Partie a contractées en vertu d'instruments internationaux, tels que, le cas échéant, le Pacte international relatif aux droits civils et politiques (PIDCP), la Convention africaine des droits de l'homme et des peuples, la Convention américaine des droits de l'homme ou la Convention européenne des droits de l'homme

Ces "... garanties devraient également être adaptées ou développées pour tenir compte du nouvel environnement technologique et des nouveaux pouvoirs procéduraux[11]

Ainsi, les dispositions du droit interne relatives à la perquisition et à la saisie de données informatiques stockées, conformément à l'article 19, qui sont soumises à des limitations, des conditions et des garanties, aident les Parties à remplir ces obligations.[12]

Dans le même temps, la convention définit des normes que les États qui l'ont ratifiée doivent réglementer "au minimum" et donc "harmoniser", dans ce cas, les pouvoirs procéduraux. Toutefois, cela n'exclut pas que les Parties se prévalent d'autres pouvoirs dans leur droit national.[13]

Si l'article 19 exige que les Parties adoptent une législation ou d'autres mesures habilitant les autorités à prendre certaines mesures en matière de perquisition et de saisie, l'article ne précise pas si ce cadre juridique doit impliquer l'utilisation de pouvoirs procéduraux généraux "traditionnels" pour la perquisition et la saisie d'objets tangibles, de pouvoirs spécifiquement conçus pour la perquisition et la saisie de données informatiques stockées, ou d'une combinaison de ces pouvoirs. [14]

Le rapport explicatif de l'article 19 fournit des indications utiles aux Parties, ainsi qu'aux États désireux d'adhérer à la Convention, lorsqu'ils s'efforcent de structurer ou de modifier leur cadre

---

[11] Comme indiqué au paragraphe 132 du rapport explicatif de la Convention.

[12] Ces obligations peuvent inclure, par exemple, qu'une ingérence doit être "conforme à la loi" (CEDH) ou "prévue par la loi" (PIDCP), ou que la "législation pertinente doit spécifier en détail les circonstances précises dans lesquelles de telles ingérences peuvent être autorisées" (voir l'Observation générale n° 16 du CCPR : Article 17 (Droit à la vie privée) adoptée lors de la trente-deuxième session du Comité des droits de l'homme, le 8 avril 1988).

[13] Voir par exemple le rapport explicatif, paragraphe 131.

[14] Aux fins du présent rapport :

- Le "pouvoir spécifique" peut être une loi, une ordonnance, une règle ou un règlement ayant force obligatoire en vertu du droit national et prévoyant spécifiquement la perquisition et la saisie de données et de systèmes informatiques ;
- Le "pouvoir général" peut être tout statut, loi, ordonnance, règle, règlement ayant une force contraignante qui ne se réfère pas spécifiquement à la perquisition et à la saisie de données et de systèmes informatiques.

juridique afin de garantir que les autorités sont suffisamment habilitées à remplir les diverses obligations découlant de chaque paragraphe de l'article 19.

En bref, dans la mesure où les éléments de l'article 19 ne peuvent pas être satisfaits en utilisant les pouvoirs de procédure généraux ou "traditionnels", l'article 19 exige des Parties qu'elles établissent des pouvoirs et des procédures qui s'ajoutent aux pouvoirs de procédure généraux ou "traditionnels" ou qui les complètent. Les parties peuvent donc envisager d'établir des pouvoirs et des procédures spécifiques données informatiques stockées pour satisfaire à ces obligations. De telles dispositions spécifiques pourraient également apporter une plus grande clarté et renforcer la sécurité juridique

**Article 19 - Perquisition et saisie de données informatiques stockées**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à procéder à des perquisitions ou à un accès similaire :

a un système informatique ou une partie de celui-ci et les données informatiques qui y sont stockées ; et

b un support de stockage de données informatiques dans lequel des données informatiques peuvent être stockées sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour garantir que, lorsque ses autorités procèdent à une perquisition ou accèdent de manière similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de croire que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour celui-ci, les autorités sont en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à sécuriser de la même manière les données informatiques auxquelles il a été accédé conformément aux paragraphes 1 ou 2. Ces mesures comprennent le pouvoir de :

a saisir ou sécuriser de la même manière un système informatique ou une partie de celui-ci ou un support de stockage de données informatiques ;

b faire et conserver une copie de ces données informatiques ;

c maintenir l'intégrité des données informatiques stockées ;

d rendre inaccessibles ou supprimer ces données informatiques dans le système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne ayant connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qu'il contient de fournir, dans la mesure du raisonnable, les informations nécessaires pour permettre l'application des mesures visées aux paragraphes 1 et 2.

5 Les pouvoirs et procédures visés au présent article sont soumis aux articles 14 et 15.

# 3 INFORMATIONS SUR LA BASE JURIDIQUE DE LA PERQUISITION ET DE LA SAISIE (PARTIE 1 DU QUESTIONNAIRE)

Cette section du rapport résume les réponses à la partie 1 du questionnaire sur la base juridique des pouvoirs de perquisition et de saisie.

## 3.1 Base juridique : vue d'ensemble

Plus de la moitié des parties évaluées[15] ont adopté des pouvoirs spécifiques pour la perquisition et la saisie de données informatiques stockées, qui peuvent également compléter les pouvoirs généraux

Certaines Parties[16] ne s'appuient actuellement que sur les pouvoirs généraux de leur législation, mais peuvent dans certains cas avoir des pratiques ou des procédures opérationnelles pour appliquer ces pouvoirs à la perquisition et à la saisie de données informatiques stockées.[17]

## 3.2 Tout type de crime

Selon l'article 14.2 de la Convention, les pouvoirs procéduraux de ce traité sont applicables non seulement aux infractions définies aux articles 2 à 11 de la Convention, mais aussi aux autres infractions commises au moyen d'un système informatique, ainsi qu'à la collecte de preuves électroniques de toute infraction. Cette approche s'applique également à l'article 19.

La plupart des Parties sont en effet en mesure d'appliquer l'article 19 à n'importe quel crime. Quelques Parties limitent l'application de ces pouvoirs en fonction d'un seuil de peine ou appliquent les pouvoirs à une catégorie spécifique d'infractions sans tenir compte du seuil applicable (par exemple, les infractions contre les systèmes informatiques, les infractions de corruption). Les cas les plus fréquents sont ceux où les pouvoirs prévus par une loi spécifique ne s'appliquent qu'à une catégorie limitée d'infractions énumérées dans cette loi.

Dans certaines parties, des outils supplémentaires (tels que des mesures d'accès secrètes) ne sont disponibles qu'en cas de criminalité grave ou organisée.

## 3.3 Données informatiques stockées

L'article 19 s'applique aux données informatiques stockées. Toutefois, la convention laisse aux Parties la possibilité de déterminer elles-mêmes les situations qu'elles considèrent comme constituant des "données informatiques stockées" ou des données en "transfert" - par exemple, un message électronique non ouvert qui attend dans la boîte aux lettres d'un fournisseur de services Internet que le destinataire le télécharge sur son système informatique peut être considéré par certaines Parties comme des données informatiques stockées

---

[15] Albanie, Argentine, Arménie, Australie, Autriche, Belgique, Bénin, Bulgarie, Cabo Verde, Cameroun, Canada, Chypre, Croatie, République dominicaine, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Israël, Italie, Japon, Kiribati, Lettonie, Liechtenstein, Luxembourg, Malte, Maurice, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Panama, Philippines, Pologne, Portugal, Roumanie, Royaume-Uni, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Sri Lanka, Suède, Suisse, Tonga, Türkiye, USA.

[16] Andorre, Azerbaïdjan, Bosnie-Herzégovine, Brésil, Chili, Colombie, Costa Rica, République tchèque, Danemark, Estonie, Islande, Lituanie, Maroc, Norvège, Pérou, Paraguay, République de Moldavie, Saint-Marin, Ukraine.

[17] Certaines de ces parties ont indiqué qu'elles étaient en train de réformer leur législation nationale en vue d'adopter des pouvoirs spécifiques pour la perquisition et la saisie de données informatiques stockées. La présente évaluation pourrait soutenir ce processus.

auxquelles s'applique l'article 19, tandis que d'autres Parties peuvent le considérer comme des données en transfert dont le contenu ne pourrait être obtenu qu'en appliquant le pouvoir d'interception. 19, alors que d'autres Parties peuvent le considérer comme des données en cours de transfert dont le contenu ne pourrait être obtenu qu'en appliquant le pouvoir d'interception.[18]

La plupart des Parties ont indiqué qu'elles prévoient une définition des données informatiques dans un texte, sans définir spécifiquement le terme "stockées". Toutefois, certaines Parties ont souligné que les données informatiques stockées sont des données déjà existantes ou disponibles au moment de la perquisition et/ou de la saisie, à l'exclusion des données futures.

D'autres Parties ont indiqué que leur cadre juridique national permet la saisie de données à valeur probante stockées de manière temporaire ou permanente sur le serveur du fournisseur (Allemagne, Suisse) et que le fait décisif est que les données "stockées" ne doivent pas être des données en transit entre deux ou plusieurs appareils (Portugal) ou des données en mouvement (Canada), car ces données ne peuvent être obtenues que par l'interception. Par exemple, la Pologne et les Pays-Bas ont explicitement indiqué qu'un courrier électronique ou des messages d'application non ouverts sont considérés comme des données informatiques stockées, tandis que la République tchèque a indiqué qu'elle considère les messages électroniques non ouverts dans la boîte de réception du fournisseur d'accès à Internet comme des données dans le flux de trafic qu'il est nécessaire d'obtenir par l'interception et l'enregistrement du trafic de télécommunications. La Suède a déclaré qu'un message électronique non ouvert serait considéré comme une donnée informatique stockée (accessible par le biais d'une recherche à distance), si le message est arrivé au moment de la recherche ou pendant celle-ci

D'autres font la distinction entre les données qui sont stockées sur un ordinateur (par exemple, une pièce jointe à un courrier électronique téléchargée et disponible hors ligne) et les données informatiques qui se trouvent sur un réseau informatique, par exemple, sur l'internet, par exemple, sur le serveur d'une personne qui exploite un service de courrier électronique disponible en ligne (Lettonie, République slovaque). Les pouvoirs de perquisition et de saisie ne s'appliquent qu'aux premières et l'obtention des secondes dépend d'un pouvoir procédural différent

En outre, certaines parties ont indiqué d'autres scénarios qu'elles rencontrent dans la pratique. Par exemple, l'Autriche a établi une distinction entre les données informatiques qui peuvent être obtenues auprès de l'abonné à la communication lui-même et les données qui doivent être collectées auprès d'un fournisseur de services et qui se présentent donc sous la forme d'une communication réelle. Alors que les premières peuvent être consultées au moyen d'une perquisition et d'une saisie, les secondes ne peuvent être consultées qu'au moyen d'une collecte en temps réel de données informatiques.

D'autres Parties ont déclaré qu'elles considéraient les crypto-monnaies comme un type particulier de données informatiques et que les mesures prévues à l'article 19 pouvaient être utilisées pour les saisir (voir exemple la Suisse et le Liechtenstein).

Une partie a souligné que son cadre juridique national ne lui permettait pas de recourir à la perquisition et à la saisie en ce qui concerne les données relatives au contenu (Panama).

Il existe également quelques Parties dont la législation nationale ne contient pas de mesures spécifiques relatives aux données informatiques et qui appliquent des mesures générales.

## 3.4 Notification des personnes concernées[19]

[18] Rapport explicatif, paragraphe 190.

[19] Voir la section 8.1.1.2 pour des exemples.

Bien que la convention ne prévoie pas de régime spécifique de notification aux personnes concernées et laisse la question à l'appréciation du droit interne, certaines Parties peuvent considérer la notification comme un élément essentiel de la perquisition et de la saisie de données informatiques stockées. Le droit interne d'autres Parties peut ne pas exiger une telle mesure.[20] Le T-CY a néanmoins estimé qu'il était utile d'obtenir des informations sur la notification en vertu des législations nationales des Parties à la Convention et a inclus une telle question dans le questionnaire. Toutefois, il est reconnu qu'il peut y avoir des situations où la notification n'est pas appropriée, par exemple lorsque, conformément à la législation nationale, une telle notification peut nuire aux enquêtes.

Il convient de noter que la plupart des Parties prévoient la notification des personnes concernées en ce qui concerne les mesures traditionnelles de perquisition et de saisie. Certaines Parties prévoient des dispositions spéciales de notification pour les perquisitions et saisies de données informatiques.

De nombreuses Parties entrent dans l'une de ces catégories où les lois nationales exigent une notification dans un sens ou dans l'autre[21]

Les réponses originales au questionnaire fournies par les parties illustrent la diversité et la complexité des exigences en matière de notification.

Un certain nombre de parties ne prévoient aucune obligation de notification, en particulier lorsque la perquisition et la saisie sont effectuées dans le cadre d'un régime secret. Toutefois, il a été souligné qu'un tel régime est soumis à des garanties importantes afin de s'assurer que tout recours à la mesure est justifié.

[20] Rapport explicatif, paragraphe 204.

[21] Albanie, Andorre, Argentine, Australie, Autriche, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Cameroun, Canada, Costa Rica, Croatie, République tchèque, Danemark, République dominicaine, Estonie, Finlande, France, Géorgie, Allemagne, Grèce, Grenade, Islande, Israël, Italie, Japon, Kiribati, Liechtenstein, Lituanie, Monaco, Monténégro, Pays-Bas, Nigeria, Norvège, Panama, Paraguay, Pérou, Pologne, Portugal, République de Moldavie, Saint-Marin, Sénégal, Sierra Leone, République slovaque, Slovénie, Espagne, Suède, Suisse, Türkiye, USA.

# 4 RECHERCHE OU ACCES SIMILAIRE (EVALUATION DE L'ARTICLE 19.1)

Cette section évalue la mise en œuvre de l'article 19.1 :

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à procéder à des perquisitions ou à un accès similaire :
>
> a un système informatique ou une partie de celui-ci et les données informatiques qui y sont stockées ; et
>
> b un support de stockage de données informatiques dans lequel des données informatiques peuvent être stockées sur son territoire.

## 4.1 Mise en œuvre de l'article 19.1 : vue d'ensemble

### 4.1.1 Mesures législatives et autres - résumé

Les Parties mettent en œuvre l'article 19.1. par le biais de diverses dispositions spécifiques (perquisition d'ordinateur, perquisition de données informatiques, perquisition de réseau après la saisie, accès à distance et secret aux données) ou générales (par exemple, perquisitions à domicile, perquisitions de locaux et de lieux ou perquisitions de voitures) dans leur droit interne.

La condition la plus importante justifiant le recours à la perquisition et à la saisie de données informatiques stockées, telle qu'indiquée dans les réponses, est l'autorisation judiciaire. La plupart des Parties[22] exigent une décision de justice[23] pour autoriser la perquisition. En Autriche, en Belgique[24] , au Cabo Verde[25] , en Estonie, en Finlande, en Grèce, en Hongrie, au

[22] Albanie, Andorre, Argentine, Arménie, Australie, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, Géorgie, Allemagne, Hongrie, Islande, Israël, Japon, Kiribati, Lettonie, Liechtenstein, Lituanie, Malte, Monténégro, Maroc, Nigeria, Macédoine du Nord, Norvège, Panama, Paraguay, Pérou, Philippines, Portugal, République de Moldavie, Roumanie, Saint-Marin, Sénégal, Sierra Leone, République slovaque, Slovénie, Espagne, Tonga, Türkiye, Royaume-Uni et États-Unis.

[23] Dans l'ensemble du texte du rapport, une décision de justice comprend une décision d'un juge d'instruction ou d'un juge similaire. Dans certaines Parties, il peut y avoir plus d'une catégorie de juges compétents pour les décisions relatives aux perquisitions et saisies.

[24] En Belgique, une ordonnance du procureur est nécessaire pour effectuer une perquisition dans un système informatique qui n'a pas été saisi, mais pour lequel toutes les conditions légales de saisie ont été remplies, alors qu'une telle ordonnance n'est pas nécessaire pour effectuer une perquisition dans un système informatique qui a été saisi dans le cadre de l'enquête.

[25] En fonction de la phase procédurale en question, tant le juge que le ministère public peuvent autoriser ou ordonner l'exécution d'une perquisition. En outre, le législateur a également prévu la possibilité pour les organes de police judiciaire d'effectuer une perquisition, sans autorisation préalable de l'autorité judiciaire, mais seulement lorsque : "a) elle est volontairement consentie par celui qui a la disponibilité ou le contrôle de ces données, à condition que le consentement donné soit, de quelque manière que ce soit, documenté ; b) dans les cas de terrorisme, de criminalité violente ou hautement organisée, lorsqu'il existe des preuves fondées de la commission imminente d'un crime qui met gravement en danger la vie ou l'intégrité d'une personne

Maroc[26] , aux Pays-Bas[27] , en Pologne, au Portugal[28] , au Sénégal, en République slovaque, en Suède et en Suisse, la perquisition peut être autorisée par l'autorité de poursuite dans tous les cas ou dans certains cas.

Les États mentionnés dans les deux groupes appliquent des motifs différents selon les phases de la procédure pénale. Par exemple, une ordonnance du procureur peut être requise dans les phases de la procédure préliminaire/de l'enquête, tandis qu'une ordonnance d'un juge peut être nécessaire dans les phases du procès/de la procédure ultérieure. D'autres États font une distinction entre les types de données recherchées ou consultées et peuvent ne pas exiger d'ordonnance judiciaire pour les recherches relatives aux informations sur les abonnés. D'autres motifs peuvent également s'appliquer en cas d'urgence ou d'autres circonstances urgentes (voir la section suivante).

Quelques exemples d'autres motifs de procédure nécessaires pour justifier l'application de la mesure qui ont été mentionnés dans les réponses :

- Brésil : raisons justifiées de penser qu'il existe des preuves d'une infraction pénale stockées à l'endroit où la recherche sera effectuée.

- Canada : il faut non seulement une autorisation judiciaire préalable pour fouiller un lieu spécifique, mais aussi une autorisation spécifique pour fouiller un ordinateur dans ce lieu. En outre, la police peut saisir un dispositif mais doit obtenir une autorisation supplémentaire avant de fouiller ce dispositif (un ordinateur ou un téléphone portable).

- Finlande : les conditions préalables à la recherche sont définies par la loi.

- Géorgie, Grèce et Philippines : motif probable.

- Islande : le principal critère concerne les exigences légales en matière de recherche. Si les données en question sont conservées par un tiers, c'est-à-dire qu'elles ne sont pas en possession d'un suspect dans l'affaire, le seuil est plus élevé que pour une recherche qui n'implique que les suspects eux-mêmes.

- Israël : un arrêt de la Cour suprême (voir également les pratiques ci-dessous) comprenait plusieurs déterminations procédurales concernant les recherches de données informatiques.

---

[26] En cas d'enquête préliminaire, une perquisition ne peut être effectuée qu'avec l'autorisation du procureur compétent et le consentement explicite de la personne concernée (article 79 du CPP), sauf s'il s'agit d'une infraction terroriste et que la personne concernée refuse de donner son consentement, auquel cas la perquisition est effectuée avec l'autorisation écrite du procureur compétent.

[27] Le DCCP permet l'exécution des pouvoirs de perquisition et de saisie par la police et, ou, par un procureur sans l'autorisation d'un tribunal. Dans le cadre néerlandais, le lieu où les pouvoirs de perquisition et de saisie sont exercés est déterminant. Par exemple, lors de la fouille d'une voiture, la police peut opérer sans autorisation préalable. De même, dans le cas de l'utilisation des pouvoirs de perquisition et de saisie dans un domicile, l'autorisation du procureur peut suffire. En même temps, dans certains cas (comme le nouvel article 557 du DCCP sur la perquisition de réseau après la saisie d'une œuvre automatisée, et l'article 125 I du DCCP sur la perquisition de réseau, souvent utilisé), l'autorisation préalable du juge (d'instruction) est requise.

[28] Au Portugal, la règle est que l'enquête est toujours dirigée par un procureur. C'est donc au procureur qu'il appartient d'autoriser une perquisition. Toutefois, dans les phases ultérieures (avant ou pendant le procès), un juge peut également donner l'ordre, si nécessaire. Il s'agit d'une situation rare, car normalement, lors des phases d'instruction et de procès, toute l'enquête a déjà été effectuée. On peut donc dire que la compétence générale pour autoriser une perquisition appartient au procureur.

- Japon : nécessité.

- Maroc : en cas de crime flagrant, présence du suspect ou de son représentant ou présence de deux témoins autres que les fonctionnaires hiérarchiquement responsables de l'officier de police judiciaire chargé de la perquisition (art. 60 du CPP).

- Pays-Bas : l'ordre mentionne explicitement les actes criminels concernés, si possible, le nom du suspect et les faits et circonstances justifiant l'exécution du pouvoir, l'espoir raisonnable que la recherche produira des informations pertinentes pour l'enquête en cours. Les éléments mentionnés sont communiqués à la police ou au procureur qui exécutera l'ordre. La plupart des éléments mentionnés ne sont pas partagés avec des entités privées, telles que les fournisseurs de services.

- Pérou : test de proportionnalité (adéquation, nécessité, proportionnalité) et suffisance des éléments de preuve.

- Portugal : si possible, présence des autorités judiciaires qui ont rendu l'ordonnance dans le cadre de la procédure.

- Roumanie : nécessité de découvrir, d'identifier et de collecter des preuves stockées dans un système informatique ou dans un support de stockage de données informatiques.

- Sénégal : les perquisitions ne sont autorisées que si les données visées sont absolument nécessaires à l'enquête, dans le strict respect du principe de légalité des preuves. Les données doivent être utiles à la manifestation de la vérité.

- Slovénie : il existe des motifs raisonnables de soupçonner qu'un délit a été commis et il doit être probable que le dispositif électronique contienne des données électroniques.

- Suisse : présomption de pertinence de la saisie - soupçon suffisant de l'infraction.

- USA : déclaration sous serment d'un agent des forces de l'ordre ou d'un avocat du gouvernement établissant l'existence d'une cause probable de croire que l'objet de la perquisition sera trouvé dans le lieu à perquisitionner.

#### 4.1.1.1 Exemples de pratiques

- Argentine[29] : preuves autres que celles pour lesquelles le mandat a été émis

  Le code de procédure pénale argentin stipule que si, dans le strict respect du mandat de perquisition, des objets sont trouvés qui fournissent la preuve de la commission d'un délit autre que celui pour lequel le mandat a été délivré, ils doivent être saisis et le juge ou le procureur concerné doit en être informé. Il s'agit de la doctrine numérique dite "plain view" : elle autorise l'ouverture d'une enquête si des preuves d'un délit autre que celui faisant l'objet de l'enquête sont trouvées lors d'une perquisition, et elle s'étend également aux preuves électroniques.

- Israël : conditions contenues dans une demande de mandat de perquisition informatique

[29] L'application d'un principe similaire a été soulignée dans la réponse de l'Arménie.

Un arrêt de la Cour suprême, CrimFH 1062/21 Urich v State of Israel (11.1.2022), comprend plusieurs déterminations procédurales concernant les perquisitions de données informatiques, y compris les informations nécessaires qu'une demande de mandat de perquisition informatique doit contenir : le but de la perquisition, les détails du dispositif informatique, les détails du propriétaire ou du détenteur de l'infraction et le statut dans l'enquête, et l'étendue des informations demandées dans la perquisition. Les décisions rendues dans l'affaire CrimFH Urich ont été adoptées et incorporées dans lignes directrices relatives à la police.[30]

- Espagne : autorisation préalable

  La perquisition et la saisie sont des mesures d'enquête qui doivent être autorisées par les tribunaux, que le dispositif soit localisé au cours d'une arrestation ou à l'occasion d'une perquisition. La législation espagnole exige une autorisation spécifique de telle sorte que même si le tribunal a délivré une autorisation générique pour la perquisition d'une adresse particulière, elle serait insuffisante pour examiner les dispositifs trouvés lors de cette perquisition, puisque l'accès au dispositif ou au système informatique nécessite une autorisation expresse à cet effet.

  Par conséquent, si, à l'occasion d'une perquisition, les forces de police en fonction localisent un dispositif et n'ont pas l'autorisation de l'enregistrer, elles ne peuvent pas le faire à ce moment-là, mais doivent demander l'autorisation préalable du juge.

- Costa Rica : procédure utilisée

  1. Déterminer la probabilité de l'existence d'un crime.
  2. Identifier le matériel susceptible de contenir des données de stockage qui pourraient être utiles à l'enquête (par exemple, des téléphones portables, des smartwatches, des ordinateurs, etc.) Il ne s'agit pas nécessairement d'un matériel spécifique, mais de tous les types de matériel d'un genre particulier (USB, ordinateurs portables, tablettes, etc.).
  3. Déterminer la raison, en fonction de l'affaire et des éléments de preuve recueillis, qui justifie la suspicion que des données potentielles importantes pour l'enquête pourraient se trouver dans le matériel identifié au point 2 (par exemple, l'accès au téléphone d'une victime dans le cadre d'un homicide pour déterminer avec qui, comment et quand la victime a interagi avant le meurtre, ou le traçage d'une adresse IP jusqu'à une maison spécifique dans le cadre d'une affaire de pédopornographie).
  4. Vérifiez l'endroit où le matériel informatique se trouve habituellement (maison, lieu de travail, extérieur, etc.).
  5. Demander à un juge d'ordonner la saisie et l'analyse des données contenues dans le matériel identifié. En outre, si le matériel se trouve dans un espace privé, il faut demander une perquisition et l'accès à ce lieu privé.
  6. Exécuter l'ordre.

### 4.1.2 Situation d'urgence ou autres circonstances urgentes

Les Parties ont fait preuve d'un degré surprenant d'uniformité dans leur approche des situations d'urgence. De nombreuses Parties présument que les perquisitions nécessitent un mandat, mais dans certaines situations, le type de mandat habituel ne peut pas toujours être obtenu selon la procédure habituelle. Les Parties définissent les situations d'urgence de différentes manières. Cependant, presque toutes les Parties ont des dispositions en cas d'urgence, soit par un texte juridique, soit dans la pratique, pour obtenir un certain type de

[30] Pour plus de détails, voir la réponse d'Israël à la question 2.1 dans le document de compilation des réponses.

mandat - peut-être une autorisation du procureur - ou pour demander un mandat par une méthode spéciale - par exemple, par téléphone. Un certain nombre de Parties exigent une ratification judiciaire ultérieure des perquisitions effectuées sans mandat judiciaire préalable. Les approches des Parties sont détaillées ci-dessous.

Certaines Parties[31] prévoient des définitions spécifiques des circonstances d'urgence dans leur législation nationale. Exemples d'éléments déclarés par les Parties comme constituant des circonstances d'urgence :

- Australie : s'il s'agit d'un acte criminel commis dans ou sur un moyen de transport, nécessité d'exercer le pouvoir d'empêcher la dissimulation, la perte ou la destruction de l'objet, circonstances graves et urgentes.

- Autriche : danger imminent - nécessité inévitable d'une intervention immédiate", par exemple si l'objectif de la mesure d'enquête serait compromis par l'attente d'une décision de l'autorité chargée des poursuites.

- Bosnie-Herzégovine et Croatie : risque de destruction des preuves, danger imminent pour la vie et la santé, prolongation de l'enquête ou empêchement de la collecte de preuves ou arrêt de la poursuite de l'activité criminelle.

- Cabo Verde : raison fondée de s'attendre à la commission imminente d'un crime mettant gravement en danger la vie ou l'intégrité d'une personne.

- Canada : circonstances d'urgence - analyse visant à déterminer s'il existe un risque imminent de perte, d'enlèvement, de destruction ou de disparition de la preuve si la recherche est retardée ou s'il existe un degré d'urgence qui nécessite une action de la part des forces de l'ordre.

- République tchèque : risque de détérioration, de destruction, de perte ou de dissimulation de l'objet important pour la procédure pénale.

- Estonie : danger immédiat pour la vie, l'intégrité physique, la liberté physique ou un intérêt patrimonial de grande valeur d'une personne, et lorsqu'il n'est pas possible de demander ou de délivrer une autorisation pertinente en temps utile.

- France : le lieu est fréquenté par une personne qui constitue une menace pour l'ordre public

- Géorgie : lorsque le report de l'action pourrait entraîner la perte de données utiles à l'enquête ou les rendre indisponibles ultérieurement, ou lorsqu'il existe une menace réaliste pour la vie ou l'intégrité physique d'une personne, ou lorsqu'un objet faisant l'objet d'une saisie a été découvert inopinément au cours d'une perquisition et que cet objet n'était pas censé être couvert par le mandat de perquisition initial.

- Allemagne : danger imminent - si la décision de justice ne peut être obtenue sans compromettre l'objectif de la mesure.

- Grenade : situations d'urgence spécifiées dans le mandat (par exemple, enlèvement, menace ou atteinte à une personne présentant un intérêt pour la sécurité nationale, ou menace ou atteinte à un enfant).

[31] Argentine, Australie, Autriche, Bosnie-Herzégovine, Croatie, République tchèque, Estonie, France, Géorgie, Allemagne, Hongrie, Islande, Maroc, Pays-Bas, Norvège, Espagne, Suisse, États-Unis.

- Hongrie : risque de retard qui compromettrait de manière significative l'objectif de la recherche.

- Islande : risque imminent que l'attente d'une décision de justice n'entraîne un préjudice pour la procédure.

- Maurice : pas de définition, mais les demandes de mandats peuvent expliquer que les circonstances sont urgentes.

- Maroc : infraction terroriste, en cas d'extrême urgence ou de crainte de perte de preuves.

- Pays-Bas : disparition raisonnablement attendue de preuves, et lorsque l'arrivée du juge d'instruction ne peut être attendue.

- Macédoine du Nord : résistance armée ou physique attendue ; suspicion d'une infraction pénale grave commise par un groupe, une organisation ou une entreprise criminelle ; perquisition censée être effectuée dans un établissement public ; menace de destruction ou de dissimulation de toute trace de l'infraction ou d'objets importants pour la procédure pénale.

- Norvège : risque de retard.

- Pologne : situation d'urgence - nécessité d'agir de toute urgence et rapidement lorsque tout retard risque d'entraîner la perte, la destruction ou la déformation de traces et de preuves.

- République de Moldova - cas ne pouvant faire l'objet d'un ajournement ou cas de flagrant délit

- Espagne : retarder l'exécution de la mesure d'enquête peut nuire à l'obtention de preuves (risque imminent de disparition totale ou partielle de l'information).

- Suède : si le retard entraîne un risque - les circonstances sont telles que la mesure perdrait sa raison d'être si elle n'était pas exécutée immédiatement.

- Suisse : danger imminent qui peut survenir ou risque réaliste de disparition des traces de l'infraction, de l'objet ou du patrimoine si la recherche n'est pas effectuée immédiatement.

- Royaume-Uni : Les circonstances urgentes peuvent inclure une menace immédiate pour la vie ou une menace crédible et immédiate pour la sécurité nationale.[32]

- États-Unis : danger imminent de destruction de preuves, danger pour la vie ou blessure corporelle grave.

D'autres Parties[33] s'appuient sur une autre source de droit pour traiter les situations d'urgence. Bien que le droit interne de ces parties ne donne pas expressément de définition de l'urgence ou des circonstances urgentes, il peut exiger, par exemple, un danger imminent pour la vie,

[32] En outre, l'enquête sur les informations électroniques protégées (The Investigation of Protected Electronic Information Revised Code of Practice August 2018) fournit une liste non exhaustive d'exemples de circonstances exceptionnelles et urgentes dans lesquelles il peut être approprié de se conformer immédiatement à un avis.

[33] Andorre, Belgique, Brésil, Bulgarie, Canada, Costa Rica, Chypre, Danemark, Estonie, Finlande, Israël, Japon, Lituanie, Panama, Slovénie, Turquie.

l'intégrité, la santé d'une personne ou la sécurité d'une nation, ou un risque de perte d'éléments de preuve.

Par exemple, le Ghana a déclaré que la LPC autorise les perquisitions sans mandat lorsqu'une arrestation est effectuée et qu'il est nécessaire de procéder à une perquisition immédiate ou qu'il existe des motifs raisonnables de soupçonner qu'un objet est un bien entaché ou qu'il fournira la preuve d'une infraction grave en vertu de la loi sur la criminalité économique et organisée.

Aux Tonga, l'article 123 de la loi sur la police pourrait être utilisé pour effectuer des recherches de données en cas d'urgence, puisqu'il prévoit des recherches sans mandat dans les cas d'infractions graves qui répondent à plusieurs autres éléments de l'article.

Certaines Parties s'appuient également sur des demandes verbales pour délivrer des mandats de perquisition/ordonnances judiciaires. Une Partie (Autriche) a indiqué que lorsque l'autorité compétente pour délivrer l'ordonnance peut être jointe par téléphone, le danger n'est pas considéré comme suffisamment imminent pour procéder sans ordonnance. Une autre Partie (Monténégro) a indiqué qu'une demande peut être adressée à un juge d'instruction par téléphone, par radio ou par d'autres moyens de communication électronique, auquel cas la transcription de l'appel doit être effectuée, certifiée et conservée avec les documents originaux. La Macédoine du Nord s'appuie également sur des demandes verbales. D'autres Parties ont déclaré que, comme pour tout mandat d'urgence, il y a un juge de garde 24 heures sur 24 et 7 jours sur 7 (Israël) ou un système de permanence 24 heures sur 24 et 7 jours sur 7 pour les juges et les procureurs (République slovaque).

En ce qui concerne les exigences procédurales à respecter après le début d'une perquisition en cas d'urgence, certaines Parties (Bosnie-Herzégovine, Bulgarie, Danemark, Géorgie, Espagne) ont indiqué que leur droit interne exigeait une validation a posteriori par un tribunal. Si la mesure d'urgence n'est pas validée, les résultats de l'enquête ne peuvent pas être utilisés comme preuves.

Quelques Parties (Albanie, Arménie, Chili, Fidji, Grèce, Pérou, Portugal) ont déclaré qu'il n'y avait pas de règles en place en ce qui concerne les situations d'urgence.

### 4.1.3 Titres légalement acquis

Les services répressifs qui effectuent des perquisitions peuvent légalement obtenir des justificatifs d'accès de différentes manières : auprès d'un collaborateur, à partir d'un support électronique auquel ils ont légitimement accès, à partir de notes sur papier, etc. L'évaluation a porté sur la mesure dans laquelle les références d'accès obtenues légalement peuvent être utilisées lors des perquisitions, et notamment sur la question de savoir si les autorités doivent obtenir une autorisation judiciaire supplémentaire pour utiliser ces références.

Les autorités compétentes de nombreuses Parties[34] sont habilitées par la législation ou la jurisprudence (Espagne, Suisse) à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant des identifiants d'accès acquis légalement.

Certaines Parties ont adopté des procédures standard et des lignes directrices internes qui réglementent l'utilisation des titres acquis légalement ( exemple, la Pologne).

[34] Andorre, Arménie, Australie, Autriche, Belgique, Brésil, Bulgarie, Canada, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Finlande, France, Géorgie, Ghana, Grèce, Islande, Israël, Japon, Liechtenstein, Monténégro, Pays-Bas, Nigeria, Panama, Philippines, République de Moldavie, Roumanie, Sénégal, Sierra Leone, Slovénie, Suède, Royaume-Uni, États-Unis.

La question n'est pas réglementée dans le droit interne de certaines Parties (Bosnie-Herzégovine, Cabo Verde, Hongrie, Lettonie, Norvège, Portugal, République slovaque, Turquie). Certaines Parties ont indiqué que, bien qu'il n'y ait pas de disposition spécifique concernant l'accès au système à l'aide d'identifiants, leur droit interne applicable prévoit que le tribunal, dans sa décision, autorise le droit d'accès et de recherche (par exemple, l'Albanie).

Plusieurs parties (Autriche, Bulgarie, Islande) ont indiqué que les autorités peuvent utiliser des informations d'identification divulguées volontairement (Allemagne, Roumanie, République slovaque, États-Unis), tandis que plusieurs (Autriche, Bulgarie, Islande) ont également indiqué spécifiquement que leurs autorités demandent d'abord à la personne qui connaît vraisemblablement le mot de passe de le divulguer volontairement avant de recourir à d'autres mesures

Un certain nombre de parties (Autriche, Brésil, République tchèque) ont souligné que la personne ne peut être contrainte de transmettre les données si cette transmission risque de violer ses droits constitutionnels, tels que le droit de ne pas s'incriminer soi-même.

Voici quelques exemples de pratiques :

- Australie : mandats de reprise de compte

  Elles permettent aux autorités de prendre le contrôle du compte en ligne d'une personne afin de recueillir des preuves concernant des infractions passibles d'une peine d'emprisonnement de trois ans ou plus. Un compte en ligne peut comprendre, par exemple, un compte sur un forum ou une place de marché du dark web, un service de courrier électronique, un compte de média social, un abonnement à un service d'information ou un profil d'utilisateur d'une plateforme de messagerie. Un mandat de reprise de compte facilite les reprises de compte secrètes et forcées (sans le consentement du titulaire du compte).

  Un mandat de prise de contrôle d'un compte permet aux autorités d'utiliser les informations d'identification d'un compte pour modifier les mots de passe ou d'autres données de connexion associées à un compte afin de verrouiller le titulaire ou l'utilisateur du compte et d'obtenir un accès exclusif à ce dernier. Toute autre activité, telle que l'accès à des données ou la réalisation d'activités d'infiltration tout en contrôlant le compte, par exemple en prenant une fausse identité, doit faire l'objet d'un mandat ou d'une autorisation distinct(e). À l'issue du mandat, l'agent doit prendre des mesures raisonnables pour redonner au titulaire du compte l'accès au compte, s'il est légal pour le titulaire de gérer le compte.

- Brésil : mesures généralement prises pour exécuter le pouvoir d'utiliser des identifiants d'accès acquis légalement

  - Les autorités compétentes doivent présenter une demande d'ordonnance judiciaire ou de mandat de perquisition à la juridiction compétente, en fournissant les faits et les preuves pertinents justifiant la nécessité d'accéder au système informatique et aux données qu'il contient au moyen d'identifiants d'accès acquis légalement.
  - Si le tribunal accorde l'autorisation, les autorités utiliseront les identifiants d'accès pour accéder au système informatique et aux données qu'il contient, conformément aux conditions spécifiées dans l'ordonnance du tribunal ou le mandat de perquisition.
  - À l'issue de la perquisition ou de l'accès, les autorités compétentes doivent soumettre à la juridiction un rapport décrivant les résultats de la perquisition ou de l'accès et fournissant une liste des données ou informations obtenues.

- Allemagne : consentement à la mesure

  Un mandat de perquisition au sens de l'article 105 du code de procédure pénale n'est pas nécessaire si la personne concernée (dans le cas de plusieurs détenteurs de la garde conjointe : tous) consent expressément à la perquisition. Il ne suffit pas de laisser faire sans s'y opposer, mais il faut un consentement silencieux et sans ambiguïté. Ce consentement à la fouille sera documenté.

- Norvège : exigence de proportionnalité

  Les dispositions générales sur la proportionnalité de l'article 170a de la loi de procédure pénale s'appliquent :
  Article 170 a :
  Une mesure coercitive ne peut être utilisée que s'il existe des motifs suffisants pour la justifier. La mesure coercitive ne peut être utilisée lorsqu'elle est disproportionnée par rapport à la nature de l'affaire et aux circonstances. La question de la proportionnalité s'appliquerait à la manière dont les identifiants d'accès sont utilisés, à la manière dont cela pourrait affecter des tiers, à la nécessité de l'utilisation et à la durée de l'accès.

### 4.1.4 Accès à distance caché

L'évaluation a également porté sur la question de savoir si les Parties peuvent accéder secrètement aux données à distance. Le droit interne de plusieurs Parties ([35] ) n'autorise pas leurs autorités à perquisitionner ou à accéder d'une autre manière à un système informatique et à ses données par le biais d'un accès à distance secret.

D'autres parties peuvent le faire surtout lorsque d'autres circonstances particulières sont réunies. Il peut s'agir de la disponibilité de la mesure uniquement pour certaines infractions[36] et d'autres circonstances particulières, telles que l'utilisation par la cible d'une technologie sophistiquée[37] ou une durée très limitée. [38]

Voici quelques exemples de mesures spécifiques d'accès à distance clandestin ou de mesures alternatives à l'accès à distance clandestin prévues par les législations nationales des parties :

- Andorre : agent de police infiltré, pouvant, le cas échéant, agir sur un système informatique (article 122 ter du CPP).

- Australie : mandat de perquisition à notification différée (partie IAAA de la loi sur les infractions), perquisition à distance et secrète d'appareils électroniques et de leur contenu (division 4 du chapitre 2 de la loi sur le développement durable).

- Belgique : recherches secrètes dans un système informatique (article 90ter du code de procédure pénale).

---

[35] Albanie, Autriche, Bosnie-Herzégovine, Brésil, Bulgarie, Costa Rica, Chypre, République dominicaine, Ghana, Grenade, Israël, Japon, Maurice, Panama, Portugal, Sierra Leone, République slovaque.

[36] Andorre, Argentine (dans certaines juridictions), Australie, Belgique, Cabo Verde, République tchèque, Danemark, Estonie, France, Géorgie, Allemagne, Hongrie, Islande, Lettonie, Lituanie, Monténégro, Pays-Bas, Norvège, République de Moldavie, Slovénie, Espagne, Suède, Türkiye.

[37] Belgique, Croatie, Finlande, France, Allemagne, Monténégro, Espagne, Suisse, Turquie, États-Unis.

[38] Chili (maximum 30 jours, le juge de la garantie peut prolonger cette période pour des périodes de même durée, avec un maximum de 60 jours).

- Chili : utilisation de programmes informatiques permettant d'accéder à distance et d'appréhender le contenu d'un appareil, d'un ordinateur ou d'un système informatique, à l'insu de son utilisateur (article 225 bis du CPP).

- République tchèque : surveillance des personnes et des objets (158d par. 3 et 4 du CPC).

- Danemark : perquisition secrète, lecture de données et interférence avec la correspondance (article 799 de la loi sur l'administration de la justice).

- Estonie : surveillance secrète, collecte secrète d'échantillons pour comparaison et conduite d'enquêtes initiales, examen secret et substitution d'un objet (article 126 du code de procédure pénale).

- Fidji : collecte en temps réel de données relatives au trafic et interception de données relatives au contenu (sections 22 et 23 de la TCA).

- Finlande : surveillance technique d'un dispositif (section 23 de la loi sur les mesures coercitives).

- France : saisie de données informatiques, 3 techniques spéciales d'enquête : l'utilisation de l'IMSI-catcher, l'enregistrement sonore et la fixation d'images, et la saisie de données informatiques.

- Géorgie : accès secret à distance à un système informatique (article 143, paragraphe 1, point b), du code pénal).

- Allemagne : recherche secrète à distance de systèmes de technologie de l'information (section 100b du StPO).

- Hongrie : surveillance secrète d'un système d'information, perquisition secrète, surveillance secrète d'une localité, interception secrète d'un envoi, interception de communications (articles 231-234 du code pénal).

- Islande : écoutes téléphoniques et autres mesures comparables (chapitre XI du PCC).

- Lettonie : contrôle des données situées dans un système de traitement automatisé des données et contrôle du contenu des données transmises (articles 219 et 220 du CPC respectivement).

- Lituanie : actions des enquêteurs de la phase préliminaire sans révéler leur identité (article 158 du CPP).

- Luxembourg : mesures spéciales d'enquête (art. 88-1 à 88-4 du CPP).

- Monténégro : mesures de surveillance secrète (chapitre 9 du CPC).

- Pays-Bas : "obtenir un accès à distance et secret" / "piratage légal" (article 126nba du DCCP ou article 181 jo 126ng du DCCP avec autorisation judiciaire préalable).

- Norvège : lecture de données (articles 216 o et 216 p du CPC).

- Macédoine du Nord : accès secret et perquisition de systèmes informatiques (article 252, paragraphe 4)

- République de Moldavie : Accès, interception et enregistrement de données informatiques (article 138 du CPC)

- Roumanie : mesure de surveillance effectuée secrètement en utilisant des informations d'identification acquises légalement (article 138, paragraphe 1, point b))

- Sénégal : installation et utilisation d'outils à distance pour obtenir des preuves utiles à une affaire (article 90-10).

- Slovénie : possibilité de contrôler le système informatique d'une banque ou d'une autre entité juridique exerçant une activité financière ou économique.

- Espagne : recherches à distance dans un système informatique (article 588 septies du CPL).

- Suède : interception de données secrètes (loi sur l'interception de données secrètes).

- Suisse : utilisation de programmes informatiques spéciaux conformément aux articles 269ter et 269quater du code pénal.

- Tonga : interception de communications électroniques (section 14 de la loi sur les délits informatiques).

- Turquie : enquête sur le délit de paris illégaux en ligne (article 5 de la loi n° 7258).

- Royaume-Uni : Mandat de brouillage d'équipement ciblé (TEI) (s99(2) de la loi sur les pouvoirs d'investigation de 2016).

- États-Unis : accès à distance pour la recherche de supports de stockage électroniques (règle fédérale de procédure pénale 41(b)(6)).

Les réponses suggèrent que l'expression "accès à distance secret" est comprise différemment par les différentes parties. Certaines Parties se réfèrent explicitement à la recherche à distance de systèmes informatiques, y compris l'introduction d'un logiciel spécial dans le système, d'autres se réfèrent aux pouvoirs de surveillance traditionnels ou à l'utilisation d'agents infiltrés.

De nombreuses Parties [39]ont souligné qu'une décision de justice est nécessaire pour autoriser une telle mesure. Une partie au moins (la Grèce) n'exige pas de décision judiciaire dans certains cas.

Certaines parties (Belgique, Danemark, Estonie, France, Géorgie, Hongrie, Lettonie, Norvège, Espagne, Suisse) ont également indiqué que la mesure prévoit la possibilité de collecter des données en temps réel et qu'il existe des exigences en matière de notification (Australie, Belgique, Danemark, Géorgie[40] , Allemagne, Lituanie, Pays-Bas).

En ce qui concerne les autres garanties, certaines Parties (Costa Rica, Danemark, Estonie, Finlande, Allemagne, Israël, Pays-Bas, Norvège, Espagne) ont déclaré que la mesure ne peut durer que pendant une période limitée. Une Partie (Arménie) a indiqué que, bien qu'aucune

[39] Andorre, Argentine, Australie, Belgique, Brésil, Canada, République tchèque, Danemark, Estonie, Finlande, Géorgie, Allemagne, Hongrie, Islande, Lettonie, Lituanie, Monténégro, Pays-Bas, Nigeria, Norvège, Espagne, Türkiye, États-Unis.

[40] La Géorgie exige également que les personnes concernées soient informées de ce pouvoir après un an.

disposition spécifique ne régisse la recherche secrète à distance, de telles mesures peuvent être mises en œuvre dans la pratique.

Voici quelques exemples de pratiques :

- France : saisie de données informatiques

  - Les articles 706-102-1 et 706-102-2 du code de procédure pénale définissent la mesure.
  - Il est possible de capturer à distance et en continu des données (textes, images, sons, etc.) sur un terminal informatique cible (ordinateur, téléphone, tablette, etc.).
  - Cette technique permet aux enquêteurs d'accéder aux données contenues dans un terminal numérique et d'intercepter les flux de données.
  - Cette solution présente l'avantage de contourner le cryptage des communications. Outre l'enregistrement des frappes au clavier et la réalisation de copies d'écran, le dispositif technique utilisé permet de récupérer des conversations (à partir d'applications telles que Skype ou WhatsApp) et des données stockées dans un système informatique.
  - Il est ainsi possible de rechercher à distance sur le disque dur d'un terminal des informations utiles aux enquêtes judiciaires. La capture des données informatiques se fait soit au moyen d'un dispositif technique inséré directement dans le support, soit par injection à distance
  - La mesure diffère de l'interception des communications électroniques en ce qu'elle vise les données informatiques de toute nature, et pas seulement les messages écrits ou sonores.

- Allemagne : perquisition secrète à distance d'un  informatique

  - La mesure est définie à l'article 100b du StPO.
  - Il peut être utilisé pour accéder à un système informatique utilisé par la personne concernée et des données peuvent être collectées à partir de ce système (recherche secrète à distance de systèmes informatiques), même à l'insu de la personne concernée.
  - Il s'agit de l'extraction en ligne de contenus de stockage électronique qui ne sont pas l'objet principal d'une communication en cours. Cette extraction s'effectue en recherchant dans les supports de stockage (par exemple, le disque dur), c'est-à-dire en recherchant dans les bases de données existantes les contenus qui y sont stockés, tels que les fichiers texte, les images, les courriers électroniques déjà reçus ou envoyés et stockés sur le système cible.
  - La mesure est effectuée par un logiciel spécialement conçu à cet effet. Il convient de s'assurer techniquement que seules les modifications indispensables à la collecte des données sont apportées au système informatique et que les modifications apportées sont automatiquement annulées à la fin de la mesure, dans la mesure où cela est techniquement possible.
  - En outre, il existe des obligations en matière d'intégrité des données et de journalisation.
  - Le logiciel peut également être introduit dans le système cible via Internet si cela est techniquement possible. La disposition n'autorise pas l'entrée clandestine dans un domicile dans le but d'insérer le programme dans un ordinateur.

- Pays-Bas : pouvoir de piratage légal et accès à distance avec autorisation judiciaire préalable sur la base d'informations didentification obtenues légalement [41]

  La loi III sur la criminalité informatique établit une base légale pour le "pouvoir de piratage" dans le DCCP (articles 126nba, 126uba et 126zpa du DCCP ou article 181 jo 126ng du DCCP avec autorisation judiciaire préalable).
  Ce nouveau pouvoir d'enquête permet à certains agents des services répressifs désignés "d'accéder secrètement à des systèmes informatisés {travaux automatisés}[42] à distance, sous certaines conditions, qui sont utilisés par des suspects, en vue d'atteindre certains objectifs d'enquête dans le domaine de la recherche d'infractions pénales graves".
  Après avoir accédé à un système informatisé (tel qu'un téléphone portable ou un serveur), la police peut mener un certain nombre d'activités d'enquête, à savoir
  - A) établir les caractéristiques spécifiques du système informatisé ou de ses utilisateurs, telles que leur identité ou leur localisation, et documenter ces informations ;
  - B) l'exécution d'un ordre d'enregistrement de communications confidentielles ou la mise sur écoute et l'enregistrement de communications ;
  - C) l'exécution d'un ordre d'observation systématique ;
  - D) documenter les données stockées dans le système informatisé ; et
  - E) rendre le contenu des données inaccessible.

### 4.1.5 Autorités compétentes qui autorisent et effectuent une perquisition

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| Albanie | Juge | Procureur, police judiciaire, expertise peuvent être impliqués |
| Andorre | Juge d'instruction | Officiers de police et autorités spécialisées désignés par le juge d'instruction |
| Argentine | Juge | Procureurs et officiers de police |
| Arménie | Juge | Officiers de police et experts techniques |
| Australie | Juge ou membre du Tribunal administratif de recours (TAR) | les autorités chargées de l'application de la loi, y compris les gendarmes ou les gendarmes qui les assistent |
| Autriche | Autorité de poursuite | Autorité d'enquête criminelle |
| Azerbaïdjan | Juge, juge d'instruction | Les autorités chargées de l'application de la loi avec l'aide d'experts techniques |
| Belgique | 39bis, § 2, alinéa 1 : officier de police judiciaire ;<br>39bis, § 2, alinéa 2 : procureur général ;<br>88ter : juge d'instruction ;<br>90ter : juge d'instruction. | Experts de la police |
| Bosnie et Herzégovine | Juge | Procureurs et autorités policières assistés par des experts en criminalistique informatique et numérique |
| Brésil | Juge | Officier de police avec expert technique (pour assurer la chaîne de détention), |

[41] Pour les conditions de déploiement de la mesure et les garanties pour les personnes, ainsi que les mesures généralement prises pour exécuter le pouvoir légal de piratage, voir la réponse individuelle à la question 2.1.4 fournie par les Pays-Bas.

[42] Dans la loi Computer Crimes III Act, les systèmes informatisés sont décrits comme des "dispositifs automatisés/transporteurs de données".

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| | | procureur avec expert technique, unités spécialisées au sein des services de police et du ministère public. |
| Bulgarie | Juge | un enquêteur, un officier de police judiciaire ou un agent des douanes. D'autres experts en informatique peuvent être présents |
| Cabo Verde | Juge, procureur | Judiciaire Police ou tout technicien ou expert habilité |
| Cameroun | Avocat de l'État, juge d'instruction | Procureur |
| Canada | Juge | Agent de la paix, agent public, expertise technique peuvent être impliqués |
| Colombie | Juge | Police judiciaire |
| Costa Rica | Juge | Parquet et/ou police judiciaire |
| Croatie | Juge d'instruction, juge | Officier de police et autre autorité spécialisée |
| Chypre | Juge | Officier de police |
| République tchèque | Juge | Officier de police |
| Danemark | Juge | Police nationale danoise |
| République dominicaine | Juge | Procureur, police spécialisée dans la cybercriminalité |
| Estonie | Procureur | Experts et autres experts techniques |
| Fidji | Juge | Police et experts techniques |
| Finlande | Juge, procureur, officier de police | Autorités policières et autres experts techniques |
| France | Juge | Procureur, officier de police, procureur adjoint. Personnes qualifiées pour effectuer des examens techniques. Les perquisitions dans des locaux spéciaux peuvent être effectuées par un magistrat. |
| Géorgie | Magistrat | Enquêteurs spécialisés ou enquêteurs réguliers assistés de spécialistes techniques |
| Allemagne | Juge | les autorités policières, douanières ou fiscales. D'autres personnes, telles que des interprètes, des experts et des témoins experts, peuvent être impliquées. |
| Ghana | Juge | Agents de police ou d'application de la loi, experts techniques et autres experts |
| Grèce | Juge, procureur | Fonctionnaires chargés de l'application de la loi, experts en criminalistique numérique, en cybersécurité, en questions juridiques et en opérations techniques |
| Grenade | Magistrat | Officiers de police |
| Hongrie | Juge, procureur, autorité d'enquête | Le procureur, la police et l'autorité fiscale et douanière nationale en tant qu'autorités chargées de l'enquête, des consultants possédant une expertise spécifique. |
| Islande | Juge | Autorités policières |
| Israël | Juge | La police nationale, l'administration fiscale, la police militaire, le département des enquêtes internes de la police, l'autorité des valeurs mobilières, l'autorité de la |

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| | | concurrence et l'autorité de protection des données. |
| Italie | Procureur | Forces de police et autres organismes chargés de l'application de la loi |
| Japon | Juge | Procureurs, substituts du procureur ou officiers de police judiciaire |
| Kiribati | Juge | Officier de police |
| Lettonie | juge d'instruction | Personnel spécialisé |
| Liechtenstein | Juge d'instruction | Unité de lutte contre la criminalité numérique de la police nationale du Liechtenstein |
| Lituanie | Juge | Fonctionnaire chargé de l'enquête préliminaire ou procureur, spécialistes des technologies de l'information |
| Luxembourg | Juge d'instruction, procureur | Police |
| Malte | Magistrat | Officiers de police |
| Maurice | Juge | Autorité d'enquête |
| Monaco | Juge, procureur | Police d'État (unité de lutte contre la cybercriminalité) |
| Monténégro | Juge d'instruction | Officiers de police, officiers du centre de criminalistique numérique |
| Maroc | Juge d'instruction (si l'enquête est ouverte), procureur (pendant la phase d'enquête) | officier de police judiciaire |
| Pays-Bas | Juge, procureur, officier de police (dans certaines circonstances, la police peut également effectuer la perquisition sans autorisation et donc à sa propre discrétion) | Procureur et officier de police. Experts en informatique |
| Nigéria | Juge | Police |
| Macédoine du Nord | Juge | Procureur et agents chargés de l'application de la loi |
| Norvège | Juge, procureur | Police, procureurs et personnel assimilé |
| Panama | Juge, procureur | Procureur |
| Paraguay | Juge | |
| Pérou | Juge | Procureur, Police nationale |
| Philippines | Juge | Agents de la force publique |
| Pologne | Juge, procureur | Procureur, officier de police |
| Portugal | Juge, procureur | Procureur, officier de police, experts spécialisés |
| République de Moldavie | Juge d'instruction, procureur | Procureur, agents chargés de l'application de la loi |
| Roumanie | Juge | spécialiste travaillant avec les organes judiciaires, un spécialiste externe ou un officier de police spécialisé, un procureur ou un officier de police enquêtant sur l'affaire. policier spécialisé, procureur ou policier enquêtant sur l'affaire |

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| Saint-Marin | Juge | Officier de police |
| Sénégal | Juge d'instruction, procureur | Juge d'instruction ; police sous la supervision du procureur ou du juge d'instruction |
| Serbie | Juge | Police |
| Sierra Leone | Juge | Agent chargé de l'application de la loi |
| République slovaque | Juge, procureur | Techniciens ou experts médico-légaux |
| Slovénie | Juge | officier de police |
| Espagne | Juge | officier de police, laboratoires d'ingénierie médico-légale |
| Sri Lanka | Magistrat | Officiers de police, experts médico-légaux sous la supervision de la police |
| Suède | Responsable de l'enquête, procureur ou juge | Autorité d'enquête en coopération avec les experts en criminalistique numérique ou d'autres personnels spécialisés |
| Suisse | Juge, procureur | Officier de police, autre autorité spécialisée |
| Tonga | Magistrat | Police |
| Tunisie | Juge, procureur | Officier de police |
| Türkiye | Juge | Unités chargées de l'application de la loi |
| Ukraine | Magistrat instructeur, juge | Enquêteur, procureur |
| Royaume-Uni | Magistrat | Officier de police |
| États-Unis d'Amérique | Juge | Agent chargé de l'application de la loi |

## 4.2 Mise en œuvre de l'article 19.1 - Évaluation

Les réponses aux questions suivantes du questionnaire ont été évaluées :

- Q 2.1.1 Veuillez résumer les mesures législatives et autres prises par votre pays pour garantir que les autorités puissent perquisitionner ou accéder de la même manière aux systèmes informatiques, aux données et aux supports de stockage de données sur votre territoire, conformément à l'article 19.1. Dans votre réponse, veuillez résumer les conditions à remplir et les étapes de la procédure généralement suivies pour obtenir l'autorisation d'une telle perquisition.
- Q 2.1.2 Des règles particulières s'appliquent-elles en cas d'urgence ou d'autres circonstances urgentes ? Dans l'affirmative, veuillez décrire ces règles et l'interprétation applicable de ce qui constitue une situation d'urgence.
- Q 2.1.3 Votre législation habilite-t-elle vos autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant des références d'accès légalement acquises ? En répondant à cette question, veuillez résumer les conditions à remplir et les mesures généralement prises pour exercer ce pouvoir.
- Q 2.1.4 Votre législation habilite-t-elle vos autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant un accès à distance secret ? Dans votre réponse, veuillez résumer les conditions à remplir et les mesures généralement prises pour exercer ce pouvoir.
- Q 2.1.5 Quelles sont les autorités compétentes qui autorisent et effectuent une recherche telle que décrite à l'article 19.1 ? Quel type d'expertise technique ou autre est requis et utilisé ?

| **Parti** | **Mesures législatives et autres** | **L'évaluation** |
|---|---|---|
| Albanie | La législation albanaise, à l'article 208/A du code de procédure pénale (ci-après le "CPP"), prévoit que c'est le tribunal qui autorise la perquisition et l'accès à des systèmes informatiques ou à des parties de ceux-ci, à la demande du procureur. Dans sa décision, le tribunal précise le système informatique (ou une partie de celui-ci) auquel il faut accéder, le droit de pénétrer (accéder) dans le système informatique, de perquisitionner dans le système informatique et d'obtenir les données informatiques demandées. Le procureur de la République ou l'officier de police judiciaire mandaté par le procureur de la République exécute ensuite la décision. Lors de l'exécution de la décision, le procureur de la République peut désigner un expert ayant une connaissance particulière du fonctionnement des systèmes informatiques ou des mesures de conservation des données informatiques.<br><br>Le CPC albanais ne contient pas de définitions en général, y compris celle des données informatiques stockées. C'est pourquoi, dans l'application de cet article, la définition utilisée est celle de la | L'Albanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Convention de Budapest. La Convention de Budapest est ratifiée et fait partie de la législation albanaise, l'interprétation des "données informatiques" est basée sur la définition de la Convention de Budapest, conformément à l'article 116 de la Constitution albanaise, qui stipule que les accords internationaux ratifiés par l'Albanie sont mis en œuvre dans le cadre de la juridiction albanaise.<br><br>La législation albanaise ne prévoit pas de règles spéciales applicables en cas d'urgence ou d'autres circonstances urgentes.<br><br>Il n'existe pas non plus de disposition spécifique concernant l'accès au système utilisant les données d'accès, mais l'article 208/A du CPC prévoit que la juridiction accorde le droit d'accès et de recherche dans sa décision.<br><br>La législation albanaise ne prévoit pas de pouvoirs procéduraux pour l'accès secret à distance.<br><br>L'Albanie a indiqué que sa législation prévoit que le tribunal est l'autorité compétente pour autoriser les perquisitions et les saisies. Le procureur fait la demande et est ensuite chargé d'exécuter la décision du tribunal en ordonnant la police judiciaire et, si nécessaire, en désignant l'expert. | |
| Andorre | Le droit andorran des perquisitions découle de la Constitution, de nombreux articles du code de procédure pénale et de la loi 22/2022 du 9 juin relative aux systèmes électroniques. Le code pénal contient également des définitions et d'autres dispositions pertinentes. En résumé, une perquisition doit être nécessaire, proportionnée et adaptée à l'objectif poursuivi. Son autorisation (par un juge) doit être spécifique, fondée en droit et en fait, et se rapporter à des délits majeurs ou à certains délits mineurs. Différents fonctionnaires de la justice pénale ou une personne privée peuvent demander une telle ordonnance.<br><br>En cas d'urgence, une perquisition peut avoir lieu si elle a été autorisée verbalement par un juge (tribunal de garde) qui la consigne ensuite par écrit. Il y a urgence lorsqu'une cible se cache dans un lieu ou est découverte en train de commettre un délit. | L'Andorre applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les titres obtenus légalement peuvent être utilisés. Le juge examinera attentivement la manière dont ils ont été obtenus. Pour le reste, la recherche suivra les procédures décrites ci-dessus. La police prendra des mesures techniques pour s'assurer que d'autres personnes ne peuvent pas utiliser les identifiants pour affecter les données à rechercher.<br>L'accès à distance dissimulé n'est pas mentionné en tant que tel dans la loi andorrane. Toutefois, dans le cas de certains délits, le code pénal permet à un juge de nommer un agent de police secret, qui pourrait agir sur les systèmes électroniques.<br><br>Les perquisitions sont autorisées par les juges d'instruction. Les perquisitions sont effectuées par des policiers spécialement formés ou entraînés conformément aux normes internationales (ISO27001 et RFC3227). | |
| Argentine | Les autorités argentines ont indiqué que leur territoire est composé de 23 provinces et de la ville autonome de Buenos Aires. Chaque province possède son propre code de procédure pénale, tout comme la ville de Buenos Aires. Ces codes coexistent avec un code de procédure pénale pour la poursuite des crimes relevant de la juridiction fédérale. Ce système procédural fédéral se trouve dans une période de transition entre deux codes de procédure pénale : le code de procédure pénale national (CPPN) et le code de procédure pénale fédéral (CPPF) qui est mis en œuvre progressivement avec l'idée qu'il remplacera le précédent sur l'ensemble du territoire.<br><br>L'art. 151 du CPPF prévoit un pouvoir spécifique de perquisition et de saisie. En vertu de cette disposition, le juge peut ordonner, à la demande d'une partie et par ordonnance motivée, la perquisition d'un système informatique ou d'une partie de celui-ci, ou d'un support de stockage de données informatiques ou électroniques, afin de saisir les composants du système, d'en obtenir une copie ou de conserver des données ou des éléments présentant un intérêt pour l'enquête.<br><br>Il convient de noter qu'il existe des dispositions spécifiques prévoyant la perquisition et la saisie de données informatiques stockées dans certains codes provinciaux et l'Argentine a mentionné dans sa réponse les provinces qui ont mis en œuvre des dispositions spécifiques, ces dispositions étant détaillées dans chaque cas (la législation de certaines provinces, qui est plus spécifique que la loi fédérale, peut présenter un intérêt). Plusieurs provinces ont récemment emboîté le pas ou prévoient | L'Argentine a introduit des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. qui n'est pas encore applicable dans l'ensemble du pays. Entre-temps, dans la pratique, l'Argentine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | de le faire, ce qui est louable. Toutefois, l'art. 151 applicable au niveau fédéral n'est pas encore en vigueur dans l'ensemble du pays. En ce sens, il est important de noter que le nouveau code de procédure pénale introduisant le système accusatoire de poursuites pénales et sa mise en œuvre est effectuée progressivement dans tout le pays par une commission bicamérale du parlement chargée du processus de suivi et de mise en œuvre du nouveau système procédural.<br><br>En Argentine, le "principe de liberté de la preuve" s'applique également aux perquisitions et aux saisies, ainsi qu'à la chaîne de conservation des preuves numériques (collecte - stockage - conservation - production - présentation - évaluation des preuves électroniques). Le code national de procédure pénale, le code fédéral de procédure pénale et les protocoles existants sont appliqués dans la juridiction fédérale.<br><br>L'article 224 du CPPN prévoit également la doctrine de la simple vue qui permet l'ouverture d'une enquête si des preuves d'un délit autre que celui faisant l'objet de l'enquête sont trouvées lors d'une perquisition, et qui s'étend également aux preuves électroniques.<br><br>Il n'est pas fait mention de l'utilisation des identifiants d'accès par les autorités dans le respect de la loi.<br><br>L'accès à distance n'est réglementé que dans certaines juridictions, car en Argentine, les provinces peuvent réglementer leurs codes de procédure.<br><br>Le juge ordonne et le ministère public exécute l'ordonnance avec les différents services spécialisés des forces de police qui interviennent pour l'exécution de la mesure. | |
| Arménie | L'article 236 du code de procédure pénale prévoit des perquisitions et des saisies électroniques sur le territoire. Une décision de justice (mandat judiciaire ou ordonnance) est nécessaire pour obtenir l'autorisation de procéder à une perquisition/saisie conformément à l'article 19.1. Les enquêteurs exécutent la perquisition/saisie et sont assistés, si nécessaire, par des experts techniques.<br><br>Il n'y a pas de dispositions spécifiques concernant les situations d'urgence. | L'Arménie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La législation arménienne autorise les autorités à perquisitionner ou à accéder à des ordinateurs en utilisant des identifiants d'accès acquis légalement. Outre l'acquisition légale des identifiants, les autorités doivent également disposer d'une autorisation légale d'accès, généralement obtenue par le biais d'un mandat ou d'une ordonnance judiciaire. Des moyens techniques ou des outils spécialisés peuvent être utilisés pour exécuter l'accès.<br><br>Il n'existe pas de législation particulière autorisant l'utilisation de l'accès à distance secret, mais, dans la pratique, il est possible d'y recourir.<br><br>Il n'existe pas de procédures opérationnelles normalisées internes ou de lignes directrices similaires. | |
| Australie | La réponse de l'Australie ne concerne que la législation du Commonwealth. L'Australie s'appuie sur une loi générale sur les perquisitions et une loi spécifique aux ordinateurs. La loi de 1914 sur les infractions (Crimes Act 1914) est à l'origine d'une série de pouvoirs de perquisition et de saisie, y compris les procédures de mandat, les approbations judiciaires et le traitement des preuves saisies. La loi de 2004 sur les dispositifs de surveillance (Surveillance Devices Act 2004) couvre les dispositifs de surveillance et l'accès secret aux données contenues dans les ordinateurs. Cette dernière loi établit un régime pour les mandats d'accès aux ordinateurs et les infractions principales nécessaires.<br><br>Les "données informatiques stockées" sont définies dans une loi, la loi de 1979 sur les télécommunications (interception et accès). En outre, les textes de la loi sur les infractions et de la loi sur le développement durable contribuent à définir ce concept.<br>Les dispositions de la loi sur les infractions relatives aux mandats définissent les exigences en matière de notification en cas de perquisition de locaux ou de personnes. Les deux lois exigent que les mandats soient délivrés par un membre du pouvoir judiciaire (qui comprend divers fonctionnaires du pouvoir judiciaire).<br><br>Les deux lois définissent les situations d'urgence et prévoient qu'en cas d'urgence, des autorisations peuvent être obtenues selon des procédures accélérées ou que des perquisitions peuvent être effectuées sans mandat. Dans le second cas, une approbation a posteriori doit être obtenue. | L'Australie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'art. 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Certains mandats permettent aux forces de l'ordre d'obtenir des informations - par exemple un code d'accès - qui permettront d'accéder aux données. En outre, lorsque certaines infractions font l'objet d'une enquête, il est possible d'obtenir des mandats de reprise de compte qui permettent de modifier les identifiants d'accès. Les enquêtes plus approfondies nécessitent un mandat complémentaire.<br><br>L'accès secret à distance peut être autorisé par un mandat pour des infractions plus graves. La notification de la perquisition à l'occupant des lieux perquisitionnés peut être retardée mais doit normalement avoir lieu dans les six mois.<br><br>Les perquisitions sont effectuées par des agents des forces de l'ordre autorisés, qui peuvent être membres d'un certain nombre de forces australiennes (spécifiées). | |
| Autriche | Plusieurs articles du code de procédure pénale prévoient la perquisition et la saisie d'objets, y compris de supports de stockage de données. Toutes les données accessibles via des supports de stockage de données peuvent être perquisitionnées, y compris lorsque les données sont protégées par un mot de passe et, dans certains cas, lorsqu'un logiciel de craquage est nécessaire. La personne en possession de l'objet ou des données (limitée si un accusé est impliqué) a l'obligation d'aider les autorités. Cette obligation s'étend à l'aide à l'accès aux informations numériques, à la réalisation de copies de sauvegarde, etc. En règle générale, il faut obtenir un ordre de l'autorité de poursuite pénale ; dans certains cas, l'autorité d'enquête pénale peut saisir des objets de sa propre initiative. Dans certains cas, les exigences procédurales sont plus élevées. Les saisies sont effectuées par les autorités d'enquête pénale, dont certaines sont spécialement formées.<br>En cas de "danger imminent", lorsqu'il existe un "besoin inévitable d'intervention immédiate", l'autorité chargée de l'enquête pénale peut agir de sa propre initiative, mais doit demander l'approbation du ministère public a posteriori.<br><br>L'accès à distance clandestin n'est pas possible. | L'Autriche applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Azerbaïdjan | La base juridique de la perquisition et de la saisie de données informatiques est principalement établie par le code de procédure pénale. Les pouvoirs de perquisition et de saisie s'appliquent aux infractions | L'Azerbaïdjan applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | commises à l'encontre ou au moyen d'un ordinateur ainsi qu'à d'autres infractions si la preuve est électronique. Les articles 177 et 242-247 du code de procédure pénale sont les articles applicables. Il n'existe pas d'exigences spécifiques en matière de notification.<br><br>En règle générale, une ordonnance du tribunal est nécessaire pour effectuer des perquisitions et des saisies à l'avance. Toutefois, à titre exceptionnel, les procédures d'enquête peuvent être exécutées sur décision motivée de l'enquêteur dans des circonstances qui ne permettent pas de retard, conformément aux articles 177.3.1, 177.3.2, 177.3.4 et 177.3.5 du CPP (interception de conversations téléphoniques ou autres et d'informations transmises par le biais de moyens de communication et d'autres moyens techniques). En outre, l'article 243. 3 du code de procédure pénale stipule que l'enquêteur ne peut procéder à une perquisition ou à une saisie sans ordonnance du tribunal que s'il existe des informations précises indiquant que des objets ou des documents cachés dans un immeuble résidentiel sont la preuve de la commission d'un crime ou de la préparation de la commission d'un crime contre une personne ou l'État ; une personne qui a préparé ou commis une infraction contre une personne ou l'État, ou une personne qui s'est évadée d'une maison d'arrêt ou d'une prison se cache dans un bâtiment résidentiel ; un cadavre humain (ou des parties d'un cadavre) se trouve dans le bâtiment ; il existe un danger réel pour la vie ou la santé d'une personne se trouvant dans le bâtiment.<br><br>L'exécution de la recherche est limitée aux paramètres de l'ordre. Seuls le service de sécurité de l'État et le ministère de l'intérieur effectuent des recherches dans les affaires de cybercriminalité. Dans les autres types d'affaires, ces services, plusieurs autres organismes chargés de l'application de la loi et le bureau du procureur effectuent des recherches. Des unités spécialisées dans la criminalistique numérique sont en place depuis de nombreuses années au sein du ministère de la justice, du ministère de l'intérieur et du service de sécurité de l'État. Ces unités sont chargées d'effectuer des enquêtes criminalistiques numériques et de traiter les preuves numériques dans les affaires impliquant des données informatiques stockées. Des lignes directrices internes n'ont pas été adoptées.<br><br>Plusieurs articles du CPP s'appliquent aux situations d'urgence. Si les actes d'enquête (énumérés dans certaines sections du CPP) ne peuvent être reportés en cas d'urgence, l'enquêteur doit remplir | 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | les obligations énoncées à l'article 443, paragraphe 2, et, conformément à un autre article, les documenter et justifier leur nécessité ainsi que l'impossibilité de retarder l'acte d'enquête pour obtenir une décision de justice. Un enquêteur peut effectuer une perquisition ou une saisie sans ordonnance judiciaire en cas d'urgence si des informations spécifiques indiquent certaines circonstances (précisées dans les réponses). Dans ce cas, les enquêteurs doivent rédiger une décision justifiant la nécessité de la perquisition ou de la saisie conformément à l'article 243.4 et en informer le tribunal et le procureur dans les 24 heures. Ils doivent également soumettre tous les documents justificatifs et connexes dans les 48 heures au tribunal exerçant le contrôle judiciaire et au procureur afin d'obtenir la validation de la mesure de perquisition. Si le tribunal est d'accord avec la position de l'enquêteur, il rendra une ordonnance validant l'enquête.<br><br>La législation n'autorise pas explicitement les autorités à utiliser des identifiants d'accès acquis légalement. Les règles générales en matière de perquisition et de saisie s'appliquent dans de tels cas ; il semble donc que des identifiants d'accès acquis légalement puissent être utilisés dans certains cas.<br><br>La législation ne prévoit pas explicitement l'accès secret à distance. | |
| Belgique | Il existe quatre bases pour les perquisitions et les saisies : une perquisition policière dans le cadre d'une enquête, en particulier d'une arrestation, qui peut être effectuée sans autorisation préalable du procureur ou du juge ; une perquisition sans saisie (par exemple, dans un cybercafé), qui nécessite l'autorisation du procureur ; une perquisition, autorisée uniquement par un juge d'instruction, qui peut être étendue à un lieu accessible autre que celui faisant l'objet de la perquisition si deux conditions préalables sont remplies ; et une perquisition, autorisée uniquement par un juge d'instruction, qui est nécessaire à l'établissement de la preuve. En outre, la proportionnalité ou la perte potentielle de preuves doivent être en jeu. Les perquisitions sont effectuées par des experts de la police.<br><br>La loi ne contient pas de définition de l'urgence, mais un procureur ou un juge d'instruction peut ordonner verbalement une recherche de données saisies dans le cadre d'une enquête. Une telle ordonnance doit être justifiée par écrit et sans délai. | La Belgique applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les titres acquis légalement peuvent être utilisés. Les règles habituelles s'appliquent. L'article 90ter du code pénal prévoit l'accès secret à distance sous certaines conditions restrictives, notamment qu'aucune autre méthode d'enquête ne suffise et que la recherche soit effectuée pour obtenir des preuves, et non pour une enquête générale. | |
| Bénin | En général, les perquisitions et les saisies tirent leur base juridique des dispositions du CPP du Bénin. Plus spécifiquement, la perquisition et la saisie des données informatiques stockées sont régies par les articles 587, 590 et 592 de la loi numéro 2017-20 du 20 avril 2018 portant code du numérique. Ces dispositions précisent les moyens et conditions de perquisition et de saisie, les autorités compétentes et les cas dans lesquels la copie des données est souhaitable.<br><br>Les pouvoirs de perquisition et de saisie s'appliquent aux infractions commises à l'encontre de systèmes d'information ou à l'aide de ceux-ci, ainsi qu'aux infractions prévues par la législation béninoise qui comportent des éléments de preuve électroniques.<br><br>Les autorités compétentes pour autoriser une perquisition sont le juge d'instruction et le procureur spécial de la cour de répression des infractions économiques et du terrorisme (CRIET). Les perquisitions doivent obligatoirement être exécutées par des officiers de police judiciaire. Les officiers de police judiciaire qui travaillent sur les perquisitions et saisies numériques ont reçu une compétence nationale de la cour d'appel de Cotonou. Ces agents dépendent du procureur de la CRIET et disposent du matériel et des moyens de transport adéquats pour protéger l'intégrité des preuves collectées.<br><br>L'article 77 du CPP et l'article 589 de la loi sur le code numérique exigent que les perquisitions et les saisies ne soient effectuées qu'avec le consentement exprès de la personne qui se trouve sur le lieu de l'opération. Ce consentement doit être consigné dans le procès-verbal de l'opération. En outre, les cibles sont invitées à fournir des références d'accès ou des informations (qui doivent également être consignées dans le procès-verbal). Si les cibles refusent de coopérer, le juge d'instruction ou la juridiction peut autoriser l'accès par n'importe quelle méthode. L'article 589/2 prévoit que, si l'infraction en cause est passible d'une peine supérieure à cinq ans d'emprisonnement, ou si la | Le Bénin applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | perquisition le justifie, le juge d'instruction peut, par ordonnance écrite, autoriser une perquisition et une saisie en l'absence du consentement de la personne concernée.<br><br>Une affaire est considérée comme urgente si la cible est en mesure d'endommager ou de détruire des données susceptibles de contenir des éléments de preuve. Dans ce cas, les règles normales de recherche peuvent être modifiées et une recherche peut être lancée avant l'obtention de l'autorisation du procureur spécial de la CRIET.<br><br>Les autorités peuvent utiliser des identifiants d'accès légalement acquis pour effectuer des recherches dans un système au-delà d'un système initialement perquisitionné. La recherche dans un système au-delà d'un système initialement recherché peut être effectuée sans autre autorisation du juge ou du procureur, par exemple sur la base des dispositions du code de procédure pénale (par exemple, les articles 40, 76 et 99).<br><br>Il n'est pas prévu d'accès secret à distance.<br><br>Des lignes directrices internes ou des procédures opérationnelles normalisées n'ont pas été créées. | |
| Bosnie et Herzégovine | Les réponses de ce groupe proviennent de quatre sources : la Bosnie-Herzégovine, la Fédération de Bosnie-Herzégovine, la Republika Srpska et le district de Brcko. Leurs codes pénaux et leurs codes de procédure pénale réglementent les procédures de manière presque identique.<br><br>Le code pénal de la Republika Srpska vise spécifiquement les données résultant du traitement électronique des données, des systèmes informatiques, des dispositifs de stockage de données et des téléphones portables. La police ou les procureurs demandent à un tribunal de délivrer un mandat, en précisant la justification de celui-ci, en fournissant des détails et en remplissant les conditions préalables, y compris la norme de suspicion raisonnable que les données ciblées sont liées à une infraction pénale. Dans certaines situations, par exemple en cas de danger probable pour la vie ou la santé ou de risque de destruction de preuves, la police ou les procureurs peuvent utiliser des méthodes non formelles - par exemple des appels téléphoniques ou des courriels - pour demander l'autorisation de perquisitionner et de saisir des données sans ordonnance écrite du tribunal. Ces actions doivent | La Bosnie-Herzégovine utilise une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'art. 19.1. Il semble que la Bosnie-Herzégovine n'ait pas entièrement mis en œuvre l'article 19.1. Des dispositions spécifiques établissant un cadre juridique pour les perquisitions et les saisies de données et de systèmes informatiques applicables dans toutes les entités de la Bosnie-Herzégovine pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | être examinées et ratifiées dans les 48 heures. En Republika Srpska, une demande orale de mandat peut être soumise lorsqu'il y a un risque de retard. Dans ce cas, le juge chargé de l'approbation rendra le même type d'ordonnance que pour les affaires courantes. Les cas urgents sont ceux où il y a un risque que des preuves soient cachées ou détruites, qu'un autre crime soit commis, que la cible s'enfuie ou qu'une personne soit mise en danger.<br><br>Dans la Fédération de Bosnie-Herzégovine, la législation actuelle ne permet pas de procéder à des saisies d'ordinateurs, étant donné que chaque manipulation doit être clairement décrite. Comme elles ne peuvent pas être clairement décrites, elles ne sont pas possibles.<br><br>La législation de Bosnie-Herzégovine n'autorise pas spécifiquement les autorités à utiliser des informations d'identification acquises légalement (bien que les enquêtes sous couverture, les écoutes téléphoniques et d'autres formes de surveillance puissent être autorisées si elles sont dûment justifiées).<br><br>Le code de procédure pénale de Bosnie-Herzégovine n'indique pas clairement si l'accès à distance secret est autorisé.<br><br>L'accès à distance clandestin n'est pas non plus possible en vertu du code de procédure pénale de la Fédération de Bosnie-et-Herzégovine. Selon l'administration de la police fédérale, la législation actuelle ne permet pas d'effectuer des accès à distance sous couverture, étant donné que chaque manipulation doit être clairement décrite. Étant donné que l'accès ne peut être clairement décrit, la mesure n'est pas possible.<br><br>L'article 234 du code de procédure pénale de la Republika Srpska autorise l'accès secret à distance.<br><br>Si l'autorisation du tribunal a été obtenue, la police et/ou les procureurs effectuent la perquisition. Ils doivent posséder des connaissances techniques spécifiques et sont souvent assistés par d'autres experts techniques. D'une manière générale, la perquisition doit être menée conformément aux règles du CPP afin de garantir le respect des droits de l'homme et la recevabilité des preuves lors du procès. | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Brésil | La base juridique pour la recherche et la saisie de données informatiques stockées est établie par la Constitution brésilienne, le code de procédure pénale et le "cadre brésilien des droits civils pour l'internet". Aucune disposition spécifique n'est consacrée à la question de la recherche et de la saisie de données. La perquisition et la saisie de données informatiques stockées sont plutôt régies par l'application analogique des règles traditionnelles de perquisition et de saisie. La règle qui fonde une telle mesure est l'article 240 du code de procédure pénale, qui englobe les données électroniques stockées, puisqu'il n'existe pas de règle spécifique dans le code de procédure pénale. Cet article permet la perquisition et la saisie de données, y compris de données informatiques stockées, avec l'autorisation d'un juge et uniquement dans les cas et de la manière prévus par la loi. Les décisions jurisprudentielles en la matière indiquent que l'article 240 est suffisant pour perquisitionner et saisir des données électroniques stockées, car une fois cette mesure accordée, la divulgation des données en est la conséquence.<br><br>Situation d'urgence ou autres circonstances urgentes :<br><br>Les tribunaux brésiliens ont interprété le concept d'urgence de manière large, reconnaissant que la protection de la vie humaine et de l'intégrité physique est un droit fondamental qui peut justifier la perquisition ou la saisie de biens sans ordonnance judiciaire. En outre, le code de procédure pénale brésilien prévoit que les autorités peuvent perquisitionner ou saisir des biens sans ordonnance judiciaire dans les cas de "délits en flagrant délit" ou lorsqu'il existe un danger imminent pour la vie ou l'intégrité physique.<br><br>Il existe également un concept d'"urgence" défini dans le code de procédure civile, qui s'applique également aux procédures pénales lorsqu'il existe des preuves de la probabilité de l'existence du droit et du risque de dommage ou de risque pour l'issue utile de la procédure (article 300).<br><br>La législation brésilienne n'autorise pas spécifiquement les autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient à l'aide d'identifiants d'accès obtenus légalement. Toutefois, si les identifiants d'accès ont été obtenus par des moyens légaux, tels qu'une ordonnance judiciaire ou un mandat de perquisition, les autorités | Le Brésil applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | compétentes peuvent les utiliser pour accéder à un système informatique et aux données qu'il contient, sous réserve des exigences et des procédures établies par la législation brésilienne.<br><br>Cette législation n'autorise pas spécifiquement les autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient par le biais d'un accès à distance secret, mais le procureur général a récemment déposé une demande d'injonction auprès de la Cour suprême à ce sujet afin de reconnaître la nécessité d'une réglementation et d'appeler le Congrès à agir.<br><br>Les autorités doivent obtenir une ordonnance ou un mandat du tribunal pour perquisitionner ou saisir des données informatiques, comme l'exigent la Constitution brésilienne et le code de procédure pénale (CPP). Cette opération doit être autorisée par une ordonnance judiciaire ou un mandat de perquisition. L'ordonnance ou le mandat doit être fondé sur des soupçons raisonnables de commission d'une infraction et doit préciser le lieu de la perquisition, le type de données ou d'informations à consulter et la durée de la perquisition. Les autorités doivent utiliser l'accès à distance secret dans le strict respect des conditions énoncées dans la décision de justice. Cette mesure doit être autorisée par un juge dans une décision motivée à la demande du procureur, ou approuvée lorsque la demande émane de la police. Toutefois, en général, la police est l'autorité chargée de mettre en œuvre la mesure, et un expert technique est nécessaire pour assurer la chaîne de contrôle. Le procureur est également habilité à mettre en œuvre la mesure, accompagné lui aussi d'un expert technique.<br><br>Les autorités ont également précisé que la Convention de Budapest est entrée en vigueur au Brésil en tant que loi ordinaire en avril 2023 et que, sur cette base, en combinaison avec l'article 240 du Code de procédure pénale, elle fournit une base juridique pour les enquêtes et les poursuites concernant les preuves électroniques de tout crime. 240 du Code de procédure pénale, elle fournit une base juridique pour les enquêtes et les poursuites concernant les preuves électroniques de tout délit.<br><br>Il convient toutefois de noter que les pouvoirs procéduraux énoncés dans la Convention sont formulés d'une manière qui nécessite une mise en œuvre ultérieure par le biais du droit national. Ils ne peuvent fonctionner correctement si le texte correspondant est simplement reproduit dans la législation | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | nationale. Des précisions supplémentaires sont nécessaires en droit interne, par exemple en ce qui concerne les autorités compétentes, car les pouvoirs énoncés dans la Convention ne précisent pas ce que doivent être les autorités compétentes, et il appartient à chaque Partie de clarifier ces détails dans son droit interne | |
| Bulgarie | Conformément aux articles 160 à 162 du code de procédure pénale, les perquisitions doivent faire l'objet d'une autorisation judiciaire préalable. Si cela n'est pas possible en cas d'urgence, l'autorisation doit être obtenue dans les 24 heures. Les perquisitions et les saisies relatives aux systèmes informatiques et aux logiciels doivent être effectuées en présence d'un expert technique. L'article 163 du code de procédure pénale prévoit des procédures détaillées pour les perquisitions ainsi que pour la collecte et la conservation des preuves.<br><br>Les autorités peuvent demander à l'utilisateur d'un système informatique de fournir des identifiants d'accès, mais il n'existe aucune obligation légale explicite pour l'utilisateur de les fournir. (L'article 159 du code de procédure pénale prévoit l'obligation de produire des objets, des documents, des données informatiques et d'autres données susceptibles d'être importantes pour l'affaire).<br><br>L'accès à distance secret n'est pas prévu. | La Bulgarie applique des pouvoirs de recherche spécifiques pour mettre en œuvre l'article 19.1. |
| Cabo Verde | Le Cabo Verde a informé que sa loi nationale sur la cybercriminalité (ci-après la "CL"), n° 8/IX/2017, aborde la question de la recherche de données informatiques. L'article 17º prévoit que s'il devient nécessaire de produire des preuves pour découvrir la vérité au cours d'un processus, des données informatiques spécifiques et déterminées stockées dans un système informatique particulier peuvent être obtenues. L'autorité judiciaire compétente autorise ou ordonne la recherche dans ce système informatique et doit, dans la mesure du possible, présider la diligence. En tant qu'autorités judiciaires, tant le juge que le ministère public peuvent autoriser ou ordonner une perquisition, en fonction de la phase de la procédure. Les preuves obtenues doivent être nécessaires à l'enquête et les données informatiques en question doivent être spécifiques et déterminées.<br><br>Le législateur cap-verdien a permis aux organes de police criminelle de procéder à des perquisitions sans autorisation préalable de l'autorité judiciaire. Toutefois, cela n'est possible qu'à deux conditions | Le Cabo Verde applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | : i) la personne qui a le contrôle des données consent à la perquisition et ce consentement est documenté ; ii) dans les cas de terrorisme, de criminalité violente ou hautement organisée, lorsqu'il existe des preuves fondées de la commission imminente d'un crime qui met gravement en danger la vie ou l'intégrité d'une personne. Toutefois, dans les deux cas, vous devez rédiger un rapport et l'envoyer à l'autorité judiciaire compétente. Si vous êtes dans le cas du paragraphe iii), vous devez informer immédiatement l'autorité judiciaire compétente pour validation.<br><br>S'il existe des raisons fondées de penser qu'un crime est sur le point d'être commis et que ce crime représente un risque grave pour la vie ou l'intégrité de toute personne, la police judiciaire peut procéder à une perquisition sans autorisation préalable d'une autorité judiciaire.<br><br>Le Cabo Verde a déclaré qu'il n'existe pas de dispositions spécifiques concernant la recherche ou l'accès à un système informatique et à ses données à l'aide d'identifiants d'accès acquis légalement.<br><br>Le Cabo Verde a déclaré qu'il n'existe pas de dispositions spécifiques pour la perquisition ou l'accès similaire à un système informatique et aux données qu'il contient en utilisant un accès à distance secret.<br><br>Selon le stade de la procédure, le juge ou le ministère public peut autoriser les perquisitions. Toutefois, même pendant la phase d'enquête, le ministère public doit obtenir l'autorisation du juge pour accéder aux messages électroniques ou à d'autres documents de communication similaires. L'organe de police judiciaire, généralement la police judiciaire, ou tout technicien ou expert chargé de cette tâche, effectue la perquisition. Des connaissances techniques sont nécessaires pour effectuer la recherche. | |
| Cameroun | A titre préliminaire, il convient de noter que le Cameroun développe continuellement sa législation sur la cybercriminalité et la cybersécurité afin de la rendre aussi complète et exhaustive que possible.<br><br>Les bases juridiques pour la recherche et la saisie de données informatiques stockées sont les suivantes :<br>- L'article 29 de la loi sur la cybercriminalité et la cybersécurité n° 2010/012 du 21 décembre 2010, qui stipule que " (1) Les opérateurs de systèmes d'information sont tenus de conserver | Le Cameroun applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix (10) ans. (2) Les opérateurs de systèmes d'information sont tenus de mettre en place des mécanismes de surveillance et de contrôle de l'accès aux données de leurs systèmes d'information. Les données stockées peuvent être accessibles lors d'enquêtes judiciaires. (3) Les installations des opérateurs de systèmes d'information peuvent être perquisitionnées ou saisies sur ordre d'une autorité judiciaire dans les conditions prévues par les lois et règlements en vigueur" ; et,<br>- l'article 41 du même statut, qui dispose que "toute personne a droit au respect de sa vie privée. Les juges peuvent prendre des mesures conservatoires, notamment de séquestre et de saisie, pour prévenir ou faire cesser une atteinte à la vie privée".<br><br>Les pouvoirs de perquisition et de saisie s'appliquent également aux infractions relevant d'autres lois que la loi sur la cybercriminalité et la cybersécurité si des éléments de preuve se trouvent sur des systèmes informatiques.<br><br>Les articles 29 et 41 donnent aux autorités judiciaires le pouvoir de perquisitionner, d'accéder et même de saisir les systèmes informatiques et les données stockées. Tout cela se fait dans le respect des conditions définies par les lois et règlements en vigueur. L'article 93 du code de procédure pénale exige que les autorités disposent d'un mandat à cet effet.<br>Il n'y a pas de règles spéciales pour les urgences domestiques ou d'autres circonstances urgentes qui sont domestiques.<br><br>Les perquisitions utilisant des informations d'identification acquises légalement sont autorisées lorsque les autorités disposent d'un mandat obtenu par le procureur de la république, conformément aux dispositions du code de procédure pénale. Les perquisitions utilisant un accès à distance secret ne sont pas prévues par la loi.<br><br>Le procureur de la République ou le juge d'instruction autorisent et effectuent les perquisitions.<br><br>Le Cameroun ne dispose pas encore de procédures opérationnelles normalisées internes ou de lignes directrices pour les perquisitions, mais il a entamé la rédaction d'un manuel de procédures pour les | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | enquêtes numériques afin de mieux traiter les enquêtes numériques en général et les perquisitions et saisies de données informatiques en particulier. | |
| Canada | L'exigence par défaut pour une perquisition policière est l'autorisation judiciaire, normalement par le biais d'un mandat général en vertu de la section 487 du code pénal. Les sous-paragraphes de la section 487 du code pénal prévoient une autorisation spécifique pour les perquisitions électroniques. Un mandat général est approprié pour la perquisition d'un ordinateur ou d'un appareil électronique. Les mandats généraux peuvent être autorisés lorsque les enquêteurs doivent utiliser des techniques innovantes qui ne sont pas spécifiquement mentionnées dans le code. Les obligations de notification associées à une perquisition informatique découlent d'autres sources de droit. Les personnes faisant l'objet d'une recherche savent qu'une recherche est en cours ou en sont informées par une copie du mandat ; pour cette raison, la notification n'est pas abordée dans le code. C'est le pouvoir judiciaire qui autorise les perquisitions et les saisies (juge de paix, juge d'une cour provinciale ou juge d'une cour supérieure de justice pénale). Pour délivrer un mandat, le tribunal doit être convaincu qu'il existe des motifs raisonnables de croire que l'objet recherché est lié à une infraction ou en fournira la preuve, ou que l'une des autres conditions d'octroi d'un mandat est remplie. Un mandat peut alors être délivré à un agent de la paix (ou à un agent public, dans certains cas), qui l'exécutera. Les agents d'exécution peuvent avoir suivi une formation de base ou avancée en informatique légale.<br><br>Une perquisition peut être effectuée sans mandat en cas d'urgence, s'il est impossible d'obtenir un mandat. La légalité d'une telle perquisition sera testée à l'aune de l'interprétation par la Cour suprême de la Charte canadienne des droits et libertés. Une perquisition dans l'urgence ne sera autorisée que s'il existe un "danger imminent de perte, d'enlèvement, de destruction ou de disparition de la preuve si la perquisition est retardée" ou s'il y a un degré d'urgence qui nécessite une action de la part des forces de l'ordre. Il existe une abondante jurisprudence dans ce domaine.<br><br>Les titres d'accès acquis légalement peuvent être utilisés, à condition que les autorisations appropriées - qui peuvent varier - soient obtenues.<br><br>L'accès à distance secret est possible en vertu d'un mandat général. | Le Canada applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Chili | Le Chili ne dispose pas d'une disposition expresse sur la perquisition et la saisie de données informatiques et de supports contenant des données informatiques. Les règles relatives à la perquisition d'espaces physiques et à la saisie d'éléments physiques ne mentionnent pas non plus de dispositifs ou de données informatiques. Il semble que dans la pratique, les dispositions des articles du code de procédure pénale peuvent éventuellement être utilisées par analogie.<br><br>Le rapport chilien note que, conformément à la législation chilienne (article 12 de la loi 21.459), lorsque l'enquête sur certains délits informatiques spécifiques établis dans ladite loi devient essentielle et qu'il existe un soupçon raisonnable, basé sur des faits concrets, qu'une personne a commis ou participé à la préparation ou à la commission de l'un des délits établis dans lesdites dispositions, le juge des garanties, à la demande du ministère public, qui doit présenter un rapport préliminaire détaillé sur les faits et l'implication possible, peut ordonner l'application des techniques prévues et réglementées dans les articles 222 à 226 du code de procédure pénale, de la manière établie par le présent règlement.<br><br>En ce qui concerne les situations d'urgence, le Chili a souligné qu'il n'existe pas de règles spéciales pour ces cas.<br><br>La législation actuelle ne donne pas spécifiquement le pouvoir de fouiller un système informatique et ses données, ou d'obtenir un accès similaire, en utilisant des identifiants d'accès obtenus légalement.<br><br>La recherche secrète à distance peut être exécutée en vertu de l'article 225 bis nouvellement adopté du CPP. 225 bis du CPC. Cette disposition autorise l'utilisation de programmes informatiques permettant d'accéder à distance et d'appréhender le contenu d'un appareil, d'un ordinateur ou d'un système informatique, à l'insu de son utilisateur. La mesure ne peut être appliquée que pendant 30 jours, le juge des garanties pouvant prolonger cette période pour des périodes de même durée, avec un maximum de 60 jours. | Le Chili applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Colombie | Le code de procédure pénale (CPP) (loi 906 de 2004) précède l'adhésion de la Colombie à la Convention de Budapest. Néanmoins, les dispositions procédurales colombiennes reconnaissent la | La Colombie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | valeur probante des preuves numériques et permettent l'identification, l'extraction et la conservation des preuves numériques grâce à l'intégration diverses normes générales et spéciales en la matière.<br><br>Le bureau du procureur général informe que l'article 236 de la loi 906 de 2004 autorise l'extraction de preuves numériques stockées dans des systèmes d'information, des dispositifs de communication ou destinées à la transmission de données, lorsqu'il y a des raisons de penser que ceux-ci ont un lien avec la commission d'un crime, ou que le suspect a transmis ou stocké des informations d'intérêt pour l'affaire. Lorsque le procureur soupçonne raisonnablement que l'accusé manipule des données par le biais de réseaux de télécommunication, il doit ordonner à la police judiciaire de conserver les informations et les équipements pertinents en vue d'une analyse médico-légale pour obtenir des preuves. La Colombie a également fourni une jurisprudence établissant que ce type de règle s'appliquait à la collecte de tout document électronique ou numérique, comme les preuves numériques stockées dans les systèmes informatiques, les téléphones cellulaires et d'autres types de systèmes. Elle a également établi que les formalités permettant d'ordonner une telle extraction d'informations ne nécessitent qu'un contrôle judiciaire ultérieur par un juge du contrôle des garanties.<br><br>Selon l'article 221 du code de procédure pénale colombien, il doit y avoir un motif fondé ou une cause probable qui justifie l'obtention d'une preuve numérique stockée sur un dispositif au motif que cette preuve : i) la commission d'un acte ou ii) rend sa commission plus probable. L'ordre d'extraction est émis et signé par le procureur titulaire de l'affaire, de manière écrite et adressé à l'expert de la police judiciaire en informatique légale dans un délai qui peut varier de 30 à 15 jours selon les cas. La saisie visée au présent article est limitée exclusivement au temps nécessaire à la saisie des informations qu'elle contient. Le matériel saisi est restitué immédiatement, si nécessaire.<br><br>La Colombie n'a pas prévu de règles en cas d'urgence. Toutefois, il a été expliqué que dans le cadre des compétences de la police judiciaire, les preuves électroniques collectées dans le cadre d'actes urgents qui sont exécutés pendant l'attention portée à une scène de crime (dans ce cas, un mandat de la police judiciaire n'est pas nécessaire, par exemple, pendant l'inspection de la scène du crime).<br><br>La Colombie ne dispose pas de mesures spécifiques pour garantir la recherche ou l'accès similaire à un système informatique et aux données qu'il contient en utilisant des identifiants d'accès acquis | systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | légalement. Enfin, elle n'a pas développé de capacités législatives relatives à l'accès à un système informatique et aux données qu'il contient à l'aide d'identifiants d'accès à distance couverts. | |
| Costa Rica | La saisie du matériel contenant les données électroniques peut être ordonnée par le procureur ou la police judiciaire afin de protéger les preuves, mais pour rechercher et analyser les données, une ordonnance d'un juge est nécessaire. En outre, même si la saisie du matériel peut être ordonnée par le procureur ou la police judiciaire, si le matériel se trouve dans un espace privé (maisons, lieux de travail non publics, etc.), vous devez également obtenir une ordonnance d'un juge vous autorisant à accéder à l'espace privé dans lequel se trouve le matériel.<br><br>Il n'y a pas de règles pour les cas d'urgence ; cependant, les situations concernant des menaces pour la vie ou l'intégrité des personnes ou la sécurité de la nation sont traitées rapidement en fonction de l'urgence de chaque cas spécifique. En outre, les enquêtes concernant les victimes de groupes vulnérables sont traitées en priorité.<br><br>Il n'y a pas d'exigence spécifique concernant la "notification" de l'ordonnance, l'autorité d'exécution donnera une copie de l'ordonnance au propriétaire, au dépositaire ou à toute personne qui se trouve au même endroit que le matériel contenant les données.<br><br>Il n'existe pas de législation spécifique concernant la recherche ou l'accès à un système informatique à l'aide d'informations d'identification acquises légalement.<br><br>Le Costa Rica n'a pas de législation concernant l'accès secret à distance à un système informatique pour obtenir des informations dans le cadre d'une affaire.<br><br>Les autorités compétentes au Costa Rica pour accéder à un système d'information afin d'obtenir des données informatiques sont le juge pénal qui ordonne l'accès et le bureau du procureur et/ou la police judiciaire qui exécute l'ordre.<br><br>Le Costa Rica n'a pas réglementé spécifiquement la preuve numérique. Il applique plutôt, par analogie, les mêmes dispositions que celles prévues pour les preuves matérielles. | Le Costa Rica applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Croatie | La recherche de biens meubles comprend également l'ordinateur et les dispositifs connectés à l'ordinateur, les autres dispositifs de collecte, de sauvegarde et de transfert des données, les communications téléphoniques, informatiques et autres, ainsi que les supports de données.<br><br>Sauf disposition contraire du CPC, une perquisition doit être ordonnée par un mandat écrit et motivé délivré par un juge d'instruction. Conformément à l'article 242, paragraphe 4, du CPC, la perquisition est effectuée par le procureur général, un enquêteur ou les autorités de police. Le terme "enquêteur" désigne un fonctionnaire qui agit sur mandat du procureur ou du juge d'instruction (police, police militaire, agent des douanes ou de l'administration fiscale). Toutefois, seules les autorités de police et les enquêteurs de police sont équipés d'outils médico-légaux et formés pour effectuer une perquisition informatique et, dans la pratique, ce sont eux qui effectuent ces mesures.<br><br>Des exceptions à l'exigence d'un mandat judiciaire s'appliquent dans les cas d'urgence décrits comme un "danger de retard". Les articles 244 et 245 du CPP décrivent en détail six circonstances dans lesquelles des perquisitions peuvent être menées sans mandat d'un juge d'instruction et sans remise d'autres documents préliminaires. Ces circonstances comprennent la résistance armée attendue ou d'autres dangers pour ceux qui exécutent la perquisition, le risque de destruction ou de dissimulation de preuves, et la nécessité d'une surprise dans certains cas.<br><br>En vertu de l'article 245, si un retard va à l'encontre de l'objectif d'une perquisition et que l'affaire concerne l'un des crimes très graves énumérés dans l'article, la perquisition peut être exécutée sur la base d'un mandat écrit et bien fondé du procureur de l'État. Dans les huit heures suivant la fin de la perquisition, le mandat doit être soumis au juge d'instruction, qui doit ratifier ou rejeter la perquisition dans les huit heures.<br>Les personnes qui utilisent l'ordinateur sont tenues de fournir leurs identifiants d'accès. Le défendeur (suspect) peut le faire sur une base volontaire.<br><br>D'autres exemples de cas sans délivrance préalable d'un mandat sont prévus à l'article 244, qui prévoit l'accès à distance secret. L'expression "accès à distance dissimulé" n'est pas explicitement décrite par la loi. Il fait référence au fait qu'une perquisition, y compris sur des dispositifs connectés au | La Croatie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | système initialement perquisitionné, peut être effectuée sans que le défendeur ou le propriétaire/possesseur d'un objet perquisitionné n'en soit informé au préalable. Toutefois, le simple fait qu'une perquisition au titre de l'article 244 puisse être secrète ou étendue à des dispositifs connectés ne constitue pas son élément distinctif : cette mesure pourrait également être exécutée lorsque le suspect est conscient qu'elle a lieu, malgré la non-délivrance du mandat ou de la déclaration de droits, ou lorsqu'il n'y a pas de dispositifs connectés. | |
| Chypre | Chypre utilise deux éléments de sa législation pour les recherches électroniques. Premièrement, l'article 27 de son code de procédure pénale exige un mandat de perquisition ou une autre ordonnance judiciaire, délivré par un juge, sur la base de l'attestation d'un officier de police concernant plusieurs exigences procédurales. Deuxièmement, lorsqu'un tribunal ordonne la perquisition de communications privées stockées dans un système informatique, les éléments de l'article 23 de la loi de 1996 sur la protection de la confidentialité des communications privées doivent être remplis.<br><br>Les mêmes exigences s'appliquent en cas d'urgence.<br><br>Comme le système met l'accent sur les mandats de perquisition et les ordonnances judiciaires, ses autorités ne s'appuient pas sur des identifiants d'accès acquis légalement, sauf si le consentement à la perquisition a été obtenu. L'accès à distance clandestin n'est pas autorisé.<br><br>Comme indiqué, les perquisitions doivent être autorisées par un juge. Elles sont menées par la police conformément à un manuel interne de criminalistique numérique. Le personnel du laboratoire de criminalistique numérique de l'unité de lutte contre la cybercriminalité est composé d'examinateurs certifiés en criminalistique informatique. | Chypre applique des pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| République tchèque | La perquisition du système informatique et des données qui y sont stockées est possible en vertu des pouvoirs généraux de perquisition à domicile (disposition 83) et de perquisition dans d'autres locaux et lieux (disposition 83a), tous deux définis dans le code de procédure pénale (CPP).<br><br>Bien que la législation ne définisse pas explicitement l'urgence, un régime spécial peut être appliqué aux mesures de remise d'un objet, de fouille personnelle et de fouille d'autres locaux et lieux dans le | La République tchèque applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | cas où cette action doit être exécutée immédiatement. Une telle situation peut se produire s'il existe un risque de détérioration, de destruction, de perte ou de dissimulation d'un objet important pour la procédure pénale.<br><br>La législation permet aux autorités d'utiliser des documents d'identité obtenus légalement. Une personne ne peut pas être contrainte de remettre ces documents si cela risque d'enfreindre l'interdiction de l'auto-accusation.<br>Il est également possible de fouiller secrètement le système informatique en vertu de la disposition 158d par. 3 du CPC. Certaines limitations s'appliquent (infraction pénale intentionnelle, proportionnalité, ordonnance du tribunal, durée de validité de l'ordonnance du tribunal limitée dans le temps).<br><br>Le président du tribunal et, dans le cadre de la procédure d'instruction, le juge, sur requête du procureur, sont habilités à ordonner une perquisition. En cas d'urgence, la perquisition peut être ordonnée, au lieu du président ou du juge compétent (article 18), par le président ou le juge dans le ressort duquel la perquisition doit être effectuée. La même procédure s'applique à la perquisition d'autres locaux et lieux.<br>Les perquisitions à domicile et les perquisitions dans d'autres locaux et lieux sont effectuées par une autorité policière. | |
| Danemark | Les arrêts de la Cour suprême ont précisé que le régime légal des perquisitions et saisies non électroniques couvre également les perquisitions et saisies de systèmes et de données électroniques. Toutes ces mesures sont explicitement réglementées dans de nombreux articles de la loi sur l'administration de la justice, et ces articles imposent des restrictions et des exigences supplémentaires à ces mesures. En règle générale, les perquisitions et les saisies nécessitent une ordonnance judiciaire délivrée si les différents éléments spécifiés dans les articles de la loi sur l'administration de la justice sont satisfaits.<br><br>Si un retard dans l'obtention d'une ordonnance du tribunal rend la perquisition inutile, la police peut décider de procéder à la perquisition et/ou à la saisie. Dans ce cas, la ratification par le tribunal de la décision de la police doit être demandée dans les 24 heures. | Le Danemark applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Dans les deux cas, la police nationale exécute les perquisitions et les saisies en faisant appel à l'expertise technique nécessaire.<br><br>L'utilisation de titres d'accès acquis légalement est couverte par les règles générales en matière de perquisition. Les réponses semblent faire référence aux articles 793 et 796 de la loi AJA, qui prévoient que la police peut fouiller d'autres objets et lieux à l'extérieur de la maison et que la décision de le faire peut être prise par la police. Une décision de la Cour suprême a également permis l'utilisation de mots de passe acquis légalement.<br><br>L'accès à distance secret par la police n'est pas inclus en soi dans la loi. Toutefois, si certaines conditions sont remplies, la police peut utiliser l'article 799 de la loi sur l'AJA dans le cadre d'enquêtes sur certains crimes graves. Cette section supprime les exigences de notification et de présence qui s'appliqueraient normalement à une perquisition. Il permet également à la police d'utiliser le code et le nom d'utilisateur d'un suspect pour accéder à distance à un compte ou à des données. D'autres dispositions peuvent également être pertinentes : La "lecture de données" et "l'interférence avec la correspondance" (qui comprend plusieurs types de données électroniques) peuvent être effectuées secrètement selon les sections 791b, 783 et 784. Voir les réponses détaillées du Danemark sur ce point. | |
| République dominicaine | La République dominicaine dispose de la loi 53-07 contre les crimes et délits de haute technologie, dont l'article 52 renvoie au code de procédure pénale, qui établit des mesures pour l'enregistrement et l'obtention de preuves. Ces mesures s'appliquent également à l'obtention et à la conservation des données contenues dans un système d'information ou ses composants, telles que les données de trafic, de connexion, d'accès ou toute autre information utile. En outre, les procureurs ou les fonctionnaires de police peuvent effectuer des perquisitions lorsqu'il existe des motifs raisonnables de croire qu'il existe des preuves utiles à l'enquête ou à la dissimulation de l'accusé, conformément aux règles et aux dispositions du code de procédure pénale.<br><br>En cas d'urgence et en l'absence du ministère public, la police peut le solliciter directement. | La République dominicaine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Avant d'effectuer les formalités prévues par le code de procédure pénale, le ministère public peut accéder ou ordonner l'accès à un tel système d'information ou à l'un de ses éléments. Il peut également charger les personnes ayant connaissance du fonctionnement d'un système d'information ou d'un de ses composants, ou des mesures de protection des données de ce système, de fournir les informations nécessaires à la réalisation des investigations pertinentes.<br><br>La législation procédurale de la République dominicaine ne prévoit pas la possibilité d'utiliser des techniques secrètes de recherche à distance. Toutefois, il est important de noter qu'il existe actuellement un projet de loi au Congrès visant à modifier la loi 53/07 sur la cybercriminalité. Ce projet stipule que ces techniques ne seraient autorisées que dans le cas d'infractions graves spécifiquement définies par la loi.<br><br>Les perquisitions ne peuvent être effectuées qu'à la demande du ministère public, sur décision judiciaire motivée. Cette procédure est menée par le ministère public avec l'assistance d'officiers de police spécialisés dans la cybercriminalité. | |
| Estonie | Les pouvoirs génériques concernant la recherche et l'examen d'un objet sont appliqués.<br>Il existe des règles générales pour les situations d'urgence. En cas d'urgence, le bureau du procureur peut autoriser l'accès secret au système informatique et l'autorisation du tribunal doit être obtenue dans les 24 heures.<br><br>En règle générale, la perquisition peut être autorisée par le bureau du procureur.<br><br>Il n'existe pas de législation spécifique concernant l'utilisation de titres d'accès obtenus légalement. Toutefois, la législation ne s'y oppose pas et les pouvoirs généraux de perquisition et de saisie sont appliqués.<br>Le cadre juridique prévoit également l'accès clandestin aux systèmes informatiques. Cette mesure nécessite l'autorisation d'un juge. | L'Estonie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Fidji | Les articles 16 et 21 de la loi sur la cybercriminalité (2021) (ci-après "TCA") prévoient la perquisition et la saisie de données informatiques stockées. La police/FICAC peut demander un mandat à un juge/magistrat pour perquisitionner un ordinateur, un programme informatique, un système informatique ou toute partie de celui-ci, un support de stockage de données informatiques, un dispositif de données informatiques, activer tout système informatique et stockage de données informatiques sur site. L'article 21 prévoit que la demande de mandat doit justifier la nécessité de la perquisition et préciser la manière dont elle sera effectuée sur le plan technique.<br><br>Les Fidji ont indiqué que les situations d'urgence ne sont pas réglementées par l'ACT.<br><br>Il apparaît que l'article 21 peut être utilisé comme base juridique pour l'utilisation d'identifiants d'accès acquis légalement.<br><br>Les autorités ont déclaré que les sections 22 et 23 du TCA, qui permettent la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu par le biais d'un mandat de perquisition, peuvent également être utilisées pour la recherche secrète à distance. L'autorisation d'un juge fait partie des conditions strictes qui doivent être remplies à cet égard.<br><br>En outre, la loi sur le contrôle des drogues illicites (Illicit Drugs Control Act) prévoit qu'un juge de la Haute Cour peut, sur demande écrite d'un inspecteur de police ou d'un officier supérieur des douanes, délivrer un mandat lorsqu'il existe des soupçons raisonnables qu'une personne a commis, commet ou est sur le point de commettre une infraction à la loi sur le contrôle des drogues illicites (Illicit Drugs Control Act). Ce mandat permet de surveiller et d'enregistrer secrètement les communications, y compris les télécommunications.<br><br>L'autorité compétente pour autoriser une perquisition est un juge, et ceux qui effectuent la perquisition sont la police et les fonctionnaires ayant une expertise technique. | Les Fidji appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |
| Finlande | Le chapitre 10 de cette loi contient des dispositions sur les mesures coercitives secrètes, tandis que le chapitre 5 de la loi sur la police traite des méthodes secrètes de collecte de renseignements. Les dispositions pertinentes relatives aux perquisitions sont énoncées au chapitre 8 de la LMC. Les articles | La Finlande applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | 20 à 29 détaillent les exigences relatives à la recherche de données contenues dans un dispositif. La recherche de données contenues dans un dispositif consiste à accéder aux données stockées dans un ordinateur, un équipement terminal ou tout autre équipement technique ou système d'information au moment de la recherche. Toutefois, les communications confidentielles qui font l'objet d'une interception, d'un contrôle des données relatives au trafic ou d'une surveillance technique conformément au chapitre 10 ne peuvent pas faire l'objet d'une perquisition.<br><br>La LMC contient des dispositions pertinentes pour la perquisition et la saisie de données informatiques stockées. Le chapitre 7 précise que les conditions préalables à la saisie d'objets ou de documents s'appliquent également aux données contenues dans des dispositifs techniques ou des systèmes d'information. Le chapitre 8 décrit les dispositions relatives à la recherche de données dans les dispositifs.<br><br>La section 21 du chapitre 8 stipule les conditions préalables à la recherche de données contenues dans un dispositif. Une recherche des données contenues dans un dispositif peut être effectuée si : (1) il y a des raisons de soupçonner qu'une infraction a été commise et que la peine la plus sévère prévue pour cette infraction est une peine d'emprisonnement d'au moins six mois, ou si l'affaire faisant l'objet de l'enquête implique des circonstances liées à l'imposition d'une amende d'entreprise ; et (2) on peut présumer que la perquisition peut conduire à la découverte d'un document ou d'une donnée à saisir. En outre, la décision relative à la perquisition des locaux peut être étendue à un dispositif technique ou à un système d'information se trouvant dans ces locaux, si la perquisition en question n'a pas pour but de trouver une personne. | |
| France | Les procédures de perquisition et de saisie varient en fonction du stade de l'enquête auquel elles ont lieu - par exemple, il existe un stade d'enquête préliminaire. Les procédures sont donc régies par différentes sections du code de procédure pénale et peuvent impliquer différents fonctionnaires du système judiciaire. Une autorisation judiciaire est requise lorsqu'une perquisition concerne l'une des sept professions spécialement protégées - par exemple, les avocats, les notaires et les journalistes - et pour les perquisitions sans consentement au stade de l'enquête préliminaire concernant certains crimes. Une autorisation judiciaire est requise pour chaque utilisation d'une technique d'enquête spéciale, conformément à l'article 706-95-11 du CPP. Selon l'article 706-102-1 du CPP, sont | La France applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | considérées comme des techniques spéciales d'enquête la mise en place d'un dispositif technique, sans le consentement des personnes concernées, dans le but d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre en quelque lieu que ce soit. Il s'agit de données stockées dans un système informatique, affichées sur un écran pour l'utilisateur d'un système de traitement automatisé de données, saisies par l'utilisateur en tapant des caractères, ou reçues et transmises par des périphériques.<br><br>Trois lois prévoient des procédures spéciales, notamment pour la recherche et la saisie de données, sans la participation d'un juge en cas de menace pour l'ordre public ou d'activités terroristes (avec quelques exceptions pour les personnes exerçant certaines professions, telles que les avocats ou les journalistes).<br><br>Les autorités peuvent fouiller un système ultérieur accessible à partir d'un système ayant fait l'objet d'une première fouille. Elles peuvent utiliser des informations d'identification acquises légalement. Elles peuvent également utiliser un accès à distance secret, en particulier pour lutter contre le crime organisé et le terrorisme. La réponse de la France détaille clairement les lois dont découlent ces pouvoirs et les techniques de police scientifique qui sont autorisées.<br><br>En règle générale, les perquisitions sont effectuées par des fonctionnaires de police (parfois d'un certain grade). Les perquisitions concernant des personnes exerçant certaines professions doivent être effectuées par un magistrat. Dans le cadre d'une enquête préliminaire sur un crime grave, un procureur peut obtenir une ordonnance judiciaire pour effectuer la perquisition sans le consentement de la personne perquisitionnée. Dans les affaires qui en sont au stade de l'enquête préliminaire ou lorsqu'un juge d'instruction est déjà engagé, les perquisitions sont guidées par les ordonnances des juges. Des experts médico-légaux peuvent être employés. | |
| Géorgie | Les règles générales du code de procédure pénale relatives aux perquisitions principalement conçues pour l'environnement physique s'appliquent aux perquisitions de données informatiques stockées. L'article 136 - Divulgation d'informations ou de documents informatiques - s'applique mutatis mutandis. | La Géorgie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'obtention d'un mandat judiciaire est une condition préalable à la perquisition. Le procureur doit démontrer au magistrat qu'il existe une cause probable. Ses exigences sont prévues par la loi.<br>La loi prévoit également une procédure différente en cas d'urgence. Dans ce cas, l'agent enquêteur peut procéder à une perquisition avec l'autorisation du procureur. Dans les 24 heures suivant la fin de la perquisition et de la saisie, le procureur doit demander au tribunal une autorisation *a posteriori.*<br><br>L'autorité chargée de l'enquête peut fouiller un système informatique à l'aide d'identifiants d'accès acquis légalement.<br>L'enquêteur et, le cas échéant, d'autres agents des services répressifs et/ou des spécialistes techniques exécutent les mandats de perquisition.<br><br>L'article 143, paragraphe 1, point b), du code de procédure pénale prévoit également un pouvoir procédural spécial d'accès secret à distance à un système informatique en vue de sécuriser des données ; cette mesure est soumise à l'autorisation d'un tribunal et limitée aux crimes graves. | |
| Allemagne | Les règles générales du code de procédure pénale relatives à la perquisition et à la saisie de locaux et de personnes sont applicables (articles 102, 103 et suivants du code de procédure pénale). L'inspection des documents d'identité et des supports de stockage électronique conformément à l'article 110 du code de procédure pénale fait partie de ces mesures de perquisition. Ces mesures permettant l'examen sont l'instrument prévu par la loi pour vérifier le contenu du stockage électronique.<br><br>Les perquisitions en vertu de l'article 102 du code de procédure pénale ne peuvent être ordonnées que par le juge conformément à l'article 105 du code de procédure pénale ; en cas d'urgence, elles peuvent également être ordonnées par le ministère public et ses enquêteurs. Pour obtenir un mandat de perquisition, le procureur dépose une demande auprès du tribunal. Les pouvoirs d'urgence existent en cas de danger imminent. En règle générale, il y a danger imminent si l'ordre ne peut être obtenu par l'autorité judiciaire sans compromettre l'objectif de la mesure. L'ordre de perquisition est généralement exécuté par le ministère public, qui peut à son tour mandater d'autres autorités d'enquête (police, douanes, autorités fiscales) pour effectuer la perquisition. | L'Allemagne applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les autorités peuvent utiliser des références légalement acquises pour accéder à un système informatique ou à des données et les fouiller, pour fouiller ou accéder de la même manière à un système informatique et à des données. Un mandat de perquisition ou le consentement de la personne concernée est nécessaire.<br><br>La recherche secrète à distance a une base juridique spécifique dans la section 100b du code de procédure pénale. En vertu de la section 100b (1), des moyens techniques peuvent être utilisés pour accéder à un système de technologie de l'information utilisé par la personne concernée et des données peuvent être collectées à partir de ce système, même à l'insu de la personne concernée, pour des crimes graves spécifiquement prévus et dans d'autres conditions prévues par la loi. Cette mesure de recherche secrète à distance de systèmes de technologie de l'information s'entend comme l'extraction en ligne de contenus de stockage électronique qui ne font pas l'objet d'une communication en cours. | |
| Ghana | La constitution sous-tend la législation sur les perquisitions et les saisies en protégeant le droit à la vie privée. En outre, trois lois sont pertinentes. En règle générale (voir les exceptions ci-dessous), le pouvoir judiciaire autorise les perquisitions et celles-ci sont exécutées par les forces de l'ordre, le cas échéant avec l'aide de plusieurs types d'experts tiers spécialisés. Les services répressifs sont susceptibles d'être chargés d'autoriser et d'exécuter les perquisitions liées à la cybercriminalité et aux données informatiques. Des procédures opérationnelles standard ou des lignes directrices internes ont été adoptées. Il n'est pas obligatoire de notifier une perquisition à la partie intéressée.<br><br>La loi sur la procédure pénale (Criminal Procedure Act) régit les perquisitions et les saisies, les autorisant sur la base d'un mandat délivré par un magistrat. Ce mandat est délivré à la suite d'une demande ex parte comprenant des preuves sous serment de l'existence de motifs raisonnables de croire que la perquisition contribuera à l'enquête ou à la prévention d'un crime. Les perquisitions et les saisies peuvent être effectuées sans mandat lorsqu'elles ont lieu dans le cadre d'une arrestation. En outre, comme indiqué à l'article 93, un agent de police peut procéder à une fouille et à une saisie sans mandat d'un colis ou d'un article dans de nombreuses circonstances.<br><br>Les procédures d'obtention d'un mandat en vertu de la loi sur la cybersécurité et de la loi sur les transactions électroniques sont similaires à celles de la LPC, mais la demande doit être faite auprès | Le Ghana applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'une juridiction supérieure. Des conditions supplémentaires doivent être remplies en vertu de la CSA (voir les articles 71 à 74).<br><br>Les deux lois fournissent principalement le cadre juridique pour traiter les infractions liées aux systèmes électroniques ou commises à l'aide de ceux-ci. Il se peut que ces lois ne couvrent pas explicitement toutes les infractions possibles. L'application des pouvoirs de perquisition et de saisie aux preuves informatiques d'infractions qui *ne* sont pas spécifiquement liées aux ordinateurs peut parfois être complexe. Toutefois, les principes généraux de la perquisition et de la saisie pourraient s'appliquer aux preuves d'infractions non liées à l'informatique. Comme indiqué dans les réponses, diverses questions et exigences peuvent entrer en ligne de compte.<br><br>Il n'existe pas de règles spécifiques pour les situations d'urgence. Toutefois, la LPC autorise les perquisitions sans mandat en cas d'arrestation. La loi sur la criminalité économique et organisée (Economic and Organized Crime Act) permet également à un agent habilité de procéder à une perquisition et à une saisie d'urgence lorsqu'il a des motifs raisonnables de soupçonner qu'un objet est un bien vicié ou qu'il fournira la preuve d'une infraction grave au sens de cette loi. Enfin, il est possible, conformément à la jurisprudence de la Cour suprême, que les preuves saisies en dehors des procédures établies soient néanmoins admissibles.<br><br>Dans certains cas, les autorités peuvent utiliser des titres d'accès acquis légalement, à condition qu'elles soient légalement habilitées à le faire - par exemple, par le biais d'un mandat ou d'une autre décision de justice - et que l'accès soit nécessaire pour obtenir les données pertinentes. De nombreuses exigences procédurales doivent être respectées.<br><br>Il n'existe pas de législation spécifique concernant l'accès à distance clandestin. | |
| Grèce | Les perquisitions nécessitent une autorisation préalable par ordonnance du procureur ou du juge, après démonstration d'une cause probable ou de motifs raisonnables de croire que les données recherchées sont pertinentes dans le cadre d'une enquête criminelle. Les services répressifs ou les organes d'enquête sont autorisés à effectuer des perquisitions, conformément au champ d'application et à l'objectif de l'ordonnance. Des experts en criminalistique numérique, en cybersécurité, en | La Grèce applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | questions juridiques et en opérations techniques peuvent être impliqués dans l'exécution des perquisitions.<br><br>Le pouvoir de perquisitionner et de saisir des systèmes informatiques et des données électroniques s'applique à toutes les infractions.<br><br>Il n'y a pas de dispositions particulières pour les cas d'urgence.<br><br>Les autorités sont autorisées à utiliser des identifiants d'accès acquis légalement avec une autorisation légale, généralement une ordonnance d'un juge ou d'un procureur. De même, l'accès à distance secret peut être utilisé si une ordonnance judiciaire ou de poursuite est obtenue au préalable. Dans les deux cas, les actions des autorités sont limitées au champ d'application et à l'objectif spécifiés par l'ordonnance. | |
| Grenade | Les autorités ont indiqué que leur législation comprend la loi sur les délits électroniques (Electronic Crimes Act), dont l'article 22 définit les pouvoirs d'accès, de perquisition et de saisie à des fins d'enquête (art. 22).<br><br>La Grenade a défini les situations considérées comme urgentes (enlèvement, menace ou atteinte à une personne présentant un intérêt pour la sécurité nationale, ou menace ou atteinte à un enfant), qui peuvent être détaillées dans le mandat autorisé par un magistrat ou un juge.<br><br>La loi ne prévoit pas de pouvoir de perquisition ou d'accès similaire à un système informatique et aux données qu'il contient par le biais d'un accès à distance secret.<br><br>L'ordonnateur du mandat doit être un magistrat. Les officiers de police du grade d'inspecteur ou d'un grade supérieur demandent et exécutent les mandats de perquisition ou désignent les agents chargés de l'exécution de ces mandats. | La Grenade applique des pouvoirs spécifiques pour mettre en œuvre l'art. 19.1. |
| Hongrie | Les ordres écrits de perquisition et de saisie peuvent être délivrés par un tribunal, un procureur ou une autorité chargée de l'enquête. Plusieurs articles du code de procédure pénale traitent de cette | La Hongrie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | question et mentionnent explicitement les données électroniques ; des perquisitions peuvent être ordonnées si leur justification répond à des normes précises. Les notaires et les avocats bénéficient de protections spéciales et le code de procédure pénale insiste sur la présence de la personne concernée ou d'un substitut adulte.<br><br>En vertu de plusieurs articles du code de procédure pénale, les perquisitions peuvent être effectuées sans ordonnance du tribunal si tout retard risque de compromettre gravement l'objectif de la perquisition. Ces perquisitions doivent être ratifiées rapidement par le tribunal a posteriori. D'autres mesures coercitives susceptibles de faciliter la perquisition peuvent également être prises. Les perquisitions électroniques sont souvent considérées comme urgentes en raison de la vulnérabilité des données électroniques.<br><br>Les perquisitions sont effectuées par la police ou une autre entité nationale chargée de l'application de la loi ou par le ministère public. Ils disposent d'un personnel spécialement formé, mais peuvent faire appel à des experts.<br><br>La législation n'interdit ni n'autorise l'utilisation d'informations d'identification obtenues légalement. En pratique, les enquêteurs ont le contrôle légal de tous les appareils et données saisis, de sorte que l'utilisation de ces identifiants est possible (et doit être enregistrée).<br><br>L'accès à distance secret est autorisé et est spécifiquement détaillé dans les sections 231-234 du CPC, fournies par la Hongrie dans sa réponse. | |
| Islande | Il n'existe pas de dispositions légales particulières et spécialisées pour la perquisition de systèmes informatiques ou de supports de stockage de données informatiques, mais la base légale de la perquisition se trouve dans l'art. 74 du code de procédure pénale n° 88/2008 (CCP), qui est une disposition générale relative aux perquisitions. 88/2008 (CCP), qui est une disposition générale relative aux perquisitions. | L'Islande applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les dispositions de l'article 75 du code de procédure pénale décrivent les conditions procédurales qui doivent être remplies pour qu'une perquisition soit autorisée. Une décision de justice est nécessaire, à moins que le propriétaire ou le responsable de l'objet n'ait donné son consentement sans équivoque.<br><br>L'urgence n'est pas définie par la loi, mais s'il existe un risque imminent que l'attente d'une décision de justice entraîne des dommages pour la procédure, une perquisition peut être effectuée sans décision de justice. Cette disposition s'applique également lorsque la perquisition vise à retrouver une personne qui doit être arrêtée et qu'elle est suivie ou qu'il y a un risque qu'elle s'échappe s'il est nécessaire d'attendre une décision de justice.<br><br>Il est courant dans la pratique, conformément aux principes de proportionnalité, de donner aux propriétaires ou aux gardiens des données contenues dans les supports de données saisis (appareils) verrouillés par des codes PIN, des mots de passe ou autres (par exemple, les téléphones portables) la possibilité de fournir volontairement à la police les informations d'accès nécessaires pour ouvrir l'appareil.<br><br>Les autorités considèrent que les mesures secrètes d'accès à distance relèvent du champ d'application du chapitre XI du Code de procédure pénale relatif aux écoutes téléphoniques et autres mesures comparables. Selon les art. 80 et 81, ces opérations peuvent impliquer des informations provenant d'entreprises de télécommunications sur les communications avec un ordinateur, y compris l'écoute ou l'enregistrement de ces communications. Les conditions suivantes s'appliquent : ordonnance du tribunal, présence d'un avocat lors de la décision sur la mesure, raison de penser que des informations d'une grande importance pour l'enquête seront obtenues de cette manière, soit le seuil des infractions (6 ans), soit la liste des infractions auxquelles la mesure peut être appliquée.<br><br>Les mesures sont mises en œuvre par les autorités policières, si nécessaire avec l'assistance d'autres autorités policières spécialisées, par exemple si une expérience ou une expertise opérationnelle ou technique est requise. | |
| Israël | Les articles 23, 23A et 28 de l'ordonnance de procédure pénale (arrestation et perquisition) ainsi que la directive du procureur général no. 7.14 et la directive de la police nationale no. 03.300.035 et la | Israël applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | jurisprudence de la Cour suprême régissent les perquisitions et les saisies en général et les perquisitions électroniques en particulier. Les perquisitions sont autorisées sur la base de demandes qui remplissent de nombreuses conditions spécifiques. Les mandats doivent être délivrés par un juge et contenir des détails sur le but de la perquisition et ses contraintes. La perquisition doit être nécessaire et l'atteinte à la vie privée de la personne concernée doit être limitée. La police nationale et plusieurs autres autorités sont habilitées à effectuer des perquisitions. Les fonctionnaires qui effectuent des perquisitions numériques doivent avoir suivi une formation spécialisée.<br><br>Il n'y a pas de règles particulières en cas d'urgence ; un juge est disponible 24 heures sur 24 et 7 jours sur 7. Les pouvoirs acquis légalement peuvent être utilisés conformément au cadre décrit. La législation n'autorise pas l'accès secret à distance. | |
| Italie | La législation italienne comprend les dispositions suivantes dans son code de procédure pénale : Article 247 - Perquisition : Une fouille personnelle est autorisée lorsqu'il y a de bonnes raisons de penser qu'une personne dissimule sur elle des preuves ou des objets connexes. Une perquisition locale est autorisée lorsqu'il y a de bonnes raisons de penser que des preuves ou des objets se trouvent dans un lieu spécifique ou lorsque l'arrestation d'un suspect est possible dans ce lieu. Dans les cas où l'on soupçonne que des données ou des informations relatives à un délit sont stockées dans un ordinateur ou un système télématique, une perquisition peut être ordonnée, complétée par des mesures visant à sauvegarder les données d'origine.<br><br>Les modifications législatives étendent désormais les ordonnances d'inspection, de perquisition et de divulgation aux données informatiques. L'article 244, paragraphe 2, du code de procédure pénale a été mis à jour. Il habilite l'autorité judiciaire à enquêter sur les affaires dans lesquelles un crime n'a pas laissé de preuves matérielles ou dans lesquelles ces preuves ont été perdues, effacées, modifiées ou dispersées. L'autorité peut également ordonner des opérations techniques, y compris celles concernant les systèmes informatiques et de télécommunications, afin de préserver et de protéger les données originales.<br><br>Urgence ou autres circonstances urgentes : la police judiciaire est habilitée à procéder à des demandes aux fournisseurs (conformément à l'article 254-bis) et/ou à des perquisitions et saisies, avant que le | L'Italie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | procureur ne prenne la direction de l'enquête conformément à l'article 352 -1bis et à l'article 354. 352 -1bis et 354.<br><br>Selon la jurisprudence de la Cour suprême, l'utilisation d'identifiants acquis légalement pour accéder à un système informatique et à ses données est reconnue comme une méthode légitime pour effectuer des recherches.<br><br>Selon la jurisprudence de la Cour suprême, si l'accès à distance secret permet de capter un flux de communication en direct entre deux ou plusieurs sujets, cela relève de l'activité d'interception légale.<br><br>Les forces de police et les autres organismes chargés de l'application de la loi peuvent effectuer une perquisition sur autorisation de l'autorité judiciaire compétente = le procureur général. Des compétences spécifiques en matière d'analyse informatique et de criminalistique sont requises. | |
| Japon | Les articles 102 et 218 du code de procédure pénale couvrent les perquisitions. Les procureurs, les officiers adjoints du ministère public ou un officier de police judiciaire doivent demander et justifier la délivrance d'un mandat par un juge. Les médias électroniques ainsi que les données électroniques peuvent faire l'objet d'une perquisition. La perquisition est exécutée par des procureurs ou des officiers de police judiciaire. Les fonctionnaires qui exécutent les perquisitions électroniques sont techniquement qualifiés.<br><br>Les perquisitions liées à l'arrestation d'une personne peuvent être effectuées sans mandat.<br><br>Il semble que l'accès à distance secret ne soit pas disponible au Japon.<br><br>Les titres légalement acquis peuvent être utilisés lors de perquisitions conformes à l'article 218. | Le Japon applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Kiribati | La loi de 2021 sur la cybercriminalité à Kiribati (Kiribati Cybercrime Act 2021) prévoit des pouvoirs procéduraux permettant aux forces de l'ordre de rechercher et de saisir des preuves électroniques. Il existe également des lois de procédure telles que le Code de procédure pénale de Kiribati et la loi de 2008 sur les pouvoirs et les devoirs de la police de Kiribati. Bien que ces lois ne traitent pas | Kiribati applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | explicitement de la perquisition et de la saisie de données informatiques stockées, elles facilitent souvent la perquisition et la saisie, même pour des données informatiques stockées.<br><br>Les pouvoirs de procédure prévus par la loi sur la cybercriminalité s'appliquent à la fois aux infractions commises à l'encontre ou au moyen d'ordinateurs et à toute autre infraction prévue par le droit national lorsque la preuve se trouve sur un système informatique.<br><br>L'article 22 de la loi sur la cybercriminalité prévoit qu'un tribunal peut délivrer un mandat de perquisition et de saisie pour des systèmes informatiques, des données et des supports de stockage situés à Kiribati. Pour obtenir ce mandat, la demande d'un officier de police doit convaincre le tribunal qu'il existe des motifs raisonnables de soupçonner que ces éléments peuvent servir de preuve pour prouver une infraction à la loi ou toute autre infraction commise au moyen d'un système informatique, ou qu'ils ont été acquis par une personne à la suite d'une infraction.<br><br>Les policiers effectuent des perquisitions, conformément à la loi sur la cybercriminalité. Une expertise en criminalistique numérique de niveau intermédiaire ou avancé est nécessaire. Les policiers des Kiribati ont besoin d'une formation et d'un renforcement de leurs capacités dans ce domaine, car il n'existe pas de cours officiels pour former les policiers des Kiribati aux techniques d'enquête en matière de cybercriminalité. L'équipe gouvernementale de réponse aux incidents de cybersécurité a également un mandat légal en vertu de la loi de 2021 sur le gouvernement numérique pour fournir une expertise technique lorsque les forces de l'ordre demandent une telle assistance.<br><br>L'article 25 de la loi sur la cybercriminalité décrit les procédures de conservation d'urgence des preuves lorsqu'un service répressif estime qu'il existe un risque élevé de perte ou d'inaccessibilité des preuves. En vertu de l'article 25, les autorités chargées de l'application de la loi peuvent émettre une notification écrite pour ordonner la conservation de ces preuves pendant 60 jours au maximum. Ils peuvent prolonger cette période jusqu'à 100 jours. Un mandat judiciaire n'est pas nécessaire.<br><br>Les pouvoirs procéduraux prévus par la loi sur la cybercriminalité permettent aux autorités chargées de l'application de la loi de recourir à toutes les mesures de recherche nécessaires, y compris | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | l'utilisation d'informations d'identification acquises légalement. Toutefois, ces pouvoirs ne sont accordés que lorsqu'un tribunal délivre un mandat de perquisition et de saisie.<br><br>Selon l'article 22 de la loi sur la cybercriminalité, l'accès à distance secret peut être utilisé lorsqu'un tribunal a délivré un mandat.<br><br>La rédaction de procédures opérationnelles standard internes est prévue pour cette année sur la base des règlements d'application de la loi sur la cybercriminalité. | |
| Lettonie | Plusieurs articles du code de procédure pénale réglementent différents types de perquisitions et de saisies, notamment celles qui concernent les données et les systèmes électroniques. Outre les perquisitions et saisies ordinaires, des "mesures d'enquête spéciales" peuvent être prises dans des cas spécifiques en vertu des articles 210 et 212 du code de procédure pénale. Ces mesures ne sont autorisées que pour certains crimes et sur la base d'une décision d'un juge d'instruction (avec quelques exceptions).<br><br>Conformément à l'article 180 du code de procédure pénale, dans les situations où des preuves peuvent être compromises ou détruites, les perquisitions peuvent être effectuées avec l'accord du procureur, mais doivent être ratifiées rapidement par le juge d'instruction.<br><br>Des titres légalement acquis peuvent être utilisés si l'examen et l'enregistrement des données sont nécessaires et si la personne concernée est présente. La procédure de recherche habituelle est suivie si les données doivent être extraites. L'accès secret à distance est possible avec l'autorisation d'un juge. Les articles 218 à 222 du code de procédure pénale détaillent les différentes procédures.<br><br>Les perquisitions et saisies ordinaires doivent être autorisées par un juge d'instruction ou un tribunal sur la base d'une demande de la personne qui dirige la procédure. Elles semblent être exécutées par des fonctionnaires chargés de l'enquête.<br><br>Les mesures d'enquête spéciales sont autorisées par la décision d'un juge d'instruction et exécutées par des autorités publiques spécialement habilitées par la loi à le faire. | La Lettonie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Liechtenstein | En général, pour perquisitionner et saisir des supports électroniques ou des données, les procureurs demandent une ordonnance à un juge d'instruction et l'ordonnance est exécutée par la police nationale, apparemment par l'unité de lutte contre la criminalité numérique. Des modifications récentes de la loi précisent que ces pouvoirs s'étendent aux supports de stockage et aux données, y compris les données protégées par des clés d'accès, des mots de passe, etc.<br><br>La loi sur la police permet à la police d'agir de sa propre initiative en cas de "danger imminent". La police nationale peut saisir des objets sans décision de justice lorsque des données risquent d'être perdues.<br><br>Des titres d'accès acquis légalement peuvent être utilisés.<br><br>En vertu de l'article 104b du CPP, la police nationale peut utiliser ses agents ou d'autres personnes dans le cadre d'enquêtes sous couverture. | Le Liechtenstein applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Lituanie | Les perquisitions et les saisies font l'objet de plusieurs articles du code de procédure pénale. En général, un procureur demande une ordonnance du tribunal, en fournissant une justification motivée de l'ordonnance, qui peut s'appliquer à des objets et à des données informatiques. L'ordonnance est exécutée par le fonctionnaire chargé de l'enquête préliminaire ou par le procureur. Des spécialistes en informatique peuvent l'assister. L'examen des données est effectué par des agents des services répressifs spécialement formés et équipés.<br><br>Le code de procédure pénale autorise les perquisitions et les saisies sans autorisation judiciaire dans les cas "urgents", lorsqu'il n'y a pas de possibilité immédiate d'obtenir une autorisation judiciaire et que les preuves risquent d'être perdues. Si la perquisition ou la saisie n'est pas ratifiée par un juge dans les trois jours, plusieurs conséquences s'ensuivent, notamment la destruction des preuves et leur inutilisation lors du procès. | La Lituanie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les identifiants d'accès peuvent être utilisés s'ils ont été légalement acquis au cours d'une enquête préliminaire. L'accès à distance secret est autorisé conformément au code de procédure pénale, en particulier aux articles 158 et 160. | |
| Luxembourg | Différents articles énumérés du CPP luxembourgeois, principalement les articles 31, 33, 63-66 et 88-1 à 88-4, constituent la base légale des perquisitions et saisies telles qu'envisagées par l'article 19. Selon les circonstances, ces mesures sont autorisées soit par le procureur général, soit par le juge d'instruction et sont exécutées par la police.<br><br>Les articles 34 et 63 du CPP consacrent le droit de l'accusé et de son conseil, ainsi que de la partie civile, d'assister à la perquisition. Toutefois, leur présence peut être écartée lorsqu'il y a lieu de craindre "la disparition imminente d'éléments dont la découverte et l'examen paraissent utiles à la manifestation de la vérité". En cas de perquisition et de saisie chez un tiers (par exemple la saisie d'un nom de domaine chez le fournisseur national de domaines) ou lors de l'analyse des données saisies par la police judiciaire, seule la police est présente. Selon le texte détaillé de l'article 31 du CPP, en cas de "crime flagrant", la police a la responsabilité (en résumé) de veiller à ce que les preuves à risque soient préservées, y compris par la saisie.<br><br>Bien qu'elles ne soient pas spécifiquement prévues par le CPC, les mesures procédurales relatives aux titres d'accès légalement acquis peuvent être appliquées en vertu de plusieurs dispositions du CPC (articles 33 à 38 et 63 à 68).<br><br>La recherche secrète à distance est possible grâce à des mesures d'enquête spéciales (articles 88-1 à 88-4). | Le Luxembourg applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Malte | Les articles généraux et spécifiques à l'informatique du code pénal régissent le pouvoir de la police d'effectuer des perquisitions avec ou sans mandat délivré par un magistrat. Une fois dans les locaux, la police peut saisir tout ce qu'elle soupçonne raisonnablement d'être lié à un délit (entre autres conditions) et empêcher que des données soient modifiées, détruites, dissimulées, etc. La police peut également exiger que les données informatiques soient livrées sous une forme portable, visible et lisible. Il n'existe pas de régime de notification. | Malte applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les pouvoirs relatifs à la recherche et à la saisie de données informatiques peuvent être appliqués à toute infraction nationale.<br><br>Plusieurs alinéas de l'article 355E du code pénal précisent les circonstances dans lesquelles un mandat n'est pas nécessaire pour une perquisition. Il s'agit notamment des cas suivants : a) l'infraction est un crime grave et 1) il existe un danger présent et imminent que la cible prenne la fuite ou 2) il existe une possibilité évidente que des preuves soient altérées ou détruites ; b) la cible est surprise pendant la commission d'une infraction ; c) l'intervention immédiate de la police est nécessaire pour empêcher la commission d'un crime grave ; et d) l'action est liée à l'arrestation de fugitifs dans certaines circonstances.<br><br>La police de Malte ne peut pas utiliser des identifiants d'accès acquis légalement pour mener des enquêtes ou des investigations secrètes à distance. De telles actions constitueraient des infractions pénales.<br><br>Les magistrats autorisent les perquisitions, qui sont exécutées par les forces de police. | |
| Maurice | Les perquisitions décrites à l'article 19.1 sont régies par l'article 28 de la loi de 2021 sur la cybersécurité et la cybercriminalité (Cybersecurity and Cybercrime Act 2021). Elles sont autorisées par les juges sur la base de demandes ex parte assermentées démontrant des motifs raisonnables pour la délivrance d'un mandat. Les mandats sont exécutés par une "autorité d'enquête", de sorte que ce pouvoir n'est pas dévolu à une autorité particulière.<br><br>L'article 28 ne prévoit pas d'exceptions aux procédures normales en cas d'urgence. Toutefois, les demandes de mandats pourraient expliquer que les circonstances sont urgentes.<br><br>Le même article donne à l'autorité chargée de l'enquête le pouvoir d'étendre la recherche si les données sont légalement accessibles à partir du système initial (sur le territoire mauricien).<br><br>Aucune législation actuelle n'autorise l'utilisation d'un accès à distance secret. | Maurice applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les agents spécialisés de l'unité informatique de la police effectuent l'examen ; il peut être fait appel à des experts locaux ou étrangers en cas de besoin. Les procédures opérationnelles standard de la police comprennent des lignes directrices concernant le traitement des preuves. Il n'existe pas de procédures établies au sein de l'unité de lutte contre la cybercriminalité, mais les agents sont formés aux normes internationales. L'unité informatique de la police est certifiée ISO et dispose d'instructions de travail internes et de lignes directrices basées sur les normes internationales. | |
| Monaco | Trois séries de lois (énumérées) régissent les perquisitions et les saisies. En particulier, la loi n° 1.435 de 2016 relative à la criminalité électronique prévoit des perquisitions de systèmes informatiques, de données et de supports de stockage de données. Cette loi introduit dans le CPP les pouvoirs procéduraux spécifiques de la CB.<br><br>Les conditions sont les mêmes que pour les saisies dans toute affaire pénale. Le pouvoir de perquisitionner et de saisir des données informatiques s'applique à toutes les infractions.<br><br>Les perquisitions et les saisies doivent être autorisées par un procureur ou un juge. L'exécution sera assurée par l'unité de lutte contre la cybercriminalité de la police nationale.<br><br>La législation monégasque contient des dispositions permettant de répondre à des situations d'urgence en cas de crime ou de délit flagrant (art. 266 du CPP) ou d'interceptions urgentes (art. 106.4. du CPP) sans définir spécifiquement les cas d'urgence ou d'urgence.<br><br>Le droit national autorise les autorités compétentes à utiliser des identifiants d'accès acquis légalement pour mener des enquêtes ou des investigations secrètes à distance.<br><br>L'accès à distance secret n'est pas explicitement prévu par le droit national. Néanmoins, les autorités peuvent procéder à l'interception de données ou à l'utilisation d'agents qualifiés. | Monaco applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Monténégro | La base juridique de la recherche de données informatiques stockées est fournie par le code de procédure pénale. En particulier, l'art. 75 prévoit la fouille des habitations et autres locaux. Son paragraphe 2 couvre la perquisition d'ordinateurs et de dispositifs similaires pour le traitement automatique des données.<br><br>Un juge d'instruction délivre un mandat de perquisition et les policiers l'exécutent.<br>L'article 78 réglemente les motifs pour lesquels une demande de perquisition doit être faite sous forme verbale en cas d'urgence (risque de retard) de la perquisition. Le risque de retard signifie toujours que si certaines actions ne sont pas menées immédiatement, il existe un risque que les preuves ne puissent pas être obtenues ultérieurement ou qu'elles soient perdues ou compromises.<br><br>Toute personne doit permettre l'accès à l'ordinateur et aux supports amovibles utilisés pour stocker des informations relatives à l'objet de la recherche (disques, disques flash USB, disques durs USB, disquettes, cassettes, etc.), et donner les informations nécessaires sur l'utilisation de l'ordinateur.<br><br>Le chapitre 9 du code de procédure pénale régit les mesures de surveillance secrète. Ces mesures ne peuvent être utilisées que pour certaines infractions et dans des circonstances particulières.<br><br>La recherche est effectuée et gérée sur place par une autorité d'enquête - un enquêteur, un officier de police judiciaire ou un agent des douanes chargé de l'enquête. | Le Monténégro applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Maroc | Des amendements législatifs au CPC sont en cours d'examen au sein du corps législatif et affecteront le droit des perquisitions et saisies et les questions connexes dans ce questionnaire. Pour cette raison, les réponses du Maroc doivent être considérées comme provisoires.<br><br>À l'heure actuelle, la recherche de données informatiques stockées est régie par des règles générales en matière de recherche, sans distinction particulière entre les preuves électroniques et les données électroniques stockées.<br>Les perquisitions de papiers, documents ou autres objets peuvent être effectuées soit par la police lorsqu'une infraction a été interrompue, soit, dans la plupart des cas, au stade de l'enquête préliminaire, avec le consentement explicite de la personne concernée et l'autorisation du ministère | Le Maroc applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Il est en train de mettre à jour sa législation et, dans l'intervalle, ses mécanismes de procédure pénale sont proches, dans la pratique, des exigences de la convention. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | public compétent. Lorsque l'affaire a atteint le stade de l'inculpation, un juge d'instruction peut ordonner une perquisition. La police judiciaire exécute les perquisitions.<br><br>Dans les affaires de terrorisme, les heures pendant lesquelles une perquisition est autorisée peuvent être prolongées si l'enquête l'exige. En cas d'extrême urgence, ou si l'on craint la perte de preuves, les perquisitions peuvent être effectuées avec l'autorisation écrite du ministère public.<br><br>Les questions concernant la recherche à l'aide d'identifiants acquis légalement et la recherche à l'aide d'un accès à distance clandestin n'ont pas reçu de réponse. | |
| Pays-Bas | Des pouvoirs de recherche de données informatiques ont été introduits dans le code de procédure pénale lorsque les Pays-Bas ont ratifié la convention sur la cybercriminalité (2006, Computer Crimes II Act).<br><br>Le code de procédure pénale a introduit à l'art. 125i DCCP le pouvoir de perquisitionner dans un système informatique ou une partie de celui-ci et dans les données informatiques qui y sont stockées ou dans un support de stockage de données informatiques afin de conserver les données. Dans la pratique, une telle perquisition informatique est combinée à une perquisition domiciliaire et les règles générales régissant la perquisition des locaux s'appliquent. Ce pouvoir ne peut être exercé que si l'on peut raisonnablement s'attendre à ce que la perquisition produise des informations utiles à l'enquête. Le pouvoir est exécuté la plupart du temps sur ordre d'un procureur, et parfois validé au préalable par un juge d'instruction.<br><br>Le code de procédure pénale permet aux autorités de perquisitionner ou d'accéder de la même manière à un système informatique et aux données qu'il contient en utilisant des informations d'identification acquises de manière légitime (articles 125i et 125k du DCCP). À cet égard, on entend par "titres d'accès acquis de manière légitime" le fait de prendre connaissance de titres d'accès par l'exercice d'un autre pouvoir procédural, tel que le témoignage.<br><br>Conformément à l'art. 126bb, paragraphe 1, du code de procédure pénale, le procureur public a différentes obligations d'informer par écrit la personne contre laquelle un pouvoir d'enquête spécial a | Les Pays-Bas appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | été exercé. La notification écrite à une personne impliquée est effectuée dès que "l'intérêt de l'enquête" le permet. Une disposition standard élaborée par le ministère public concernant les "procédures opérationnelles standard" est en vigueur.<br>En cas de circonstances urgentes, liées à une disparition raisonnablement attendue de preuves, et lorsque l'arrivée du juge d'instruction ne peut être attendue, le procureur peut procéder à la perquisition (article 97 du code de procédure pénale).<br><br>Le code de procédure pénale a également introduit en 2019 des mesures visant à "accéder secrètement à des systèmes informatisés à distance". | |
| Nigéria | Trois lois constituent les principales bases des perquisitions électroniques. De manière générale, la section 29 de la loi sur la police de 2020 et les sections 143 et 144 (perquisitions) et la section 333 (saisies) de la loi sur l'administration de la justice pénale de 2015 (ACJA) fournissent la justification juridique des perquisitions et des saisies en vertu des lois nigérianes, y compris les perquisitions et les saisies de données électroniques. Dans les deux cas, un officier de police demande à un tribunal l'autorisation de procéder à une perquisition ou à une saisie.<br><br>La troisième loi, la loi sur la cybercriminalité, spécifie en détail la demande ex parte, les infractions pour lesquelles des mandats seront émis, les pouvoirs qui peuvent être autorisés et l'exigence de motifs raisonnables de croire que les données recherchées seront pertinentes. En vertu de l'article 45, les perquisitions ne sont autorisées que par un tribunal et sont exécutées par la police.<br><br>Le Nigeria dispose de lois autres que celles mentionnées ci-dessus qui traitent de diverses infractions pour lesquelles des données et d'autres preuves électroniques sont nécessaires pour obtenir des ordonnances conservatoires de la part des tribunaux ou pour prouver les éléments de l'infraction. Ces lois peuvent également définir des procédures spécifiques pour la recherche et la saisie de données électroniques dans le cadre des infractions qu'elles prévoient. Par exemple, les sections 58(1) et 58(2)(d) du Nigeria Data Protection Act, 2023, prévoient la perquisition et la saisie de données et de preuves électroniques et la procédure est similaire à celle de la section 45(1) du Cybercrimes Act. | Le Nigeria applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Chaque service d'enquête habilité à effectuer des perquisitions a adopté des procédures opérationnelles standard internes.<br><br>L'article 45 (1) devrait être utilisé en cas d'urgence, puisque les mandats sont obtenus par requête ex parte. Par exemple, dans les affaires impliquant des mineurs, les procédures formelles seront supprimées. L'article 45 (1) envisage les cas d'urgence (extrême) ou d'urgence. Pour clarifier la manière dont cette section est appliquée, le Nigeria a fourni une illustration (tirée d'une affaire réelle). Un fournisseur de services de réseau (C) facilite la communication entre les appareils A et B et la communication vise à interférer avec l'ordinateur ou le système de réseau d'une institution publique au Nigeria. Conformément à l'article 39 de la loi sur la cybercriminalité, C a intercepté la communication et en informe l'organisme chargé de l'application de la loi (ICPC). À ce stade, C met à la disposition de l'ICPC toutes les informations dont il dispose sur les appareils A et B, y compris la localisation et les enregistrements de la communication. Un agent de l'ICPC saisit alors le tribunal ex-parte, avec une déclaration sous serment, pour obtenir une ordonnance de perquisition et de saisie des appareils A et B. L'article 45 permet à la fois l'utilisation d'informations d'identification légalement acquises et l'accès à distance clandestin. En vertu de l'article 45(2)(f)(g) de la loi sur la cybercriminalité, un agent est légalement habilité à "utiliser toute technologie pour ..." (f) ou "exiger de la personne qu'elle se conforme à la loi sur la cybercriminalité" (g). (f) ou "exiger de la personne en charge de ..." (g) d'entrer les données d'identification et d'avoir ensuite l'accès requis. L'article 45(e) prévoit les cas où une recherche secrète à distance serait applicable. | |
| Macédoine du Nord | Plusieurs articles du code de procédure pénale couvrent les perquisitions et saisies traditionnelles et, séparément, les perquisitions et saisies électroniques. En général, un procureur demande un mandat à un tribunal, mais la police peut demander un mandat s'il y a un risque de retard. Dans les deux cas, si le mandat est accordé, la perquisition est exécutée par le procureur et la police. La police technique spécialisée peut également être impliquée.<br><br>Dans l'un des quatre types d'urgence définis à l'article 191 du CPP, une perquisition peut être exécutée sans mandat et sans certaines autres protections procédurales. L'un des types d'urgence est le risque de destruction de traces du crime ou d'objets importants pour la procédure. | La Macédoine du Nord applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'utilisation d'identifiants d'accès légalement acquis n'est pas définie dans le CPC, mais ce dernier décrit une manière suffisamment large d'obtenir des preuves, de sorte que la criminalistique en direct peut être utilisée comme outil. Selon l'art. 184, paragraphes 1 et 2, du code de procédure pénale, les preuves en direct peuvent être utilisées comme outil. 1 et 2 du CPP, en relation avec les articles 192 et 195 para. 1, 2 et 3 et de l'art. 198 para. 1, 2 et 3 du CPC, il est possible de procéder à des expertises en direct. Toute personne effectuant la procédure doit être autorisée à utiliser l'outil en question et doit être en mesure de démontrer l'authenticité de toutes les actions entreprises. En vertu de l'article 184, les utilisateurs de l'ordinateur ou ceux qui y ont accès doivent "fournir toutes les informations nécessaires pour que les objectifs de la recherche puissent être atteints sans entrave". En outre, l'exemple de cas fourni en réponse à la question 2.2.6 indique que les informations d'identification peuvent être utilisées pour étendre une recherche.<br><br>L'accès à distance secret est autorisé en vertu de l'article 252 du code de procédure pénale, intitulé "Objet et types de mesures d'enquête spéciales". Cet accès ne peut être utilisé que lorsqu'aucune autre méthode d'obtention des preuves n'est suffisante. Le ministère de l'intérieur envoie une demande au ministère public, qui la transmet au tribunal. Le tribunal délivre l'ordonnance relative à la méthode spéciale d'enquête pour une période déterminée ne dépassant pas un an. L'ordonnance sera réévaluée dans les 30 jours. | |
| Norvège | Les articles du code de procédure pénale norvégien applicables couvrent l'ensemble des perquisitions et des saisies, et non les données électroniques en particulier. En l'absence d'autorisation écrite de la personne concernée, une ordonnance du tribunal est généralement nécessaire au préalable. Certains types de données électroniques, y compris les données relatives aux abonnés, peuvent être accessibles sans ordonnance judiciaire.<br><br>Dans certains cas urgents, un procureur peut ordonner une perquisition et une saisie sans ordonnance du tribunal, conformément au code de procédure pénale, mais la décision doit être enregistrée et expliquée rapidement. Un fonctionnaire de police peut procéder à la perquisition et à la saisie d'objets, etc., sans ordonnance du tribunal dans certaines circonstances limitées, notamment en cas de découverte de nouveaux éléments de preuve lors d'une perquisition. Un procureur doit ratifier cette | La Norvège applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | décision dans les plus brefs délais. Au-delà de ces circonstances, il existe une autre sphère très restreinte d'utilisation possible des pouvoirs procéduraux de la police en cas d'urgence.<br><br>Il apparaît que les identifiants d'accès légalement acquis peuvent être utilisés dans certaines limites spécifiées si leur utilisation est proportionnée aux faits de l'espèce.<br><br>L'accès à distance secret sous forme de lecture de données est autorisé dans deux sections du code de procédure pénale. Il doit être autorisé par un tribunal et n'est possible que pour certains crimes.<br><br>Les procureurs demandent l'autorisation du tribunal pour les perquisitions et celles-ci sont exécutées par les procureurs et les officiers de police, y compris avec l'assistance d'experts techniques. Une formation technique approfondie est incluse dans la formation de la police norvégienne. | |
| Panama | Au Panama, la base légale pour la saisie de données informatiques stockées est l'article 314 du code de procédure pénale, qui autorise le procureur à saisir des données dans le cadre d'une enquête. La saisie de la correspondance privée ou de documents nécessite l'autorisation préalable du juge des garanties, sur la base de l'article 310 du code de procédure pénale. Cette disposition s'applique à tous les appareils, et pas seulement aux appareils électroniques, ce qui en fait la base légale pour accéder à n'importe quel appareil afin de rechercher des documents privés.<br>Après la saisie de l'appareil, du support ou du moyen de stockage, la défense doit être informée, mais sa présence n'est pas obligatoire. S'il est nécessaire d'accéder immédiatement aux appareils et de les fouiller, la défense doit être présente. La saisie des données est soumise au contrôle ultérieur du juge des garanties, qui doit respecter le secret professionnel et la confidentialité des documents. La loi ne prévoit pas de cas d'urgence, un contrôle a posteriori étant de toute façon toujours nécessaire.<br><br>L'article 310 du code de procédure pénale permet au procureur général d'agir dans des situations d'urgence sous le contrôle ultérieur du juge des garanties. Ces situations d'urgence comprennent la prévention des infractions, la réponse aux demandes d'assistance, l'arrestation d'individus en train de commettre une infraction, la conservation des preuves et la conduite des procédures immédiatement après une perquisition. | Le Panama applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Le Panama ne mentionne pas la possibilité ou l'impossibilité de rechercher ou d'accéder à un système informatique avec des données d'accès obtenues légalement. En outre, il est important de noter que le code de procédure pénale établit le principe de la liberté de la preuve.<br><br>Dans ce pays, il n'existe aucune référence au concept d'accès à distance clandestin.<br><br>Les autorités compétentes qui autorisent et effectuent une perquisition conformément aux dispositions de l'article 19.1 sont les bureaux du procureur général qui composent le ministère public, en tant qu'organe qui dirige l'enquête pénale. S'il s'agit d'une saisie de données, la légalisation correspondante doit être demandée au juge des garanties, dans un délai de 10 jours, pour que l'utilisation judiciaire de ces données puisse avoir lieu, et s'il s'agit d'informations confidentielles, telles que des communications ou des données privées, l'autorisation préalable du juge du contrôle des garanties constitutionnelles est requise. | |
| Paraguay | Le Paraguay a indiqué qu'il appliquait les modifications du code pénal paraguayen, la loi n° 4439/2011 qui "modifie et étend divers articles de la loi n° 1160/97 "code pénal", et les normes procédurales prévues à l'article 192 des opérations techniques et à l'article 200 de l'intervention des communications et à l'article 214 du code de procédure pénale paraguayen. Le Paraguay a établi ses pouvoirs par le biais de la liberté de la preuve, à l'article 173 du code de procédure, qui fonctionne avec le principe de la recherche de la vérité, régi par l'article 172 du code de procédure. Il s'agit d'une règle générale pour tous les types de preuves. Il n'y a pas de règlement spécifique qui inclut des règles spécifiques qui sont le sujet de la preuve numérique, il y a seulement des bonnes pratiques par le ministère public, comme l'application des principes d'expertise, en ce qui concerne la chaîne de possession, etc.<br><br>La détermination des "circonstances urgentes" au Paraguay dépend de cas spécifiques et de la violation des droits légaux, en particulier si les auteurs de cybercriminalité sont pris en flagrant délit. Par conséquent, le ministère public et la police nationale sont tenus d'agir. Le code pénal paraguayen contient une disposition légale relative à l'avancement juridictionnel des preuves pour demander des expertises urgentes. L'article 217 décrit la procédure, selon laquelle les experts sont sélectionnés et nommés par le juge ou le ministère public au cours de la phase préparatoire, à moins qu'il ne s'agisse | Le Paraguay applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'une avance juridictionnelle de preuves. En outre, l'article 320 traite de l'avance juridictionnelle des preuves, permettant des activités essentielles telles que la reconnaissance, la reconstruction, l'inspection ou l'expertise qui sont considérées comme définitives et irréproductibles, ou lorsque l'obtention d'une déclaration pendant le procès est jugée difficile en raison d'obstacles. Pour mener à bien ces actions, des ordonnances judiciaires sont nécessaires, et elles sont demandées par le ministère public. Dans les affaires impliquant des preuves numériques, en vertu du principe de la liberté de la preuve, le ministère public doit décrire avec précision les faits enquêtés et la technologie utilisée pour commettre les actes allégués. Par conséquent, il est tenu de préciser les preuves numériques potentielles que le juge doit ordonner de saisir.<br><br>Il n'est pas fait mention de l'utilisation des identifiants d'accès par les autorités dans le respect de la loi. L'accès à distance n'est pas encore autorisé.<br><br>Les autorités compétentes qui autorisent les perquisitions sont les juges pénaux de garantie et les juges pénaux d'attention permanente qui ont une compétence matérielle et territoriale. | |
| Pérou | Les perquisitions et les saisies sont régies par l'article 217 du code de procédure pénale et par la loi n° 27697. Les mesures qui restreignent les droits sont appliquées pour enregistrer ou accéder de la même manière aux systèmes informatiques, aux données et aux supports de stockage de données sur le territoire. En ce qui concerne les conditions à remplir : Conformément au numéro 1 de l'article 203 du code de procédure pénale, la saisie doit être motivée par le critère de "proportionnalité" et par le critère de "suffisance des éléments de preuve" : a) En ce qui concerne la "proportionnalité", la mesure de saisie restrictive doit satisfaire à ce critère en tenant compte des critères établis par la jurisprudence nationale. b) En ce qui concerne la "suffisance des éléments de preuve", la mesure restrictive de saisie doit satisfaire à ce critère grâce à l'analyse des éléments qui fournissent des preuves pertinentes pour l'enquête, qui partent du soupçon initial et qui peuvent arriver.<br><br>L'article 217 du code de procédure pénale précise qu'au cours d'une "inspection", terme apparenté à une "perquisition" (conformément au paragraphe 191 du rapport explicatif de la Convention de Budapest), des mesures coercitives réelles peuvent être mises en œuvre par le biais d'une "saisie". Il s'agit notamment de la confiscation d'objets susceptibles de servir de preuves ou de faire l'objet d'une | Le Pérou applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | confiscation. Ces mesures doivent être documentées avec précision et identifiées de manière appropriée, et la chaîne de possession doit être maintenue. La "saisie" peut ainsi être considérée comme un complément à l'exécution d'une "inspection". Il est important de noter que la "saisie" n'est pas la même chose que l'"inspection" ou la "perquisition". Ce dernier terme appartient à une catégorie similaire à la terminologie utilisée pour les perquisitions, les examens de données ou les inspections, conformément au paragraphe 191 du Rapport explicatif de la Convention de Budapest.<br><br>Aucune règle spécifique ne s'applique en cas d'urgence ou d'autres circonstances urgentes. En revanche, en cas de flagrant délit, les mesures restrictives de droits telles que la saisie sont soumises à une validation judiciaire.<br><br>L'utilisation de justificatifs d'accès légalement acquis pour l'enregistrement ou l'accès n'est pas une exigence obligatoire pour chacune des mesures de limitation des droits actuellement en vigueur. Cette absence d'exigence n'implique pas que si les titres d'accès sont obtenus, par exemple par la soumission volontaire du titulaire du titre d'accès aux fins d'enregistrement ou d'accès à un système informatique et à ses données, ils ne peuvent pas être utilisés. La législation actuelle n'interdit pas la fourniture volontaire de titres d'accès par le détenteur, car cela relève de son droit de gérer les données qu'il juge appropriées. Dans la pratique, lors de l'exécution d'une "inspection" et de la "saisie" ultérieure de biens, il peut arriver que le propriétaire des biens (appareils électroniques) fournisse volontairement des mots de passe ou des schémas d'accès, démontrant ainsi son intention claire de coopérer. Ces actions sont consignées dans le registre correspondant des biens saisis, qui peut être exécuté ou non, et cette décision n'a pas d'incidence sur l'exécution de la mesure, ni sur d'éventuelles validations judiciaires ultérieures, le cas échéant.<br>L'accès à distance n'a pas été réglementé et n'a pas encore fait l'objet de discussions.<br><br>Les mesures restrictives de saisie sont requises par le procureur, autorisées par le juge par une résolution dûment motivée et exécutées par le procureur et/ou la police nationale. Le personnel qui exécute la mesure doit avoir des connaissances informatiques de base minimales pour mener à bien une perquisition. | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Philippines | Les perquisitions sont autorisées par des mandats, qui sont délivrés par des juges après constatation d'un motif probable sur la base d'une demande vérifiée et étayée et d'affidavits. Ces documents préliminaires doivent indiquer les fondements de la perquisition et spécifier en détail la stratégie de perquisition et de saisie. Les services répressifs spécialisés dans la cybercriminalité et les analystes en criminalistique numérique effectuent des perquisitions impliquant des données électroniques.<br><br>Les pouvoirs de perquisition et de saisie s'appliquent à toutes les infractions.<br><br>Il n'y a pas de règles particulières pour les situations d'urgence.<br><br>L'utilisation de titres d'accès acquis légalement est autorisée en vertu du pouvoir d'ordonner à toute personne de fournir des informations pour faciliter les perquisitions et les saisies.<br><br>L'accès à distance secret n'est pas disponible. | Les Philippines appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |
| Pologne | Les décisions autorisant les perquisitions sont rendues par un tribunal ou un procureur, sauf dans les cas d'urgence décrits ci-dessous. Le code de procédure pénale prévoit de nombreuses conditions pour les perquisitions électroniques, conformément aux règles générales sur les perquisitions et les saisies et aux règles spécifiques aux procédures électroniques. Ces conditions comprennent des exigences en matière de documentation, la présence des personnes concernées ou de substituts appropriés, etc. Les perquisitions peuvent être effectuées par un procureur, par la police ou par des fonctionnaires d'une autorité spécialisée, en fonction de la loi applicable ou de l'ordonnance d'un tribunal ou d'un procureur. Les techniciens de la police scientifique suivent une formation spécialisée. Si des données sont conservées et examinées, l'examen doit être effectué par des agents appartenant à certaines unités de police ou de médecine légale.<br><br>Les situations d'urgence sont définies comme celles dans lesquelles un retard pourrait entraîner la perte ou l'altération de preuves ou de pistes - par exemple, si la mise hors tension d'un système au cours d'une saisie entraîne la perte de données. Dans ce cas, une perquisition peut être effectuée, mais l'unité qui y procède doit présenter un mandat du chef de l'unité ou une carte d'identité. Ensuite, la perquisition doit être ratifiée par un tribunal ou le procureur. La personne concernée doit être | La Pologne applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | informée de son droit à une décision, doit la recevoir dans un délai de sept jours et dispose de droits supplémentaires dans de telles situations.<br><br>Il semble que les recherches puissent être étendues à l'aide d'informations d'identification obtenues légalement, lorsque cela est documenté. Les lignes directrices de la police autorisent également l'utilisation d'appareils ou de programmes informatiques donnant accès à des données cryptées ou protégées par un mot de passe, y compris lorsque ces mesures sont utilisées pour des équipements liés à l'objet initialement recherché.<br><br>Le code de procédure pénale polonais ne contient pas de dispositions explicites concernant la recherche à distance d'un système informatique ou l'accès à distance clandestin. Toutefois, l'accès à distance dissimulé semble être autorisé. Une telle recherche peut être autorisée par un tribunal ou un procureur, en fonction du stade de la procédure, de l'acte à accomplir et du type de données recherchées. Des techniciens de la police scientifique ou d'autres experts exécutent l'accès. | |
| Portugal | Les perquisitions et les saisies ne sont pas régies par le régime général du CPP mais par les dispositions de la loi sur la cybercriminalité, la loi n° 109/2009, telle qu'amendée. Dans le cadre de ce système, les perquisitions peuvent être effectuées lorsqu'elles sont autorisées par un procureur dans les phases d'enquête ou par un juge dans les phases ultérieures. Ces autorités doivent être présentes lors de l'exécution de l'ordre, si possible. Dans la plupart des cas, l'exécution proprement dite est effectuée par la police et, si nécessaire, par des experts supplémentaires.<br>Il n'existe pas de disposition légale concernant les situations d'urgence, mais le Portugal a l'intention de ratifier le deuxième protocole additionnel, ce qui implique que les situations d'urgence seront incluses dans une future loi nationale. Toutefois, la police peut effectuer une perquisition sans autorisation judiciaire préalable 1) avec le consentement volontaire et documenté de la personne concernée, ou 2) dans le cadre d'enquêtes sur certains crimes graves, lorsqu'il existe des preuves fondées d'un crime imminent présentant un risque grave pour la vie ou la santé d'une personne. Dans ces cas, pour préserver l'admissibilité des preuves, la perquisition doit être documentée et ratifiée rapidement par l'autorité compétente. | Le Portugal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'utilisation d'informations d'identification acquises légalement et l'accès à distance clandestin ne sont pas prévus par la loi. | |
| République de Moldavie | La Moldavie s'appuie sur plusieurs lois générales pour la recherche de données électroniques. Ces pouvoirs s'appliquent à toutes les infractions prévues par le code pénal. Les perquisitions sont autorisées par un juge d'instruction (ou, dans les cas urgents décrits ci-dessous, par un procureur). Les perquisitions sont exécutées par les forces de l'ordre et/ou le procureur (l'un ou l'autre est nécessaire, mais les deux peuvent être présents). Des spécialistes de la médecine légale peuvent être impliqués. Le parquet général a adopté des lignes directrices pour les enquêtes sur la cybercriminalité.<br><br>L'article 127 du code de procédure pénale traite de la présence, pendant la fouille, de la personne fouillée ou de divers représentants éventuels. En outre, le code de procédure pénale ne prévoit aucune exigence spécifique en matière de notification.<br><br>"Dans les cas non susceptibles d'ajournement ou en cas de flagrant délit", conformément à l'article 125 du CPP, les perquisitions peuvent être effectuées sur ordonnance motivée d'un procureur, et non du juge d'instruction, sous réserve de la ratification de l'acte par ce dernier dans les 24 heures.<br><br>En vertu d'un mandat de perquisition et de l'article 125 du code de procédure pénale, les forces de l'ordre peuvent accéder aux données à l'aide d'informations d'identification acquises légalement.<br><br>L'accès à distance secret peut être utilisé principalement en vertu d'une loi de 2023 et de l'article 138 du CPP. | La Moldova applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Roumanie | Les perquisitions et les saisies sont autorisées par le tribunal compétent (qui peut varier) à la demande du procureur. Le procureur ou l'officier de police judiciaire sera présent lors de l'exécution du mandat, de même que le défendeur et éventuellement un avocat. L'exécution effective du mandat n'est effectuée que par des spécialistes techniques attachés à l'autorité judiciaire ou par des policiers spécialisés. Si l'accusé est détenu, la présence de son avocat lors de la perquisition est obligatoire. | La Roumanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Il n'existe pas de règles particulières pour les situations d'urgence. Toutefois, s'il est établi au cours d'une perquisition que les données cibles se trouvent dans un système ou un support de stockage accessible à partir de l'objet initial de la perquisition, les données cibles sont copiées et conservées et une demande d'extension du mandat est introduite.<br>Les pouvoirs acquis légalement peuvent être utilisés. Les suspects et les personnes mises en cause ne sont pas obligés de révéler leurs pouvoirs.<br><br>En vertu de l'article 138, paragraphe 1, point b), du code de procédure pénale, l'autorité compétente peut, sur ordre du tribunal, accéder secrètement à un système informatique, directement ou à distance. Ce pouvoir est une mesure de surveillance effectuée secrètement à l'aide d'informations d'identification acquises légalement et il est différent de la perquisition d'ordinateur prévue à l'article 168 du code de procédure pénale. | |
| Saint-Marin | Saint-Marin a déclaré qu'il n'existe actuellement aucune législation spécifique sur la perquisition et la saisie de données informatiques stockées. Il a également été indiqué que la jurisprudence n'est pas encore très développée en ce qui concerne les questions liées aux données informatiques. Il semble que des principes juridiques analogues soient largement appliqués.<br><br>Par ailleurs, les autorités ont informé que la Cour de cassation s'est prononcée sur l'acquisition de données informatiques dans le cadre d'une procédure pénale (arrêt n° 8 du 15 novembre 2021). Ce processus comprend plusieurs étapes : d'abord, une fouille physique des appareils contenant les données, suivie d'une fouille informatique pour extraire les informations pertinentes, et enfin, la saisie de ces données à titre préliminaire. Si une recherche informatique immédiate n'est pas possible pour des raisons techniques, le dispositif physique ou une copie judiciaire complète est saisi pour une analyse plus approfondie. L'ordonnance de saisie doit être précise et indiquer exactement quelles données sont recherchées et à quelles fins d'enquête.<br><br>Les perquisitions peuvent être effectuées par des officiers de police judiciaire, soit par délégation du pouvoir judiciaire, soit de leur propre initiative en cas d'urgence et de nécessité. | Saint-Marin applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient apporter plus de clarté et de sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'article 78 du code de procédure pénale légitime les perquisitions en stipulant que la police doit agir avec la prudence nécessaire et recueillir des preuves à charge et à décharge.<br><br>Cas d'urgence : Les autorités saint-marinaises ont indiqué que s'il n'est pas possible d'attendre une décision de justice, l'article 58-duodecies du code de procédure pénale permet aux officiers de police de saisir le corps du délit et les objets connexes de leur propre initiative. Ils doivent ensuite soumettre le procès-verbal dans les 48 heures au juge d'instruction, qui doit le valider dans les 96 heures si les conditions sont réunies, sinon la mesure est nulle et non avenue.<br><br>Il a également été indiqué que les forces de police sont autorisées à accéder à un système informatique sur délégation du pouvoir judiciaire si les références d'accès sont légalement acquises. En l'absence de titres d'accès légalement acquis, mais avec l'autorisation du pouvoir judiciaire, le Corps de gendarmerie - Unité de police opérationnelle et judiciaire peut être autorisé à effectuer un accès à distance au système informatique.<br><br>Le tribunal de Saint-Marin autorise la police à mener des enquêtes, des perquisitions et des saisies, qu'elle effectue ou qu'elle suscite de manière indépendante en ce qui concerne les infractions. Pour analyser les données, les fichiers et le matériel informatique saisis, la police travaille avec des experts techniques du domaine sous la direction du juge. | |
| Sénégal | La perquisition et la saisie de données électroniques sont régies par les articles 90-1 à 90-14 du CPP, tels que modifiés en 2016. Ces dispositions sont applicables aux infractions commises à l'encontre des systèmes d'information ou au moyen de ceux-ci. Elles s'appliquent également à tous les autres types d'infractions dont les éléments de preuve peuvent être trouvés dans les systèmes d'information.<br><br>Selon les articles 90-4 à 90-6 et 90-8 du CPP, les perquisitions sont autorisées et contrôlées par le procureur de la République ou par un juge d'instruction. Elles sont exécutées par le juge d'instruction ou par la police judiciaire sous le contrôle du procureur ou du juge d'instruction. Les perquisitions ne sont autorisées que si les données visées sont absolument nécessaires à l'enquête, dans le strict respect du principe de légalité des preuves. Les données doivent être utiles à la manifestation de la | Le Sénégal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | vérité. Le responsable du système doit être informé de la recherche effectuée et des données copiées, supprimées ou rendues inaccessibles.<br><br>L'article 90-6 traite des cas d'urgence en ce sens que, si la saisie de parties d'un système d'information n'est pas souhaitable, les données qui seraient utiles à la manifestation de la vérité peuvent être copiées, y compris en utilisant des supports de stockage appartenant à des personnes autorisées à utiliser le système.<br><br>Il semble que les articles 90-11 et 90-9 permettent l'utilisation d'identifiants acquis légalement, puisqu'ils autorisent les fonctionnaires à utiliser toute mesure technique appropriée pour collecter des données relatives à des communications spécifiques transmises par l'intermédiaire d'un système d'information. Les fonctionnaires peuvent également utiliser des procédés techniques, des programmes, etc., pour restaurer des données effacées ou pour attribuer des actes. L'utilisation de ces mesures/procédures n'est permise que lorsqu'elle est nécessaire à l'obtention des preuves et doit être autorisée et supervisée par le procureur ou le juge d'instruction.<br><br>L'article 90-10 permet aux autorités compétentes d'installer et d'utiliser des outils à distance pour obtenir des preuves utiles à une affaire. | |
| Serbie | Article 19.1 Les perquisitions sont demandées par les procureurs, autorisées ou ordonnées par les tribunaux et exécutées par la police. La demande et l'ordre sont fondés sur un doute raisonnable quant à l'existence d'un délit (après un rapport sur le délit ou sa découverte accidentelle). Les ordres de perquisition peuvent s'appliquer aux ordinateurs, aux systèmes, aux données et aux supports de stockage. Les pouvoirs généraux de perquisition et de saisie prévus par le CPP s'appliquent à toutes les infractions prévues par le code pénal ; les pouvoirs d'enquête spéciaux relatifs aux perquisitions et saisies électroniques ne s'appliquent qu'à certaines infractions (précisées et fournies dans la réponse de la Serbie). Que l'ordre découle de pouvoirs généraux ou de pouvoirs d'enquête spéciaux, les preuves électroniques peuvent être recherchées. Les unités spécialisées de la police disposent de l'expertise nécessaire. La police et les unités spécialisées ont adopté des procédures opérationnelles standard non publiques. | La Serbie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Conformément à l'article 158 du CPC, les perquisitions et les saisies peuvent être effectuées sans ordonnance judiciaire dans certaines circonstances urgentes (énumérées dans la réponse de la Serbie). La Serbie a déclaré que l'interaction entre l'article 147 du CPC et l'article 158 indique clairement que les données électroniques et les dispositifs de stockage font partie des catégories d'objets qui peuvent être saisis dans de telles circonstances urgentes.<br><br>L'utilisation de titres légalement acquis est autorisée s'ils sont remis volontairement ou acquis par les forces de l'ordre dans le cadre de l'exécution d'une mesure approuvée par un tribunal.<br><br>Le code de procédure pénale ne fait pas de distinction entre l'accès à distance régulier et l'accès à distance secret. L'un ou l'autre peut être demandé par le ministère public et approuvé par le tribunal. Plus précisément, si les éléments de l'article 161 du CPP sont réunis, un tribunal peut ordonner (sur requête du ministère public) "des recherches informatiques sur des données à caractère personnel et d'autres données déjà traitées et leur comparaison avec des données relatives au suspect et à l'infraction pénale". | |
| Sierra Leone | La perquisition et la saisie de données informatiques stockées sont prévues à l'article 10 de la loi de 2021 sur la cybersécurité et la criminalité en Sierra Leone (Sierra Leone Cybersecurity and Crime Act 2021).<br><br>Les autorités ont indiqué que, conformément à l'article 10 de la loi 202 sur la cybersécurité et la criminalité en Sierra Leone, un agent d'exécution peut demander à un juge de la Haute Cour un mandat autorisant l'accès, la saisie ou la sécurisation d'un système informatique, d'un programme, de données ou d'un support de stockage de données informatiques qui peuvent être nécessaires comme éléments de preuve d'une infraction dans le cadre d'une enquête ou d'une procédure pénale, ou qui ont été acquis par une personne à la suite de la commission d'une infraction.<br><br>Il n'y a pas de règles particulières concernant les urgences ou d'autres circonstances urgentes. | La Sierra Leone applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La législation autorise les autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant des identifiants d'accès acquis légalement.<br><br>La législation n'autorise pas les autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant un accès à distance secret.<br><br>L'autorité compétente qui autorise est le juge et ceux qui effectuent une perquisition sont les forces de l'ordre comme la police et d'autres autorités compétentes. | |
| République slovaque | La perquisition du système informatique et des données qui y sont stockées est possible en vertu des pouvoirs généraux de perquisition à domicile (section 99), d'inspection d'autres locaux et terrains (section 101) et de perquisition personnelle (section 102) du code de procédure pénale.<br><br>Selon le stade de l'enquête, une ordonnance doit être obtenue auprès d'un tribunal ou d'un procureur. La demande doit être dûment justifiée.<br><br>Les situations d'urgence ne font pas l'objet d'une réglementation spécifique, mais les procureurs et les juges disposent d'un système de permanence 24 heures sur 24 et 7 jours sur 7 pour traiter les affaires urgentes.<br><br>Le CPC ne prévoit pas l'utilisation d'identifiants d'accès acquis légalement. Ces identifiants peuvent être remis volontairement par la personne visée ou obtenus sur ordre d'un tribunal ou d'un procureur. L'accès secret à distance n'est pas autorisé par le CPC.<br><br>Les autorités d'autorisation sont le tribunal ou le procureur, en fonction de la mesure exécutée, du stade de la procédure et du type de données demandées. Les mesures sont exécutées par des spécialistes de la police scientifique, qui ont une formation particulière et des qualifications classées. | La République slovaque applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Slovénie | Deux articles principaux du code de procédure pénale, les articles 219 bis et 223 bis, traitent des perquisitions et des saisies de données électroniques. Il doit exister des motifs raisonnables justifiant une perquisition (voir ci-dessous). Si de tels motifs existent, une perquisition peut être effectuée sur la base 1) du consentement écrit préalable de la personne concernée ou 2) d'une ordonnance judiciaire écrite et bien fondée, basée sur une demande élaborée par le ministère public et la police. L'exécution de la perquisition est effectuée par des policiers spécialement formés.<br><br>S'il existe un danger direct et grave pour la sécurité des personnes ou des biens et qu'une ordonnance écrite ne peut être obtenue en temps utile, le juge d'instruction peut ordonner oralement la perquisition sur la base d'une demande orale du procureur. Cette action doit être documentée et ratifiée dans les douze heures, faute de quoi les preuves doivent être détruites.<br><br>Les propriétaires ou les utilisateurs de dispositifs électroniques doivent fournir l'accès à l'objet, les clés d'accès au cryptage ou les mots de passe, ainsi que toutes les explications nécessaires sur le fonctionnement de l'objet. Les personnes qui refusent de coopérer peuvent être sanctionnées, y compris par une peine d'emprisonnement (sauf pour les personnes appartenant à certaines catégories, comme les prévenus). Apparemment, ces informations d'identification peuvent ensuite être utilisées.<br><br>L'accès à distance secret n'est pas disponible, sauf dans des circonstances très limitées concernant les institutions financières. | La Slovénie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |
| Espagne | La perquisition du système informatique ou des données situées dans des dispositifs informatiques ou des systèmes de stockage de masse a été explicitement réglementée par le code de procédure pénale espagnol en 2015. La réforme de la loi opérée par la LO 13/2015 a intégré dans les mesures procédurales l'article 588 sexies (e) inspiré de l'article 19 de la Convention de Budapest.<br><br>L'Espagne a fait savoir que, dans la pratique, la recherche de dispositifs informatiques est effectuée à la connaissance de l'intéressé, qui peut donner son consentement à l'exécution de cette diligence et que ce n'est qu'en l'absence d'un tel consentement que l'autorisation judiciaire sera nécessaire. L'article 588 bis (a) LECrim prévoit que les mesures de recherche technologique, à moins qu'il n'y ait le consentement de la personne concernée, ne peuvent être approuvées qu'au moyen d'une *décision* | L'Espagne applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | *judiciaire délivrée dans le plein respect des principes de spécialité, d'adéquation, d'exceptionnalité, de nécessité et de proportionnalité de la mesure*.<br><br>Le droit espagnol prévoit expressément, dans plusieurs articles de sa législation procédurale, la notification de la mesure de recherche tant à l'accusé qu'aux tiers concernés (articles 566, 569 et 588).<br><br>La législation espagnole prévoit certaines exceptions en cas d'urgence, c'est-à-dire dans les cas où le fait de retarder l'exécution de la mesure d'enquête risque de compromettre l'obtention, dans des conditions appropriées, d'éléments de preuve susceptibles d'être utilisés comme éléments de preuve dans le cadre d'une procédure pénale.<br><br>Selon la jurisprudence, si des références sont obtenues légalement lors d'une perquisition et que le juge autorise leur utilisation, il n'y a pas de problème juridique à les utiliser pour analyser un dispositif. Cette utilisation des références est considérée comme légale si elles ont été obtenues sans violer les droits fondamentaux.<br><br>L'article 588 septies (i) permet au juge d'autoriser la perquisition à distance d'un ordinateur, d'un dispositif électronique ou d'un système à l'insu du propriétaire dans le cas de crimes spécifiques. La décision judiciaire doit préciser l'étendue et les modalités de l'accès, le logiciel à utiliser, les agents autorisés à effectuer la recherche et les mesures visant à préserver l'intégrité des données. Les fournisseurs de services et les propriétaires de systèmes doivent coopérer avec les enquêteurs, qui peuvent également ordonner à toute personne ayant connaissance du système de fournir les informations nécessaires. La mesure ne peut durer plus de trois mois, et la responsabilité de ceux qui ne coopèrent pas est engagée.<br><br>La fouille doit être autorisée par l'autorité judiciaire. Les forces de police des unités spécialisées procèdent à la fouille et à l'analyse de l'appareil, qui peut se faire physiquement ou par renversement partiel. L'examen technique est effectué sur une copie-miroir du système analysé afin d'éviter toute altération du contenu original, et le dispositif saisi est tenu à la disposition de l'autorité judiciaire. | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Sri Lanka | Les perquisitions et saisies de données informatiques stockées sont principalement régies par la loi sur la criminalité informatique (Computer Crime Act No. 24 of 2007) et le code pénal. D'autres lois (précisées dans la réponse du Sri Lanka) peuvent s'appliquer. Les pouvoirs découlant de la loi sur la criminalité informatique concernent principalement les infractions commises à l'encontre ou au moyen d'ordinateurs. Ils peuvent également s'appliquer à d'autres infractions si un ordinateur ou des données électroniques font partie intégrante de la commission de l'infraction ou détiennent des preuves liées à l'infraction. Conformément à l'article 18 de la CCA, les perquisitions et les saisies dans des circonstances non urgentes ne peuvent être autorisées et effectuées qu'en vertu d'un mandat délivré par un magistrat. Les fonctionnaires de police qui accèdent aux ordinateurs dans le cadre d'enquêtes menées en vertu de la loi sur la criminalité informatique doivent être préalablement certifiés par l'inspecteur général de la police comme étant compétents en matière d'enquêtes numériques. Les experts en médecine légale peuvent être utilisés sous la supervision de la police.<br><br>Il semble qu'aucune ligne de conduite ou procédure opérationnelle standard n'ait été adoptée, mais les articles 20 à 24 de la loi sur la criminalité informatique détaillent les procédures relatives aux perquisitions (l'utilisation normale de l'ordinateur ne doit pas être entravée ; le policier a le pouvoir d'arrêter, de perquisitionner et de saisir ; le policier doit enregistrer les données saisies et y donner accès ; il a le devoir d'aider à l'enquête ; la confidentialité des informations obtenues au cours d'une enquête).<br><br>L'article 18/2 de la loi sur la criminalité informatique autorise les perquisitions sans mandat si l'enquête doit être menée d'urgence, s'il existe une probabilité que les preuves soient perdues, détruites, modifiées ou rendues inaccessibles et s'il est nécessaire de préserver le caractère confidentiel de l'enquête.<br><br>Le Sri Lanka n'est pas autorisé à utiliser des titres d'accès acquis légalement.<br><br>La législation sri-lankaise ne prévoit pas l'accès secret à distance. | Le Sri Lanka applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |
| Suède | La perquisition et la saisie sont couvertes par plusieurs règles générales du code de procédure pénale (par exemple, la perquisition des locaux, la fouille corporelle) et par des règles spécifiques aux | La Suède applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données et dispositifs électroniques (accès à distance couvert appelé interceptions de données secrètes). Il existe des exigences en matière de notification et de présence de la personne concernée ou d'un témoin. Un ordre autorisant la perquisition de locaux (qui peut conduire à la perquisition d'appareils électroniques et de données) est normalement délivré par le responsable de l'enquête (de l'autorité policière) ou par un procureur. Le responsable de l'enquête et sa complexité déterminent qui autorise les perquisitions et les saisies. Au stade où une personne est raisonnablement soupçonnée d'avoir commis l'infraction, l'enquête est dirigée par le procureur, à moins qu'il ne s'agisse d'une affaire moins complexe. La mesure dans laquelle des mesures coercitives sont nécessaires déterminera si l'enquête est considérée comme suffisamment complexe pour être dirigée par un procureur.<br><br>Si la perquisition est de grande ampleur ou entraîne des désagréments extraordinaires, elle ne doit être effectuée qu'en vertu d'une ordonnance rendue *par un tribunal*, à moins que le retard n'entraîne un risque. L'expression "si le retard entraîne un risque" signifie que la mesure coercitive serait inutile si elle n'était pas exécutée immédiatement. Dans ce cas, la police peut procéder à une perquisition sans ordonnance. Les objets trouvés lors d'une perquisition et dont on peut raisonnablement supposer qu'ils sont importants pour l'enquête peuvent être saisis. Les objets trouvés par ailleurs peuvent être saisis sur ordre du responsable de l'enquête ou du procureur. Si un retard comporte des risques, les objets peuvent être saisis en l'absence d'ordre. L'exécution des perquisitions est menée par l'autorité chargée de l'enquête, idéalement en coopération avec des experts en criminalistique numérique ou d'autres personnels spécialisés. Les cas particulièrement complexes sont traités par des experts du Centre national de police scientifique de l'autorité de police.<br><br>Les titres d'accès acquis légalement peuvent être utilisés, sous réserve des exigences habituelles en matière de perquisition et de saisie.<br><br>L'accès à distance secret, appelé interception de données secrètes, est possible, mais il ne peut être approuvé que si les raisons de cet accès l'emportent sur l'effet sur les droits de la personne recherchée (dans le cas d'un système informatique, la personne recherchée est normalement la cible). L'autorisation d'accès est demandée par un procureur et le tribunal tient une audience avec un représentant public désigné. En cas d'urgence, un procureur peut approuver cet accès avant que | mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | l'affaire ne soit entendue par le tribunal. L'accès à distance secret n'est possible que si la mesure est d'une importance extraordinaire dans les cas où il y a une peine potentielle d'au moins deux ans d'emprisonnement ou en relation avec une certaine liste de crimes. Dans ces cas, l'autorité d'exécution doit désigner au moins une personne ayant des compétences particulières pour mener à bien la mesure.<br><br>La Suède a fourni des documents auxiliaires utiles et des informations sur sa législation et sa pratique en matière de perquisitions et de saisies. | |
| Suisse | Les règlements relatifs aux perquisitions et saisies non électroniques couvrent également les perquisitions et saisies de systèmes et de données électroniques. En outre, le code pénal prévoit explicitement, en partie, les perquisitions et les saisies de données électroniques et de stockage. En règle générale, les perquisitions et les saisies peuvent être autorisées par une ordonnance écrite, délivrée si les différents éléments spécifiés dans les articles pertinents du code pénal sont satisfaits. En principe, un procureur peut également ordonner une perquisition sans autorisation du tribunal. Par conséquent, une perquisition ne nécessite généralement pas l'autorisation d'un tribunal. Toutefois, la personne faisant l'objet de la perquisition peut demander que les documents appartenant à des catégories protégées soient mis sous scellés, tandis que la levée des scellés doit être prononcée par un tribunal indépendant. L'exécution des perquisitions est effectuée par la police et, si nécessaire, par des experts techniques supplémentaires.<br><br>Les cas d'urgence sont ceux où la police a besoin d'un accès immédiat à des données ou à des archives qui viennent d'être découvertes, où un danger imminent peut survenir ou où un retard risque réellement d'entraîner la perte des traces de l'infraction, de l'objet ou des avoirs. Exceptionnellement, en cas de danger imminent, une perquisition peut être effectuée par la police sans ordre écrit préalable, mais l'action doit être signalée rapidement et doit être confirmée par écrit par l'autorité pénale compétente. Il existe une distinction entre les saisies et l'obtention de preuves par la police. La question de savoir si l'absence de mandat rend les preuves irrecevables est tranchée au cas par cas.<br><br>L'utilisation de titres acquis légalement est autorisée par la jurisprudence de la Cour suprême. | La Suisse applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'accès à distance est possible avec des informations d'identification obtenues légalement, à condition que les exigences de la CrimPC soient respectées. D'autres articles de la CrimPC autorisent une surveillance limitée, sans contenu, de la correspondance par télécommunication, dans le cadre de paramètres très restrictifs. | |
| Tonga | La section 9 du Computer Crimes Act [Cap 4.02] régit les perquisitions et saisies électroniques, qui ne peuvent être effectuées (à quelques exceptions près) que sur délivrance d'un mandat par un magistrat. La demande de mandat sous serment et l'affidavit doivent être étayés par des motifs raisonnables de soupçonner qu'un ordinateur, un système, des données, etc., peuvent constituer des preuves matérielles d'une infraction ou ont été acquis à la suite d'une infraction. La police procède à la perquisition et à la saisie (voir les autres détails ci-dessous), en respectant les procédures prévues par l'article, telles que l'inventaire de ce qui a été saisi. La loi peut exiger que le fonctionnaire de police qui exécute la mesure ait un certain grade. Il n'y a pas d'obligation de notification.<br><br>Il n'existe pas de législation spécifique aux recherches électroniques dans les situations d'urgence. Toutefois, l'article 123 de la loi sur la police pourrait être utilisé pour effectuer des recherches de données en cas d'urgence, puisqu'il prévoit des recherches sans mandat dans les cas d'infractions graves qui répondent à plusieurs autres éléments de l'article. Les questions de sécurité nationale ou les menaces pour la vie peuvent constituer des situations d'urgence. Les enquêtes urgentes ou la destruction probable de preuves peuvent constituer des situations d'urgence. Comme expliqué plus en détail dans la réponse des Tonga, plusieurs autres lois prévoient des perquisitions en cas d'urgence et des perquisitions et saisies sans mandat en cas d'urgence si certaines conditions sont remplies.<br><br>Il n'existe pas de législation spécifique concernant l'accès à l'aide d'identifiants acquis légalement. Dans la pratique, les demandes de mandats génériques incluent des demandes d'obtention d'identifiants d'accès, de sorte que ces mandats couvrent l'acquisition d'identifiants d'accès. Ce mécanisme a été utilisé dans le cadre d'enquêtes menées au titre de diverses lois.<br><br>Plusieurs lois, dont la loi sur la police, prévoient des pouvoirs de surveillance discrète. Plus précisément, l'article 14 de la loi sur les délits informatiques (Computer Crimes Act) prévoit l'interception des communications électroniques si certaines conditions sont remplies. | Les Tonga appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les perquisitions au titre de l'article 19.1 sont autorisées par un magistrat ou un juge de la Cour suprême, en fonction de la loi concernée. Les perquisitions sont effectuées par des officiers de police ou des "officiers ou personnes autorisés" qui assistent la police. Ces personnes autorisées peuvent être des membres du CERT Tonga ou d'autres spécialistes de la police scientifique.<br><br>En collaboration avec des spécialistes, la police tongienne élabore des procédures opérationnelles standard pour l'utilisation des appareils Cellebrite. Le CERT Tonga est en train de rédiger des procédures opérationnelles standard concernant sa collaboration avec la police. | |
| Tunisie | | |
| Türkiye | Les perquisitions et saisies électroniques sont régies par au moins deux lois. C'est un juge qui ordonne la mesure, en supposant que la base de celle-ci est suffisante. Lorsqu'un retard peut être préjudiciable, un procureur peut ordonner une perquisition. L'ordonnance du procureur doit être ratifiée par le juge dans les plus brefs délais ; si le délai expire ou si la décision n'est pas ratifiée, les données collectées doivent être détruites. La perquisition ou la saisie est effectuée par des unités chargées de l'application de la loi. Des experts légistes peuvent être impliqués ou les objets saisis peuvent être envoyés à des experts légistes pour examen.<br><br>En cas d'urgence, le procureur peut ordonner une perquisition sous réserve de la ratification du tribunal susmentionnée. Il s'agit notamment des cas où il existe un risque de perte de données, où le délit faisant l'objet de l'enquête est passible d'une lourde peine ou où le suspect a été placé en détention pour empêcher la falsification des preuves.<br>Il semble que l'utilisation de références acquises légalement ne soit pas autorisée.<br><br>L'accès à distance secret peut être utilisé dans le cadre d'enquêtes sur les paris en ligne. Le code de procédure pénale ne réglemente pas cette pratique en ce qui concerne d'autres infractions. | La Turquie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.1. |
| Ukraine | L'Ukraine applique plusieurs dispositions du code de procédure pénale") qui présente certaines caractéristiques qui mettent en œuvre l'article 19 de la Convention. L'art. 159 prévoit la possibilité d'un accès temporaire aux objets et documents qui consiste à fournir à la partie à la procédure pénale | Il semble que l'Ukraine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | la personne en possession de ces objets et documents, mais il reste à déterminer comment ces dispositions s'étendent aux données informatiques.<br><br>Conformément à la deuxième partie de l'article 159 du code de procédure pénale ukrainien, l'accès temporaire aux objets et aux documents s'effectue sur la base d'une décision du juge d'instruction ou du tribunal.<br><br>L'examen des données informatiques est effectué par l'enquêteur, le procureur.<br><br>Les réponses précisent que, conformément aux exigences de l'article 159 du code de procédure pénale, lorsque des données informatiques sont connues, un procureur ou un enquêteur est habilité à exercer un accès temporaire aux systèmes d'information électroniques, aux systèmes informatiques ou à des parties de ceux-ci, aux terminaux mobiles des systèmes de communication, en prenant une copie des informations contenues dans ces systèmes d'information électroniques, ces systèmes informatiques ou des parties de ceux-ci, ces terminaux mobiles des systèmes de communication, sans les retirer. Par ailleurs, si l'on ne connaît pas le lieu de stockage du système informatique ou des données stockées, ainsi que le support de stockage informatique dans lequel les données informatiques peuvent être stockées, l'autorité visée à l'article 234 du code de procédure pénale ukrainien est habilitée à effectuer une perquisition afin d'identifier et d'enregistrer des informations sur les circonstances d'une infraction pénale, de trouver l'instrument d'une infraction pénale.<br><br>Dans les cas urgents liés à la préservation de la vie humaine et des biens ou à la poursuite directe de personnes soupçonnées d'avoir commis un crime, une autre procédure établie par la loi pour pénétrer dans le domicile d'une personne ou dans d'autres biens, y effectuer une inspection et une fouille est possible. La base procédurale pour effectuer une perquisition urgente est la partie 3 de l'article 233 du code de procédure pénale. 233 du code de procédure pénale.<br><br>Selon la sixième partie de l'article 234 du code de procédure pénale ukrainien, lors d'une perquisition, un procureur a le droit de surmonter les systèmes de protection logique si la personne présente lors de la perquisition refuse de les ouvrir ou d'enlever (désactiver) le système de protection logique ou si la perquisition est effectuée en l'absence de personnes. Cette règle peut être interprétée comme le | informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | pouvoir de perquisitionner ou d'accéder de la même manière à un système informatique et aux données qu'il contient en utilisant des identifiants d'accès légalement acquis. | |
| | Les pouvoirs procéduraux qui s'appliquent à la perquisition et à la saisie de données informatiques stockées découlent de divers textes législatifs, dont certains sont applicables à l'ensemble du territoire du Royaume-Uni (ci-après "le Royaume-Uni") et d'autres non.<br><br>Plus précisément, le Police and Criminal Evidence Act 1984 (PACE), applicable en Angleterre et au Pays de Galles, prévoit des pouvoirs généraux. Un mandat de perquisition PACE peut autoriser la recherche d'un dispositif électronique ou de données électroniques. Il semble que des dispositions générales similaires soient applicables en Irlande du Nord par le biais du Police and Criminal Evidence Order de 1989.<br><br>Il n'existe pas de disposition légale spécifique prévoyant la perquisition et la saisie de données informatiques stockées ou de données ou systèmes informatiques basés sur le cloud en Écosse. Les pouvoirs permettant la perquisition et la saisie de données informatiques stockées en Écosse découlent de pouvoirs de perquisition plus généraux préexistants en vertu de la loi de 1995 sur la procédure pénale (Écosse) et de la loi de 2016 sur la justice pénale (Criminal Justice Act).<br><br>En vertu du Regulation of Investigatory Powers Act 2000 (RIPA), qui s'applique à l'ensemble du territoire britannique, les autorités peuvent exiger d'une personne qu'elle divulgue une clé, un code, un mot de passe, un algorithme ou d'autres données pour accéder à des informations protégées, définies comme des données auxquelles il est impossible d'accéder ou qui ne peuvent être rendues intelligibles sans la clé.<br><br>En ce qui concerne les règles applicables en cas d'urgence ou d'autres circonstances urgentes, en vertu de l'APCE, les organismes chargés de l'application de la loi peuvent demander l'accès aux données détenues par une personne en cas d'urgence, ou demander que la personne conserve les données jusqu'à ce qu'un mandat de l'annexe 1 de l'APCE soit obtenu. | Le Royaume-Uni applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. Des dispositions spécifiques aux données et systèmes informatiques établissant un cadre juridique pour la perquisition et la saisie de données et systèmes informatiques applicables en Angleterre, en Écosse, au Pays de Galles et en Irlande du Nord pourraient permettre une plus grande clarté et renforcer la sécurité juridique |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les forces de l'ordre peuvent utiliser les données de connexion trouvées lors d'une perquisition légale pour accéder aux appareils électroniques sur place. L'article 49 de la loi RIPA permet aux autorités d'exiger d'une personne qu'elle divulgue une clé, un code ou un mot de passe pour un système informatique. Le non-respect d'une notification au titre de l'article 49 constitue une infraction au titre de l'article 53 de la RIPA.<br><br>Les autorités compétentes peuvent obtenir un mandat d'ingérence ciblée dans les équipements (TEI) en vertu de l'article 99(2) de l'Investigatory Powers Act 2016 (IPA) pour accéder à un système informatique et aux données qu'il contient au moyen d'un accès à distance secret. Les mandats d'ingérence dans l'équipement autorisent l'ingérence physique et à distance dans l'équipement dans le but d'obtenir des communications ou des données sur l'équipement. Un mandat TEI donne également à une personne le pouvoir légal d'intercepter la communication stockée.<br><br>Les ordonnances sont autorisées par un tribunal d'instance. Cette procédure semble être applicable dans tous les pays du Royaume-Uni.<br><br>Les TEI peuvent être émis par le secrétaire d'État (ou les ministres écossais), ou par un responsable de l'application de la loi tel que défini à l'annexe 6 de l'IPA. Les décisions d'émettre un mandat de brouillage d'équipement doivent également être approuvées par un commissaire judiciaire.<br><br>Les perquisitions de dispositifs électroniques dans des locaux au Royaume-Uni sont normalement effectuées par des agents mandatés par l'une des 43 forces de police territoriales d'Angleterre et du Pays de Galles, par la police écossaise, par le service de police d'Irlande du Nord ou par l'agence nationale de lutte contre la criminalité (National Crime Agency).<br><br>Il convient de noter qu'un rapport spécial préparé par la commission juridique indépendante sur les mandats de perquisition en Angleterre et au Pays de Galles, publié en 2020, recommandait expressément de "mettre à jour les pouvoirs d'application de la loi afin qu'ils s'appliquent plus clairement aux appareils et aux données électroniques et qu'ils permettent de saisir et de copier efficacement les preuves numériques". | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| États-Unis | La Constitution, les règles fédérales de procédure pénale et les lois constituent la base de la législation sur les perquisitions et les saisies. Normalement, un mandat de perquisition est nécessaire et est obtenu sur demande d'un juge indépendant. La demande doit être étayée par une déclaration sous serment des forces de l'ordre ou de l'accusation justifiant la perquisition (voir ci-dessous). Les perquisitions sont effectuées par des agents des forces de l'ordre habilités.<br><br>En cas d'urgence - par exemple, si les données risquent d'être détruites de manière imminente ou s'il existe un danger pour la vie ou des blessures corporelles graves - les forces de l'ordre peuvent être en mesure de perquisitionner et de saisir les données sans mandat.<br>Les forces de l'ordre ont généralement besoin d'un mandat ou d'un consentement pour utiliser des données d'identification acquises légalement.<br><br>L'accès à distance caché est possible, et nécessite généralement un mandat, si l'une des bases (dans les règles fédérales de procédure pénale) pour l'utilisation de l'accès à distance caché peut être établie. L'une de ces bases est que l'emplacement de l'ordinateur à perquisitionner "a été dissimulé par des moyens technologiques". | Les États-Unis appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. |

# 5 EXTENSION D'UNE RECHERCHE A UN AUTRE SYSTEME (EVALUATION DE L'ARTICLE 19.2)

Cette section évalue la mise en œuvre de l'article 19.2 :

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour garantir que, lorsque ses autorités procèdent à une perquisition ou accèdent de manière similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de croire que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour celui-ci, les autorités sont en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système.

## 5.1 Mise en œuvre de l'article 19.2 : vue d'ensemble

### 5.1.1 Mesures législatives et autres, procédure d'extension de la recherche - résumé

La Convention ne précise pas comment l'extension d'une recherche doit être autorisée ou entreprise, ce qui relève du droit national. Les parties ont donc adopté différentes approches.

De nombreuses Parties[43] ont mis en œuvre la mesure par des dispositions spécifiques dans leur droit interne.

De nombreux États[44] exigent qu'un tribunal autorise cette mesure.

En général, la plupart des États[45] utilisent la même procédure pour étendre une perquisition que pour d'autres perquisitions. Une Partie (Cabo Verde) a également précisé qu'elle n'avait pas encore appliqué la mesure d'extension de la recherche.

En revanche, la Suède, par exemple, s'appuie sur des compétences générales pour mettre en œuvre l'art. 19.1. Elle met en œuvre l'extension des recherches par le biais d'un pouvoir spécifique, intitulé "recherche à distance", qui permet de rechercher des données stockées dans un système d'information lisible en dehors de l'équipement de communications électroniques utilisé pour effectuer la recherche.

L'évaluation de l'article 19.2 porte uniquement sur la question de savoir si une Partie a développé le pouvoir d'extension de la recherche pour des situations purement nationales,

---

[43] Albanie, Australie, Belgique, Cabo Verde, Canada, Croatie, Fidji, France, Allemagne, Grèce, Hongrie, Israël, Japon, Lettonie, Monténégro, Pays-Bas, Norvège, Macédoine du Nord, Portugal, Roumanie, Sénégal, Sierra Leone, Slovénie, Espagne, Suède, Turquie, États-Unis.

[44] Albanie, Andorre, Arménie, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Canada, Costa Rica, Croatie, Chypre, République tchèque, Danemark, Estonie, France, Géorgie, Allemagne, Ghana, Islande, Israël, Japon, Lettonie, Liechtenstein, Lituanie, Monténégro, Pays-Bas, Nigeria, Norvège, Macédoine du Nord, Paraguay, Pérou, Philippines, Roumanie, Saint-Marin, Sénégal, Serbie, République slovaque, Slovénie, Espagne, Türkiye, Royaume-Uni, États-Unis.

[45] Albanie, Andorre, Australie, Autriche, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Costa Rica, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Géorgie, Grèce, Hongrie, Islande, Japon, Lettonie, Liechtenstein, Lituanie, Monténégro, Pays-Bas, Nigeria, Norvège, Panama, Pérou, Paraguay, Portugal, Roumanie, Sénégal, République slovaque, Slovénie, Türkiye, États-Unis.

c'est-à-dire lorsque le système informatique initial et un système informatique connecté se trouvent sur le territoire de cette Partie. Le fait qu'une partie puisse étendre la recherche à des systèmes informatiques situés en dehors de son territoire n'a pas d'incidence sur l'évaluation de la mise en œuvre de l'article 19.2. Cette évaluation concerne exclusivement les mesures qu'une partie est tenue de prendre au niveau national "sur son territoire".

L'article 19.2 ne traite pas des perquisitions et saisies transfrontalières, qui permettraient aux États de perquisitionner et de saisir directement des données stockées sur le territoire d'autres États sans devoir passer par les voies habituelles de l'entraide judiciaire. Le fait que l'article 19.2 ne traite pas de cette question est toutefois sans préjudice des situations dans lesquelles une Partie peut rapidement étendre la perquisition ou l'accès similaire à un autre système informatique sous certaines conditions sur le territoire d'autres Parties, comme c'est le cas dans plusieurs États (Andorre, Autriche, Belgique, Brésil, Estonie, Islande, Pays-Bas, Portugal, Sénégal, Espagne). Des informations sur ces mesures sont également incluses dans les sections suivantes de ce chapitre, car elles présentent toujours un intérêt pour le T-CY.

Conformément à l'article 39, paragraphe 3, aucune disposition de la Convention n'exige ou n'invite une Partie à établir des pouvoirs ou des procédures autres que ceux contenus dans la présente Convention, ni n'empêche une Partie de le faire. La Convention étant muette sur cette question, elle ne protégerait pas une Partie qui choisirait d'accéder à des systèmes informatiques situés sur le territoire d'autres Parties de la responsabilité légale en vertu des lois de la Partie dans laquelle le système informatique accédé pourrait être situé.

### 5.1.2 Motifs de croire que les données recherchées sont stockées dans un autre système sur son territoire

Lorsqu'elles établissent des motifs de croire que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur leur territoire, les Parties s'appuient soit sur des règles établies dans leur cadre juridique général (comme la République tchèque ou la Norvège), soit sur un texte couvrant spécifiquement la perquisition et la saisie de données informatiques (Australie), soit sur des lignes directrices qui mettent en œuvre les règles établies par le droit interne des Parties (Bosnie-et-Herzégovine), soit sur d'autres procédures opérationnelles normalisées (Pays-Bas).

De nombreuses Parties ne définissent pas nécessairement les termes "motifs de croire" ou "motifs raisonnables", mais leur droit interne énumère les conditions qui doivent être remplies pour autoriser une prolongation des perquisitions. Par exemple, la Belgique exige que la prolongation soit nécessaire pour établir la vérité sur l'infraction faisant l'objet de l'enquête. En outre, il ne doit pas exister d'autres mesures moins intrusives permettant d'atteindre le même résultat ou il doit y avoir un risque de perte de preuves sans cette prolongation. La prise d'autres mesures (par exemple, plusieurs mandats de perquisition) serait donc disproportionnée.

Plusieurs parties ont également indiqué que ces motifs sont déterminés en fonction des circonstances spécifiques de chaque cas.

Voici d'autres exemples d'éléments de motifs de croire (ou d'alternatives) qui ont été mentionnés dans les réponses des pays :

- Analyse et examen des paramètres de l'appareil contenant les données pertinentes (Autriche).

- Localisation du système informatique (Bosnie-Herzégovine).

- "Probabilité suffisante ou positive" que les données se trouvent à l'endroit indiqué (Costa Rica).
- Établir l'existence des données et, si possible, l'emplacement des autres appareils connectés (Croatie).
- Soupçon raisonnable que l'objet ou la personne important pour la procédure pénale se trouve dans l'appartement ou d'autres locaux utilisés pour l'hébergement ou appartenant à la personne (République tchèque).
- La perquisition peut conduire à la découverte d'un document ou de données à saisir ou à copier (Finlande).
- Données intéressant l'enquête, objets, documents et données informatiques utiles à la manifestation de la vérité (France).
- Perte imminente de données, existence d'un soupçon initial (Allemagne).
- Soupçon raisonnable que les données sont stockées dans un autre système informatique et que les données sont jugées pertinentes pour l'enquête (Hongrie).
- Faits indiquant la probabilité que des motifs de recherche existent (Monténégro).
- Situations dans lesquelles il est considéré comme plus probable qu'improbable que l'accusé ait commis l'infraction pénale en question (Norvège).
- Soupçon initial qu'un acte punissable a été commis et peut constituer un crime (Pérou).
- Informations sur la base desquelles les autorités peuvent raisonnablement supposer que les objets recherchés se trouvent dans les locaux donnés ou qu'un suspect s'y trouve (Pologne).
- "Indices" que les preuves se trouvent dans un lieu réservé ou ne sont pas librement accessibles au public (Portugal).
- Démonstration que les données recherchées ont été trouvées dans un autre système informatique et qu'elles étaient accessibles à partir du système initial (Portugal).
- Ensemble d'éléments ou de faits indiquant qu'il est probable que des données stockées dans un système autre que le système initial puissent contribuer à la manifestation de la vérité (Sénégal).
- Probabilité que le dispositif électronique contienne des données électroniques ou des traces d'un acte criminel qui peuvent être découvertes et qui sont pertinentes pour les procédures pénales (Slovénie).
- "Raisons fondées de considérer" - indications rationnelles qu'un deuxième système contenant des données pertinentes pour l'enquête est hébergé (Espagne).
- La recherche peut être étendue dans les cas suivants : a) dans un système d'information lisible que la personne raisonnablement soupçonnée de l'infraction est susceptible d'avoir utilisé ; ou b) les autorités peuvent effectuer une recherche s'il y a des raisons extraordinaires de penser que des informations potentiellement importantes peuvent être trouvées (Suède).

- Présomption de pertinence de la saisie et de soupçon suffisant. Celle-ci est établie sur la base de preuves concrètes (Suisse).

- Fondement de la conviction que les appareils ou les données à rechercher se trouvent dans le district concerné (États-Unis)

Voici quelques exemples de pratiques :

- Australie : motifs raisonnables

  La section 4 du chapitre 2 de la loi sur le développement durable stipule que pour demander un mandat d'accès à un ordinateur, un agent des services répressifs doit avoir des motifs raisonnables de soupçonner que

  - une ou plusieurs infractions pertinentes ont été, sont, sont sur le point d'être ou sont susceptibles d'être commises ; et
  - une enquête sur ces infractions est, sera ou sera probablement menée ; et
  - l'accès aux données contenues dans un ordinateur (l'ordinateur cible) est nécessaire, dans le cadre de cette enquête, pour permettre l'obtention de preuves :
    - la commission de ces infractions ; ou
    - l'identité ou la localisation des délinquants.

- Liechtenstein : il s'agit d'établir des motifs de croire

  Les autorités compétentes établissent généralement qu'elles ont des "raisons de croire" que les données recherchées sont stockées dans un autre système informatique ou dans une partie de son territoire, par les moyens suivants :

  - 1. Entretiens de la police avec des suspects ou des témoins.
  - 2. Les adresses IP indiquent des données de localisation différentes.
  - 3. Les moniteurs ou les stations d'accueil sont dépourvus d'ordinateur ou d'ordinateur portable.
  - 4. Toute autre référence du système informatique à des systèmes externes qui ne sont pas présents.

### 5.1.3 "Sur son territoire " et au-delà

Comme tous les articles de la section 2 de la Convention, l'article 19, paragraphe 2, ne concerne que les mesures qui doivent être prises au niveau national. Bien que l'extension des recherches à un autre territoire soit une mesure qui dépasse le cadre de la présente évaluation, cet aspect intéresse le T-CY depuis de nombreuses années.[46] C'est pourquoi des informations sur l'application de ce pouvoir au-delà de son territoire sont également fournies dans diverses parties du présent rapport.

Le droit interne de certaines Parties exige que le système connecté se trouve sur le territoire de l'État qui exécute la mesure (Arménie, Bosnie-Herzégovine (y compris l'entité de la Fédération de Bosnie-Herzégovine), Bulgarie, Costa Rica, Lettonie, Paraguay, États-Unis d'Amérique ).[47]

---

[46] Voir les travaux du T-CY sur l'accès transfrontalier aux données, sur les preuves en nuage, ou sur les enquêtes d'infiltration et l'extension des recherches. Comité de la Convention sur la cybercriminalité - Cybercriminalité

[47] Le droit des États-Unis d'Amérique (règle 41) prévoit des limitations géographiques aux circonstances dans lesquelles un tribunal peut autoriser un mandat de perquisition. La base la plus courante pour

Plus précisément, le Costa Rica entend par territoire un lieu physique (mer, air, terre, etc.) dans lequel il exerce ses pouvoirs souverains. Il exige que le système informatique dans lequel les données sont stockées se trouve sur son territoire ou que le fournisseur du service ait un bureau commercial ouvert au Costa Rica. Le Paraguay a fait référence à son exigence d'implication de l'élément de compétence territoriale dans le processus et au fait que le lieu de l'événement doit être indiqué. Le droit interne des États-Unis incorpore des limitations géographiques aux circonstances dans lesquelles un tribunal peut autoriser un mandat de perquisition.

Le droit interne des autres parties[48] n'impose pas que le système connecté se trouve sur le territoire de la partie qui exécute la mesure.

Cet aspect de l'évaluation ne concerne que la capacité d'une Partie à étendre les recherches sur son propre territoire physique, c'est-à-dire lorsque le système informatique initial et un système informatique connecté se trouvent sur le territoire de cette Partie. Toutefois, de nombreux États peuvent étendre la mesure à l'accès à des données éventuellement situées à l'étranger.[49] Ils ont indiqué que les conditions suivantes doivent normalement être remplies pour pouvoir rechercher des données susceptibles d'être stockées en dehors de leur territoire :

- Albanie : il est nécessaire de préciser la localisation possible des données, afin que le tribunal puisse autoriser la mesure.

- Andorre : point de connexion tel qu'une boîte aux lettres andorrane, un nuage connecté au système ou une adresse électronique, etc.

- Australie : accès autorisé par un fonctionnaire compétent du pays étranger.

- Belgique : les autorités doivent accomplir les actes à partir du territoire de la Belgique, notification de l'État concerné.

- Bosnie-Herzégovine (Republika Srpska) : si l'accès à partir du système informatique d'un suspect est autorisé, les systèmes informatiques auxquels il est possible d'accéder peuvent être perquisitionnés, même s'ils sont situés dans un autre pays.

- Brésil : le fait que des données puissent être stockées à l'étranger n'est pas un problème lors de l'accès au nuage, tant que les données stockées sont légalement accessibles depuis le territoire brésilien

---

demander un mandat est la situation où les biens à perquisitionner ou à saisir sont situés dans le district du juge qui délivre le mandat, qui sera en toutes circonstances sur le territoire des États-Unis. La règle 41 autorise les juges fédéraux à délivrer des mandats autorisant les forces de l'ordre à accéder à distance à des supports de stockage électronique aux États-Unis et à saisir des informations stockées électroniquement, que le support ou l'information se trouve ou non dans le district du juge, dans deux circonstances qui se produisent dans le cadre d'enquêtes sur la cybercriminalité. La première, applicable en l'espèce, est celle où l'emplacement du support ou de l'information à rechercher "a été dissimulé par des moyens technologiques".

[48] Albanie, Andorre, Australie, Autriche, Belgique, Bosnie-Herzégovine (applicable à l'entité de la Republika Srpska et au district de Brcko), Brésil, Croatie, République tchèque, Danemark, Estonie, Finlande, France, Géorgie, Hongrie, Allemagne, Islande, Israël, Italie, Japon, Lettonie, Liechtenstein, Lituanie, Monténégro, Pays-Bas, Nigeria, Norvège, Pérou, Pologne, Portugal, Sénégal, République slovaque, Slovénie, Espagne, Suède, Suisse, Türkiye.

[49] Voir également la section suivante sur la perte de la connaissance de la localisation.

- Croatie : la mesure s'applique à l'ordinateur et aux dispositifs connectés à l'ordinateur.

- République tchèque : le dispositif à partir duquel les données sont disponibles doit être situé sur son territoire ; les données peuvent être situées sur le territoire d'un pays étranger.

- Danemark : s'applique aux données accessibles à partir de l'ordinateur de la personne (même si les messages numériques n'ont pas encore été obtenus techniquement auprès du fournisseur d'accès à l'internet).

- Estonie : aucune limitation.

- Fidji : les pouvoirs s'appliquent aux données trouvées ou accessibles à partir de Fidji.

- Finlande : les pouvoirs s'appliquent aux données susceptibles d'être localisées à l'intérieur des frontières géographiques de la Finlande. Parfois, une base au cas par cas est envisagée dans les cas où les données peuvent être consultées (mais pas nécessairement stockées) en Finlande.

- France : dans le cas d'un nuage - si le matériel informatique permet une connexion à un service à distance, les enquêteurs pourront en principe y accéder. Si les données sont stockées à l'étranger, les autorités utilisent l'article 32 de la Convention sur la cybercriminalité.

- Géorgie : l'accès doit être effectué à partir de son territoire et doit être licite (y compris en utilisant des applications auxquelles on s'est connecté pendant les recherches).

- Allemagne : dans les cas d'informatique en nuage, lorsqu'il n'est pas possible de déterminer où se trouvent les données.

- Hongrie : le système informatique à partir duquel les données sont accessibles doit être situé sur son territoire.

- Liechtenstein : lorsque l'accès à un système informatique distant (par exemple, un service dans un nuage) est disponible à partir de son territoire.

- Luxembourg : toutes les données stockées ou accessibles sur le territoire luxembourgeois ou à partir de celui-ci peuvent être consultées et recherchées.

- Malte : tout acte commis en dehors de Malte qui aurait constitué une infraction s'il avait été commis à Malte. si l'acte affecte un ordinateur, un logiciel, des données ou des documents d'appui situés à Malte ou liés ou connectés d'une quelconque manière à un ordinateur situé à Malte.

- Norvège : mesure prise sur le territoire norvégien à l'encontre d'un citoyen norvégien ou d'une entreprise norvégienne ayant des bureaux en Norvège ; les données doivent être librement extraites du lieu de stockage à l'étranger, rester sur le serveur étranger et aucune modification ne doit être apportée aux informations.[50]

- Philippines : Toute partie du système informatique utilisé doit se trouver dans la juridiction des Philippines, y compris à l'intérieur du pays et dans la zone maritime

[50] Voir annexe, Cour suprême de Norvège - Ordonnance - HR-2019-610-A (affaire Tidal).

- Pologne : il n'est pas possible d'établir où les données sont stockées.

- Portugal : une recherche peut être étendue, quelle que soit la localisation du système distant.

- Sénégal : sous réserve des accords internationaux applicables, un juge peut collecter des données stockées dans un système situé en dehors du territoire sénégalais, à condition que ce système soit accessible à partir d'un système ayant fait l'objet d'une première recherche. Cette extension doit être nécessaire à la manifestation de la vérité ou il doit y avoir des risques de perte de preuves. L'extension ne doit concerner que les systèmes auxquels ont accès les personnes autorisées à utiliser le système initial. Le juge doit informer le responsable du système, sauf si son identité ou son adresse est introuvable.

- Espagne : ce qui est déterminant, ce n'est pas l'emplacement physique des données, mais l'endroit d'où elles sont accessibles.

- Suisse : si les identifiants d'accès sont acquis légalement et que les conditions d'une recherche sont remplies, un accès à distance est généralement possible s'il est effectué à partir de la Suisse

- Türkiye : le système informatique "utilisé par le suspect" sur le territoire turc a un lien avec le système "utilisé par le suspect" dans un autre pays.

- Royaume-Uni : les mandats délivrés en vertu de l'IPA ont un effet extraterritorial. Pour l'ITE, cette question est couverte par les articles 126 et 127 de la loi sur la protection des renseignements personnels.

- États-Unis : l'emplacement du média ou de l'information à rechercher "a été dissimulé par des moyens technologiques".

D'autres parties ([51] ) ont déclaré que cet aspect n'était pas abordé dans leur législation nationale ou qu'elles procédaient en fonction des circonstances spécifiques de chaque cas.

Bien qu'il n'y ait pas d'exigence affirmative qu'un système connecté soit situé sur les territoires du Chili, du Pérou, de Saint-Marin, de la Sierra Leone et de la République slovaque, ces parties ont souligné que l'applicabilité territoriale de leur législation nationale est limitée à leur sol et ont précisé qu'en ce qui concerne les données situées à l'étranger, d'autres mécanismes disponibles en vertu du droit international, tels que l'accord multilatéral sur le blanchiment d'argent, doivent être appliqués.

Le Canada a déclaré que son droit est limité par le principe de territorialité et que l'extension extraterritoriale d'une perquisition ne serait autorisée qu'après la promulgation d'une loi autorisant explicitement une telle extension. La Grenade, la République de Moldavie et les Tonga ont indiqué que les perquisitions/saisies sont limitées aux données ou systèmes se trouvant physiquement sur leur territoire.

### 5.1.4 Perte (connaissance) de la localisation / "localisation inconnue".

Grâce à l'informatique en nuage, les autorités de justice pénale sont plus souvent confrontées à des problèmes lorsque l'emplacement des données n'est pas connu ou qu'il n'est pas possible

[51] Islande, Israël, Japon, Lituanie, Monténégro, Maroc, Slovénie.

de les localiser.[52] Il arrive même que le fournisseur de services ne connaisse pas l'emplacement exact des données. Compte tenu de l'importance d'une réponse efficace de la justice pénale face aux difficultés croissantes d'obtention de preuves dans les affaires de "perte (de connaissance) de la localisation", apprendre comment un parti aborde ces situations peut être bénéfique pour d'autres.

En général, les parties ont souligné qu'elles faisaient d'abord tous les efforts raisonnables pour connaître l'emplacement des données. Les Parties ont également souligné qu'elles utilisent les mécanismes de coopération internationale chaque fois que cela est possible. Quelques États n'ont pas expliqué comment ils procèdent lorsque ces processus échouent ou ne peuvent être utilisés. Cependant, la plupart des Parties ayant répondu ont déclaré que, si elles n'avaient pas d'autre choix, elles étendraient sciemment une recherche à un autre pays *dans certaines circonstances.* Ces circonstances peuvent être très limitées. La section ci-dessous détaille les approches des États sur ces questions.

En cas de perte (de connaissance) de la localisation, de nombreuses parties[53] continuent à faire comme si les données se trouvaient sur leur territoire.

Toutefois, certaines parties ont précisé les éléments suivants qui doivent être respectés :

- Australie : la personne qui exécute un mandat d'accès à un ordinateur est physiquement présente en Australie. En outre, le lieu où les données sont conservées est inconnu ou ne peut être raisonnablement déterminé.

- Canada : l'emplacement des données n'est pas connu, par exemple dans certains scénarios du "dark web" ou lorsqu'un système informatique a établi des tunnels cryptés vers des dispositifs de stockage de données situés dans des lieux inconnus.

- République tchèque : possibilité de saisir et de rechercher des données disponibles à partir d'un appareil situé en République tchèque.

- Danemark : si le délit est soumis au droit danois de punition, s'il fait l'objet d'une enquête par les autorités danoises et si le délit a un effet au Danemark.

- Fidji : si le mandat de perquisition le permet techniquement, les données peuvent être saisies, mais si d'autres méthodes techniques doivent être utilisées, un autre mandat de perquisition doit être demandé jusqu'à ce que toutes les voies techniques soient épuisées.

- France : ce qui est déterminant, c'est l'endroit d'où les autorités ont accès et non la localisation des données.

- Allemagne : la mesure ne peut être utilisée que lorsqu'il n'est pas possible de déterminer où se trouvent les données.

---

[52] Voir par exemple le Comité de la Convention sur la cybercriminalité (T-CY), Criminal justice access to electronic evidence in the cloud : Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group, 16 septembre 2016. Voir également Sansom, Gareth (2008) sur le problème de la "localisation" dans le cyberespace.
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/TCY/
Gareth%20Samson%20Site web%20Location.pdf

[53] Allemagne, Australie, Autriche, Bosnie-Herzégovine, Canada, Croatie, Danemark, Espagne, Estonie, France, Hongrie, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Sénégal, Slovénie, Suède, Suisse, Turquie.

- Hongrie : le système d'information par lequel les données sont accessibles doit se trouver en Hongrie.

- Maurice : L'approche mauricienne dépend du type de données recherchées et de leur localisation possible. "S'il s'agit d'un domaine, il y a une chance de récupérer les données à condition qu'elles soient accessibles depuis l'île Maurice.

- Pays-Bas : des mesures raisonnables sont prises pour établir une localisation ; ces mesures doivent être proportionnelles.

- Espagne : ce qui est décisif, c'est l'endroit d'où les données sont accessibles.

- Suède : la mesure est prise dans le cadre d'une enquête criminelle suédoise et est donc liée à une suspicion de crime relevant de la juridiction suédoise ; la mesure est prise à l'aide d'un équipement situé en Suède ; la mesure est prise de manière à ce que l'information recherchée ne soit pas effacée ou affectée d'une autre manière en ce qui concerne son contenu.

- Suisse : ce qui est déterminant, c'est l'endroit d'où l'on accède aux données.

- Türkiye : le système informatique "utilisé par le suspect" sur le territoire turc a un lien avec le système "utilisé par le suspect" dans un autre pays.

- États-Unis : l'emplacement du média ou de l'information à rechercher "a été dissimulé par des moyens technologiques".

Quelques États (Chili, Costa Rica, Paraguay) ont indiqué que dans de tels cas, ils ne recherchent pas les données si la localisation ne peut être déterminée. Les Parties utilisent divers moyens pour déterminer ces données.

Plus précisément, le Costa Rica a déclaré qu'il essayait de trouver le siège du fournisseur afin d'identifier le pays concerné. Si le lieu ne peut être déterminé, l'affaire est rejetée. Le Paraguay a indiqué qu'il applique le principe in dubio pro reo et rejette l'affaire. La Grenade a indiqué que si la localisation ne peut être déterminée après que tous les moyens d'obtenir cette information ont été mis en œuvre, la procédure est arrêtée.

Un certain nombre d'Etats (Andorre, Belgique, Bulgarie, Finlande, Israël, Japon, Lettonie, Norvège, Royaume-Uni, Etats-Unis) procèdent au cas par cas et l'exécution de la mesure dépend de plusieurs éléments. Une Partie (République dominicaine) a déclaré que dans les cas où l'emplacement exact des données est inconnu, une demande de conservation est faite au fournisseur de services, qui indiquera l'emplacement des données stockées. L'autre partie (Sierra Leone) a indiqué que, jusqu'à présent, elle n'a pas rencontré de situations dans lesquelles il n'a pas été possible de déterminer où les données recherchées sont stockées.

Certains de ces États ont indiqué les éléments suivants qui sont pris en compte par les autorités lorsqu'elles exercent ces pouvoirs :

- Belgique : Accès depuis la Belgique, (notification non requise, l'Etat concerné n'étant pas connu).

- Bulgarie : tente de déterminer l'emplacement des données à distance en utilisant tous les moyens possibles ; les étapes suivantes dépendent de la décision de l'autorité qui poursuit les données.

- Japon : L'article 32 de la Convention sur la cybercriminalité est respecté, il existe un consentement légal et volontaire d'une personne ayant l'autorité légale de divulguer

les enregistrements. Cette approche est également confirmée par un précédent judiciaire.

- Norvège : tente d'obtenir des informations auprès d'autres États, d'EUROPOL et des CERT. Lorsque cela est possible, l'article 32 de la Convention sur la cybercriminalité est utilisé pour obtenir le consentement.

Quelques États ont indiqué que la question n'est pas abordée dans leur droit interne (Géorgie) ou qu'ils utilisent des procédures opérationnelles pour déterminer la localisation des données (Panama, République slovaque) sans préciser davantage comment ils procèdent si la localisation des données ne peut être déterminée.

Voici quelques exemples de pratiques :

- Bosnie-Herzégovine : étapes de l'identification des données

  Les autorités doivent d'abord tenter d'identifier l'emplacement des données recherchées en utilisant tous les moyens disponibles, tels que la recherche d'adresses IP, la cartographie du réseau et d'autres méthodes techniques. Si les autorités ne sont pas en mesure de déterminer l'emplacement des données en utilisant ces méthodes, elles doivent alors soumettre au tribunal une demande de mandat de perquisition et de saisie des données de tout système informatique qui peut raisonnablement contenir les données recherchées.

- Finlande : éléments à prendre en compte lors de la mise en œuvre de la mesure

  Dans chaque cas, les autorités s'efforcent d'établir l'emplacement des données par tous les moyens disponibles. Si la localisation n'est pas établie, les points suivants, entre autres, sont pris en considération en fonction du cas :

  - nature de l'infraction faisant l'objet de l'enquête et les éventuels accords bilatéraux et multilatéraux contraignants au niveau international ;
  - le respect du principe de diligence raisonnable et des obligations qui en découlent
  - la nationalité et le pays de résidence permanente du suspect ;
  - le lieu de commission de l'infraction, les liens éventuels avec un autre État, le lieu où le dommage s'est produit et la localisation des victimes et des témoins ;
  - l'impact de la mesure et des procédures sur la souveraineté de l'autre État ;
  - l'impact de la mesure et des procédures sur les personnes cibles ;
  - la mesure n'interfère pas dans les affaires intérieures de l'autre État à quelque titre que ce soit, ni ne vise des informations ou des services nécessaires à l'accomplissement des tâches essentielles de l'autre État ;
  - la mesure ne causera aucun dommage matériel, ne supprimera ni ne modifiera les données et ne provoquera aucun dysfonctionnement des appareils cibles ;
  - les recours juridiques dont disposent les personnes visées.

## 5.2 Mise en œuvre de l'article 19.2 - Évaluation

Les réponses aux questions suivantes du questionnaire ont été évaluées :

- 2.2.1 Veuillez résumer les mesures législatives ou autres que vous avez prises pour garantir que vos autorités sont en mesure d'étendre la recherche telle que décrite à l'article 19.2.
- 2.2.2 Veuillez résumer la procédure (y compris les autorisations requises et les techniques d'investigation appliquées) pour étendre une recherche ou un accès similaire à un autre système dans la pratique.
- 2.2.3 Veuillez résumer la manière dont votre cadre juridique applique l'élément "motifs de croire" de l'article 19, paragraphe 2, y compris la manière dont les autorités compétentes établissent généralement qu'elles ont des "motifs de croire" que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur son territoire.
- 2.2.4 Veuillez résumer la manière dont votre cadre juridique applique l'élément "sur son territoire" de l'article 19.2, en indiquant notamment si votre cadre impose ou non une exigence positive selon laquelle le système connecté doit se trouver sur votre territoire.54
- 2.2.5 Comment procédez-vous lorsqu'il n'est pas possible de déterminer où les données recherchées sont stockées ("perte de (connaissance de) situations de localisation") ?

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Albanie | L'Albanie a indiqué que les pouvoirs spécifiques d'extension de l'enregistrement sont prévus à l'article 208/A, paragraphe 2, du CPC.<br><br>La procédure est la même que pour la saisie d'un système informatique sur le territoire : le tribunal autorise le procureur à sa demande, puis le procureur ou l'officier de police judiciaire procède à la perquisition et à la saisie. Le procureur peut également désigner un expert si nécessaire. Les techniques d'enquête dépendent des spécificités de la situation et du type de données informatiques recherchées.<br><br>En ce qui concerne la manière dont les autorités appliquent les "motifs de croire", l'Albanie a indiqué que l'article 208/a du CPC stipule que c'est le tribunal qui décide s'il existe des motifs raisonnables de croire que les données informatiques sont stockées dans un autre système informatique. Il n'y a pas de définition des motifs raisonnables et la décision est souvent prise au cas par cas. | L'Albanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

54 Voir les paragraphes 192 et 193 du rapport explicatif.

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En ce qui concerne la manière dont les autorités appliquent l'expression "sur son territoire", l'Albanie a indiqué que l'article 208/a du CPC ne précise pas l'emplacement du système informatique initial, ni l'emplacement du système informatique connecté au système informatique initial. Il n'y a donc pas d'exigence procédurale liée à la localisation du système informatique, s'il est légalement accessible à partir du système informatique initial.<br><br>Il n'existe aucune disposition procédurale pour le cas où il n'est pas possible de déterminer où les données recherchées sont stockées, les "situations de perte de connaissance de la localisation", mais dans l'interprétation de l'article 208/A du CPC, il est nécessaire de spécifier la localisation possible des données et du système informatique pour que le tribunal autorise la perquisition et la saisie.<br><br>Par ailleurs, l'article 32 du Code pénal peut être utilisé pour saisir des données accessibles au public dont la localisation est indéterminée. 32 du Code de procédure pénale peut être utilisé pour saisir des données accessibles au public dont la localisation est indéterminée. | |
| Andorre | Il n'existe pas de législation spécifique concernant l'article 19.2. 19.2. Les procédures de recherche et les techniques d'enquête décrites précédemment sont également applicables ici. Les juges peuvent autoriser de telles extensions, par exemple à une partie du nuage liée au système initialement recherché.<br><br>Les motifs de croire sont établis de différentes manières habituelles, par exemple par des informations provenant d'un tiers ou par des preuves obtenues lors de la recherche initiale.<br><br>Les systèmes d'information ne peuvent faire l'objet d'une recherche que s'ils se trouvent sur le territoire de l'Andorre. Toutefois, les données situées en dehors du territoire andorran peuvent faire l'objet d'une recherche si elles sont connectées d'une manière ou d'une autre à un système situé dans le pays - par exemple, par une adresse électronique ou une partie liée du nuage. Si la localisation des données ne peut être déterminée, l'Andorre adopte une approche au cas par cas. | L'Andorre applique les pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2.<br>Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Argentine | Le CPC au niveau fédéral n'a pas de règle spécifique concernant l'article 19.2, mais le pouvoir procédural est mis en œuvre par le biais de pouvoirs généraux et de pratiques acceptées. L'Argentine a signalé que certaines législations provinciales, comme celles de Salta et de Mendoza, prévoient des règles spécifiques. | L'Argentine applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2.<br>Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Arménie | L'Arménie a indiqué qu'elle avait mis en œuvre des mesures législatives et autres pour permettre l'extension des recherches, comme le prévoit l'article 19, paragraphe 2, lorsqu'il y a des raisons de croire que les données se trouvent sur le territoire et si les données sont légalement accessibles à partir du système initial ou disponibles pour celui-ci. L'Arménie mentionne l'article 236 comme base juridique pertinente pour la mise en œuvre de l'article 19, paragraphe 2. 19.2. Toutefois, la manière dont cette disposition répond aux exigences de l'article 19, paragraphe 2, n'est pas claire. 19.2.<br><br>En règle générale, les autorités demanderont une autorisation judiciaire (sur la base des motifs susmentionnés) pour étendre la recherche. Si la recherche étendue est autorisée, diverses techniques d'investigation peuvent être utilisées, y compris la demande de coopération d'un propriétaire ou d'un administrateur, l'émission d'assignations ou de mandats, ou l'utilisation de moyens techniques pour accéder aux données et les récupérer.<br><br>Les "raisons de croire" sont interprétées comme des motifs raisonnables indiquant que les données recherchées sont stockées sur le territoire de l'Arménie. Pour ce faire, les autorités s'appuient généralement sur des informations d'enquête, des renseignements ou des preuves, qui peuvent inclure des informations obtenues lors d'une perquisition initiale, des informations provenant d'informateurs, des analyses techniques ou d'autres facteurs.<br><br>En vertu du cadre juridique, l'élément "sur son territoire" exige que les données soient censées être stockées sur le territoire arménien et que le système connecté soit situé dans la juridiction territoriale. | Bien qu'il semble que l'Arménie applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2, la manière dont l'article 236 répond aux exigences de l'article 19.2 n'est pas claire. 236 répond aux exigences de l'Art. 19.2. de la CB. Des dispositions plus spécifiques permettraient une plus grande clarté et renforceraient la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les autorités arméniennes ne peuvent pas agir lorsque la localisation des données ne peut pas être déterminée. La connaissance de l'emplacement des données est une condition obligatoire (comme dans le cas d'une recherche traditionnelle où l'adresse exacte est requise). | |
| Australie | Plusieurs articles de la loi sur les infractions et de la loi sur le développement durable permettent aux forces de l'ordre présentes sur les lieux de la perquisition d'accéder à des données à distance. Ces perquisitions doivent être effectuées conformément aux procédures décrites ci-dessus. L'Australie utilise une norme de suspicion de "motifs raisonnables que les données constituent des éléments de preuve".<br>Les lois australiennes n'exigent pas explicitement que le système connecté se trouve en Australie. Un mandat peut être délivré pour permettre la perquisition d'une personne dont la localisation ne peut être prédite ; l'accès à distance ne dépend pas de la localisation des données. La loi sur le développement durable prévoit des perquisitions extraterritoriales dans certaines circonstances, avec l'autorisation de l'État étranger concerné et un mandat australien en bonne et due forme. | L'Australie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'art. 19.2. |
| Autriche | Le pouvoir de saisir les données d'un support de stockage comprend les données accessibles à partir de ce support, mais non stockées sur celui-ci. L'ordonnance doit étendre la saisie à d'autres supports et systèmes. Cette procédure s'applique lorsqu'il y a des raisons de penser que les autres supports ou systèmes se trouvent en dehors de l'Autriche ; le cadre juridique n'impose pas d'exigence positive quant à leur présence sur le territoire autrichien. De même, la perte de connaissance de l'emplacement des données n'empêche pas la saisie.<br><br>L'élément "motifs de croire" est établi sur la base des circonstances de l'affaire. | L'Autriche applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Azerbaïdjan | L'article 19.2 ne contient pas de dispositions spécifiques concernant l'extension des perquisitions, mais les dispositions générales relatives aux perquisitions et aux saisies s'appliquent. Les autorités chargées de l'application de la loi ou de l'enquête doivent présenter des preuves et des justifications à un tribunal pour démontrer la nécessité et la pertinence de l'extension. Ces présentations comprennent souvent des détails sur l'enquête, la pertinence des données recherchées et le lien potentiel entre le système initial et le second système. Si les preuves le justifient, une autorité judiciaire rendra une ordonnance d'extension, décrivant la portée de l'extension et désignant les systèmes auxquels il faut accéder ainsi que la date limite de la | L'Azerbaïdjan applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | recherche. Les services répressifs ou d'enquête exécutent alors l'accès dans le cadre des paramètres de l'ordonnance.<br><br>Les "raisons de croire" sont mises en œuvre en tant que "raisons suffisantes", conformément à l'article 242, paragraphe 1, du code de procédure pénale, pour croire que des éléments peuvent avoir une importance probante et se trouver à certains endroits ou avec certaines personnes. Cette raison est démontrée par la présentation de preuves et d'informations obtenues dans le cadre d'une enquête, y compris des métadonnées, des enregistrements de communications ou une surveillance ou un contrôle numérique. Il est alors possible de demander une ordonnance d'extension de la perquisition.<br><br>L'expression "sur son territoire" est appliquée par le biais de l'article 3 du CPC, qui prévoit que le CPC est applicable sur l'ensemble du territoire de la république sans limitation, sauf si d'autres articles du code prévoient des exceptions. Le code de procédure pénale n'impose pas explicitement l'obligation pour un système raccordé de se trouver sur le territoire. L'application des règles régissant le champ d'application territorial de la législation en matière de procédure pénale est déterminée par les accords internationaux dont l'Azerbaïdjan est signataire. Ainsi, bien que l'application par défaut soit de rester sur le territoire, il est suggéré que le cadre juridique permette une certaine flexibilité dans le traitement des aspects transfrontaliers des enquêtes, ce qui pourrait permettre des scénarios dans lesquels le système connecté se trouve physiquement en dehors des frontières territoriales, mais dans le champ d'application des accords.<br><br>L'Azerbaïdjan déploie des efforts considérables pour localiser les données lorsque leur emplacement n'est pas clair (voir réponses). Il n'a pas indiqué son approche lorsque la localisation des données ne peut être déterminée. | |
| Belgique | Les articles 88ter et 39bis prévoient qu'un juge d'instruction peut ordonner l'extension d'une recherche dans un système d'information à un système connecté (dans la mesure où il est accessible aux utilisateurs normalement autorisés), même si le second système se trouve dans un lieu différent ou en dehors du territoire belge. Ces articles précisent les procédures et les conditions préalables requises, y compris le fait qu'aucune méthode d'investigation autre que l'extension de la recherche ne sera adéquate. S'il s'avère que les données recherchées se trouvent en dehors de la Belgique, que leur emplacement soit identifiable | La Belgique applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | ou non, les données sont simplement copiées, et non rendues inaccessibles. L'État étranger concerné est alors notifié s'il est connu. Ces procédures doivent être autorisées par un juge d'instruction.<br><br>L'expression "raisons de croire" n'est pas définie dans la loi, mais les conditions préalables à l'action figurent dans les lois, comme décrit précédemment.<br><br>Le système belge n'impose pas qu'un système soit situé sur le territoire belge. Il présume plutôt que les enquêtes doivent être limitées au territoire national, sauf dans la mesure où, comme indiqué, la Belgique a adopté une approche "prudente mais pragmatique" de l'extraterritorialité. | |
| Bénin | L'article 587/1 de la loi sur le code numérique prévoit expressément l'extension des recherches à un second système accessible au premier. En pratique, le juge d'instruction donne l'ordre approprié et celui-ci est exécuté par un service d'enquête de la police, auquel peut être adjoint un expert technique.<br><br>Les "raisons de croire" de l'article 19.2 se fondent sur des indices concrets et raisonnables qui justifient l'émission d'un ordre de perquisition par un juge d'instruction ou un procureur. L'article 587 de la loi sur le code numérique couvre expressément les données stockées sur le territoire béninois qui sont utiles à la manifestation de la vérité. Comme indiqué plus haut, l'article prévoit la perquisition des systèmes ou des supports de stockage à la disposition du premier système.<br><br>Par "sur son territoire", on entend soit qu'un système est situé partiellement ou totalement sur le territoire béninois, soit qu'un système est situé partiellement ou totalement en dehors du territoire béninois, mais qu'il est disponible à partir du territoire béninois.<br>L'article 587/2 précise que, si les autorités savent à l'avance qu'un système se trouve en dehors du territoire national, le juge d'instruction obtient les données par commission rogatoire.<br><br>Lorsque la localisation des données ne peut être déterminée mais qu'elles sont stockées dans un nuage ou dans un autre service externe, les autorités peuvent s'adresser au fournisseur de services de la cible en lui communiquant toutes les informations disponibles afin d'obtenir sa coopération. Dans les cas où les informations disponibles permettent d'accéder aux données sans qu'il soit nécessaire de les géolocaliser au | Le Bénin applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | préalable, les autorités peuvent procéder à l'accès et déterminer la localisation ultérieurement si la preuve est indispensable. | |
| Bosnie et Herzégovine | La Bosnie-Herzégovine n'a pas de mesures législatives ou autres spécifiques concernant la prolongation des perquisitions, comme le prévoit l'article 19.2. Après une première perquisition d'appareils dûment scellés, les enquêteurs peuvent déterminer qu'une partie d'un système connecté se trouve dans un lieu différent de celui où la perquisition a eu lieu. Dans ce cas, un second mandat sera obtenu si les données sont censées se trouver dans le pays. Dans le cas contraire, il sera fait appel à l'entraide judiciaire.<br><br>Dans les codes de la Bosnie-Herzégovine, de la Fédération de Bosnie-Herzégovine et du district de Brcko, les procédures d'extension de la recherche suivent les règles habituelles décrites ci-dessus.<br><br>Le code de procédure pénale de la Republika Srpska ne contient aucune disposition particulière concernant l'extension des recherches aux systèmes connectés. La raison en est la définition de la loi du "système informatique", qui est défini comme tout dispositif ou ensemble de dispositifs (électroniques) mutuellement connectés ou liés. Il n'y a donc pas d'exigences particulières. Les procédures normales sont suivies. S'il existe des raisons suffisantes de penser que le système connecté est impliqué dans la commission d'une infraction pénale, une nouvelle décision de justice peut être obtenue.<br><br>En Bosnie-Herzégovine et dans la Fédération de Bosnie-Herzégovine, les "motifs de croire" sont généralement interprétés de la même manière, c'est-à-dire que la demande de mandat doit, dans chaque cas, inclure des faits concrets (tels que le type de données recherchées) tendant à indiquer que les données souhaitées se trouveront dans le système à perquisitionner. La norme en vigueur en Republika Srpska est plus exigeante. Au lieu de "raisons de croire", pour permettre l'extension de la recherche, la loi exige des "raisons suffisantes de soupçonner" que les données se trouvent à distance.<br><br>Bosnie-Herzégovine et Fédération Les autorités de Bosnie-Herzégovine ne peuvent étendre une recherche que si l'on pense que les données se trouvent sur le territoire. Dans le district de Brcko, la loi ne précise pas si ces limites territoriales s'appliquent ; en Republika Srpska, il n'y a pas de restrictions légales concernant les limites territoriales. En d'autres termes, en Republika Srpska, les systèmes d'un autre pays | La Bosnie-Herzégovine applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2.<br>Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | peuvent faire l'objet d'une recherche s'ils sont liés à un système initial qui fait l'objet d'une recherche conformément à la procédure en vigueur et s'ils peuvent être atteints à partir de ce système.<br><br>Les quatre codes en vigueur dans le pays n'envisagent pas tous spécifiquement les cas de "perte de connaissance" de la localisation. Le code de Bosnie-Herzégovine autorise les autorités à effectuer une recherche de données dont la localisation est inconnue, mais seulement après avoir démontré à un tribunal une tentative détaillée et rigoureuse de déterminer la localisation. Dans ce cas, les procédures légales habituelles doivent être suivies. Le code du district de Brcko, en ce qui concerne ce type de recherches, ne tient pas compte de la localisation des données et se concentre sur la localisation du propriétaire ou du contrôleur des données. | |
| Brésil | Bien que la mesure décrite à l'article 19, paragraphe 2, ne soit pas prévue par la législation brésilienne, les autorités peuvent étendre une perquisition ou un accès similaire à un autre système informatique ou à une partie de celui-ci si elles ont des raisons de croire que les données recherchées sont stockées dans un autre système ou une partie de celui-ci sur leur territoire et que ces données sont légalement accessibles à partir du système d'origine ou disponibles pour celui-ci. L'extension de la perquisition doit être autorisée par une ordonnance du tribunal ou un mandat de perquisition et doit respecter les exigences et procédures spécifiques établies par le droit brésilien, sur la base de l'article 240 ordinaire pour une perquisition et une saisie générales. Même si elle n'est pas expressément prévue dans un article du code de procédure pénale, elle a été acceptée par la jurisprudence.<br><br>En pratique, l'extension d'une perquisition ou d'un accès similaire à un autre système au Brésil nécessite une ordonnance ou un mandat du tribunal, fondé sur une suspicion raisonnable de commission d'une infraction, spécifiant le lieu de la perquisition, le type de données ou d'informations à consulter et la durée de la perquisition. Les autorités peuvent utiliser des techniques de police scientifique pour localiser et accéder aux données ou informations pertinentes sur l'autre système, ou recourir à des opérations d'infiltration ou à des informateurs confidentiels pour recueillir des informations sur l'autre système ou sur les données ou informations recherchées.<br><br>Les "raisons de croire" signifient qu'il y a suffisamment d'éléments pour étayer cette affirmation. | Le Brésil applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'expression "sur son territoire" est appliquée d'une manière qui exige généralement que le système connecté soit situé au Brésil. Le droit brésilien n'exige pas que le système connecté soit situé au Brésil, mais les autorités doivent avoir compétence sur le système ou les données recherchées pour étendre légalement la recherche ou l'accès similaire à ce système. Le droit brésilien reconnaît la compétence sur les données informatiques stockées ou accessibles sur son territoire, que le système informatique lui-même soit ou non physiquement situé au Brésil. Par conséquent, si les autorités ont des "motifs raisonnables" de croire que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci au Brésil, et que les données sont légalement accessibles à partir du système d'origine ou disponibles pour celui-ci, elles peuvent étendre la perquisition ou l'accès similaire à ce système, même s'il est physiquement situé dans une autre juridiction<br><br>Dans les cas où les autorités brésiliennes ne peuvent pas déterminer où les données demandées sont stockées, ou lorsque l'emplacement des données est inconnu, elles peuvent utiliser diverses techniques d'investigation pour essayer de localiser les données, en utilisant l'expertise technique pour effectuer une analyse approfondie du ou des systèmes informatiques en question afin d'essayer de localiser les données recherchées. Cela peut inclure l'utilisation d'outils de récupération de données, l'analyse des journaux système, l'examen des métadonnées et d'autres techniques. Dans le cas d'une perquisition et d'une saisie nécessitant l'accès au nuage, le fait qu'il puisse être stocké à l'étranger n'est pas un problème tant que les données stockées sont accessibles depuis le territoire brésilien et qu'une autorisation judiciaire a été accordée. Si l'on sait que les systèmes informatiques ou les données recherchées se trouvent en dehors du Brésil, les mécanismes d'entraide judiciaire peuvent être utilisés pour demander l'assistance d'autorités étrangères afin de localiser les données. | |
| Bulgarie | Aucune législation spécifique n'a été adoptée. Bien que les extensions de recherches soient généralement effectuées sans autorisation préalable, elles doivent être approuvées par le tribunal dans les 24 heures. Dans ce cas, la présence de données informatiques pertinentes sur un autre système d'information sera décrite dans le protocole créé lors de la perquisition initiale.<br><br>En règle générale, l'expert en informatique ou l'officier de police présent sur les lieux de la perquisition initiale déclare qu'il y a des "raisons de croire" que des données informatiques pertinentes pour l'affaire se trouvent dans un autre lieu. | Il semble que la Bulgarie étende les perquisitions sur la base des dispositions applicables pour autoriser les perquisitions. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Si l'on découvre que les données sont stockées à l'étranger, d'autres mesures de coopération internationale sont prises, à savoir la conservation accélérée des données conformément à la Convention de Budapest.<br><br>Les autorités s'efforcent de recueillir autant de preuves que possible pour déterminer où les données sont stockées. Les autorités procèdent au cas par cas.<br><br>Les dispositions applicables sont mentionnées au point 4.2. | |
| Cabo Verde | Le Cabo Verde a informé que sa CL permet l'extension d'une recherche à un autre système informatique, ou à une partie différente du système faisant l'objet de la recherche, à condition que les données soient légitimement accessibles à partir du système initial. Cette extension nécessite une autorisation ou un ordre de l'autorité compétente, en vertu des paragraphes 1 et 2 de l'article 17, n° 5. S'il s'avère nécessaire de produire des preuves au cours de la procédure de découverte de la vérité, l'autorité judiciaire compétente peut autoriser ou ordonner la perquisition d'un système informatique spécifique afin d'obtenir des données informatiques spécifiques et déterminées. Dans la mesure du possible, l'autorité doit présider à l'exercice de la diligence raisonnable. L'ordonnance a une durée de validité maximale de 30 jours, sous peine de nullité.<br><br>Selon la législation cap-verdienne, l'extension d'un régime de recherche est la même que celle d'une autorisation initiale. En résumé, si une recherche autorisée par une autorité judiciaire doit être étendue à un autre système, la partie intéressée doit démontrer que l'accès à l'autre système est possible à partir du système initial et demander à l'autorité judiciaire compétente l'autorisation d'effectuer la recherche. La demande doit préciser le système ou la partie du système à perquisitionner.<br><br>Le Cabo Verde a déclaré que sa norme n'applique pas l'élément "sur son territoire". Elle fait plutôt référence aux données recherchées dans un autre système informatique ou dans une partie différente du système faisant l'objet de la recherche. La loi n'exige pas non plus explicitement que le système connecté soit situé sur son territoire. Toutefois, cette norme n'a pas encore été appliquée dans des cas spécifiques. | Le Cabo Verde applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Le Cabo Verde a déclaré que la législation existante ne couvre pas les cas où il n'est pas possible de déterminer où les données recherchées sont stockées ("situations de perte (de connaissance) de la localisation"). | |
| Cameroun | La loi ne contient pas encore de dispositions relatives à l'extension des recherches, comme le prévoit l'article 19, paragraphe 2. Les termes "raisons de croire" et "sur son territoire" ne sont donc pas précisés (dans ce contexte). | Le Cameroun n'est pas encore en conformité avec l'article 19.2. |
| Canada | Selon le paragraphe 487(2.1) du Code pénal, une recherche peut être étendue aux données qui sont disponibles dans le système informatique initialement recherché. Les procédures sont les mêmes que celles décrites ci-dessus.<br><br>Les "motifs de croire" sont définis comme des motifs raisonnables et probables de croire qu'une infraction a été commise et qu'il y a des preuves à trouver à l'endroit où la perquisition doit avoir lieu. Il existe une jurisprudence abondante sur le type de preuves qui peuvent être utilisées pour justifier la délivrance de mandats, ainsi que sur les conséquences de demandes de mandats défectueuses ou inappropriées.<br><br>Le champ d'application du droit canadien est circonscrit par le principe de territorialité. L'extension extraterritoriale d'une recherche ne serait autorisée qu'après la promulgation d'une loi autorisant explicitement une telle extension.<br><br>Lorsque la localisation des données ne peut être déterminée, il peut être possible d'obtenir un mandat général. Si ce mandat autorise la recherche de données qui sont "disponibles pour" un système, "il est permis de penser que le champ d'application territorial du pouvoir de recherche peut être étendu sans le savoir en dehors du territoire en question". | Le Canada applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Chili | Le droit interne chilien ne prévoit pas de pouvoir spécifique pour cette mesure.<br><br>La recherche peut être étendue si elle est autorisée par un tribunal. | Le Chili applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2.<br>Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En pratique, pour étendre une perquisition ou obtenir un accès similaire à un autre système, la procédure requiert une autorisation judiciaire.<br><br>L'article 12 de la loi 21.459 prévoit l'existence de soupçons raisonnables, fondés sur des faits précis, selon lesquels une personne a commis ou est sur le point de commettre l'une des infractions visées aux articles 1, 2, 3, 4, 5 et 7 de la loi.<br><br>Toutes les règles mentionnées s'appliquent à tous les crimes commis sur le territoire conformément aux règles générales.<br>Il n'y a pas de disposition spécifique pour les cas où les données recherchées ne peuvent pas être déterminées ("situations de perte (de connaissance) de la localisation"). Toutefois, le Chili a précisé que ses autorités ne peuvent recourir à cette mesure que pour les données présentes sur le territoire chilien. Dans les cas où les données se trouvent sur un autre territoire, la coopération internationale d'un autre État est requise. | plus grande clarté et renforcer la sécurité juridique. |
| Colombie | La réglementation colombienne n'aborde pas textuellement le problème de la localisation du système ou de parties du système à l'intérieur ou à l'extérieur de la juridiction pour la collecte de preuves numériques. Néanmoins, la Colombie a indiqué que dans la pratique, cela se fait si les données sont accessibles par l'expert informatique à partir d'une partie du système qui se trouve dans la juridiction colombienne.<br><br>Une ordonnance écrite signée par le procureur en charge de l'affaire est nécessaire, qui doit tenir compte de l'emplacement du système et des données stockées. Pour pouvoir être consultées, les données doivent être accessibles par l'expert en informatique à partir d'une partie du système qui se trouve dans la juridiction colombienne. Si c'est le cas et que les données sont accessibles, quel que soit l'endroit où elles sont stockées, elles sont extraites via la partie du système relevant de la juridiction nationale.<br><br>Dans ce cas, les règles de procédure suivantes sont observées : i) une ordonnance écrite signée par le procureur est examinée par un juge de contrôle dans les trente-six (36) heures suivant la fin des activités médico-légales. ii) l'ordonnance doit préciser la nécessité, la proportionnalité et l'utilité des informations obtenues, y compris des données ne relevant pas de la juridiction nationale, dans le cadre de l'affaire | La Colombie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | concernée. iii) des mesures d'enquête doivent être prises pour vérifier si des données ne relèvent pas de la juridiction nationale.<br><br>Pour déterminer avec précision si des données peuvent échapper à la juridiction, des mesures d'investigation doivent être prises, notamment i) l'examen de l'architecture du système, ii) l'évaluation de sa complexité, de son emplacement et des processus critiques, iii) l'identification des données stockées, iv) l'examen de la documentation technique, des informations d'identification actives et des privilèges qui y sont associés.<br><br>Les données de pré-identification sont potentiellement pertinentes en tant qu'éléments de preuve dans l'affaire. v) En outre, la police judiciaire peut demander l'autorisation d'étendre les recherches par le biais d'un rapport au bureau du procureur général, comme le prévoit l'article 209 du code de procédure pénale.<br><br>La Colombie a indiqué que des difficultés peuvent survenir à cet égard lorsque : i) en cas d'incident informatique, la priorité est la récupération du système et non l'enquête sur ce qui s'est passé, ce qui limite la coopération avec les autorités ; ii) l'administrateur n'a aucun intérêt à clarifier ce qui s'est passé, de sorte que la coopération est abandonnée et que l'affaire n'aboutit pas.<br><br>Étant donné que la Colombie ne dispose pas de législation en la matière, elle a détaillé les décisions judiciaires de la Cour suprême de justice, où ces questions ont été résolues comme suit :<br><br>Lorsque les données sont stockées en dehors du territoire national mais sont accessibles à partir d'une partie du système qui est sous la garde des autorités d'enquête judiciaire ou, en tout état de cause, sont accessibles par les mêmes entités à partir du territoire national, il suffit que les experts en informatique indiquent dans leurs rapports que :<br>i) Les activités ont été lancées sur la base d'un ordre légalement émis sur le territoire colombien.<br>ii) que ces activités ont été menées sur le territoire national sur un système ou une partie d'un système qui, de par son architecture, peut avoir d'autres parties du système ou des données en dehors du territoire.<br>iii) que ces données ou parties du système sont techniquement accessibles depuis le territoire national et que, par conséquent, les données sont pertinentes et assurables depuis la juridiction colombienne. | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En ce qui concerne la manière dont les autorités procèdent lorsque l'emplacement exact ne peut être déterminé, la Colombie a indiqué que la principale préoccupation n'est pas tant la possibilité d'identifier précisément la juridiction de chaque partie du système ou le stockage concret des données si celles-ci sont accessibles et conservables depuis la juridiction colombienne par le biais des formalités légales en vigueur. Dans le cas présent, cette interprétation a été faite sur la base de l'article 236 du code de procédure pénale colombien, qui autorise l'extraction de données résultant de la transmission de données par le suspect.<br><br>En revanche, si le système n'est pas accessible depuis la juridiction colombienne parce qu'il se trouve entièrement à l'étranger, ils ont indiqué que la Cour suprême de justice a souligné que la coopération judiciaire en la matière est nécessaire pour acquérir tout type de preuve numérique. Cela a été fait sur la base de l'application des dispositions des articles 484 et 485 du code de procédure pénale colombien. Enfin, la Colombie a indiqué que le non-respect de ces canaux a entraîné l'exclusion de preuves matérielles pour cause d'illégalité dans les procédures judiciaires. | |
| Costa Rica | Si, au cours de l'enquête, ou même pendant la perquisition et la saisie des données initiales, il est déterminé qu'une autre pièce de matériel (située au Costa Rica) contient des informations importantes pour l'enquête, le juge peut étendre son mandat pour saisir et analyser ces nouvelles données. Le bureau du procureur et/ou la police judiciaire exécuteront ensuite l'ordonnance.<br><br>Au Costa Rica, les "motifs de croire" sont assimilés à une "probabilité suffisante ou positive", de sorte que lorsque l'accès à des informations similaires à celles prévues à l'article 19.2 est demandé, le procureur doit démontrer dans sa demande au juge qu'en raison des faits et des preuves disponibles à ce moment-là, il existe une probabilité suffisante qu'elles se trouvent à l'endroit indiqué, et à son tour, le juge doit évaluer et analyser cette probabilité positive dans sa décision, en justifiant de manière adéquate son ordonnance.<br><br>L'expression "sur son territoire" désigne le lieu physique où le Costa Rica exerce ses pouvoirs souverains. En l'occurrence, il faut que le système (matériel) qui stocke les données se trouve au Costa Rica ou que le fournisseur du service ait un bureau commercial ouvert au Costa Rica.<br>Il n'existe pas de règle spécifique pour les situations dans lesquelles il n'est pas possible de déterminer où les données recherchées sont stockées ("situations de perte (de connaissance) de la localisation"). | Le Costa Rica applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Croatie | L'article 257, paragraphe 1, du code de procédure pénale croate dispose que la perquisition et la saisie concernent à la fois l'ordinateur et les dispositifs connectés à l'ordinateur.<br><br>La perquisition est effectuée sur la base d'un mandat judiciaire indiquant l'objet de la mesure. L'extension de la perquisition à cet autre système informatique peut, selon la jurisprudence, être effectuée soit par le biais d'un mandat judiciaire initial indiquant la possibilité d'étendre la perquisition, soit sur la base d'un mandat judiciaire ultérieur indiquant un autre système informatique à perquisitionner.<br><br>Les motifs de croire doivent être établis soit par la localisation de l'appareil connecté, indiquée dans le raisonnement de la décision et dérivée des mesures d'enquête précédemment entreprises. Cela dépend principalement des circonstances factuelles de l'affaire.<br><br>Ni le code lui-même, ni la jurisprudence ne précisent si cette disposition (article 257, paragraphe 1, du code de procédure pénale) s'applique uniquement aux dispositifs connectés qui se trouvent physiquement sur le territoire de la République de Croatie ou si la recherche peut être étendue aux dispositifs connectés situés dans un lieu inconnu/à l'étranger. | La Croatie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Chypre | Chypre peut étendre les recherches conformément à l'article 19, paragraphe 2, si elle obtient un mandat de perquisition supplémentaire conformément aux procédures standard décrites ci-dessus. Pour obtenir un tel mandat, les autorités doivent montrer qu'elles ont de bonnes raisons de soupçonner que des données informatiques sont stockées dans un autre système informatique spécifié qui n'a pas fait l'objet d'une perquisition à des fins de preuve.<br><br>Les demandes de mandat de perquisition doivent contenir des informations sur l'objet de la perquisition et les objets, documents ou données recherchés. En outre, elles doivent contenir des informations spécifiques sur les locaux ou le lieu pour lesquels le mandat de perquisition est demandé. Par conséquent, un deuxième mandat de perquisition étendant la recherche à un ordinateur connecté peut être délivré si 1) il existe des informations selon lesquelles une infraction a été commise et 2) il y a des motifs raisonnables de croire que dans un local ou une zone spécifique pourraient se trouver des objets, des données, des documents ou d'autres éléments de preuve liés à l'affaire. | Chypre applique des pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Si l'endroit où se trouvent les preuves recherchées n'est pas connu - c'est-à-dire si l'on sait qu'une infraction a été commise mais que l'on ne sait pas qu'un lieu ou un endroit précis contient des preuves pertinentes pour l'affaire - un mandat peut ne pas être délivré, car il ne sera pas possible de préciser dans la demande de mandat l'endroit où se trouvent les objets, les documents ou les données ou autres preuves recherchées.<br><br>Chypre ne revendique pas le droit d'étendre les recherches en dehors de son territoire. | |
| République tchèque | Les mesures concernées comprennent des dispositions relatives aux perquisitions à domicile (disposition 83) et aux perquisitions dans d'autres locaux et lieux (disposition 83a), toutes deux définies dans le code de procédure pénale (CPP). Si les autorités chargées de l'application de la loi sont en mesure de télécharger des données à partir d'un ordinateur ou d'un appareil connecté situé sur le territoire de la République tchèque, elles sont compétentes pour agir de la sorte, à moins qu'elles ne sachent que ces données se trouvent sur le territoire d'un État étranger. Si les données se trouvent sur le territoire d'un État étranger, la voie de la coopération judiciaire internationale doit être utilisée.<br><br>La procédure applicable à l'extension des recherches est la même que pour les perquisitions à domicile, à savoir le code de procédure pénale (CPP). L'autorisation d'accéder aux données disponibles sur l'appareil se trouvant sur le lieu de la perquisition est incluse dans l'ordonnance du tribunal autorisant la perquisition.<br><br>Selon la jurisprudence, la condition essentielle pour la perquisition est le soupçon raisonnable que dans l'appartement ou d'autres locaux utilisés pour le logement ou dans les locaux qui lui appartiennent, se trouve l'objet ou la personne importante pour les procédures pénales. La condition préalable est l'existence de faits ou de preuves susceptibles de convaincre l'observateur objectif que l'objet ou la personne en question peut se trouver dans les locaux perquisitionnés.<br><br>L'appareil sur lequel les données sont stockées ou à partir duquel elles sont disponibles doit être situé sur le territoire de la République tchèque et les autorités chargées de l'application de la loi doivent être en mesure de les télécharger. Si l'on sait que les données se trouvent sur le territoire d'un État étranger, il convient d'utiliser la voie de la coopération judiciaire internationale. D'autre part, il ressort de la réponse concernant les exemples typiques (cas d'utilisation) que les autorités pourraient utiliser la mesure également lorsque les données sont stockées sur un système informatique à l'étranger. | La République tchèque applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Danemark | La loi part du principe qu'une recherche dûment autorisée inclut le contenu des messages numériques que la personne concernée a reçus et qui sont accessibles à partir de l'ordinateur ayant fait l'objet de la recherche initiale. Une décision de la Cour suprême a autorisé des perquisitions lorsque les serveurs contenant les données cibles étaient connus pour se trouver hors du Danemark. Si l'extension d'une recherche nécessite l'accès à de nouvelles cibles, une nouvelle décision de justice doit être obtenue.<br><br>Les "raisons de croire" découleront des indicateurs de la recherche initiale.<br><br>L'approche des situations dans lesquelles la localisation des données est inconnue est régie par la décision de la Cour suprême susmentionnée. Dans son verdict, la Cour a noté que le crime était soumis au droit danois de punition, que l'affaire faisait l'objet d'une enquête par les autorités danoises et que la recherche pouvait être menée sans impliquer d'autorités étrangères. Pour ces raisons, le fait que les informations se trouvent physiquement sur des serveurs situés en dehors du Danemark, en l'occurrence en Californie et au Luxembourg, n'a pas d'importance. La Cour suprême n'a pas explicitement déclaré que cette règle s'appliquerait à d'autres situations similaires. Toutefois, étant donné que la localisation physique des données est souvent aléatoire, la réponse au questionnaire conclut que la localisation des données est insignifiante si les conditions susmentionnées sont remplies. Cette conclusion serait également conforme aux articles 6 et 9 du code pénal (règles sur la compétence danoise en matière pénale), en vertu desquels il est généralement admis que les délits commis sur l'internet ou dans le domaine de l'information peuvent être poursuivis au Danemark s'ils ont eu un effet dans ce pays. | Le Danemark applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| République dominicaine | La République dominicaine a indiqué qu'elle ne prévoit aucune restriction lorsqu'elle a des raisons de croire que les éléments de preuve se trouvent dans un autre système connecté ou accessible par le système pour lequel le mandat de perquisition est initialement détenu.<br><br>Les autorités compétentes agissent rapidement pour préserver les données contenues dans un système d'information ou ses composants, ou les données relatives au trafic du système, lorsqu'elles risquent d'être perdues ou modifiées. Étant donné que la législation n'impose aucune restriction dans les cas où les données se trouvent dans un système connecté ou sont accessibles par le système d'origine, les autorités peuvent effectuer des recherches dans les systèmes adjacents et connectés. | La République dominicaine applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Actuellement, le code de procédure pénale autorise les fonctionnaires du ministère public ou de la police à effectuer des perquisitions dans des lieux ou des objets lorsqu'il existe des "motifs raisonnables de croire" qu'il existe des preuves utiles à l'enquête.<br><br>Le cadre juridique de la République dominicaine établit que le concept de "territoire" s'applique dans les situations suivantes : i) Lorsque l'auteur ou l'instigateur de l'infraction agit sur le territoire national. ii) Lorsque l'auteur ou l'instigateur de l'infraction agit depuis l'étranger mais a des effets sur le territoire dominicain. iii) Lorsque l'origine ou les effets de l'infraction se trouvent à l'étranger, mais que des moyens sont utilisés sur le territoire national. iv) Lorsqu'il y a une complicité depuis le territoire dominicain.<br><br>Dans les cas où l'emplacement exact des données n'est pas connu, une demande de conservation est adressée au fournisseur de services, qui indiquera l'emplacement des données stockées.<br><br>Enfin, il est important de noter que le Congrès est actuellement saisi d'un projet de loi visant à modifier la loi sur la cybercriminalité (Cybercrime Act).<br>comprendrait des pouvoirs de recherche à distance qui pourraient être utilisés dans de tels scénarios. | |
| Estonie | Le droit national ne prévoit aucune limite à l'extension de la recherche. Il est possible d'accéder légalement au système informatique et d'étendre la recherche aux systèmes connectés. Les autorités indiquent que les dispositions relatives à la perquisition et à l'examen d'un objet s'appliquent. Pour l'accès clandestin, une autorisation judiciaire supplémentaire est nécessaire.<br><br>Le cadre juridique ne définit pas les "motifs de croire". Il est indiqué que l'accès doit être légal conformément à la législation nationale.<br>La législation n'exige pas que la recherche en ligne ait lieu en Estonie. L'extension de la recherche en ligne au cyberespace n'est donc pas exclue. Il n'est pas non plus exigé explicitement que l'emplacement physique des données soit identifié ou déterminé. | L'Estonie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Fidji | Les Fidji ont indiqué que la base juridique de l'extension de la recherche est fournie par les sections 21.3 et 21.4 de l'accord de coopération technique. Ces dispositions prévoient ce qui suit : Lorsque un agent de police Lorsqu'un officier de police ou une autre personne autorisée en vertu de la présente loi est autorisé à perquisitionner ou à accéder de la même manière à un système informatique, un programme, des données ou un support de stockage de données informatiques spécifiés, en vertu du paragraphe (1), et qu'il a des raisons de croire que les données recherchées sont stockées dans un autre système informatique, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour celui-ci, l'officier de police ou l'autre personne autorisée peut étendre la perquisition ou l'accès similaire à cet autre système ou à ces autres systèmes.<br><br>Un mandat d'un juge doit être émis pour autoriser cette mesure.<br><br>Les "raisons de croire" ne peuvent être confirmées qu'après les recherches initiales, afin de vérifier s'il est nécessaire d'étendre la recherche. Les avocats seront guidés par des experts techniques numériques.<br><br>L'article 3, paragraphe 2, du traité sur le commerce des armes définit le champ d'application de l'expression "sur son territoire". Il contient une variété de cadres juridictionnels, mais exclusivement trouvés ou accessibles aux Fidji.<br><br>Il a également été noté que dans les cas où il n'est pas possible de déterminer où les données demandées sont stockées, un avis juridique est pris, ce qui suggère qu'une approche au cas par cas peut être adoptée. Plus précisément, si le mandat de perquisition le permet techniquement, les données peuvent être saisies, mais si d'autres méthodes techniques doivent être utilisées, un autre mandat de perquisition doit être demandé jusqu'à ce que toutes les voies techniques soient épuisées. | Les Fidji appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |
| Finlande | La LMC contient des dispositions sur les perquisitions et les mesures coercitives secrètes aux chapitres 8 et 10. En vertu de ces dispositions, la recherche de données contenues dans un dispositif s'entend de la recherche spécifiquement orientée vers les données présentes dans un ordinateur, un terminal ou un autre dispositif technique ou système d'information correspondant au moment de la recherche. Elle inclut également d'autres dispositifs techniques ou systèmes d'information correspondants. Les recherches à distance peuvent être effectuées en tant que recherche de données contenues dans un dispositif lorsqu'elles | La Finlande applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | sont nécessaires à la conduite appropriée d'une enquête criminelle ou en raison de l'urgence de l'affaire. La recherche de données est effectuée sans utiliser le dispositif présent dans les locaux ou en possession de la personne faisant l'objet de la recherche.<br>Dans le cas d'une recherche étendue, une nouvelle décision doit être prise concernant la recherche des données stockées dans un dispositif. Comme cette décision est généralement prise par une personne habilitée à procéder à une arrestation et, en cas d'urgence, par un officier de police, elle n'a pas posé de problème dans la pratique. La demande et la décision de rechercher des données stockées dans un appareil précisent généralement la cible de la recherche. Il est important de noter que la recherche de données dans un dispositif peut être effectuée sur les données stockées dans le dispositif au moment de la recherche. Il est interdit d'effectuer des recherches multiples dans les données stockées dans un appareil pour contourner la confidentialité des communications sensibles ou les réglementations régissant l'interception des télécommunications et la surveillance des données relatives au trafic.<br><br>La CMA autorise la recherche de données contenues dans un appareil s'il existe des motifs raisonnables de croire que la recherche peut conduire à la découverte de documents ou de données pertinents. La décision d'étendre la recherche à d'autres appareils ou systèmes d'information peut résulter d'entretiens, d'analyses matérielles ou d'opérations de renseignement criminel qui fournissent des informations sur les appareils et les services utilisés dans l'infraction. Le mode opératoire de l'infraction influencera également l'étendue de la recherche de données.<br><br>La CMA et la loi sur la police ne prévoient pas explicitement la compétence territoriale de la police dans le cyberespace, mais dans la pratique, les autorités finlandaises s'appuient sur les règles et les interprétations du droit international. En règle générale, les pouvoirs de la police ne s'appliquent qu'en Finlande. En pratique, cela signifie traditionnellement que seuls les serveurs situés en Finlande et les données qu'ils contiennent sont concernés. Des enquêtes sont menées pour localiser les données, et si les données sont susceptibles d'être localisées à l'intérieur des frontières géographiques de la Finlande, les pouvoirs de police s'appliquent aux données. Dans la pratique, la recherche de données sur un appareil est parfois envisagée au cas par cas, même si les données sont accessibles en Finlande.<br><br>Aucune loi n'a été promulguée ni aucune instruction ou réglementation publiée à ce sujet, mais l'interprétation finlandaise est que si la localisation des données est inconnue et accessible, l'obtention des | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données par des mesures coercitives nationales doit être envisagée au cas par cas. Dans ce cas, il n'est pas nécessaire d'obtenir le consentement, mais la recherche de données contenues dans un dispositif est effectuée comme une recherche à distance conformément à une décision à cet effet. La mesure ne peut être mise en œuvre si l'on soupçonne que les données se trouvent dans un pays susceptible d'avoir une attitude négative ou agressive à l'égard de la mesure. En règle générale, la mesure ne doit pas porter atteinte à la souveraineté d'un État. | |
| France | Le CPC prévoit l'extension des recherches à des systèmes ultérieurs s'ils sont accessibles à partir du système initialement recherché. Les procédures habituelles sont suivies.<br><br>Deux sections du CPP définissent les "motifs de croire" comme des données présentant un intérêt pour l'enquête et comme des données (ou d'autres éléments) utiles à la manifestation de la vérité.<br><br>En principe, selon l'article 57-1 du CPP, les systèmes connectés à un système perquisitionné peuvent également faire l'objet d'une perquisition. Il ne semble pas que les enquêteurs aient l'obligation légale de déterminer systématiquement si les données sont stockées en dehors du territoire. Toutefois, si l'on sait qu'elles sont hors du territoire, les enquêteurs français procèdent par voie d'entraide judiciaire. Si les enquêteurs savent à l'avance que les données se trouvent hors du territoire, ils peuvent les collecter et les conserver sans y accéder dans l'attente de la résolution de l'entraide judiciaire.<br><br>En revanche, les données dont la localisation est inconnue peuvent être transmises à l'écran utilisé pour la recherche. Sur le plan juridique, l'accent n'est pas mis sur la localisation du serveur, mais sur la localisation de l'accès au serveur. | La France applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Géorgie | Il n'existe pas de règle législative directe autorisant l'extension des perquisitions. Toutefois, les perquisitions sont régulièrement prolongées dans la pratique, les cas qui nécessitent une prolongation sont traités comme des urgences et les règles d'urgence sont invoquées (article 112 du code de procédure pénale). Les règles applicables aux pouvoirs procéduraux généraux décrites ci-dessus s'appliquent en cas de prolongation des perquisitions.<br>Les normes de preuve concernant la localisation des données sont pertinentes en ce qui concerne les recherches initiales et la même norme s'applique aux extensions. | Il n'existe pas de règle législative directe autorisant l'extension des recherches ; cependant, les recherches sont régulièrement étendues dans la pratique et les cas qui nécessitent une extension des recherches sont traités comme des situations d'urgence. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Il n'existe pas de règle législative faisant référence à l'élément "sur son territoire". Selon la pratique judiciaire, les perquisitions et les saisies ont été considérées comme effectuées en Géorgie tant que l'accès au système informatique connecté a été effectué sur le territoire de la Géorgie. Toutefois, à ce jour, il n'y a pas de clarté définitive sur cette question.<br><br>La législation et la pratique judiciaire n'ont pas abordé la question des cas où il n'est pas possible de déterminer où les données recherchées sont stockées ("situations de perte (de connaissance) de la localisation"). | |
| Allemagne | L'article 110, paragraphe 3, du code de procédure pénale autorise l'extension de la recherche à des supports de stockage physiquement séparés des lieux de la recherche initiale, s'il est possible d'y accéder à partir du support de stockage électronique et si, dans le cas contraire, il existe un risque de perte des données recherchées.<br><br>Le nombre de niveaux intermédiaires entre l'ordinateur de l'objet de la recherche et le support de stockage séparé dans l'espace n'a pas d'importance.<br><br>Une décision de justice est nécessaire et requiert des soupçons de perte imminente de données.<br><br>En principe, les données doivent être stockées sur des supports en Allemagne. Toutefois, dans les cas où le lieu de stockage physique ne peut être déterminé, que le serveur et donc les données se trouvent en Allemagne ou à l'étranger, un lieu de stockage en Allemagne ne peut en principe être exclu dans tous les cas. La simple possibilité d'une localisation à l'étranger ne peut pas déclencher une obligation d'assistance internationale. Toutefois, s'il est établi que le support de stockage en question se trouve à l'étranger et que la recherche transfrontalière, en tant qu'accès direct unilatéral aux données stockées dans le pays en question, est donc exclue, une demande d'entraide judiciaire doit être introduite. | L'Allemagne applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Ghana | Les lois et procédures relatives aux perquisitions et saisies en général s'appliquent également lorsque les recherches sont étendues. L'article 99, paragraphe 1, de la loi sur les transactions électroniques permet à un agent chargé de l'application de la loi qui exécute un mandat de perquisition en vertu de cette loi de | Le Ghana applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | faire et d'emporter une copie de tout programme ou enregistrement contenu dans un ordinateur autre que l'ordinateur initialement perquisitionné si l'agent a des motifs raisonnables de croire que le programme ou l'enregistrement constitue une preuve de la commission d'une autre infraction. Les autorités ont également souligné que l'agent chargé de la perquisition et de la saisie peut également perquisitionner d'autres ordinateurs que ceux initialement perquisitionnés s'il a des motifs raisonnables de croire que le programme ou l'enregistrement est une preuve de la commission de la même infraction. Cette disposition repose sur le principe du pouvoir discrétionnaire dans l'interprétation des lois, qui s'applique au Ghana en tant que pays de common law.<br><br>Les "motifs de croire" que des données sont stockées sur le territoire doivent être raisonnables et étayés. Normalement, les motifs seront établis par un ou plusieurs des éléments suivants : au moment de la perquisition et de la saisie, un agent des services répressifs a des connaissances ou des informations raisonnablement fiables sur la base desquelles une personne prudente penserait qu'un système contient des preuves pertinentes ; les preuves (y compris les preuves numériques) de l'enquête indiquent un lien entre l'infraction et le deuxième système ; l'expertise technique indique que les preuves peuvent se trouver sur le deuxième système ; et la documentation, les enregistrements et l'analyse indiquent la même chose.<br><br>Les lois ghanéennes limitent la juridiction pénale du Ghana à son territoire physique avec certaines exceptions limitées (et courantes) (voir les réponses et les notes ci-dessous concernant l'extension en dehors du territoire). L'application de ce cadre et la détermination de la présence de données sur le territoire s'effectuent par le biais d'une analyse technique, de la criminalistique numérique et de la consultation d'experts.<br><br>Des efforts considérables (détaillés dans les réponses) peuvent être déployés pour identifier l'emplacement des données. Lorsque les données ne peuvent être localisées au Ghana, les autorités peuvent procéder conformément à la loi de 2010 sur l'entraide judiciaire (loi 807) en demandant l'assistance d'un État étranger. Toutefois, plusieurs des cas d'utilisation décrits dans les réponses semblent indiquer que les recherches seront étendues en dehors du territoire physique si nécessaire. | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Grèce | Des mesures législatives et autres prévoient qu'une recherche peut être étendue lorsque les autorités ont des motifs raisonnables de croire que les données recherchées sont stockées dans un autre système sur le territoire du pays. Les autorités doivent obtenir une autorisation légale supplémentaire décrivant l'extension de la recherche et précisant sa portée et son objectif. La législation garantit que les données sont légalement accessibles à partir du premier système. Lorsque la recherche est étendue, des spécialistes techniques et des outils spécialisés sont disponibles.<br><br>Les "raisons de croire" sont généralement établies par une accumulation de preuves crédibles. Il peut s'agir de preuves numériques, de témoignages, de documents, d'analyses techniques et d'informations provenant d'autres enquêtes.<br><br>L'expression "sur son territoire" est interprétée comme incluant les systèmes en nuage, quel que soit l'endroit où ils existent physiquement, même s'ils se trouvent en dehors du territoire grec, pour autant qu'ils soient connectés à un système initialement recherché qui est situé sur le territoire de la Grèce.<br><br>Des efforts déterminés sont déployés pour déterminer l'emplacement des données. Ces efforts peuvent inclure l'analyse technique et la criminalistique numérique, la collaboration avec les fournisseurs de services et la coopération internationale. Les autorités peuvent demander l'autorisation d'un tribunal pour des mesures d'investigation plus larges. Si la localisation des données ne peut être déterminée, les perquisitions et les saisies sont autorisées et exécutées comme décrit ci-dessus. | La Grèce applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Grenade | La Grenade a indiqué que la législation actuelle ne prévoit pas cette mesure. Les mandats de perquisition pour obtenir le système informatique sont spécifiques à un lieu physique ou à une entité. Des mandats supplémentaires doivent être demandés en cas de découverte d'autres systèmes, et la perquisition ou la saisie doit être spécifique, comme indiqué dans le mandat.<br><br>Les autorités ont également indiqué que l'élément "motifs de croire" est établi uniquement sur la base des faits présentés par les agents enquêteurs dans leur déclaration sous serment. La déclaration sous serment sert de préambule à l'enquête et peut inclure d'autres sources d'information ou de preuve. | La Grenade applique les pouvoirs généraux pour mettre en œuvre l'art. 19.2. Des dispositions plus spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'élément "sur son territoire" s'applique à l'emplacement physique du système dans la juridiction de la Grenade.<br><br>Enfin, il a été signalé que si la localisation ne peut être déterminée après que tous les moyens d'obtenir cette information ont été utilisés, le processus est interrompu. | |
| Hongrie | Deux décrets gouvernementaux prévoient l'extension des recherches aux données accessibles à partir d'un système initial, quel que soit l'emplacement des données, tant que les mesures de sécurité ne doivent pas être contournées. "Si nécessaire, une ordonnance pour une nouvelle recherche peut être obtenue. Toutefois, en cas d'urgence, le ministère public et l'autorité chargée de l'enquête peuvent procéder à une perquisition de tout élément de preuve qui pourrait être perquisitionné en vertu d'une ordonnance. Ces procédures doivent être justifiées et les procédures connexes (création d'un procès-verbal de perquisition) sont réglementées.<br><br>Les motifs raisonnables de procéder à une fouille sont évalués sur la base des faits propres à chaque cas.<br><br>Le code pénal hongrois établit des règles de compétence pénale. Lorsque certains crimes sont allégués, cette compétence peut s'étendre à des actes commis par des ressortissants non hongrois en dehors de la Hongrie. La section 9 du code pénal hongrois régit les procédures pour les affaires relevant de la juridiction pénale hongroise. Cette section permet aux autorités d'atteindre des systèmes situés n'importe où s'ils sont accessibles via des systèmes situés en Hongrie sans violer les mesures de sécurité. Ainsi, les perquisitions sont autorisées (à condition qu'elles soient conformes à l'article 9) lorsque la localisation des données est inconnue.<br><br>Les preuves recueillies en violation de cet article sont irrecevables au procès. | La Hongrie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Islande | Les autorités se réfèrent aux réponses précédentes au questionnaire, il semble que les mêmes conditions s'appliquent à l'extension d'une recherche que celles qui s'appliquent à la recherche.<br><br>L'expression "sur le territoire" n'est pas définie par la loi. La législation islandaise ne réglemente pas expressément la compétence d'exécution, mais le principe général de territorialité doit être respecté. | L'Islande applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | D'après le cas d'utilisation fourni, il semble que de telles mesures soient appliquées dans la pratique, le plus souvent probablement en relation avec des données "dans le nuage".<br><br>Il n'existe pas de dispositions spéciales sur la procédure d'extension d'une perquisition ni de règles internes, mais les conditions applicables à l'extension d'une perquisition sont les mêmes que celles qui s'appliquent à une perquisition. La recherche devra se faire dans le respect des conditions énoncées dans l'ordonnance de perquisition rendue par le tribunal. Par exemple, s'il apparaît qu'une partie des données est stockée ailleurs que directement sur le site visé par le mandat de perquisition, on tentera simplement d'accéder à ces données si possible à partir du système informatique concerné, si et dans la mesure où cela semble conforme à la décision de justice.<br><br>Les mêmes principes s'appliqueraient à l'établissement des motifs de croire que dans une affaire de perquisition et de saisie initiale, c'est-à-dire que s'il y a des raisons de croire que des objets, y compris des documents, doivent être saisis s'il y a des raisons de croire qu'ils, ou des choses ou des informations qu'ils contiennent, ont une valeur probante dans une affaire pénale, qu'ils ont été acquis de manière criminelle ou qu'ils peuvent faire l'objet d'une confiscation, comme le prévoit l'article 68 du code de procédure pénale.<br><br>Comment le cadre juridique s'applique-t-il "sur le territoire" : "situations de perte (de connaissance) de la localisation" : La compétence pour effectuer une recherche à distance lorsqu'il n'est pas possible de déterminer où les données recherchées sont stockées n'est pas réglementée dans la législation islandaise. La décision sera prise au cas par cas. La police essaiera d'établir la localisation avec l'aide de collègues internationaux et, selon les circonstances, demandera l'entraide judiciaire et/ou le réseau 24/7 de la Convention de Budapest. | permettre une plus grande clarté et renforcer la sécurité juridique. |
| Israël | L'ordonnance de procédure pénale autorise les recherches informatiques en se connectant ou en communiquant avec un ordinateur. Ainsi, la définition d'une perquisition informatique inclut l'extension de la perquisition. Les demandes de mandats doivent demander l'autorisation d'étendre la recherche.<br><br>L'ordonnance est muette sur les extensions en dehors du territoire d'Israël. Le cadre juridique n'aborde pas explicitement les éléments "sur votre territoire" ou "raisons de croire" de l'article 19.2. 19.2. Dans la pratique, l'élément "motifs de croire" est rempli sur la base de preuves préliminaires indiquant si le suspect | Israël applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | utilise des services Internet dont les serveurs peuvent être situés ou non sur le territoire israélien. Par exemple, des captures d'écran ou d'autres preuves médico-légales obtenues de la victime peuvent montrer que le suspect a communiqué avec la victime via Instagram ou Telegram. Lorsque la localisation des données ne peut être déterminée, une approche au cas par cas est adoptée. | |
| Italie | Les activités de perquisition et de saisie peuvent être étendues à tout système informatique qui semble être lié au système principal et directement accessible à partir de celui-ci. Dans ce cas, selon la jurisprudence de la Cour suprême, les deux systèmes interconnectés sont traités comme un seul système, selon une fiction juridique.<br><br>Lors d'une perquisition et d'une saisie, la police judiciaire peut certifier formellement que le système est connecté à un autre et procéder à la perquisition.<br><br>En ce qui concerne l'expression "sur son territoire", l'Italie n'a pas d'exigences légales spécifiques.<br><br>Dans les cas de perte de localisation, la police judiciaire utilise la même approche que si les données étaient localisées sur le territoire italien. | L'Italie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Japon | Les articles 99 et 218 du CPC stipulent que les supports connectés peuvent être saisis, après que les données ont été copiées, si l'on peut "raisonnablement supposer" qu'ils sont utilisés pour conserver les enregistrements traités par l'ordinateur initial. Aux stades antérieurs, les perquisitions peuvent être étendues par des mandats supplémentaires.<br><br>Les procédures d'extension des recherches sont par ailleurs les mêmes que pour les autres recherches.<br><br>L'élément "raisons de croire" de l'article 19.2 est déterminé par les faits du cas d'espèce et la probabilité que le support ait effectivement été utilisé pour conserver les documents visés.<br><br>Le droit japonais n'aborde pas spécifiquement la question de l'expression "sur son territoire". L'approche du Japon est déterminée au cas par cas. Lorsque la localisation des données est inconnue, le Japon suit sa jurisprudence et l'article 32 de la Convention de Budapest. | Le Japon applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Kiribati | L'article 22 de la loi sur la cybercriminalité, paragraphes 4 et 5, autorise les autorités chargées de l'application de la loi qui effectuent une perquisition et une saisie à étendre la perquisition conformément à l'article 19.2 lorsqu'elles ont des raisons de croire que les données informatiques recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur le territoire et que ces données informatiques sont légalement accessibles à partir du système informatique initial ou disponibles pour ce dernier.<br><br>La procédure est la même que pour les perquisitions effectuées en vertu de l'article 19.1. Les autorités chargées de l'application de la loi doivent émettre un avis écrit pour prolonger la fouille.<br><br>L'élément "motifs de croire" de l'article 19.2 est abordé dans la section 25 de la loi sur la cybercriminalité. Il prévoit notamment qu'un officier de police doit être convaincu que les données informatiques spécifiées, y compris les données relatives au contenu et au trafic, sont raisonnablement nécessaires aux fins d'une enquête criminelle et qu'il existe un risque que ces données soient détruites ou rendues inaccessibles.<br><br>Dans le contexte de la loi sur la cybercriminalité, le territoire est la juridiction de Kiribati, y compris les navires et les avions battant son pavillon ou enregistrés en vertu de sa législation.<br><br>Les services répressifs de Kiribati ont tendance à s'arrêter au stade où la localisation des données ne peut être déterminée. Elle a désormais la possibilité de faire appel à l'équipe de réponse aux incidents de cybersécurité de Kiribati pour ses capacités avancées. Cette possibilité n'a pas encore été mise en œuvre. | Kiribati applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |
| Lettonie | Conformément à l'article 219 du code de procédure pénale, les perquisitions peuvent être étendues sur le territoire de la Lettonie sur la base de l'autorisation donnée par un juge d'instruction de perquisitionner le système initial. Un second mandat n'est pas nécessaire et les procédures sont celles déjà décrites.<br><br>La loi ne définit pas les "motifs de croire", mais son texte reprend la formulation de l'article 19 de la Convention de Budapest. L'élément "sur son territoire" de l'article 19 est inclus dans l'article 219 du code de procédure pénale de la Lettonie. | La Lettonie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'article 219, paragraphe 2.1, du CPP dispose que les données stockées en dehors de la juridiction d'un État peuvent être consultées sur décision d'un juge d'instruction. Si leur localisation est déterminée ultérieurement au cours de la procédure, la Lettonie communiquera alors avec l'État concerné. | |
| Liechtenstein | Les perquisitions et les saisies peuvent être prolongées par l'obtention d'une nouvelle ordonnance de perquisition ou de saisie (pour laquelle il existe des mécanismes rapides). Ce nouvel ordre est obtenu de la manière habituelle, c'est-à-dire sur demande d'un procureur et décision d'un tribunal. En outre, la police nationale peut saisir des objets sans ordonnance du tribunal lorsque des données risquent d'être perdues.<br><br>Les "raisons de croire" sont normalement établies par des interrogatoires de suspects ou de témoins menés par la police, des adresses IP présentant des données de localisation différentes, des postes de travail dont les ordinateurs sont absents et des références dans le système à des systèmes qui ne sont pas présents. Par "sur son territoire", on entend sur le territoire du Liechtenstein ou accessible à partir d'un système situé sur le territoire du Liechtenstein. Il semble que son droit autorise le Liechtenstein à rechercher des données dont la localisation est inconnue si l'accès aux données est possible depuis le Liechtenstein. | Le Liechtenstein applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Lituanie | Les perquisitions sont étendues conformément aux procédures décrites ci-dessus. Si une perquisition/saisie a été effectuée et que des comptes et des identifiants sont découverts ultérieurement au cours de l'examen, une action secrète distincte doit être autorisée par un tribunal pour permettre aux enquêteurs de poursuivre leur travail.<br><br>Les termes "raisons de croire", "sur son territoire" et "perte de connaissance de la localisation" ne sont pas définis dans la loi. Les exigences habituelles sont suivies lorsque la localisation des données n'est pas connue. | La Lituanie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Luxembourg | Les procédures utilisées pour étendre une perquisition en vertu de l'article 19, paragraphe 2, sont les mêmes que celles décrites précédemment, y compris les autorisations et les techniques d'enquête appliquées. Le mandat de perquisition est émis pour une personne physique ou morale spécifique, à l'adresse mentionnée dans le mandat "ou en tout autre lieu". Cela signifie que les mandats de perquisition n'ont normalement pas besoin d'être étendus parce qu'ils contiennent les mots "ou tout autre lieu". Toutefois, si la perquisition doit être étendue à une autre personne, un nouveau mandat est émis. La base juridique de l'extension de la recherche est l'art. 33 concernant la perquisition et la saisie dans le cadre | Le Luxembourg applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'un crime flagrant, et l'art. 65 concernant les perquisitions et saisies effectuées dans le cadre d'une enquête judiciaire menée par le juge d'instruction.<br><br>Les "raisons de croire" sont mises en œuvre de la manière suivante. Les juges d'instruction et, en cas de délit flagrant, le procureur de la République, décident des actes d'instruction utiles à l'enquête, dans les limites normales des pouvoirs de ces magistrats. Les perquisitions doivent avoir pour objet la découverte d'objets nécessaires ou utiles à la manifestation de la vérité ou susceptibles d'être confisqués. Les perquisitions ne peuvent être ordonnées que pour corroborer des preuves ou des indices existants relatifs à une infraction connue et précise, et *non* pour rechercher des délits ou des crimes ou des preuves de ceux-ci.<br><br>Toutes les données stockées ou accessibles sur le territoire luxembourgeois ou à partir de celui-ci peuvent être consultées et recherchées (que la localisation des données soit connue ou non). | |
| Malte | Comme décrit ci-dessus, un mandat d'un magistrat est nécessaire pour qu'une perquisition puisse être étendue conformément à l'article 19.2. Une perquisition sans mandat peut être effectuée lorsque les motifs énumérés ci-dessus sont présents.<br><br>Les "raisons de croire" sont interprétées selon le principe du soupçon raisonnable.<br><br>Les réponses décrivent une large compétence en matière d'infractions pénales. Le pouvoir d'investigation est une question distincte. À cet égard, la réponse 2.3.2 laisse entendre qu'il n'y a pas d'exigence affirmative qu'un système informatique se trouve sur le territoire maltais.<br><br>La police déploie des efforts considérables pour déterminer l'emplacement des données et pour exploiter les appareils et les données disponibles. La police retournera à la planche à dessin pour rechercher d'autres emplacements qui auraient pu être manqués et qui pourraient permettre de récupérer davantage de données. | Malte utilise des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Maurice | Conformément à l'article 28, les demandes de recherche et les ordonnances qui en découlent précisent les paramètres de la recherche envisagée. Si une extension de la recherche est nécessaire, une deuxième ordonnance doit être obtenue.<br><br>Au lieu de "motifs de croire", l'article 28 utilise "motifs raisonnables de croire". Selon une jurisprudence constante, le caractère raisonnable est évalué par un test objectif qui prend en compte toutes les circonstances environnantes. En règle générale, ces circonstances comprennent les déclarations des témoins et les preuves documentaires soumises au juge par le biais d'une déclaration sous serment.<br>L'élément "sur son territoire" de l'article 19.2 est explicite dans l'article 28.<br><br>Lorsque la localisation des données ne peut être déterminée, l'approche mauricienne dépend du type de données recherchées et de leur localisation possible. "S'il s'agit d'un domaine quelconque, il y a une chance de récupérer les données à condition qu'elles soient accessibles depuis l'île Maurice. Dans le cas contraire, les autorités ne peuvent agir que dans les limites des pouvoirs qui leur sont conférés par la loi. | Maurice applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |
| Monaco | La législation monégasque contient des dispositions permettant d'étendre une perquisition à un autre système informatique accessible à partir du système initial, dans le cadre d'une perquisition autorisée (art. 255 du CPP).<br><br>L'extension d'une recherche suit la même législation et les mêmes procédures que celles décrites ci-dessus. Les techniques d'investigation dépendent du type de système et de la méthode d'accès. Si la recherche initiale est autorisée, elle peut être étendue à un autre système accessible à partir du premier.<br><br>Les "motifs de croire" découlent de l'enquête et de la collecte de données. Ces motifs doivent découler d'une suspicion suffisante.<br><br>L'élément "sur son territoire" de l'article 19.2 est interprété comme suit : pour saisir des ordinateurs ou des supports de stockage de données, le matériel doit se trouver sur le territoire. Si le matériel se trouve dans un autre pays (connu), une coopération internationale sera demandée. Si les données sont accessibles depuis le territoire monégasque, il est permis de les collecter et de les exploiter, que leur emplacement soit dans un pays étranger connu ou inconnu. | Monaco applique une combinaison de pouvoirs généraux et spécifiques pour mettre en œuvre l'art. 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Monténégro | L'art. 75.2 du CPC prévoit que la perquisition et la saisie s'appliquent aux ordinateurs et aux dispositifs similaires de traitement automatique des données auxquels l'ordinateur est connecté. Il est nécessaire d'obtenir un mandat de perquisition auprès du tribunal. En outre, la demande doit, entre autres, contenir les faits indiquant la probabilité qu'il existe des raisons de procéder à la perquisition.<br><br>Les autorités ont déclaré que le droit interne ne prévoit pas d'exigence positive selon laquelle le système connecté doit se trouver sur le territoire du Monténégro et qu'aucun exemple pratique n'est disponible. La réponse n'indique pas clairement comment les autorités procèdent dans les situations de perte de localisation. | Le Monténégro applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Maroc | À l'heure actuelle, la recherche étendue de données informatiques stockées est régie par les règles générales en matière de recherche, sans discrimination spécifique pouvant correspondre à des preuves électroniques et à des données électroniques stockées.<br>L'article 101 du code de procédure pénale prévoit que les perquisitions peuvent avoir lieu partout où l'on peut trouver des éléments utiles à la manifestation de la vérité. Les extensions de perquisitions sont effectuées selon les mêmes règles que celles qui régissent les autres perquisitions.<br><br>Certaines questions sont restées sans réponse. | Le Maroc applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Pays-Bas | L'article 125j du code de procédure pénale prévoit la possibilité de procéder à une fouille de réseau si, au cours de la fouille, des données pertinentes semblent être stockées ailleurs sur un réseau, ce qui permet à la personne qui effectue la fouille de fouiller également des réseaux informatiques à partir d'ordinateurs situés sur les lieux de la fouille. La fouille de réseau ne peut être effectuée que dans la mesure où le réseau est légalement accessible aux personnes régulièrement présentes sur les lieux.<br><br>L'article 557 du code de procédure pénale prévoit la possibilité d'effectuer la recherche en réseau également à partir d'un autre lieu, tel qu'un poste de police.<br><br>Le cadre national néerlandais n'impose pas d'exigence affirmative que le système connecté et/ou racine se trouve sur le territoire néerlandais. Selon l'interprétation actuelle du droit international, la recherche de | Les Pays-Bas appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | réseau ne peut aller au-delà de la juridiction néerlandaise, sans demande d'entraide judiciaire, à condition que l'emplacement de l'œuvre automatisée soit connu. Toutefois, si l'emplacement est inconnu et ne peut être déterminé avec un effort raisonnable, le procureur peut supposer que l'œuvre automatisée et/ou les données se trouvent dans la juridiction néerlandaise. | |
| Nigéria | La section 45 de la loi sur la cybercriminalité (voir en particulier 45 (2) (e)) autorise l'extension des perquisitions en vertu de mandats délivrés conformément à cette loi. Les procédures prévues par cette section sont décrites ci-dessus. Lorsque des systèmes sont saisis et que l'enquête permet de relier les éléments de preuve à un autre système pertinent, le mandat peut être étendu en modifiant l'ordonnance initiale du tribunal ou en demandant une seconde ordonnance.<br><br>La nécessité d'une seconde décision judiciaire dépend de la manière dont la décision initiale a été rendue. Si l'ordonnance initiale ne couvrait qu'un dispositif ou un système informatique particulier, une seconde ordonnance s'appliquant au nouveau dispositif ou système serait nécessaire. Toutefois, lorsque l'ordonnance initiale est de nature générale, il peut ne pas être nécessaire d'obtenir une seconde ordonnance. Par exemple, le tribunal peut rendre une ordonnance omnibus comme suit : "une ordonnance ... autorisant les agents de l'ICPC à pénétrer, perquisitionner et saisir l'ordinateur portable marqué HP-24J-C234 dans le bureau du comptable général et tout autre ordinateur ou dispositif électronique ou système qui y est connecté et qui est utilisé dans les opérations de la plateforme GIFMIS". Ici, sans la phrase en gras, les agents seraient limités à la perquisition et à la saisie de l'ordinateur portable marqué "HP-24J-C234".<br><br>Les "raisons de croire" sont décidées par le tribunal sur la base d'une évaluation objective des faits qui lui sont présentés. L'expression "sur son territoire" est une question de compétence, également évaluée par le tribunal.<br><br>Si l'emplacement des données ne peut être déterminé, l'agent peut demander au tribunal de rendre une ordonnance générale. En reprenant l'exemple ci-dessus, l'ordonnance omnibus pourrait être la suivante : "une ordonnance ... permettant aux agents de l'ICPC de récupérer ... (mentionner/décrire la nature des données) où qu'elles se trouvent ou puissent être trouvées". | Le Nigeria applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Macédoine du Nord | Les mesures et procédures d'extension de la recherche sont les mêmes que celles décrites ci-dessus.<br><br>Les "raisons de croire" sont mises en œuvre en évaluant les preuves obtenues précédemment afin de s'assurer qu'une perquisition aboutira aux preuves nécessaires, tout en tenant compte du droit à la vie privée.<br><br>Le cadre juridique reconnaît directement la Convention de Budapest et intègre donc l'élément "sur son territoire".<br><br>Aucune réponse directe n'a été donnée à la question 2.2.5 concernant les procédures à suivre lorsque la localisation des données est inconnue. Toutefois, la réponse à la question 2.3.2 indique que les mêmes procédures (et les mêmes articles du CPC) s'appliquent lorsque les recherches sont étendues *et que* la localisation des données ne peut être déterminée. | La Macédoine du Nord applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Norvège | Le code de procédure pénale autorise les perquisitions et les saisies sans ordonnance du tribunal, mais sur ordre d'un procureur ou d'un officier de police présent sur les lieux, en cas d'urgence. Ces décisions doivent être documentées et peuvent nécessiter une ratification par le tribunal. Ces extensions sans mandat peuvent impliquer des recherches dans les systèmes informatiques, les données et les supports de stockage.<br><br>Selon le cas, les enquêteurs peuvent demander une ordonnance subséquente du tribunal pour couvrir la prolongation.<br>En droit norvégien, l'expression "raisons de croire" signifie généralement qu'il est "plus probable qu'improbable" que l'accusé a commis l'infraction pénale en question.<br><br>L'expression "sur son territoire" peut être comprise comme appliquée dans l'affaire Tidal, que la Norvège a fournie. Dans cette affaire, l'accès aux données pertinentes s'est fait par le biais d'une mesure coercitive prise sur le sol norvégien à l'encontre d'une société norvégienne ayant des bureaux en Norvège. La décision a été prise par des tribunaux norvégiens, dans le respect des garanties de l'État de droit. La perquisition n'a donné accès qu'aux données que l'entreprise elle-même avait stockées et qu'elle pouvait librement extraire d'un stockage à l'étranger. Les données sont restées inchangées sur le serveur étranger. | La Norvège applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Lorsque la localisation des données est inconnue, les fonctionnaires décident au cas par cas de la marche à suivre. | |
| Panama | Actuellement, un projet de loi est en cours d'examen à l'Assemblée nationale des députés, qui prévoit des mesures de recherche de données, quel que soit leur emplacement (à l'intérieur ou à l'extérieur du territoire), à condition que les données requises soient accessibles au public au Panama et que la personne autorisée à les divulguer dans le pays étranger donne son consentement légal et volontaire pour les divulguer (article 338-C du projet de loi n° 632). Ce projet de loi est actuellement examiné par la commission du gouvernement, de la justice et des affaires constitutionnelles et n'a pas franchi d'autres étapes.<br><br>Les autorités panaméennes ont indiqué que la base juridique de l'extension de la perquisition serait les articles mentionnés précédemment : l'article 310 et l'article 314 du code de procédure pénale. S'il s'agit d'une saisie de données effectuée après une perquisition en présence de la défense, l'extension de la perquisition sera soumise à un contrôle ultérieur. Dans le cas de documents privés ou de correspondance, on pourrait faire valoir qu'il existe un risque de perte de preuves, et la procédure serait également menée sous le contrôle ultérieur du juge des garanties.<br><br>Le cadre juridique du Panama applique les "motifs de croire" en considérant que le droit procédural impose au procureur le devoir de mener une enquête objective, c'est-à-dire qui soit favorable et défavorable à l'accusé ou aux personnes intéressées par les résultats de l'enquête (article 24 du code de procédure).<br><br>Le cadre juridique du Panama applique l'expression "sur son territoire" conformément aux articles 310, 314 et 317 du code de procédure pénale de la République du Panama, pour l'inspection des données d'un système informatique, en tant qu'exigence imposée par la législation du Panama, est l'autorisation d'un juge des garanties et la notification en bonne et due forme de toutes les parties concernées afin de sauvegarder les droits et garanties constitutionnels.<br><br>La procédure Panama, lorsqu'il est impossible de déterminer où sont stockées les données recherchées ("situations de perte (de connaissance) de l'emplacement"), consiste à effectuer des recherches à l'aide de | Le Panama applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | mots ou d'expressions clés contenus dans les documents ou la base de données (page 62 du Guide des services d'experts). | |
| Paraguay | Grâce aux meilleures pratiques, des opérations techniques et des expertises sont menées et, lorsqu'il est possible d'étendre les recherches, des extensions des opérations techniques sont effectuées. De même, les points d'expertise qui doivent être traités sont étendus, ce qui est déterminé par le tribunal pénal impliqué dans le processus et exécuté par les experts, conformément aux directives d'enquête fournies par le ministère public.<br><br>Dans la pratique, la procédure d'extension d'une perquisition ou d'un accès similaire à un autre système est décrite comme suit : Obtenir un mandat de perquisition et saisir les appareils électroniques et liés aux TIC ; procéder à une analyse des types d'appareils saisis et à une analyse superficielle des données potentiellement stockées sur les appareils et des systèmes informatiques et des capacités de traitement des données qu'ils possèdent. Sur la base de cette analyse, adresser une requête au juge pénal compétent en précisant les informations supposées stockées, telles que le type de données, les fichiers de documents, les fichiers audio et/ou vidéo, ou d'autres types de fichiers tels que les exécutables, etc.<br><br>L'expression "motifs de croire" se réfère aux plaintes, à l'analyse des événements qui se sont produits, en fonction des possibilités d'action offertes par l'objet saisi, telles que la possibilité de stocker des données et la capacité de communication par l'intermédiaire de l'appareil, que ce soit par le réseau téléphonique ou l'internet, etc.<br><br>L'expression "sur son territoire" se réfère à la législation procédurale de toutes les matières qui exigent traditionnellement l'implication de l'élément de compétence territoriale dans le processus. La législation ne mentionne pas qu'il doit être lié au territoire, mais par les lois procédurales, le lieu de l'événement doit être consigné.<br>L'étendue de la perquisition est laissée à l'appréciation du procureur chargé de l'enquête, mais cette situation s'inscrit dans le cadre de l'application du critère d'objectivité prévu à l'article 54. | Il semble que les autorités s'appuient uniquement sur la pratique pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Pérou | Le titre X du code de procédure pénale établit les circonstances d'extension d'une perquisition, et l'article 19.2 valide ces extensions. Le procureur doit ensuite demander l'autorisation à un juge, en fournissant les | Le Pérou applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | locaux nécessaires, d'autoriser la mesure de restriction des droits par le biais d'une résolution judiciaire motivée confirmant la saisie des biens. Cette disposition relative à l'extension des recherches dans l'espace physique est utilisée par analogie pour la recherche de données.<br><br>Il est important de noter que lors de la mise en œuvre de mesures de limitation des droits telles que l'"inspection" et la "saisie" sur des biens contenant des données informatiques stockées et des supports de stockage de données sur le territoire national, il est possible d'étendre la perquisition ou l'enquête, y compris la saisie des objets faisant l'objet de l'enquête à des fins de validation. Cette extension est effectuée conformément aux dispositions du code de procédure pénale.<br><br>En outre, il est possible de demander une validation judiciaire dans les cas où l'autorisation judiciaire initiale d'"inspection" et de "saisie" ne spécifie pas de lieu particulier pour l'exécution de la mesure. Concrètement, cela signifie que le procureur, agissant en vertu d'une résolution judiciaire, peut prolonger la mesure de limitation des droits pendant son exécution afin d'élargir le champ de l'enquête. Par exemple, si un mandat de perquisition est délivré pour une résidence spécifique mais que des preuves suggèrent un lien avec des résidences voisines non couvertes par l'autorisation initiale, la perquisition de ces propriétés voisines peut être poursuivie. Pour plus de précisions sur cette question, on peut se référer aux articles 214°, 217°, 316° et 318° du code de procédure pénale, qui concernent l'inspection, la perquisition et la saisie.<br><br>La validation de l'exigence relative à la confirmation de la saisie de biens fait l'objet d'une procédure prévue au titre X du code de procédure pénale. Les mesures restrictives des droits sont appliquées aux données informatiques stockées et aux supports de stockage de données sur le territoire, ces mesures restrictives de la loi telles que la perquisition et la saisie sont développées dans un espace spécifique tel que prescrit dans le code de procédure pénale, cependant, conformément à l'article 316 du code de procédure pénale, la saisie peut également être applicable en tant que mesure de coercition (établissant une fonction de précaution) sur le bien pendant la phase d'enquête préparatoire qui n'a pas été préalablement exigée par le procureur.<br><br>L'élément "raison de croire" est lié aux différents degrés de suspicion abordés dans le système juridique national. En ce sens, le soupçon initial requis par le procureur pour engager une procédure préliminaire en | l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | réponse à une information criminelle est un facteur crucial dans la recherche de données. Les guides de collecte des preuves numériques servent également ces objectifs au cours de l'enquête.<br><br>L'élément "sur son territoire" est limité aux dispositions énoncées dans l'article cité de la Constitution ; dans ce contexte, aucune exigence n'est imposée pour affirmer la connexion des systèmes sur le territoire national. Toutefois, lorsque les serveurs sont situés en dehors du territoire national, d'autres mécanismes du droit international sont appliqués pour les demandes d'information.<br><br>Bien que cela ne soit pas expressément prévu par la loi, les autorités péruviennes ont interprété que Dans les cas où la localisation des données stockées ne peut être déterminée, le code de procédure pénale autorise la poursuite de la collecte d'informations, même si la localisation des données n'est pas connue au moment de la demande d'autorisation de la mesure restrictive auprès du juge. À cet égard, les règles de procédure péruviennes élargissent les possibilités d'obtenir des données. | |
| Philippines | Les perquisitions peuvent être étendues en utilisant les mêmes procédures et avec les mêmes exigences que celles décrites ci-dessus. Un nouveau mandat n'est pas nécessaire pour que les forces de l'ordre puissent procéder à une recherche étendue.<br><br>Aux Philippines, les forces de l'ordre doivent non seulement avoir des "raisons de croire", mais aussi être certaines que les données recherchées sont légalement accessibles à partir du système initial faisant l'objet du mandat ou disponibles pour celui-ci.<br><br>L'expression "sur son territoire" est interprétée comme signifiant qu'une partie du système informatique visé doit se trouver dans la juridiction philippine.<br><br>Les recherches peuvent être effectuées (dans le respect des règles habituelles) tant qu'un système ciblé est connecté au système initialement recherché, quel que soit l'emplacement physique du second système. | Les Philippines appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Pologne | Comme décrit plus en détail ci-dessus, une perquisition peut être prolongée en cas d'urgence, sous réserve d'une ratification ultérieure. Voir l'article 220, paragraphe 3, du code de procédure pénale. Il semble que | La Pologne applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | les perquisitions *ne puissent* être prolongées *qu'*en cas d'urgence, mais les "cas d'urgence" semblent être définis de manière très large.<br><br>Par "raisons de croire", on entend des informations vérifiables - des informations provenant de sources susceptibles de constituer des éléments de preuve dans le cadre d'une procédure pénale - qui ont été obtenues au cours d'une enquête et documentées de manière appropriée. Ces informations doivent indiquer que des suspects ou des éléments susceptibles de constituer des preuves sont présents là où l'on s'y attend.<br><br>Le cadre juridique n'exige pas que le système connecté se trouve sur le territoire polonais. La procédure habituelle d'extension de la recherche est utilisée lorsque la localisation des données est inconnue. | |
| Portugal | Selon l'article 15 de la loi sur la cybercriminalité, une recherche initiale peut être étendue à un autre système, ou à une partie différente du système initial, si les données sont légalement accessibles à partir du système initial. Cette extension nécessite l'autorisation de l'autorité compétente.<br><br>Lors de la planification d'une recherche et de l'émission d'une ordonnance d'autorisation, il est de bonne pratique d'inclure, à titre prospectif, une autorisation d'extension de la recherche.<br><br>Les perquisitions peuvent également être étendues par la police en cas d'urgence, dans les limites décrites ci-dessus.<br>L'expression "raisons de croire" n'est pas définie dans la loi. Dans chaque cas, les procureurs doivent déterminer si les faits répondent aux critères de la loi sur la cybercriminalité, à savoir s'il est nécessaire de recueillir des preuves pour établir la vérité.<br><br>Les recherches peuvent être étendues indépendamment de la localisation du système distant ou si la localisation des données est inconnue. Le cadre juridique ne s'applique pas "sur son territoire" à ces extensions. | Le Portugal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| République de Moldavie | Il n'existe pas de mesures législatives spécifiques concernant la prolongation des perquisitions. Toutefois, la Moldova utilise l'article 125/4 du CPP lorsque les perquisitions doivent être prolongées. Comme indiqué | La Moldova applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | ci-dessus, cette disposition autorise les perquisitions sur la base d'une ordonnance motivée du procureur général, sous réserve de la ratification de l'action par le juge d'instruction, dans les cas non susceptibles d'être reportés ou dans les cas de flagrant délit.<br><br>En vertu de l'article 125 du code de procédure pénale, un mandat d'accès aux données peut être délivré s'il existe des motifs raisonnables de penser que les données constitueront des preuves. Les "motifs de croire" que les données peuvent être stockées dans un autre système sur le territoire peuvent être fournis par les experts légistes qui aident à la perquisition et à la saisie.<br><br>Les recherches sont limitées au territoire de la Moldavie. Certains articles du CPC relatifs à l'assistance internationale peuvent être pertinents. Toutefois, les réponses de la Moldavie indiquent également qu'elle a le pouvoir de procéder à des perquisitions lorsque la localisation des données est inconnue (un second mandat peut être demandé). | l'article 19, paragraphe 2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Roumanie | En vertu de l'article 168 du code de procédure pénale, s'il est établi, au cours d'une perquisition, que les données cibles se trouvent dans un système ou un support de stockage accessible à partir de l'objet initial de la perquisition, les données cibles sont copiées et conservées, et une demande d'extension du mandat est introduite. L'article 168 ne fait pas référence à l'emplacement de l'autre système ou dispositif informatique, la seule condition étant que les données se trouvant dans un autre système ou dispositif soient accessibles à partir du système initialement perquisitionné. Une localisation inconnue n'est pas pertinente puisque le texte suppose que les données sont accessibles à partir de la localisation initiale, sans tenir compte de la localisation des données ciblées.<br><br>Les recherches informatiques ne sont pas effectuées en direct, mais dans des conditions de laboratoire sans connexion Internet. Étant donné que la recherche informatique est effectuée dans des conditions de laboratoire sans accès à l'internet, l'extension de la recherche est peu probable.<br>L'expression "raisons de croire" n'est pas utilisée dans la loi d'application. Au lieu de "raisons de croire", la loi utilise "il est constaté que les données recherchées se trouvent sur un autre...". Les procureurs doivent démontrer que les données visées ont été trouvées dans un autre système informatique accessible à partir du système initial. | La Roumanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Saint-Marin | Saint-Marin a indiqué qu'il n'existe pas de législation ou de jurisprudence spécifique pour la perquisition et la saisie de données informatiques stockées à Saint-Marin. Par conséquent, ces questions ne sont pas explicitement réglementées et sont traitées par l'application de principes juridiques analogues.<br><br>Conformément à l'article 68 du code de procédure pénale, si la nature de l'infraction est telle qu'il est plausible d'obtenir des preuves au moyen de documents ou d'objets détenus par la personne soupçonnée, par d'autres personnes ou dans des lieux où l'on présume qu'ils sont cachés, une perquisition peut être effectuée pour les trouver.<br><br>Si une recherche déléguée permet d'identifier des données dans un lieu autre que celui spécifié dans le décret judiciaire, mais que ce dernier stipule que "les données doivent être recherchées où qu'elles se trouvent", les autorités compétentes peuvent étendre la recherche à d'autres lieux raisonnables. Si le décret en question spécifie un lieu particulier, tel qu'une maison ou un serveur, la police n'est pas en mesure d'effectuer une recherche dans un autre lieu sans la délivrance d'un nouveau décret. Dans ce cas, l'information est rapidement transmise au président du tribunal, qui peut alors autoriser des perquisitions supplémentaires.<br><br>Toutefois, en ce qui concerne l'interprétation de l'expression "sur son territoire", les autorités ont souligné que, compte tenu de l'absence d'une réglementation spécifique et d'un nombre important de précédents jurisprudentiels, il faut supposer que le système informatique faisant l'objet de la mesure doit être physiquement situé sur le territoire de la République de Saint-Marin. S'il est nécessaire de rechercher un système informatique connecté au système présent à Saint-Marin, mais situé en dehors de son territoire, une demande formelle doit être adressée à l'État étranger concerné. | Saint-Marin applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Sénégal | Conformément aux amendements de 2016, les articles 90-2 et 90-3 du CPC prévoient l'extension des recherches à un système autre que le système initialement recherché (comme spécifié à l'article 19 de la Convention de Budapest).<br><br>Sous réserve des accords internationaux applicables, le juge peut recueillir des données stockées dans un système autre que le système initial situé dans un autre lieu sur le territoire sénégalais ou en dehors de celui-ci, à condition que le système ultérieur soit accessible à partir du système initial. Cette extension | Le Sénégal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | doit être nécessaire à la manifestation de la vérité ou il doit y avoir des risques de perte de preuves sans cette extension. L'extension ne doit concerner que les systèmes auxquels ont accès les personnes autorisées à utiliser le système initial. Le juge doit informer le responsable du système, sauf si son identité ou son adresse est introuvable.<br><br>La loi ne contient pas de définition de "sur son territoire" ou de "raisons de croire". Il appartient au juge de définir et d'appliquer ces notions. Néanmoins, il apparaît que la notion de "territoire national" peut être dérivée de son sens constitutionnel : un espace limité dans lequel un Etat exerce sa souveraineté. Les "raisons de croire" au sens de l'article 19 pourraient inclure un ensemble d'éléments ou de faits indiquant qu'il est probable que des données stockées dans un système autre que le système initial puissent contribuer à la détermination de la vérité. | |
| Serbie | Il n'existe pas de loi spécifique concernant la prolongation des perquisitions. Toutefois, lorsqu'il apparaît au cours d'une perquisition qu'une prolongation est souhaitable, une demande urgente de prolongation est adressée au juge de la mise en état de permanence.<br><br>Les "raisons de croire" que des données sont stockées dans un système connecté sont établies par des preuves électroniques et des indices de preuves électroniques lors de la perquisition/saisie initiale.<br><br>Le CPC limite la portée du code pénal au territoire de la Serbie, avec quelques exceptions limitées basées sur des traités et dans des conditions strictes.<br><br>Dans la plupart des cas où la localisation des données ne peut être déterminée, les services répressifs étendront la perquisition/saisie à ces données, à condition que la perquisition/saisie initiale ait été ordonnée et que les données ciblées soient accessibles par des moyens légaux. | La Serbie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Sierra Leone | Les autorités sierra-léonaises ont indiqué que l'article 10 (5) de la loi de 2021 sur la cybersécurité et la criminalité (Cybersecurity and Crime Act 2021) prévoit la possibilité d'une recherche étendue. Lorsqu'un agent d'exécution ou une personne autorisée à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci a des motifs raisonnables de croire que les données recherchées sont stockées dans un autre système informatique en nuage et qu'il y a des motifs raisonnables de croire que | La Sierra Leone applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | ces données sont accessibles à partir du système initial ou disponibles pour celui-ci, l'agent d'exécution peut étendre la perquisition ou l'accès à cet autre système.<br><br>Les autorités ont indiqué qu'elles utilisaient le même mandat pour les perquisitions et les saisies et que leurs procédures s'appliquaient en vertu de l'article 10 de la loi.<br><br>Le cadre juridique de la Sierra Leone applique les "motifs de croire" de la manière suivante : Dans une demande de mandat d'accès à des données spécifiques stockées dans un autre système informatique ou une partie de celui-ci, l'agent d'exécution doit indiquer les motifs de la demande. L'agent d'exécution doit indiquer les raisons pour lesquelles il estime qu'une recherche d'enquête peut être entravée ou compromise si un agent d'enquête n'y a pas accès.<br><br>Les autorités ont indiqué que le mandat visé à l'article 10 ne s'applique qu'au territoire de la Sierra Leone, bien qu'il ne soit pas nécessaire que le système connecté soit situé en Sierra Leone. Il n'existe pas de cas où il n'est pas possible de déterminer où les données recherchées sont stockées ("situations de perte (de connaissance) de la localisation"). | |
| République slovaque | La République slovaque cite les articles 91 et 116 du CPC comme fondement de l'extension des recherches. Elle ne semble pas aborder cette question, mais les réponses indiquent également que l'extension des recherches peut être autorisée en obtenant une ordonnance de recherche dans un système ultérieur. La mise en œuvre de l'extension des recherches par le biais des dispositions citées nécessite davantage de clarifications.<br><br>Les "motifs de croire" sont établis par des éléments de preuve autres que les éléments de preuve cibles, conformément au CPC, ou par des informations obtenues dans le cadre d'une autre enquête. Ce terme n'est pas défini dans la loi.<br><br>Le code de procédure pénale ne prévoit pas explicitement qu'un système informatique connecté doit être situé sur le territoire de la République slovaque. L'expression "sur son territoire" est définie dans le code pénal. La République slovaque ne procédera pas à des perquisitions et à des saisies de données qui ne se | La République slovaque applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. Toutefois, il serait souhaitable de clarifier davantage la base juridique applicable. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | trouvent pas sur son territoire. Dans de tels cas, elle agit soit sur la base de traités, soit sans base conventionnelle, conformément au chapitre cinq, partie cinq, du CPC (non fourni).<br><br>Les réponses n'ont pas abordé les cas où l'emplacement des données ne peut être déterminé. | |
| Slovénie | L'article 219 bis du CPP autorise la perquisition de dispositifs électroniques accessibles à partir d'un objet initialement perquisitionné, à condition que la perquisition initiale soit conforme aux exigences légales. Si le mandat initial mentionne explicitement la possibilité d'étendre la recherche, ce mandat suffira à autoriser l'extension. Dans le cas contraire, un mandat ultérieur doit être obtenu selon les mêmes règles que celles applicables au premier mandat.<br>Les "raisons de croire" se traduisent par la probabilité qu'une infraction pénale a été commise. Il doit également y avoir une probabilité que le dispositif électronique ciblé contienne des données électroniques permettant d'identifier une cible, etc., ou que l'on découvre des preuves d'un acte criminel pertinentes ou utilisables dans le cadre de la procédure pénale. La probabilité est jugée sur la base de l'ensemble des faits, y compris le fait que les appareils ou les systèmes sont connectés.<br><br>Le cadre juridique n'impose pas explicitement qu'un système électronique connecté se trouve sur le territoire slovène et n'aborde pas non plus la question de la localisation des données. L'article 219a du code de procédure pénale a été récemment mis à jour pour permettre l'extension des recherches aux dispositifs et systèmes connectés. | La Slovénie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Espagne | L'article 588 sexies c 3 du code de procédure pénale ne permet l'accès à un deuxième système informatique qu'avec l'autorisation d'un juge, lorsque les informations recherchées sont hébergées sur ce système et peuvent être obtenues légalement à partir du dispositif initial faisant l'objet de l'enquête.<br><br>L'article 588e(c) exige une nouvelle décision judiciaire pour l'extension d'une perquisition, qui doit être justifiée de la même manière que l'autorisation initiale. En cas d'urgence, les agents peuvent agir sans autorisation judiciaire préalable mais doivent en informer le tribunal dans les 24 heures et justifier l'urgence. Le juge doit valider ou révoquer la mesure dans les 72 heures. Si la preuve est stockée dans le nuage et que le type de fichier est connu, les agents peuvent agir à partir de l'ordinateur où commence | L'Espagne applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | l'intervention. Une recherche simple peut être effectuée en visualisant et en téléchargeant la preuve, tandis qu'une recherche complexe peut nécessiter l'utilisation d'un logiciel spécialisé en criminalistique.<br><br>Si les données d'intérêt sont hébergées sur une plateforme gérée par un prestataire de services, les agents peuvent demander leur conservation dans l'attente d'une autorisation judiciaire. Le contenu d'un compte de messagerie peut être consulté indépendamment de l'endroit où se trouvent les serveurs du gestionnaire de la messagerie, s'il est accessible à partir d'un système disposant d'une autorisation judiciaire. Dans certaines enquêtes, il peut être nécessaire d'accéder physiquement à un serveur, ce qui requiert une collaboration policière et judiciaire internationale.<br>L'article 588 sexies c.3º du code de procédure pénale (LECrim) définit le terme "motifs de croire" comme "raisons fondées de considérer", qui est utilisé lorsqu'il existe des indications que l'enquêteur utilise un deuxième système contenant des données d'enquête pertinentes. Les forces de l'ordre doivent informer l'autorité judiciaire et demander l'autorisation de perquisitionner le second système si elle n'a pas déjà été accordée pour la première ordonnance. Si l'on soupçonne qu'un deuxième système peut contenir des données pertinentes et qu'il est interconnecté avec le premier, il est probable qu'une autorisation judiciaire ait été demandée au début de l'enquête pour accéder aux deux systèmes.<br><br>Ce scénario ne limite pas l'exercice de l'enregistrement étendu et, conformément à la législation espagnole, ne requiert pas la connaissance de l'emplacement du système ciblé si des indications rationnelles montrent que des données pertinentes y sont stockées. | |
| Sri Lanka | L'extension des recherches est régie par la partie II de l'ACC, c'est-à-dire par les mêmes procédures que celles utilisées pour les recherches au titre de l'article 19.1. Les autorisations et les techniques d'enquête sont les mêmes.<br><br>Les "raisons de croire" que des données ciblées sont stockées dans un système connecté sur le territoire sont également régies par la partie II, mais la section spécifique n'est pas claire.<br><br>L'élément "sur son territoire" est mis en œuvre par la procédure prévue par la loi n° 2 de 1978 sur l'organisation judiciaire. | Le Sri Lanka applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Dans les cas où la localisation des données ne peut être déterminée, l'autorité d'enquête compétente aura toute latitude pour décider de la marche à suivre. | |
| Suède | Des articles du code de procédure pénale prévoient que les perquisitions peuvent être étendues. Il existe deux bases pour étendre une recherche : a) dans un système d'information lisible que la personne raisonnablement soupçonnée de l'infraction est susceptible d'avoir utilisé, les autorités peuvent rechercher des informations potentiellement importantes pour l'enquête ; ou b) les autorités peuvent effectuer une recherche s'il existe des raisons extraordinaires de supposer que des informations potentiellement importantes peuvent être trouvées . Une ordonnance autorisant de telles perquisitions peut être émise par le responsable de l'enquête, un procureur ou un tribunal. Si la perquisition est de grande ampleur ou entraîne des désagréments extraordinaires, elle ne doit être effectuée qu'en vertu d'une ordonnance rendue *par un tribunal*, à moins que le retard ne comporte des risques. Dans ce cas, la police peut procéder sans ordonnance. L'exécution des perquisitions est menée par l'autorité chargée de l'enquête, idéalement en coopération avec des experts en criminalistique numérique ou d'autres personnels spécialisés. Les cas particulièrement complexes sont traités par des experts du Centre national de police scientifique de l'autorité policière.<br><br>Le principe général de territorialité doit être respecté. La législation sur les mesures coercitives ne réglemente pas expressément l'élément "sur son territoire". Cet élément n'a pas non plus été réglementé en ce qui concerne la recherche à distance.<br><br>La législation relative à l'obtention de données électroniques stockées physiquement en dehors de la Suède est en cours d'élaboration. Une législation a été proposée pour traiter cette question dans certains cas. En outre, la Cour suprême a décidé en mars 2023 que les perquisitions à distance s'étendant à des États étrangers étaient autorisées sous certaines conditions (voir le rapport de cas fourni par la Suède). Ces conditions sont notamment que la recherche soit effectuée à l'aide d'un équipement situé en Suède et que les données ne soient pas supprimées ou que leur contenu ne soit pas affecté. De telles recherches peuvent être effectuées aussi bien lorsque la localisation des données est inconnue que lorsque les autorités connaissent le pays dans lequel les données sont stockées. | La Suède applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Suisse | Il est permis d'étendre une recherche à partir d'un ordinateur initial ayant fait l'objet d'une recherche légale à des données accessibles dans un système connecté ou un stockage ultérieur. Cette recherche étendue doit être autorisée par le mandat initial ou par un nouveau mandat. Les données du nuage accessibles à partir du nœud initialement perquisitionné sont considérées comme couvertes par le premier mandat.<br><br>Les "motifs de croire" sont mis en œuvre sur la base de preuves concrètes suggérant l'existence de données nécessaires et pertinentes, ainsi que des conditions préalables habituelles de suspicion suffisante, de proportionnalité et de caractère raisonnable de la mesure concernée.<br><br>Selon la jurisprudence de la Cour suprême, un compte et des données peuvent être recherchés s'ils sont accessibles depuis la Suisse, même s'ils sont situés en dehors de son territoire (toujours en supposant que les conditions préalables sont remplies). Cet arrêt régit également les cas où la localisation des données n'est pas connue. | La Suisse applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |
| Tonga | Aucune législation ne traite spécifiquement de l'extension des perquisitions, mais la disposition relative aux perquisitions et aux saisies de la loi sur les délits informatiques (Computer Crimes Act), par le biais de sa définition du système informatique, permet l'extension de la perquisition conformément à l'article 19.2. Les procédures habituelles pour les perquisitions au titre de l'article 19.1 sont également applicables aux perquisitions au titre de l'article 19.2.<br><br>L'expression "motifs de croire" est exprimée par "motifs raisonnables de soupçonner" à l'article 9 de la loi sur la criminalité informatique. Les magistrats décident si les preuves présentées dans une demande de la police et dans une déclaration sous serment à l'appui satisfont à cette norme.<br><br>Actuellement, l'élément "sur son territoire" est interprété comme signifiant que seules les données ou les systèmes se trouvant physiquement dans les Tonga peuvent faire l'objet d'une recherche. Les systèmes connectés, les données, etc., situés en dehors des Tonga ne peuvent faire l'objet d'une perquisition, même s'ils sont accessibles depuis les Tonga. Les Tonga espèrent adopter un nouveau projet de loi sur la criminalité informatique qui permettrait d'étendre les recherches au-delà de leur territoire physique. | Les Tonga appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les Tonga déploient des efforts considérables pour localiser les données. Elles n'ont pas répondu concernant leur approche lorsque la localisation des données ne peut être déterminée. (voir question ci-dessous). | |
| Tunisie | | |
| Türkiye | Les données stockées dans un système accessible à partir d'un système initialement recherché peuvent également faire l'objet d'une recherche. Le système supplémentaire doit être considéré comme étant utilisé par le suspect. Les procédures habituelles sont utilisées et les fonctionnaires de justice habituels sont impliqués.<br><br>En vertu de l'article 134 du code de procédure pénale, le mandat doit reposer sur de forts soupçons fondés sur des preuves concrètes, sans qu'il y ait d'autre moyen d'obtenir les preuves.<br><br>Si un système "utilisé par le suspect" se trouve dans un autre pays mais est accessible à partir d'un ordinateur "utilisé par le suspect" sur le site de la perquisition initiale situé en Turquie, la perquisition élargie est considérée comme ayant lieu en Turquie (en supposant que les exigences procédurales habituelles ont été respectées). Il semble que ce soit l'approche adoptée lorsque la localisation des données est inconnue.<br><br>Les recherches effectuées dans un autre pays à partir d'autres sites - par exemple, un laboratoire de police - sont considérées comme un accès non autorisé. | La Turquie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.2. |
| Ukraine | Il n'y a pas de règle spécifique pour se conformer à l'art. 19.2. La possibilité semble résulter d'une application des règles générales.<br><br>L'Ukraine interprète que l'élément de l'article 19.2 "sur son territoire", qui inclut que le système connecté soit sur le territoire de l'Ukraine, n'impose pas une exigence positive dans la législation de l'Ukraine. | Il semble que l'Ukraine applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.2. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Royaume-Uni | Les autorités britanniques ont fait savoir que l'APCE ne permet pas l'extension automatique d'une perquisition à d'autres locaux et que, dans certains cas, un nouveau mandat de perquisition sera nécessaire. Dans certains cas, un mandat de perquisition peut être délivré pour tous les locaux contrôlés par une | Le Royaume-Uni applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | personne spécifiée dans la demande de mandat de perquisition, auquel cas la perquisition peut être étendue à un autre système informatique situé dans ces locaux. Lorsque des informations électroniques sont accessibles depuis des locaux, un agent de police peut exiger la production de ce matériel "sous une forme qui peut être emportée et dans laquelle il est visible et lisible ou à partir de laquelle il peut être facilement produit sous une forme visible et lisible".<br><br>La même approche semble être utilisée dans le cadre du Police and Criminal Evidence Order (applicable à l'Irlande du Nord) de 1989 qui s'appuie sur des pouvoirs généraux.<br><br>En Écosse, il n'existe pas de pouvoir spécifique permettant d'étendre les recherches. La procédure serait la même que pour l'instruction initiale d'examiner le premier appareil.<br><br>Pour l'accès à un système à distance lorsque, par exemple, le dispositif a été retiré des locaux, un TEI au titre de l'IPA 2016 peut être requis.<br><br>En ce qui concerne l'élément "motifs de croire" de l'article 19, paragraphe 2, les autorités britanniques ont indiqué que l'APCE s'applique en général à l'Angleterre et au Pays de Galles et que les perquisitions au titre de l'APCE sont autorisées dans les locaux situés sur le territoire de l'Angleterre et du Pays de Galles.<br><br>Les mandats délivrés par l'IPA ont un effet extraterritorial ; pour le TEI, cet effet est couvert par les sections 126 et 127 de l'IPA. Pour l'Écosse, dans la mesure où cela est pertinent, le pouvoir des shérifs ou des juges de paix de délivrer des mandats est limité par des questions de compétence.<br><br>La manière dont les autorités britanniques procèdent lorsqu'il n'est pas possible de déterminer où se trouve la source de données est une décision opérationnelle des services répressifs, qui dépend des circonstances de l'enquête. | Des dispositions spécifiques aux données et systèmes informatiques établissant un cadre juridique pour la perquisition et la saisie de données et systèmes informatiques applicables en Angleterre, en Écosse, au Pays de Galles et en Irlande du Nord pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| États-Unis | Les mandats sont délivrés pour la recherche d'éléments situés dans le district judiciaire où siège le juge qui les a délivrés. Pour rechercher des données situées dans un autre district judiciaire mais accessibles à partir de l'appareil initialement recherché, les autorités doivent obtenir un autre mandat dans le second | Les États-Unis appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.2. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | district. Par ailleurs, si les données sont détenues par un fournisseur de services, elles peuvent être obtenues grâce à un mandat délivré en vertu d'une certaine loi.<br><br>Il n'y a pas de procédures spéciales ou de bases légales pour étendre une perquisition ; les procédures habituelles de mandat sont utilisées.<br><br>Les "raisons de croire" sont mises en œuvre en établissant une cause probable que l'objet ciblé sera trouvé dans le lieu à perquisitionner et en décrivant spécifiquement ce lieu et ce qui doit être saisi.<br><br>La jurisprudence américaine en matière de compétence exige qu'un fournisseur de services ait des contacts minimaux avec les États-Unis avant que les autorités chargées de l'application de la loi puissent exiger la divulgation de données (en vertu d'un mandat approprié).<br><br>Un juge fédéral peut délivrer un mandat pour accéder à distance à un stockage électronique et saisir ses données, que le stockage ou les données se trouvent ou non dans le district du juge, lorsque l'emplacement des données a été dissimulé par des moyens technologiques. | |

# 6 SAISIE OU SECURISATION SIMILAIRE DES DONNEES INFORMATIQUES CONSULTEES (EVALUATION DE L'ARTICLE 19.3)

Cette section évalue la mise en œuvre de l'article 19.3 :

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à sécuriser de la même manière les données informatiques auxquelles il a été accédé conformément aux paragraphes 1 ou 2. Ces mesures comprennent le pouvoir de :
>
> a saisir ou sécuriser de la même manière un système informatique ou une partie de celui-ci ou un support de stockage de données informatiques ;
> b faire et conserver une copie de ces données informatiques ;
> c maintenir l'intégrité des données informatiques stockées ;
> d rendre inaccessibles ou supprimer ces données informatiques dans le système informatique consulté.

## 6.1 Mise en œuvre de l'article 19.3 : vue d'ensemble

### 6.1.1 Mesures législatives et autres, procédure de saisie - résumé

De nombreuses Parties ont éprouvé des difficultés à décrire leur capacité à satisfaire aux exigences de l'article 19.3 et ont été invitées à fournir des informations supplémentaires pour clarifier la manière dont l'article 19.3 était mis en œuvre. Il a été supposé que les Parties disposaient en fait des pouvoirs nécessaires et qu'il leur suffisait d'expliquer la base de ces pouvoirs.

L'article 19.3 comporte quatre éléments

- la saisie et la sécurisation d'un système informatique ou d'une partie de celui-ci ou d'un support de stockage de données informatiques,
- la copie et la conservation de données informatiques,
- le maintien de son intégrité, et
- en le supprimant ou en le rendant inaccessible.

#### 6.1.1.1 Saisie ou sécurisation similaire d'un système informatique ou d'une partie de celui-ci ou d'un support de stockage de données informatiques

Presque toutes les Parties peuvent saisir le matériel informatique et les supports de stockage de données informatiques et aucun problème important n'a été rencontré lors de l'évaluation en ce qui concerne cet élément. Étant donné que, dans la plupart des juridictions, le matériel informatique et les supports de stockage sont considérés comme des objets tangibles, les Parties peuvent utiliser leurs pouvoirs de perquisition traditionnels pour les saisir.

Voici quelques exemples de pratiques :

- Géorgie : Motifs de saisie

  Un article, un document, une substance ou tout autre objet contenant des informations essentielles à l'affaire peut être saisi s'il y a des raisons valables de

penser qu'il est conservé dans un certain lieu, avec une certaine personne et s'il n'est pas nécessaire de le rechercher.

- Japon : jurisprudence pertinente

  La Cour suprême a estimé que lorsqu'il est probable que des informations liées aux faits présumés du crime sont enregistrées sur un support d'enregistrement et qu'il existe un risque d'endommager les informations enregistrées si les autorités chargées de l'application de la loi vérifient sur place si ces informations sont effectivement enregistrées, il est permis aux autorités chargées de l'application de la loi de saisir ledit support d'enregistrement sans en inspecter le contenu sur place.

- Lituanie :

  S'il est nécessaire de saisir des objets ou des documents utiles à l'enquête sur une infraction pénale et que l'on sait exactement où ils se trouvent ou qui les détient, l'officier de police judiciaire ou le procureur peut procéder à une saisie. Si les objets ou documents doivent être saisis, le procureur présente une demande de saisie motivée, sur la base de laquelle le tribunal autorise ou refuse la saisie.

#### 6.1.1.2 Faire et conserver une copie des données informatiques

Lorsqu'elles ont répondu à la question de l'établissement et de la conservation d'une copie des données informatiques, la plupart des Parties[55] ont indiqué qu'elles disposaient d'un tel pouvoir. Le plus souvent, les Parties ont indiqué que ce pouvoir découlait de compétences procédurales générales, d'une loi spécifique aux données électroniques, ou de la pratique, y compris des lignes directrices écrites .[56]

Exemples de pratiques consistant à faire des copies de données informatiques au lieu de les saisir :

- France : copie sur place

  La saisie de données informatiques peut se faire soit en plaçant sous contrôle judiciaire le système informatique ou le support de données informatiques sur lequel les données sont stockées (ex : ordinateur, tablette, téléphone, disque dur, clé USB, etc.), soit en réalisant une copie en présence des personnes dont la présence est requise lors de la perquisition. Dans ce dernier cas, le procureur de la République (ou le juge d'instruction) peut ensuite ordonner l'effacement définitif des données sur le système informatique ou le support de stockage de données qui n'a pas été placé sous contrôle judiciaire.

- Norvège : copie sur place

---

[55] Albanie, Allemagne, Australie, Autriche, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chypre, Espagne, Estonie, Fidji, Finlande, France, Géorgie, Ghana, Grèce, Hongrie, Islande, Israël, Japon, Lettonie, Liechtenstein, Lituanie, Maurice, Norvège, Panama, Paraguay, Pays-Bas, Philippines, Portugal, République de Moldavie, République dominicaine, République tchèque, Royaume-Uni, Sénégal, Sierra Leone, Slovénie, Suède, Suisse, Tonga, Türkiye, États-Unis d'Amérique.

[56] Par exemple, Israël a indiqué que les procédures spécifiques de perquisition et de saisie sont précisées dans la directive n° 7.14 du procureur de l'État sur les principes d'action concernant la saisie, la fouille, la copie et l'examen des ordinateurs et des données informatiques. 7.14 sur les principes d'action concernant la saisie, la recherche, la copie et l'examen des ordinateurs et des données informatiques. La Norvège a souligné que les instructions de la Direction de la police dans la circulaire 2010-7 intitulée "Traitement des saisies dans les procédures pénales" décrivent plus en détail le processus de saisie d'objets contenant des données.

Le support de stockage ou un dispositif contenant un support de stockage peut être saisi, ou les informations d'un support de stockage peuvent être saisies en les copiant sur place. La copie peut se faire par miroir ou par copie de fichier et une copie de sauvegarde doit être effectuée et conservée pendant la même durée que le miroir/la copie de fichier.

- Espagne : copier pour minimiser les dommages

  La saisie du support physique peut, dans certains cas, porter préjudice au propriétaire des données. Dans ce cas, il peut être conseillé de copier les données en garantissant des conditions appropriées d'authenticité et d'intégrité. L'organe judiciaire décide de saisir l'appareil ou de faire une copie du contenu, en fonction des circonstances de l'enquête en cours. Si l'appareil est destiné à l'usage exclusif du défendeur et si le contenu illégal est volumineux (comme dans les cas d'abus sexuels sur des enfants), l'appareil est généralement saisi physiquement pour un examen complet de l'appareil. Toutefois, s'il s'agit, par exemple, d'une activité criminelle menée à partir du système informatique d'une entreprise qui n'est pas impliquée dans l'action illégale, le système de copie est généralement utilisé.

Exemples de pratiques concernant la réalisation de copies de données informatiques après la saisie - réalisation et conservation d'une copie pour préserver l'intégrité des données :

- Paraguay : si les données numériques saisies risquent d'être altérées ou de disparaître, ou si elles sont difficiles à conserver ou périssables, des reproductions, des copies ou des certifications de leur existence seront effectuées et le maintien de leur état sera ordonné.

- Slovénie : Après la saisie d'un dispositif électronique, les données sont sécurisées sous forme électronique en les stockant sur un autre support de données approprié de manière à préserver l'identité et l'intégrité des données et la possibilité de les utiliser dans la suite du processus, ou une copie identique de l'ensemble du support de données est effectuée.

- Roumanie : Afin d'assurer l'intégrité des données informatiques stockées sur les objets saisis, le procureur ordonne d'en faire des copies.

#### 6.1.1.3 Maintien de l'intégrité des données informatiques stockées pertinentes

Le maintien de l'intégrité des preuves fait partie intégrante de la procédure pénale. Peut-être parce que cela va de soi, les Parties ont souvent eu des difficultés à expliquer la source de leur pouvoir de maintenir l'intégrité des données saisies. Finalement, la plupart des Parties ont indiqué que ce pouvoir découlait de compétences procédurales générales, d'une loi spécifique aux données électroniques, ou de la pratique et/ou de lignes directrices. Plusieurs Parties ont souligné que leurs autorités compétentes ont adopté des politiques ou des procédures concernant la "chaîne de conservation" des preuves (y compris électroniques) dans les enquêtes et les procédures pénales.

Certaines Parties ont également mentionné diverses périodes pendant lesquelles les données doivent être conservées. Par exemple, au Monténégro, les données (considérées comme des objets) peuvent être conservées au maximum pendant deux mois. Aux Philippines, en revanche, les autorités chargées de l'application de la loi peuvent demander une prolongation du délai pour achever l'examen du support de stockage des données informatiques et pour en faire la restitution, mais en aucun cas pour une période supérieure à trente (30) jours à compter de la date d'approbation de la mesure par le tribunal. Au Canada, les données peuvent

être conservées pendant trois mois, à moins qu'une prolongation ne soit accordée par un juge pour conserver les données jusqu'à un an.

Voici quelques exemples de pratiques :

- Autriche :[57] Le support de données saisi doit faire l'objet d'une sauvegarde légale en fonction du type et de l'étendue des données. Cette sauvegarde doit toujours prendre la forme d'une sauvegarde d'image. Une sauvegarde partielle peut également être effectuée dans certains cas. Une image de sauvegarde servira de base à la création d'une copie de travail, qui fera l'objet d'enquêtes et de recherches. Une telle image est créée à l'aide de mécanismes de sécurité judiciaire appropriés (lecture seule, blocage de l'écriture). La valeur de hachage garantit l'intégrité des données : Elle fait référence au contenu des données du support sauvegardé au moment de la sauvegarde et au contenu des données de l'image créée, et sert à prouver l'immuabilité de l'image.

- République tchèque : La sécurisation est toujours effectuée d'une manière qui permet de démontrer que les données n'ont pas été manipulées (protocole d'action détaillé, mise sous scellés, présence d'une troisième personne non impliquée, etc.) Les supports saisis sont mis sous scellés (placés dans un conteneur prévu à cet effet, décrits, photographiés, etc.) La saisie de données peut également avoir lieu sous une forme non physique, auquel cas on utilise généralement ce que l'on appelle un "hachage", une somme de contrôle qui identifie de manière unique la partie saisie des données et qui est pratiquement analogue à la mise sous scellés. Le hachage est inclus dans le procès-verbal en tant qu'identification indubitable de l'objet saisi. Il est possible de cloner des fichiers, des dossiers, des disques durs, etc. Dans la pratique, le disque d'origine doit, si possible, être conservé en lieu sûr et n'être sorti pour être cloné qu'en cas de nécessité.

- Sénégal : Indépendamment de l'obligation imposée aux autorités de maintenir l'intégrité des données, le CPP permet aux autorités d'exiger de toute personne en possession ou sous le contrôle de données qu'elle en protège l'intégrité.

#### 6.1.1.4 Rendre inaccessibles ou supprimer les données informatiques du système informatique consulté

La situation concernant la suppression des données ou le fait de les rendre inaccessibles est moins claire. Très peu de Parties (par exemple l'Albanie, le Cabo Verde, la République dominicaine, les Fidji, Maurice, les Philippines, le Portugal, le Sénégal et la Sierra Leone) disposent d'une loi spécifique accordant ce pouvoir. La plupart s'appuient sur un pouvoir implicite pour satisfaire à cet élément de l'article 19, paragraphe 3 : si nous saisissons des données, la personne ou l'entité faisant l'objet de la perquisition ne peut y avoir accès[58] . Cette approche signifie que les fonctionnaires qui effectuent une saisie doivent s'assurer qu'ils ont retiré les données visées de tous les endroits où elles sont stockées, et pas seulement qu'ils en ont retiré une copie.

Il convient toutefois de noter que le pouvoir conféré par l'article 19, paragraphe 3, s'applique à la fois aux dispositifs saisis sur place (par le biais de l'article 19, paragraphe 3) et à ceux saisis sur place (par le biais de l'article 19, paragraphe 3). 19.3 s'applique à la fois aux dispositifs saisis sur place (par le biais de l'art. 19.3.a., par exemple la saisie d'un serveur de

[57] La "Directive pour le traitement des objets saisis" adoptée en Autriche expose des aspects plus généraux et juridiques (entre autres) de la saisie de dispositifs de stockage de données électroniques (voir annexe ; disponible en allemand et non accessible au public).

[58] Au moins jusqu'au moment où les autorités peuvent être tenues de restituer les données en vertu de la loi.

domaine hébergeant un site web illicite) et les données informatiques supprimées ou rendues inaccessibles à partir du lieu où le mandat de perquisition a été exécuté (par le biais de l'article 19.3.d., par exemple un site web illicite rendu inaccessible par l'exécution du mandat de perquisition). 19.3.d., par exemple un site web illicite rendu inaccessible par les autorités), par opposition au fait de s'assurer spécifiquement qu'un site web est inaccessible par le biais d'un engagement avec d'autres personnes, comme par l'intermédiaire de fournisseurs de services.

Les réponses ont été insuffisantes pour permettre de conclure à la possibilité de rendre les données inaccessibles sans les supprimer. Certaines Parties (France, Pays-Bas) ont déclaré qu'elles avaient le pouvoir de supprimer des données en ligne ou de les rendre inaccessibles, par exemple, par le biais d'une notification et d'un retrait ou d'autres moyens pour rendre un site web inaccessible dans le cadre d'une enquête criminelle (par exemple, en relation avec des cas d'abus sexuels sur des enfants dont les documents ont été produits et sont diffusés). L'article 19.3 n'exige pas spécifiquement ce pouvoir. Ce pouvoir intéresse de plus en plus les parties, par exemple dans les cas de matériel d'abus sexuel d'enfants.

Certaines Parties (par exemple l'Allemagne, Andorre, l'Autriche, le Brésil, la Finlande, la Lituanie et la Slovénie) n'ont pas adopté de dispositions spéciales pour désactiver ou supprimer des données informatiques dans un système informatique accessible et s'appuient sur la disposition générale relative à la saisie ou à la confiscation d'objets prévue par leur cadre, qui ne mentionne pas spécifiquement les perquisitions et saisies électroniques.

Plusieurs Parties ont souligné que ce pouvoir est également important dans le contexte de la saisie de crypto-monnaies (Liechtenstein, Suisse). Une Partie a précisé qu'elle avait adopté des lignes directrices nationales à cet égard (Géorgie).

Voici quelques exemples de pratiques :

- Belgique : Lorsqu'il n'est pas possible de copier les données stockées, pour des raisons techniques ou en raison du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, ainsi qu'aux copies de ces données qui sont disponibles pour les personnes autorisées à utiliser le système informatique. Si les données font l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou si elles constituent un danger pour l'intégrité des systèmes informatiques ou pour les données stockées, traitées ou transmises par l'intermédiaire de ces systèmes, le procureur utilise tous les moyens techniques appropriés pour rendre les données inaccessibles ou, après en avoir pris copie, pour les supprimer.

- Finlande : Jurisprudence pertinente : A a été reconnu coupable de distribution aggravée et de possession d'une image indécente d'un enfant et a été condamné à confisquer à l'État les fichiers vidéo et image illégaux stockés sur les disques durs d'un ordinateur portable appartenant à B, l'épouse de A, et d'un disque dur externe appartenant à A. Après avoir supprimé les fichiers, la Cour d'appel a décidé que l'ordinateur et le disque dur devaient être restitués à leurs propriétaires. Le ministère public a demandé la confiscation de l'ordinateur portable et du disque dur externe ou, à tout le moins, l'écrasement du disque dur de l'ordinateur de B. Pour les motifs énoncés dans l'arrêt de la Cour suprême, la confiscation de l'ordinateur portable et du disque dur externe a été ordonnée au profit de l'État. La décision de confiscation est devenue caduque si, aux frais du propriétaire de l'appareil, les fichiers illégaux étaient retirés de l'appareil, soit en retirant et en détruisant le disque dur de l'appareil, soit en écrasant tous les fichiers du disque dur de manière à garantir leur retrait après que les fichiers légaux ont été copiés conformément aux instructions du propriétaire et lui ont été restitués.

- États-Unis : le support original est généralement saisi et conservé par les services de police, ce qui rend les données inaccessibles à leur propriétaire. Dans certaines circonstances, notamment dans le cas d'entreprises en activité, les forces de l'ordre collaboreront avec le propriétaire des données pour créer une copie identique des données afin que l'entreprise puisse continuer à fonctionner même après l'exécution d'un mandat. Le propriétaire des données peut également demander au gouvernement de lui restituer les données ou demander au tribunal de les lui restituer ou d'en faire une copie.

#### 6.1.1.5 Procédures en cas d'impossibilité de déterminer l'emplacement des données

Cette section du questionnaire comprenait également une question sur les procédures applicables lorsque la localisation des données ne peut être déterminée. Presque toutes les parties ont indiqué qu'elles appliquaient les mêmes mesures lorsqu'elles étendent une recherche (conformément à l'article 19, paragraphe 2) et dans les situations où il est impossible de déterminer où les données recherchées sont stockées.[59]

[59] Les lecteurs sont invités à consulter le chapitre précédent de ce rapport.

### 6.1.2 Autorités compétentes qui autorisent et effectuent une saisie

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| Albanie | Juge | Procureur, police judiciaire, expertise peuvent être impliqués |
| Andorre | Juge d'instruction | Officiers de police et autorités spécialisées désignés par le juge d'instruction |
| Argentine | Juge | Procureurs et officiers de police |
| Arménie | Juge | Enquêteurs et experts techniques |
| Australie | Magistrat, ou juge de paix ou autre personne employée par un tribunal d'un État ou d'un territoire, autorisé à délivrer des mandats de recherche ou d'arrêt. | Les autorités chargées de l'application de la loi, y compris les gendarmes ou les gendarmes qui les assistent |
| Autriche | Autorité de poursuite | Autorité d'enquête criminelle |
| Azerbaïdjan | Juge, juge d'instruction | Les autorités chargées de l'application de la loi avec l'aide d'experts techniques |
| Belgique | 39bis, § 2, alinéa 1 : officier de police judiciaire ;<br>39bis, § 2, alinéa 2 : procureur général ;<br>88ter : juge d'instruction ;<br>90ter : juge d'instruction. | Experts de la police |
| Bosnie et Herzégovine | Juge | Procureurs et autorités policières assistés par des experts en criminalistique informatique et numérique |
| Bénin | | |
| Brésil | Juge | Officier de police avec expert technique, procureur avec expert technique, unités spécialisées au sein des services de police et du ministère public |
| Bulgarie | Juge | Un enquêteur, un officier de police judiciaire ou un agent des douanes chargé de l'enquête. D'autres experts en informatique peuvent être présents |
| Cameroun | Avocat de l'État, juge d'instruction | Officier de police |
| Canada | Juge | Agent de la paix, agent public, expertise technique peuvent être impliqués |
| Colombie | Juge | Police judiciaire |
| Costa Rica | Juge | Parquet et/ou police judiciaire, autorités spécialisées |
| Croatie | Juge d'instruction, juge | Officier de police et autre autorité spécialisée |
| Chypre | Juge | Officier de police |
| République tchèque | Juge | Officier de police |
| Danemark | Juge | Police nationale danoise et autres experts |

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| République dominicaine | Juge | Procureur, police spécialisée dans la cybercriminalité |
| Estonie | Juge, procureur | Experts et autres experts techniques |
| Fidji | Juge | Police et experts techniques |
| Finlande | Procureur, officier de police | Autorités policières et autres experts techniques |
| France | Juge, juge d'instruction, officier de police | Procureur, officier de police, procureur adjoint. Personnes qualifiées pour effectuer des examens techniques |
| Géorgie | Juge | Enquêteurs avec l'aide d'enquêteurs spécialisés ou d'autres spécialistes techniques du National Forensics Bureau |
| Allemagne | Juge | Officier de police, procureur |
| Ghana | Juge, police, bureau de la criminalité économique et organisée (EOCO), bureau du procureur spécial, sécurité nationale, bureau national d'investigation, service judiciaire du Ghana. | La police, l'Office de lutte contre la criminalité économique et organisée (EOCO), le bureau du procureur spécial, la sécurité nationale, le bureau national d'investigation, le service judiciaire du Ghana. |
| Grèce | Juge, procureur | Les services répressifs et leurs unités spécialisées (division de la cybercriminalité et division de la police scientifique en Grèce) |
| Grenade | Magistrat, juge | Officier de police (Unité de criminalistique numérique) |
| Hongrie | Juge, procureur, autorité d'enquête | Le procureur, la police et l'autorité fiscale et douanière nationale en tant qu'autorités chargées de l'enquête, des consultants possédant une expertise spécifique. |
| Islande | Juge, officier de police | Autorités policières |
| Israël | Juge | La police nationale, l'administration fiscale, la police militaire, le département des enquêtes internes de la police, l'autorité des valeurs mobilières, l'autorité de la concurrence. |
| Italie | Procureur | Forces de police et autres organismes chargés de l'application de la loi |
| Japon | Juge | Procureurs, substituts du procureur ou officiers de police judiciaire |
| Kiribati | Juge | Officier de police |
| Lettonie | Juge d'instruction | |
| Liechtenstein | Juge d'instruction | Unité de lutte contre la criminalité numérique de la police nationale du Liechtenstein |
| Lituanie | Juge | le responsable de l'enquête préliminaire ou le procureur, les spécialistes des technologies de l'information du Centre lituanien d'expertise médico-légale, le Centre |

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| | | d'enquête criminelle ou d'autres spécialistes de l'application de la loi. |
| Luxembourg | Juge d'instruction, procureur | Police, experts techniques |
| Malte | Magistrat | Officiers de police, experts techniques |
| Maurice | Juge | La police, la Commission indépendante contre la corruption |
| Monaco | Juge, procureur, juge de libertes | Police nationale (unité de lutte contre la cybercriminalité), experts en informatique |
| Monténégro | Juge d'instruction | Officiers de police, officiers du centre de criminalistique numérique |
| Maroc | Juge d'instruction (si l'enquête est ouverte), procureur (pendant la phase d'enquête) | officier de police judiciaire |
| Pays-Bas | Juge, procureur | Procureur et officier de police |
| Nigéria | Juge | Police |
| Macédoine du Nord | Juge | Procureur et agent de la force publique |
| Norvège | Juge, procureur, officier de police | Police (NCIS Norvège/NC3), procureurs et personnel spécialisé |
| Panama | Juge des garanties | Procureur |
| Paraguay | Juge | Procureur |
| Pérou | Juge | Procureur, Police nationale |
| Philippines | Juge | Agents de la force publique |
| Pologne | Juge, procureur | Officier de police et autres experts spécialisés |
| Portugal | Procureur | Officier de police, experts spécialisés |
| République de Moldavie | Juge d'instruction, procureur | Procureur, agent de la force publique |
| Roumanie | Juge | Officier de police, procureur ou officier de police enquêtant sur l'affaire |
| Saint-Marin | Juge | Officier de police |
| Sénégal | Juge d'instruction, procureur | Juge d'instruction ; police sous la supervision du procureur ou du juge d'instruction |
| Serbie | Juge | Police |
| Sierra Leone | Juge | Agent chargé de l'application de la loi |
| République slovaque | Juge, procureur | Techniciens ou experts médico-légaux |
| Slovénie | Juge | officier de police |
| Espagne | Juge | Procureur, officier de police, laboratoires d'ingénierie médico-légale |
| Sri Lanka | Magistrat | Officiers de police, CERT, experts nommés par le tribunal |
| Suède | Responsable de l'enquête, procureur ou juge | Autorité chargée de l'enquête |
| Suisse | Juge, procureur | Officier de police, autre autorité spécialisée |
| Tonga | Magistrat | Officiers de police, CERT, experts médico-légaux étrangers |
| Tunisie | | |

| Parti | Autorité compétente qui autorise une recherche | Autorité compétente qui effectue une recherche |
|---|---|---|
| Türkiye | Juge, procureur | Unités chargées de l'application de la loi (avec expertise médico-légale) |
| Ukraine | Magistrat instructeur, juge | Enquêteur, procureur |
| Royaume-Uni | Magistrat | Officier de police |
| États-Unis d'Amérique | Juge | Agent chargé de l'application de la loi |

## 6.2 Mise en œuvre de l'article 19.3 - Évaluation

Les réponses aux questions suivantes ont été évaluées :

- 2.3.1 Veuillez résumer les mesures législatives ou autres que votre pays a prises pour s'assurer que vos autorités sont en mesure de saisir ou de sécuriser de la même manière des données informatiques telles que décrites à l'article 19.3. Dans votre réponse, veuillez résumer les conditions à remplir et les étapes de la procédure généralement suivies pour obtenir l'autorisation d'une telle saisie.
- 2.3.2 Appliquez-vous les mêmes mesures lors de l'extension d'une recherche (conformément à l'article 19, paragraphe 2) et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées ?
- 2.3.3 Quelles sont les autorités compétentes qui autorisent et effectuent une saisie telle que décrite à l'article 19.3 ? Quel type d'expertise technique ou autre est requis et utilisé ?

| **Parti** | **Mesures législatives et autres** | **L'évaluation** |
|---|---|---|
| Albanie | L'Albanie a indiqué qu'en vertu de l'article 208/A du CPP, c'est le tribunal qui autorise le procureur à ordonner à l'officier de police judiciaire d'exercer les pouvoirs visés à l'article 19.3.<br><br>L'Albanie a également indiqué que la même procédure et les mêmes pouvoirs s'appliquent à l'extension d'une perquisition, mais qu'il n'existe pas de disposition spécifique dans le cas d'une localisation indéterminée de données informatiques.<br><br>L'article 209/A du CPP dispose que "...3. En exécutant la décision du tribunal, le procureur ou l'officier de police judiciaire autorisé par le procureur adopte des mesures : a) pour empêcher toute autre action ou pour sécuriser le système informatique ou une partie de celui-ci ou d'un autre dispositif de stockage de données ; b) pour extraire et obtenir des copies des données informatiques ; c) pour empêcher l'accès aux données informatiques, ou pour retirer ces données des systèmes informatiques accessibles ; d) pour assurer l'inviolabilité des données stockées pertinentes.<br><br>Les autorités compétentes pour autoriser et effectuer la saisie visée à l'article 19, paragraphe 3, sont le procureur du Roi ou l'officier de police judiciaire si le procureur du Roi le décide. Comme mentionné ci-dessus, le procureur peut désigner un expert connaissant le fonctionnement des données informatiques ou les mesures de protection des données informatiques. | L'Albanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Andorre | Les procédures relatives à l'art. 19.3 sont les mêmes que celles décrites précédemment. Les articles 26 et 87 du code pénal répondent à certains éléments de l'art. 19.3 - la saisie et la sécurisation des systèmes et des supports, la fabrication et la copie de données, et le maintien de l'intégrité des preuves. En outre, les autorités judiciaires ont le pouvoir de rendre les données inaccessibles ou de les supprimer : un juge d'instruction peut ordonner l'assistance technique de la police pour prendre les mesures nécessaires. | L'Andorre applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Argentine | Il n'existe aucune disposition expresse en vigueur dans l'ensemble du pays qui remplisse tous les éléments de l'article 19.3. L'Argentine applique le principe de la liberté de la preuve.<br><br>Il est important de mentionner que le Code fédéral de procédure pénale (CPPF), dans ses articles 151 et suivants, réglemente la saisie de données informatiques ou électroniques : Art. 151 "le juge peut ordonner, à la demande d'une partie et par ordonnance motivée, la perquisition d'un système informatique ou d'une partie de celui-ci, ou d'un support de stockage de données informatiques ou électroniques, afin de saisir les éléments du système, d'en obtenir une copie ou de conserver des données ou des éléments présentant un intérêt pour l'enquête". La mise en œuvre de cette disposition dans l'ensemble du pays n'est pas achevée et se poursuit.<br><br>Les mêmes limitations s'appliquent que celles prévues pour la saisie des documents. L'examen est effectué sous la responsabilité de la partie qui l'a demandé. Une fois que les éléments du système ont été saisis ou qu'une copie des données a été obtenue, les règles relatives à l'ouverture et à l'examen de la correspondance sont appliquées. La restitution des éléments qui n'ont pas de rapport avec le processus sera ordonnée ainsi que la destruction des copies des données. L'intéressé peut faire appel au juge pour obtenir la restitution des éléments ou la destruction des données.<br><br>L'art. 153 régit la procédure d'enregistrement et de conservation des preuves qui seront enregistrées au moyen d'une bande magnétique ou d'autres moyens techniques similaires garantissant la fidélité de l'enregistrement. L'enregistrement est remis ou conservé par le représentant du ministère public qui prévoit les mesures de sécurité correspondantes, en appliquant les mesures prévues pour la saisie et la chaîne de possession. Le représentant du ministère public veille à ce qu'il ne soit pas connu des tiers. À la fin de la procédure, par arrêt ou ordonnance de non-lieu, les enregistrements sonores des communications et les transcriptions qui en ont été faites sont placés en lieu sûr, à l'abri de l'accès du public. Ces dernières ne peuvent être consultées que sur décision de justice. | L'Argentine a introduit des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. qui n'est pas encore applicable dans l'ensemble du pays. Entre-temps, dans la pratique, l'Argentine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. 19.3. De plus amples informations pourraient clarifier la manière dont les éléments spécifiques, en particulier les points c-d de l'article 19, paragraphe 3, du Code pénal, sont appliqués. 19.3 de la CB. Des dispositions spécifiques pourraient apporter plus de clarté et de sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La législation ne prévoit pas la saisie ou la sécurisation similaire des données qui ont été consultées dans le cadre d'une extension de la recherche. | |
| Arménie | L'Arménie a indiqué qu'elle avait mis en place des mesures législatives et autres pour permettre aux autorités de saisir ou de sécuriser de manière similaire un système ou un support de stockage, d'effectuer et de conserver des copies des données, de maintenir l'intégrité des données et de supprimer les données ou de les rendre inaccessibles.<br><br>L'Arménie se réfère à l'art. 236 comme base juridique applicable pour la mise en œuvre de tous les éléments de l'article 19.3. 19.3. Toutefois, bien qu'il semble qu'il réponde à certains des éléments de l'article 19.3, il ne semble pas répondre aux exigences de l'article 19.3. 19.3, elle ne semble pas répondre aux exigences de l'art. 19.3.d de la CB.<br><br>Des mesures et des étapes procédurales similaires sont utilisées lorsque les recherches sont étendues en vertu de l'article 19.2. Les autorités ne peuvent procéder que lorsqu'il est possible de déterminer que les données sont stockées sur le territoire arménien.<br><br>Les autorités judiciaires délivrent des autorisations de saisie si les preuves présentées répondent aux exigences légales. Les services répressifs exécutent la saisie et peuvent faire appel à des experts médico-légaux ou autres. | L'Arménie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. Cependant, la manière dont cette disposition répond aux exigences de l'article 9.3.d. du Code pénal arménien n'est pas claire. 9.3.d. de la CB. Des dispositions plus spécifiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Australie | L'Australie peut satisfaire aux éléments de l'article 19.3 grâce à de nombreux articles de la loi sur les infractions (Crimes Act) et de la loi sur le développement durable (SD Act), ainsi qu'aux procédures des forces de police. Les dispositions spécifiques aux ordinateurs autorisent expressément la saisie des appareils et des données, ainsi que la copie des données. Les forces de police disposent de procédures visant à préserver l'intégrité des données ; en outre, les deux lois interdisent la modification des données. En ce qui concerne la suppression des données ou le fait de les rendre inaccessibles, la loi sur les infractions prévoit que les appareils et les fichiers informatiques peuvent être saisis si leur possession est susceptible de constituer une infraction. Dans ce cas, les autorités ne sont pas tenues de remettre une copie de l'objet à la personne concernée, comme c'est normalement le cas. En vertu d'une loi ou d'une décision de justice, la restitution de l'objet peut être exclue et celui-ci peut être conservé par les autorités ou éliminé. En vertu de la loi sur le développement durable, un mandat de "perturbation des données" peut être obtenu. Il permet aux autorités de perturber les données pour empêcher la commission d'une infraction couverte par la loi. | L'Australie applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'art. 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'Australie applique les mêmes mesures pour étendre une recherche et dans les situations où la localisation des données ne peut être déterminée.<br><br>De la même manière que précédemment, les perquisitions prévues à l'article 19.3 sont autorisées par un membre du pouvoir judiciaire et exécutées par un membre de certains organismes australiens chargés de l'application de la loi. | |
| Autriche | L'article 111 du code de procédure pénale définit une partie du régime des perquisitions et des saisies, y compris la saisie et la sécurisation similaire des données ou des systèmes et la réalisation d'une copie des données. Un décret de 2022, intitulé "Lignes directrices pour le traitement des objets saisis", aborde en détail les questions de la copie, de la sécurisation et du maintien de l'intégrité des données saisies. Une section du code pénal concernant les saisies prévoit effectivement de supprimer les données ou de les rendre inaccessibles, tandis que plusieurs sections de la loi autrichienne sur les médias prévoient explicitement la même chose.<br><br>Les mêmes mesures s'appliquent aux recherches étendues. Dans certaines circonstances et sous réserve de certaines règles, l'extension des perquisitions est possible même si elle n'a pas été autorisée initialement. Les saisies sont autorisées et exécutées comme décrit ci-dessus. | L'Autriche applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Azerbaïdjan | Il n'existe pas de dispositions spécifiques concernant les éléments de l'article 19.3, mais, dans la pratique, les dispositions générales relatives à la collecte et à la conservation des preuves s'appliquent pour satisfaire aux exigences de l'article 19.3.<br><br>Les articles 245 et 251 du CPP stipulent que, si possible, les objets qui ont été enlevés doivent être emballés, scellés et conservés dans les locaux de l'autorité d'enquête ou du tribunal, ou remis pour conservation à un représentant de l'autorité étatique compétente, qui doit être averti de sa responsabilité légale, et que les objets qui ont été saisis mais non enlevés doivent être scellés et remis pour conservation à leur propriétaire ou possesseur ou aux membres adultes de leur famille, qui doivent s'engager à ne pas les détourner, les endommager ou les détruire, et qui doivent être avertis de leur responsabilité légale. À cet égard, les mêmes mesures sont partiellement appliquées en cas de prolongation d'une perquisition et dans les situations où la localisation des données ne peut être déterminée.<br><br>Les autorités d'autorisation et d'exécution sont les mêmes que pour les perquisitions effectuées en vertu de l'article 19.1. | L'Azerbaïdjan applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Belgique | Comme le détaille la Belgique, plusieurs sections du code prévoient les éléments de l'article 19.3, y compris le fait de rendre les données inaccessibles dans certains cas ou de les supprimer. Ces dispositions s'appliquent également lorsque les perquisitions sont étendues et qu'il n'est pas possible de déterminer l'emplacement des données. Les autorités habituelles sont chargées d'autoriser et d'exécuter ces saisies. | La Belgique applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |
| Bénin | Les articles 589 et 590 de la loi sur le code numérique précisent les procédures et étapes requises. Elles sont les mêmes que celles mentionnées à l'article 19.2. Les autorités compétentes pour autoriser une saisie en vertu de l'article 19.3 sont le juge d'instruction et le procureur de la République. La police judiciaire exécute la saisie en utilisant des méthodes qui préservent l'intégrité physique du matériel et l'intégrité des données saisies. L'expertise technique est fournie soit par la police technique et scientifique, soit par le laboratoire d'investigation numérique du Centre National d'Investigations Numériques (CNIN). | Le Bénin applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. |
| Bosnie et Herzégovine | Les différents codes en vigueur dans le pays ont des approches différentes de ce paragraphe particulier de la Convention de Budapest.<br><br>Le code de la Bosnie-Herzégovine n'a pas mis en œuvre la législation relative aux éléments de l'article 19.3.<br><br>Le CPC de la Fédération de Bosnie-et-Herzégovine prévoit les différents modes de saisie des données, décrits à l'article 19.3.<br><br>Le code de procédure pénale de la Republika Srpska semble seulement prévoir la recherche par le biais d'une copie de données informatiques (article 19.3.b). Lorsqu'il existe des motifs suffisants de soupçonner qu'il existe des preuves d'une infraction pénale sur des dispositifs électroniques temporairement confisqués, un tribunal peut ordonner la création d'une copie judiciaire. La copie judiciaire sera créée par des fonctionnaires autorisés spécialement formés ou par un autre expert en présence d'un fonctionnaire autorisé.<br><br>Ces fonctionnaires feront un rapport sur sa création, en décrivant et en identifiant exactement l'objet. L'objet saisi et sa copie sont ensuite conservés par le tribunal ou sous son contrôle. | La Bosnie-Herzégovine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Il apparaît que plusieurs éléments de l'art. 19.3 n'ont pas été transposés dans le droit interne de la Bosnie-Herzégovine. Des dispositions spécifiques aux données et systèmes informatiques applicables à toutes les entités de Bosnie-Herzégovine pourraient apporter plus de clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Le CPC du district de Brcko ne comprend pas les éléments de l'article 19.3. Toutefois, il a été signalé que, dans la pratique, certaines des formes de saisie prévues par ce paragraphe se produisent. C'est notamment le cas de a (saisie des données), c (maintien de l'intégrité des données) et d (dans la modalité de suppression des données).<br><br>Les éléments de l'article 19.3a sont mis en œuvre par la confiscation temporaire de cas sur la base d'une décision de justice ou par l'obtention de données auprès de l'ISP/OSP sur la base d'une décision de justice, ce qui est prescrit dans le CPC BD BiH. En pratique, sur la base d'une décision de justice, une partie ou la totalité d'un système faisant l'objet d'une perquisition est temporairement confisquée. Ensuite, les autorités demandent une ordonnance autorisant la perquisition de l'objet confisqué.<br><br>Les éléments de l'article 19.3b sont mis en œuvre en les incluant dans l'ordonnance du tribunal pour la perquisition. Dans la demande de mandat, la police demandera que l'ordonnance autorise la création d'une copie médico-légale à conserver en plus de l'appareil original faisant l'objet des recherches et d'une image médico-légale de l'espace mémoire de l'appareil. Dans la plupart des cas, le tribunal rendra une ordonnance contenant ces éléments.<br><br>En ce qui concerne l'article 19.3c, dans la pratique, si les données sont en possession d'un ISP, la police soumettra une demande pour que l'ISP stocke les données. Ce stockage est volontaire. Si les données sont en possession des autorités à la suite d'une perquisition,<br><br>les meilleures pratiques standard en matière de criminalistique numérique sont appliquées pour garantir l'intégrité des données informatiques stockées et pour enregistrer toute modification inévitable des données.<br><br>En ce qui concerne l'article 19.3d, le code pénal (en particulier les articles 78 et 391) autorise les confiscations dans de nombreuses circonstances. Il s'agit notamment des cas où la confiscation est exigée par l'intérêt de la sécurité générale et des bonnes mœurs et des cas où les objets ont été impliqués dans la commission d'un délit, notamment l'endommagement de données ou de programmes informatiques ou la falsification informatique et l'exploitation de mineurs à des fins de pornographie ou l'initiation de mineurs à la pornographie.<br><br>Il n'existe pas de règles spécifiques concernant la saisie de données en cas d'extension des recherches. Toutefois, il a été signalé que les règles et principes généraux relatifs à la saisie des données s'appliqueraient lors de l'extension des recherches, y compris en cas de "perte de localisation". En d'autres termes, la Bosnie-et-Herzégovine, la Fédération de | |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Bosnie-et-Herzégovine et la Republika Srpska peuvent saisir des données dans un lieu inconnu de la même manière qu'elles étendent les perquisitions.<br><br>En ce qui concerne les autorités compétentes, les procureurs (et, en Republika Srpska, les fonctionnaires habilités avec l'autorisation du procureur) obtiennent des tribunaux l'autorisation de procéder à des perquisitions et à des saisies. La police et les experts techniques exécutent l'ordre. | |
| Brésil | Les autorités ont déclaré que le texte de l'art. 19.3 de la Convention de Budapest s'applique directement en tant que législation nationale, alors que le droit national général ne prévoit pas explicitement de mesures de saisie des données. Les dispositions générales du code de procédure pénale s'appliquent par analogie et les autorités compétentes ont le pouvoir de saisir ou de mettre en sécurité les données informatiques qui ont été perquisitionnées ou auxquelles il a été accédé de manière similaire. Cela comprend la saisie du matériel informatique et des supports de stockage de données. Dans ce contexte, le terme "saisir" est interprété de manière similaire à la définition donnée dans la Convention. Il s'agit de retirer le support physique sur lequel les données sont enregistrées ou de faire et de conserver une copie de ces données. Il comprend également la saisie des programmes nécessaires pour accéder aux données. En outre, l'expression "sécurité similaire" est reconnue pour refléter d'autres moyens par lesquels les données sont supprimées ou leur contrôle est pris. En ce qui concerne l'article 19.3.d, la pratique consistant à rendre les données inaccessibles, que ce soit par le biais du cryptage ou d'autres mesures techniques, nécessite une autorisation judiciaire. Le terme "suppression" est interprété dans le sens où les données sont supprimées ou rendues inaccessibles, mais non détruites. La saisie n'implique pas la suppression définitive des données saisies.<br><br>Les autorités compétentes doivent disposer d'une décision de justice ou d'un mandat de perquisition fondé sur une suspicion raisonnable d'infraction, précisant le lieu, le type de données et le délai de la saisie. La procédure de saisie doit préserver l'intégrité des données et toutes les copies effectuées doivent être conservées en toute sécurité.<br><br>Le Brésil assure le respect des mesures décrites à l'article 19.3 de la Convention de Budapest en maintenant la chaîne de possession, comme le prévoit le code de procédure pénale. La chaîne de possession comprend plusieurs étapes, notamment l'identification, l'isolement, la fixation, la collecte, l'emballage, le transport, la réception, le traitement, le stockage et l'élimination des éléments de preuve. | Le Brésil applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'article 158-C du code de procédure pénale souligne que la collecte des preuves doit être effectuée de préférence par un expert officiel qui effectuera les procédures de garde à vue nécessaires, même dans les cas où des examens complémentaires sont requis.<br><br>Pour procéder à une saisie en vertu de l'article 19.3, les autorités compétentes, qui sont généralement des organismes chargés de l'application de la loi (tels que la police fédérale, la police d'État ou d'autres unités spécialisées chargées d'enquêter sur la cybercriminalité et les infractions connexes), auront normalement besoin d'une ordonnance du tribunal ou d'un mandat de perquisition autorisant la saisie, sur la base d'un soupçon raisonnable de commission d'une infraction, et précisant le lieu où se trouvent les données informatiques, le type de données à saisir et le délai de la saisie. Ils peuvent également demander l'assistance d'experts techniques, tels que des spécialistes en informatique légale ou des analystes de preuves numériques, pour aider à la saisie et à l'analyse des données informatiques. | |
| Bulgarie | Lors d'une perquisition, les autorités chargées de l'enquête ont le pouvoir de saisir tout objet (y compris un système d'information) dont elles pensent qu'il contient des éléments de preuve en rapport avec l'infraction faisant l'objet de l'enquête. Selon la pratique, lors d'une perquisition, l'option préférée est de prendre le support de stockage des données informatiques. Si cela s'avère difficile, une copie judiciaire peut être réalisée en présence d'un expert en informatique et remise à l'autorité qui effectue la perquisition.<br><br>La saisie doit être autorisée par un juge.<br><br>En ce qui concerne les éléments spécifiques de 19.3 :<br>a) La saisie des moyens de stockage pertinents est la méthode préférée et la plus souvent utilisée par les forces de l'ordre pour sécuriser les données informatiques dans le cadre d'une enquête.<br>b) Une copie des données informatiques est effectuée dans les cas où la saisie des données informatiques n'est pas possible (par exemple, lorsqu'un fournisseur d'hébergement héberge plusieurs systèmes informatiques virtuels sur un seul disque dur). La procédure est décrite dans le protocole de perquisition et de saisie ou la copie est préparée en présence de l'enquêteur et remise aux autorités chargées de l'application de la loi dans le cadre d'un protocole distinct.<br>c) L'intégrité des données informatiques est maintenue soit en les saisissant, soit en en faisant une copie. | La Bulgarie applique des pouvoirs de saisie spécifiques pour mettre en œuvre l'article 19.3. Il n'est toutefois pas certain que la Bulgarie ait le pouvoir de supprimer des contenus ou de les rendre inaccessibles s'ils ne sont pas entre les mains d'un fournisseur de services - s'ils sont stockés par une entreprise, par exemple. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Il semble que l'article 163 du CPC soit également applicable. Il prévoit en détail la mise sous scellés des supports de stockage informatique saisis, l'enregistrement physique détaillé de la mise sous scellés et des procédures spéciales permettant de lever les scellés sur le support de données pour faire avancer l'enquête.<br>d) En vertu de l'article 16, paragraphe 2, de la loi sur le commerce électronique, les fournisseurs d'hébergement doivent rendre le contenu inaccessible s'ils ont été informés par les forces de l'ordre que le contenu est illégal. (Les fournisseurs ont une obligation distincte de retirer le contenu ou de le rendre inaccessible s'ils réalisent eux-mêmes que le contenu est illégal). | |
| Cabo Verde | Selon l'article 18 de la CL, l'autorité judiciaire compétente, qui dans l'ordre juridique cap-verdien comprend les juges et les magistrats du ministère public, peut autoriser ou ordonner la saisie de données informatiques lors d'une perquisition informatique. Si une telle ordonnance ou autorisation existe, la saisie doit prendre les formes suivantes : i) saisie du support où le système est installé ou saisie du support où les données informatiques sont stockées, ainsi que les dispositifs nécessaires pour les lire ; ii) réalisation d'une copie des données, sur un support autonome, qui sera jointe au processus ; iii) préservation, par des moyens technologiques, de l'intégrité des données, sans les copier ou les supprimer ; ou iv) suppression ou blocage non réversible de l'accès aux données. Au moins dans le cas du paragraphe v), la copie est faite en double exemplaire, l'un des exemplaires étant scellé et confié au secrétaire judiciaire du service où se déroule le procès et, si cela est techniquement possible, les données saisies sont certifiées par des moyens de signature numérique.<br><br>Le ministère public demandera au juge l'autorisation de saisir. S'il s'agit d'un organe de police judiciaire, il adressera toujours une demande au ministère public. Le ministère public autorisera ou demandera l'autorisation au juge si cela ne relève plus de sa compétence, comme indiqué précédemment. Si la police effectue une saisie en dehors des cas d'autorisation ou d'ordonnance préalable, elle doit soumettre la saisie à l'autorité judiciaire compétente pour validation dans les 72 heures.<br><br>Il s'agit des mêmes mesures que lors de l'extension d'une perquisition, qui est le régime général de saisie des données informatiques, quelle que soit la manière dont elles ont été obtenues. La loi n'aborde pas les situations où il est impossible de déterminer l'emplacement des données demandées. Toutefois, ce cas de figure ne s'est pas encore présenté dans la pratique. En tout état de cause, la première obligation de toute personne effectuant une perquisition informatique est de déterminer l'emplacement précis des données. | Le Cabo Verde applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Au Cabo Verde, le juge ou le ministère public, en tant qu'autorité judiciaire compétente, peut autoriser ou ordonner la saisie de données informatiques conformément à l'article 18 de la CL. La loi cap-verdienne contient une disposition qui exige que les données ou documents informatiques saisis susceptibles de révéler des informations personnelles ou intimes qui pourraient compromettre la vie privée du détenteur ou d'un tiers soient présentés au juge. Le non-respect de cette obligation entraîne la nullité de la procédure. Le juge examinera alors la possibilité d'ajouter les données ou les documents au processus, en tenant compte des intérêts du cas concret. Les organes de police judiciaire, c'est-à-dire les entités qui effectuent la saisie physique des données, peuvent, sans autorisation préalable de l'autorité judiciaire, effectuer cette saisie au cours d'une perquisition informatique légitimement ordonnée et exécutée, ainsi qu'en cas d'urgence ou de risque de retard. En ce qui concerne les connaissances techniques nécessaires, la loi ne prévoit pas d'exigences particulières. | |
| Cameroun | L'article 29 de la loi camerounaise sur la cybercriminalité autorise expressément les autorités à saisir les installations des systèmes d'information des opérateurs sur ordre ou sur la base d'un mandat délivré par les autorités judiciaires.<br><br>Les perquisitions et les saisies sont soumises au respect des conditions énoncées dans le code de procédure pénale.<br><br>Les perquisitions et les saisies sont autorisées par le procureur de la République ou le tribunal compétent. Les forces de police les exécutent en collaboration avec des institutions techniques telles que l'Agence nationale des technologies de l'information et de la communication (ANTIC).<br><br>Des procédures n'ont pas encore été clairement établies pour gérer les situations où l'emplacement des données ne peut être déterminé. | Le Cameroun applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Cependant, il n'est pas clair comment les pouvoirs d'effectuer et de conserver une copie des données, de maintenir l'intégrité des données et de supprimer les données ou de les rendre inaccessibles conformément à l'article 19.3 b-d sont mis en œuvre au Cameroun. |
| Canada | La section 487 du code pénal et ses sous-parties traitent de la recherche, de la saisie et de la copie de données. En ce qui concerne la mise en œuvre de l'art. 19.3.c., dans une réponse très détaillée, le Canada se réfère à l'Art. 490 du Code pénal comme étant la disposition applicable. Cette disposition prévoit un pouvoir général régissant la procédure relative aux biens périssables, y compris leur restitution au propriétaire légitime ou à d'autres personnes ayant légalement droit à leur possession. En outre, la législation nationale pertinente pour la mise en œuvre de l'art. 19.3.c. se trouve dans les sections 31.1 à 31.8 de la Loi sur la preuve au Canada (LPC) qui concernent les données informatiques et les documents électroniques (authentification des documents électroniques, règle de la meilleure preuve). Le Canada a également présenté des décisions de justice qui donnent un aperçu du cadre juridique applicable au maintien de l'intégrité des | Le Canada applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données. Il a également été souligné qu'un ensemble de cours obligatoires doit être suivi avec succès par un membre des forces de l'ordre par l'intermédiaire de l'Institut d'apprentissage de la criminalité technologique du Collège canadien de police afin de garantir la cohérence des pratiques médico-légales dans l'ensemble du Canada.<br><br>Plusieurs articles du code pénal prévoient la mise en œuvre de l'article 19, paragraphe 3, point d). 19.3.d. Il s'agit notamment de la section 487.01 qui prévoit un mandat autorisant l'utilisation de tout dispositif, technique ou procédure d'enquête ou tout acte décrit dans le mandat qui, s'il n'était pas autorisé, constituerait une perquisition ou une saisie abusive à l'égard d'une personne ou de ses biens, et qui peut répondre aux exigences de l'article 19.3.d.<br><br>Les mêmes mesures sont appliquées dans les situations où la localisation des données ne peut être déterminée que lorsque les recherches sont étendues conformément à l'article 19, paragraphe 2.<br><br>Comme décrit précédemment, les saisies sont autorisées par les juges. Les saisies sont exécutées par des agents de la paix (ou éventuellement par des officiers publics). Des agents disposant d'une expertise technique particulière peuvent être impliqués. | |
| Chili | Le Chili n'a pas de disposition expresse concernant la saisie de données informatiques et de supports contenant des données informatiques. Il semble qu'en pratique, les dispositions du code de procédure pénale relatives à la saisie de preuves matérielles puissent probablement être utilisées par analogie. Les pouvoirs généraux prévus à l'art. 217 du CPP, qui régissent la saisie d'objets et de documents, peuvent être utilisés.<br><br>L'autorisation est accordée par une ordonnance du tribunal délivrée à la demande du procureur. | Le Chili applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Colombie | L'article 236 de la loi 906 de 2004 permet de sécuriser et de copier les preuves numériques obtenues tout en préservant leur intégrité selon les normes médico-légales établies. À cette fin, plusieurs aspects fondamentaux doivent être vérifiés :<br><br>1. L'accès au dispositif ; le lieu où se trouve le dispositif qui stocke ou contient les données : Au cours de cette première phase, la police judiciaire et le procureur chargé de l'enquête doivent rendre des ordonnances permettant l'accès au lieu ou à l'appareil où les données sont stockées. i) Accès aux preuves numériques trouvées dans le cadre d'une procédure | La Colombie applique les pouvoirs généraux de perquisition et de saisie, la jurisprudence, les pratiques acceptées et les manuels sur la chaîne de possession pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'arrestation. ii) Accès à l'espace physique où se trouve l'appareil par le biais de perquisitions et de saisies. iii) Accès à l'appareil à l'aide d'un registre personnel. iv) Accès à l'espace ou à l'appareil avec l'accord de la victime.<br><br>2. Accès aux données stockées dans les appareils saisis ; une fois que la saisie de l'appareil est terminée, le procureur peut ordonner l'extraction des données stockées avec l'aide d'un expert en informatique légale. Le processus d'extraction des données doit être documenté dans un rapport d'expert, détaillant les méthodes scientifiques et techniques employées, l'efficacité des outils utilisés pour l'analyse légale, le processus spécifique appliqué aux preuves, y compris le déballage et l'analyse, ainsi que les conclusions de l'expert à l'issue de l'analyse.<br><br>3. Accès aux données lorsque la saisie de l'objet n'est pas possible ; il y a des cas où la taille de l'objet, sa connexion à des systèmes plus complexes, ou l'aspect pratique ne permet pas la saisie physique de l'objet. Dans ces cas, le procureur pénètre dans l'espace où se trouve le système avec l'autorisation du propriétaire du site ou avec un mandat de perquisition et ordonne la conservation de la preuve numérique, conformément aux dispositions de l'article 236 du CPP.<br><br>4. Le fait de rendre les données inaccessibles ou de les retirer du système à partir duquel elles ont été récupérées ; il n'existe pas de règle directe concernant cette action spécifique. Toutefois, le Manuel de la chaîne de possession et de la police judiciaire du bureau du procureur général confère aux experts en criminalistique des fonctions qui leur permettent, dans le cadre du processus d'identification et d'extraction des données stockées dans un système informatique, de changer et de prendre le contrôle des utilisateurs et des identifiants qui peuvent être utilisés pour l'élimination ou la modification de la preuve numérique.<br><br>La Colombie a ajouté un autre mécanisme couramment utilisé pour suspendre l'accès du public à un contenu spécifique ou la suppression de données après qu'elles ont été conservées, en utilisant la figure du "rétablissement du droit des victimes" figurant à l'article 22 du code de procédure pénale colombien. En vertu de cette mesure, un procureur peut demander une mesure de précaution à un juge de la République, toute action, y compris la suppression, la suspension de l'accès ou toute autre mesure jugée pertinente pour un élément de données, afin d'éviter les effets d'un crime ou d'en inverser les conséquences dans le cadre de la protection des victimes. Cette action a été utilisée avec succès pour désactiver des domaines à contenu pornographique, supprimer des contenus offensants ou illégaux sur des systèmes tiers, ou suspendre l'accès à certaines données par le suspect. | informatiques sont recommandées pour plus de clarté et de sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Costa Rica | Le Costa Rica a indiqué qu'il n'existe pas de législation spécifique régissant la perquisition ou la saisie de données informatiques stockées, mais que la loi régissant la perquisition, la saisie et l'examen de documents privés et l'intervention dans les communications est appliquée. Il est important de noter que les autorités ont indiqué que cette loi assimile explicitement les preuves numériques aux preuves physiques ou documentaires. Selon cette même loi, une fois que le dispositif électronique a été saisi ou que la base de données contenant la preuve numérique d'intérêt a été localisée, il est nécessaire d'obtenir un contrôle judiciaire pour son acquisition. Une fois cette autorisation accordée, il incombera à la police technique d'effectuer les procédures judiciaires d'obtention (sauvegarde) et d'analyse de l'information, le tout étant consigné dans un rapport présenté à la procédure judiciaire.<br><br>La saisie du matériel contenant des données électroniques peut être ordonnée par le procureur ou la police judiciaire afin de protéger les preuves, mais la recherche et l'analyse des données nécessitent l'ordonnance d'un juge en raison du droit à la vie privée du propriétaire.<br><br>Si vous ne pouvez pas déterminer si les données se trouvent sur le territoire du Costa Rica et si le fournisseur du service n'a pas de bureau ouvert dans notre pays, le juge n'étendra pas la recherche, et nous devons donc compter sur la coopération internationale. | Le Costa Rica applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Croatie | Les articles 261 et 263 du CPP prévoient expressément la saisie des appareils électroniques et des données, ainsi que leur conservation. Les données sont retirées ou rendues inaccessibles sur décision du juge d'instruction ; elles sont normalement restituées dans un délai de six mois à compter de la date de la saisie, mais leur restitution peut être interdite pour plusieurs raisons liées à des infractions pénales.<br><br>L'article 262 du CPP protège certains objets contre la saisie. En général, ces protections concernent les objets détenus par des catégories de personnes privilégiées - par exemple, les avocats de la défense et les journalistes - et les documents gouvernementaux secrets. Les protections peuvent être levées si une personne appartenant à une catégorie privilégiée est soupçonnée de complicité criminelle.<br><br>Les mesures sont appliquées indépendamment de l'emplacement des données. | La Croatie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Chypre | Même en l'absence d'une loi spécifique le permettant, il semble que, dans la pratique, les quatre modalités de saisie, décrites à l'article 19.3, peuvent être exécutées, par une mention spécifique dans l'ordonnance du juge qui en décide. Il semble que toutes ces modalités soient prévues dans un manuel de procédures interne utilisé par la police.<br>Le Digital Forensic Lab (DFL) de la Cyber Crime Unit est responsable de la saisie ou de la sécurisation d'un système informatique ou d'une partie de celui-ci ou d'un support de stockage. Il est également chargé d'effectuer et de conserver des copies des données, d'en préserver l'intégrité, de les supprimer ou de les rendre inaccessibles. | Chypre applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| République tchèque | Les mesures concernées comprennent des dispositions relatives à l'obligation de remettre ou de céder des objets (disposition 78) et au retrait d'objets de la possession (disposition 79), toutes deux définies dans le code de procédure pénale (CPP).<br><br>Lorsqu'il s'agit de maintenir l'intégrité des données informatiques stockées, des procédures opérationnelles standard internes sont utilisées.<br><br>La demande de remise ou de restitution d'un objet peut être faite par le président du tribunal et, dans le cadre de la procédure préliminaire, par le procureur général ou l'autorité de police. Si l'objet n'est pas remis ou restitué volontairement, il peut être retiré de la possession sur ordre du président du tribunal et, dans le cadre de la procédure préliminaire, sur ordre du procureur ou de l'autorité de police. L'autorité de police doit avoir obtenu l'accord préalable du procureur pour rendre cette ordonnance ; sans cet accord, l'autorité de police ne peut rendre cette ordonnance que si l'accord préalable ne peut être obtenu et si l'affaire ne peut être retardée.<br><br>Si l'autorité qui a émis l'ordre ne procède pas elle-même au retrait de l'objet de la possession, celui-ci sera effectué par l'autorité de police sur la base de l'ordre.<br><br>Étant donné qu'il repose sur l'application de pouvoirs généraux, il serait souhaitable de clarifier davantage la manière dont le cadre s'applique à la réalisation de copies de données et à la suppression de données en particulier.<br><br>Il est également possible d'appliquer l'ordonnance de conservation des données ou l'ordonnance de refus d'accès aux données conformément à la disposition 7b du CPC. | La République tchèque applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 3. Il serait souhaitable de clarifier davantage la manière dont le cadre s'applique à la réalisation de copies de données et à la suppression de données en particulier. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les autorités appliquent les mêmes mesures lors de l'extension d'une recherche et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées. | |
| Danemark | Les réponses n'ont pas abordé directement les éléments a à d de l'article 19.3. Les perquisitions et les saisies sont largement réglementées par l'AJA. En vertu de l'article 802, les données informatiques sont couvertes par le terme "objets" et cet article définit les conditions de la saisie d'une personne soupçonnée d'un délit. Les règles et procédures habituelles sont donc appliquées et les fonctionnaires habituels sont impliqués dans la saisie des données.<br>Les réponses indiquent que les règles et procédures habituelles sont appliquées et que les fonctionnaires habituels sont impliqués lorsque les recherches sont étendues et que la localisation des données ne peut être déterminée. | Il semble que le Danemark applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Il serait souhaitable d'obtenir davantage d'informations sur la mise en œuvre d'éléments spécifiques de l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient apporter plus de clarté et renforcer la sécurité juridique. |
| République dominicaine | La législation de la République dominicaine établit que, avant d'obtenir un ordre judiciaire, le ministère public, avec l'aide des agences d'investigation de l'État, a le pouvoir de i) Saisir ou sécuriser un système d'information ou l'un de ses composants, en tout ou en partie ; ii) Faire et conserver des copies du contenu du système d'information ou de l'un de ses composants ; d) Ordonner le maintien de l'intégrité du contenu d'un système d'information ou de l'un de ses composants ; e) Collecter ou enregistrer des données à partir d'un système d'information ou de l'un de ses composants par l'application de mesures technologiques (art. 54).<br><br>La législation de la République dominicaine ne fait aucune différence en ce qui concerne l'application des mêmes mesures lors de l'extension d'une recherche, de sorte que les mêmes mesures s'appliquent.<br><br>Dans la législation de la République dominicaine, l'autorité compétente qui autorise l'ordonnance est un juge. La saisie est effectuée par le ministère public assisté par des agents d'unités de police spécialisées dans la cybercriminalité. Ces agents doivent appartenir à l'une des agences spécialisées, qui disposent de l'expertise technique nécessaire pour mener à bien le processus de chaîne de possession de la preuve numérique. | La République dominicaine applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |
| Estonie | Le CPC ne contient aucune disposition spécifique concernant la collecte de données informatiques. Des pouvoirs génériques d'application de la loi sont utilisés (par exemple, les pouvoirs prévus à l'article 215 du CPC) ainsi que des | L'Estonie applique les pouvoirs généraux de perquisition et de saisie |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | pouvoirs génériques de perquisition et de saisie (article 91 du CPC). Pour l'examen des objets (systèmes informatiques, supports de données, etc.), les articles 86 et 87 du CPC sont utilisés (inspection d'un document, d'un autre objet ou d'un élément de preuve physique et rapport d'inspection, respectivement). Outre les articles pertinents du CPC, la police utilise des lignes directrices internes non publiques sur la collecte et le traitement des preuves électroniques. En fonction de l'affaire et des besoins, une copie médico-légale du support de données est effectuée ou des objets sont saisis et examinés ultérieurement.<br>Les mêmes dispositions et principes que pour l'extension d'une recherche s'appliquent.<br><br>En règle générale, les perquisitions et les saisies peuvent être autorisées par le bureau du procureur. Certaines exceptions sont prévues pour les avocats et les notaires. | pour mettre en œuvre l'article 19.3. Il semble que l'Estonie n'ait pas le pouvoir de supprimer des données ou de les rendre inaccessibles. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Fidji | Les articles 16 et 21(3)(4) du TCA fournissent une base juridique pour cette mesure. Ainsi, la police/FICAC peut demander un mandat à un juge/magistrat pour saisir le système informatique ou toute partie de celui-ci, le support de stockage de données informatiques, faire et conserver une copie des données informatiques en utilisant un équipement sur place, maintenir l'intégrité des données informatiques stockées, rendre inaccessibles ou supprimer les données informatiques dans le système informatique consulté, imprimer la sortie des données informatiques, sécuriser le système informatique/le support de stockage de données informatiques ou une partie de celui-ci.<br><br>Les autorités ont indiqué qu'elles appliquaient les mêmes mesures lorsqu'elles étendaient une recherche, mais pas dans les situations où il n'est pas possible de déterminer quand les données recherchées ont été stockées.<br><br>L'autorité compétente pour autoriser la saisie est le juge, et ceux qui effectuent la perquisition sont la police et les fonctionnaires ayant une expertise technique. | Les Fidji appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. |
| Finlande | Aucune disposition ne réglemente spécifiquement les pouvoirs de l'article 19.3. 19.3. La Finlande utilise plutôt les dispositions généralement prévues pour la saisie de biens matériels pour mettre en œuvre l'art. 19.3.<br><br>Selon la CMA, des objets, des biens ou des documents peuvent être saisis s'il existe des motifs raisonnables de soupçonner qu'ils sont pertinents en tant qu'éléments de preuve, qu'ils sont impliqués dans une infraction pénale ou qu'ils sont susceptibles d'être confisqués. Cela s'applique également aux informations contenues dans des dispositifs techniques ou des systèmes d'information. Les dispositions du chapitre 7 de la loi sur les mesures coercitives concernant | La Finlande applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. qui sont étendus par le droit national pour couvrir également les données informatiques. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | un document s'appliquent également à un document sous forme de données. Ces dispositions comprennent le pouvoir de saisir le matériel informatique, les supports de stockage de données informatiques et le support de données.<br><br>La section 3 énonce des règles sur l'interdiction de la saisie et de la copie concernant les personnes proches et le droit au silence. La section 13 concerne la gestion d'un objet saisi. La personne qui effectue la saisie prend possession de l'objet, du bien et du document saisis ou les place sous bonne garde.<br><br>Il n'existe pas de disposition légale explicite stipulant l'obligation de maintenir l'intégrité des données informatiques stockées. Cependant, selon la loi sur les mesures coercitives, chapitre 7, section 13, paragraphe 3, l'objet de la saisie doit être préservé dans son état d'origine et géré avec soin, et cette exigence s'applique également aux données. En outre, la loi sur les mesures coercitives, chapitre 8, sections 24 à 26, prévoit des dispositions pour les ordonnances de conservation des données qui garantissent l'intégrité des données avant de copier ou de saisir les dispositifs.<br><br>En ce qui concerne le fait de rendre inaccessibles ou de supprimer les données informatiques contenues dans le système informatique consulté, les autorités ont indiqué que le chapitre 7 de la loi sur la protection des données autorise la saisie des données, même si elles peuvent être confisquées. En cas de contenu illégal, la copie des données n'est pas une mesure suffisante et permet de rendre le contenu (code pénal, chapitre 10, section 5, paragraphe 1).<br><br>L'objet de la saisie peut être laissé à la personne qui l'avait en sa possession, à moins que cela ne compromette l'objectif de la saisie. L'objet de la saisie est conservé en tant que tel et est géré avec soin. Des tests peuvent être effectués sur un objet saisi à des fins de preuve s'ils sont nécessaires pour élucider l'infraction.<br><br>La Finlande applique les mêmes mesures pour étendre une recherche lorsqu'il n'est pas possible de déterminer où les données recherchées sont stockées. La localisation des données n'affecte pas, en tant que telle, la prise de décision concernant la mesure coercitive. Si le lieu est inconnu, une attention particulière sera portée à la question et, dans la mesure du possible, un examen judiciaire explicite sera effectué avant de prendre la mesure. Si l'entraide doit être demandée, les règles de la coopération judiciaire internationale seront suivies. | |
| France | Plusieurs articles du CPC permettent de satisfaire aux éléments de l'article 19.3. En particulier, en ce qui concerne l'article 19.3d, une autorité judiciaire peut demander la fermeture d'un site web ou supprimer l'accès aux données hébergées sur un site web (après les avoir saisies à des fins d'analyse et d'enquête). Dans l'affaire Bitzlato, l'autorité | La France applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | judiciaire a obtenu la fermeture du site français de ce Virtual Assets Service Provider (VASP) poursuivi pour activités illégales.<br><br>Dans les limites décrites ci-dessus, les procédures habituelles sont suivies lorsque la localisation des données est inconnue.<br><br>Les fonctionnaires de police effectuent les perquisitions. Dans les affaires qui en sont au stade de l'enquête préliminaire ou lorsqu'un juge d'instruction est déjà engagé, les perquisitions sont guidées par les ordonnances des juges. | |
| Géorgie | Les dispositions générales du code de procédure pénale relatives à la saisie physique et à la divulgation de données informatiques sont appliquées. Les pouvoirs concernés sont soumis à une autorisation judiciaire. En général, la perquisition et la saisie sont autorisées dans le cadre de la même procédure et dans le même mandat. Plusieurs articles du CPC, dont l'article 136 qui traite spécifiquement des perquisitions informatiques, prévoient tous les éléments de l'article 19.3.<br><br>Les autorités appliquent les mêmes mesures que lors de l'extension d'une recherche.<br><br>Les pouvoirs sont exercés par les forces de l'ordre. | La Géorgie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Allemagne | Les dispositions générales du code de procédure pénale relatives aux objets susceptibles de constituer des preuves pour l'enquête s'appliquent mutatis mutandis aux données stockées sur un support de données, qui doivent généralement être traitées de la même manière que les autres objets saisis. Si les données sont sous la garde d'une personne connue et ne sont pas remises volontairement, elles doivent être formellement saisies conformément à l'article 94 (2) du code de procédure pénale. Conformément à l'article 98, paragraphe 1, du code de procédure pénale, les saisies ne peuvent être ordonnées que par le tribunal et, en cas de danger imminent, elles peuvent également être ordonnées par le ministère public et ses enquêteurs.<br><br>Conformément à l'article 110, paragraphe 3, deuxième phrase, du code de procédure pénale, la saisie est également autorisée en cas d'extension des recherches (conformément à l'article 19, paragraphe 2) et dans les situations où il est impossible de déterminer où les données recherchées sont stockées. | L'Allemagne applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. Il serait souhaitable de clarifier la mise en œuvre de l'article 19.3d. 19.3d serait souhaitable. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Si les données sont stockées dans un système qui ne peut être copié, les supports de données peuvent être saisis (dans le respect du principe de proportionnalité). La saisie et l'analyse des données sont effectuées par des spécialistes, ce qui garantit l'intégrité des données (voir les commentaires relatifs au point 2.4.1).<br><br>Si les données confisquées contiennent des éléments incriminants, elles ne sont pas restituées à la personne en possession de laquelle elles se trouvaient, mais elles sont effacées dans les délais généraux d'effacement.<br><br>Il n'y a pas de référence expresse à la disposition ou aux pratiques prévues par le droit interne pour rendre inaccessibles ou supprimer des données informatiques dans le système informatique consulté (19.3.d de la Convention). | |
| Ghana | En vertu de la LTA, un agent des services répressifs peut saisir tout ordinateur, enregistrement électronique, programme, information, document ou objet lors de l'exécution d'un mandat en vertu de la loi (en supposant qu'il existe des motifs raisonnables de le faire). Une personne autorisée peut assister l'agent. L'agent peut accéder aux informations de décryptage nécessaires pour décrypter un enregistrement requis pour l'enquête. L'agent peut faire et emporter une copie de tout enregistrement ou programme contenu dans l'ordinateur ou dans tout autre ordinateur dont on pense qu'il contient des preuves d'une autre infraction. Les données saisies doivent être correctement documentées et la chaîne de possession doit être maintenue. En fonction des circonstances et des lois applicables, les personnes ou entités concernées par la saisie peuvent être notifiées. Normalement, une perquisition et une saisie sont autorisées par les autorités judiciaires. Toutefois, cinq organes chargés des poursuites, de la sécurité et de l'application de la loi peuvent autoriser et exécuter des perquisitions et des saisies dans des circonstances appropriées. Il convient de noter que les dispositions de la LTA en matière de perquisition et de saisie peuvent être utilisées en plus des pouvoirs d'arrestation, de perquisition et de saisie d'un organisme chargé de l'application de la loi prévus par d'autres lois.<br><br>Comme décrit en détail dans les réponses, les procédures prévues par la CSA (et les autorités concernées) sont similaires, en particulier en ce qui concerne les motifs raisonnables de la saisie et les nombreuses exigences procédurales en matière de protection.<br><br>Les mêmes mesures sont appliquées lorsque les recherches sont étendues (comme dans l'article 19.2) et dans les situations où la localisation des données ne peut être déterminée. | Le Ghana applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Il serait souhaitable de clarifier la mise en œuvre de l'article 19.3.d. 19.3.d. serait souhaitable. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Grèce | La législation prévoit des saisies (à l'aide des procédures décrites ci-dessus) qui impliquent le pouvoir de sécuriser les données, de les copier, de les conserver et d'en maintenir l'intégrité, ainsi que de supprimer les données ou de les rendre inaccessibles.<br><br>Les mêmes mesures sont appliquées lorsque la localisation des données ne peut être déterminée que lorsque les recherches sont étendues. Les autorités compétentes et les experts impliqués sont les mêmes. La Grèce dispose d'une division de la cybercriminalité et d'une division de la police scientifique. | La Grèce applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Grenade | La Grenade a fait savoir qu'elle se fondait sur les informations disponibles/recueillies :<br><br>1. L'enquêteur établit la nécessité de l'enquête<br>2. Une déclaration sous serment des circonstances est présentée au magistrat<br>3. Le mandat de perquisition est accordé sur la base des paramètres et des affirmations figurant dans la déclaration sous serment.<br>4. Exécution d'un mandat de perquisition sur la cible/le suspect<br><br>La loi réglemente le retrait du système de son emplacement d'origine et non la copie de données. Rendre les données inaccessibles ou supprimer le contenu du système informatique n'est applicable qu'en cas de violation de la vie privée ou de pornographie enfantine (dans cette loi), couverts par l'article 32 (2).<br><br>La Grenade n'applique pas les mêmes mesures lors de l'extension d'une recherche et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées.<br><br>La saisie des données peut être autorisée par un magistrat ou un juge et exécutée par l'unité de criminalistique numérique. Une assistance technique peut être demandée au fournisseur de services local ou à l'entreprise de télécommunications. | La Grenade applique des pouvoirs spécifiques pour mettre en œuvre l'art. 19.3. Toutefois, il apparaît que l'art. 19.3.b de la CB n'a pas été mis en œuvre, tandis que la loi nationale mettant en œuvre l'art. 19.3.d a un champ d'application plus étroit que celui requis par la CB. Des dispositions plus spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Hongrie | L'article 315 du CPC couvre tous les éléments de l'article 19.3.<br><br>Les ordres de saisie peuvent être émis par un tribunal, le ministère public ou le chef de l'autorité d'enquête concernée. Les procédures suivies lorsque la localisation des données est inconnue sont les mêmes que celles suivies lorsque les | La Hongrie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | recherches sont étendues. Des ordres de perquisitions supplémentaires peuvent être obtenus et l'urgence de la situation peut être prise en compte. Les saisies sont exécutées par la police ou une autre entité nationale chargée de l'application de la loi ou par le ministère public. Ils disposent d'un personnel spécialement formé mais peuvent faire appel à des experts. | |
| Islande | La disposition générale relative à la saisie d'objets figure à l'article 68, paragraphe 1, du code pénal. 68.1 du CCP.<br><br>L'art. 68.2 contient une règle de proportionnalité. Comme indiqué dans le rapport explicatif des dispositions respectives, des moyens moins intrusifs peuvent être utilisés pour obtenir des preuves. Par exemple, la police peut demander au propriétaire ou au gardien d'autoriser l'accès à des éléments de preuve potentiels, afin qu'ils puissent être vus et photographiés pour les besoins de l'enquête. La police peut également demander au propriétaire ou au dépositaire de fournir des informations sur un objet, par exemple en remettant une photocopie ou une autre forme de copie d'un document ou des copies d'informations électroniques provenant d'un ordinateur. Ce remède plus doux pourrait, entre autres, être utilisé lors de la perquisition des locaux d'une entreprise au lieu de saisir, et donc d'enlever, les documents originaux et les ordinateurs qui s'y trouvent.<br><br>L'article 69 du Code de procédure pénale stipule que la police peut saisir des objets sans décision de justice. Toutefois, le deuxième paragraphe contient une clause de non-responsabilité qui stipule que si les objets sont détenus par une personne autre que l'accusé et qu'il n'y a pas de risque qu'ils soient détruits ou éliminés, la saisie doit être décidée par une décision de justice, sauf si le propriétaire ou le détenteur a donné son consentement sans équivoque.<br><br>Toutefois, comme l'a stipulé la Cour suprême d'Islande, bien qu'il soit permis de saisir un objet sans décision de justice, cf. art. 69.1 du CCP, l'Art. 68 du même code ne doit pas être interprété de manière à ce que la police puisse enquêter sur le contenu matériel des appareils électroniques sans décision de justice.<br>Dans la pratique, les autorités policières font généralement une copie des documents saisis.<br><br>L'intégrité des données informatiques stockées est préservée par la saisie des données. Une chaîne de contrôle est généralement mise en place à l'aide de rapports de perquisition et de saisie, puis de rapports de rappel sur le traitement des éléments.<br><br>En général, la police rend les données inaccessibles en saisissant l'ordinateur ou l'objet sur lequel elles sont stockées. | L'Islande applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En outre, le règlement n° 880/2019 relatif au traitement, à la garde et à la vente des biens et articles saisis, suspendus et confisqués. L'article 20 du règlement contient des dispositions sur le traitement et l'enregistrement des données électroniques qui semblent contenir certains éléments de l'art. 19.3 de la Convention. | |
| Israël | Les procédures relatives à l'article 19.3 sont les mêmes que celles décrites ci-dessus, y compris lorsque les recherches sont étendues ou lorsque la localisation des données ne peut être déterminée.<br><br>Le cadre juridique autorise la saisie des données. En pratique, dans la plupart des cas, les autorités compétentes saisissent le dispositif physique sur lequel les données informatiques sont stockées et créent ensuite, à l'aide d'outils de police scientifique, une copie des données informatiques stockées. Dans le cas de données informatiques stockées en dehors d'Israël, les autorités compétentes saisissent le dispositif à partir duquel les données sont accessibles, puis "saisissent" les données en créant une copie. Occasionnellement, la saisie de données informatiques se fait par le retrait des données, dans les cas où l'appareil sur lequel les données sont stockées n'a pas été saisi ou a été saisi puis rendu à son propriétaire.<br><br>En vertu de l'article 39 de l'ordonnance de procédure pénale, après une condamnation pénale, le tribunal peut ordonner la confiscation, y compris la destruction d'un objet saisi qui a été utilisé pour commettre un délit. Cela peut inclure la destruction de données informatiques. | Israël applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. |
| Italie | Le code de procédure pénale italien comprend l'article 254-bis, qui prévoit la saisie de données informatiques auprès des fournisseurs de services informatiques, télématiques et de télécommunications. Cet article permet à l'autorité judiciaire d'ordonner la saisie des données conservées par ces fournisseurs, telles que les données relatives au trafic ou à la localisation. Il permet d'acquérir ces données en les copiant sur un support approprié, en s'assurant de leur conformité avec les données originales et en empêchant toute modification. Les fournisseurs de services sont également tenus de conserver les données originales en toute sécurité. En pratique, la saisie peut être exécutée en demandant à l'administrateur de l'espace informatique de mettre les données hors ligne, d'interdire tout accès ultérieur, de modifier les identifiants d'accès ou de créer une copie légale des données stockées. Toutefois, cette disposition ne semble pas englober toutes les situations prévues par l'article 19.3. 19.3. | L'Italie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique, notamment en ce qui concerne la copie (article 19, paragraphe 3, point b)) et l'effacement des données ou le fait de les rendre inaccessibles (article 19, |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'Italie a indiqué qu'elle applique les mêmes mesures lorsqu'elle effectue des recherches, y compris dans les cas où elle n'est pas sûre de l'endroit où se trouvent les données recherchées.<br><br>Selon l'art. 252, l'autorité judiciaire ordonne la saisie de tout autre type de données (trouvées lors d'une perquisition) stockées dans un ordinateur ou un système télématique. | paragraphe 3, point d)) dans les cas où les données auxquelles les autorités accèdent en vertu des paragraphes 1 et 2 ne se trouvent pas dans les locaux des fournisseurs de services. |
| Japon | Plusieurs articles (largement décrits ci-dessus) du CPC se combinent pour permettre au Japon de satisfaire à tous les éléments de l'article 19.3 a à d.<br><br>En général, les mêmes considérations - en particulier les faits du cas individuel - sont évaluées lorsqu'une recherche est étendue et lorsque la localisation des données ne peut être déterminée. Les mêmes fonctionnaires sont impliqués aux mêmes étapes. | Le Japon applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Kiribati | La loi sur la cybercriminalité prévoit la saisie de données informatiques selon les procédures décrites ci-dessus. Les saisies sont autorisées par un tribunal et exécutées par la police, éventuellement avec une assistance technique.<br><br>Les services répressifs de Kiribati ont tendance à s'arrêter au stade où la localisation des données ne peut être déterminée, plutôt que d'étendre les recherches. | Kiribati applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. Toutefois, la manière dont les pouvoirs de maintenir l'intégrité des données et de supprimer les données ou de les rendre inaccessibles conformément à l'article 19, paragraphe 3, points c) et d), sont mis en œuvre à Kiribati n'est pas claire. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Lettonie | La Lettonie peut saisir et rechercher des données et des systèmes. Les articles 191 et 192 du CPC satisfont à l'exigence selon laquelle les Parties doivent être en mesure d'effectuer et de conserver des copies des données et d'en préserver l'intégrité. Les données peuvent rester sous la garde d'un organisme non étatique, mais elles sont soumises aux | La Lettonie applique une combinaison de pouvoirs de perquisition et de saisie |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | restrictions de l'article 191 - par exemple, que les données soient conservées en l'état pendant la période nécessaire aux besoins de la procédure. La Lettonie a le pouvoir de supprimer les données.<br><br>En vertu de l'article 219 du CPC, la Lettonie semble disposer de tous les pouvoirs requis par l'article 19.3 de Budapest. | généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Liechtenstein | Deux sections du CPC prévoient certaines des exigences de l'article 19.3. Afin de préserver l'intégrité des données informatiques saisies, le nombre de fichiers saisis et la taille totale du stockage sont comparés directement après le processus de copie. Si un tribunal ordonne que des données soient rendues inaccessibles, un appareil ou un système entier sera saisi par la police nationale. Les données ne sont pas effacées lors des perquisitions.<br><br>Comme indiqué, les mêmes mesures sont appliquées lorsque la localisation des données est inconnue que lorsqu'une recherche est étendue - c'est-à-dire que le Liechtenstein peut effectuer de telles recherches si l'accès aux données est possible à partir du Liechtenstein.<br><br>Les mandats délivrés par un tribunal à la demande d'un procureur sont exécutés par l'unité de lutte contre la criminalité numérique de la police nationale. Cette unité dispose de l'expertise et des ressources nécessaires pour effectuer des expertises informatiques, y compris, par exemple, des portefeuilles officiels pour la saisie de crypto-monnaies. | Le Liechtenstein applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Lituanie | Les articles 94, 145, 147 et 155 (et 158 en cas d'accès clandestin) du code de procédure pénale répondent à plusieurs exigences de l'article 19, paragraphe 3. Les actions concernées peuvent être autorisées par un procureur, mais doivent souvent être autorisées par un tribunal.<br><br>Les mêmes exigences s'appliquent lorsque l'emplacement des données n'est pas connu que lorsqu'une recherche est étendue.<br><br>Les perquisitions et les saisies sont autorisées par un tribunal à la demande du procureur. L'ordre est exécuté par le fonctionnaire chargé de l'enquête préliminaire ou par le procureur. L'examen des données est effectué par des agents des services répressifs spécialement formés et équipés. Des spécialistes des technologies de l'information peuvent apporter leur aide. | La Lituanie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Luxembourg | Les procédures utilisées pour saisir ou sécuriser de la même manière des données en vertu de l'article 19, paragraphe 3, sont les mêmes que celles décrites précédemment. Les dispositions des articles 33 et 66 du CPC (fournies par le Luxembourg) couvrent explicitement les quatre éléments de l'article 19.3.<br><br>Les mêmes mesures sont appliquées lorsqu'une recherche est étendue que lorsque l'emplacement des données ne peut être déterminé, tant que le support de stockage des données peut être accessible à partir du territoire physique. La police spécialisée effectue des saisies de preuves électroniques et fait appel à du matériel et du personnel supplémentaires si nécessaire. | Le Luxembourg applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Malte | Les procédures décrites ci-dessus sont également utilisées en ce qui concerne les exigences de l'article 19.3 : les magistrats autorisent les saisies et la police (et éventuellement des experts techniques) les exécutent. Les mêmes mesures sont utilisées lorsque la localisation des données ne peut être déterminée.<br><br>Conformément au chapitre 9 de l'article 355L du code pénal, "*la police a le pouvoir de pénétrer dans les locaux, maisons, bâtiments ou enceintes utilisés, occupés ou contrôlés, même temporairement, par une personne en état d'arrestation, et de les fouiller, si elle a des motifs raisonnables de soupçonner qu'il existe des éléments de preuve, autres que des éléments soumis à un privilège légal, qui se rapportent à l'infraction ou à une infraction connexe, et cette fouille doit être limitée à ce qui est raisonnablement nécessaire pour découvrir ces éléments de preuve".*<br><br>Conformément au chapitre 9, article 355P du code pénal *: "La police, lorsqu'elle se trouve légalement dans des locaux, peut saisir tout ce qui s'y trouve si elle a des motifs raisonnables de croire qu'il a été obtenu à la suite de la commission d'une infraction ou qu'il constitue un élément de preuve en rapport avec une infraction ou qu'il fait l'objet d'un signalement dans le système d'information Schengen et qu'il est nécessaire de le saisir pour éviter qu'il ne soit dissimulé, perdu, endommagé, altéré ou détruit*<br><br>En vertu du chapitre 9 de l'article 355Q du code pénal, "*la police peut, outre le pouvoir de saisir une machine informatique, exiger que toute information contenue dans un ordinateur soit livrée sous une forme permettant de l'emporter et dans laquelle elle est visible et lisible".* | Malte applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'art. 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En ce qui concerne l'article 19, paragraphe 3, point d) - *"rendre inaccessibles ou supprimer ces données informatiques dans le système informatique consulté"*, le magistrat peut demander à l'autorité compétente de procéder à la suppression du contenu ou d'une partie de celui-ci. Cette communication peut se faire par le biais d'un mandat/décret. | |
| Maurice | Les saisies décrites à l'article 19.3 sont régies par l'article 28 et suivent les mêmes procédures que les perquisitions visées à l'article 19.1. Un tribunal a le pouvoir d'autoriser une saisie. La police (et la Financial Crimes Commission) exécute la saisie.<br><br>L'article 28 reprend pour l'essentiel les termes de l'article 19.3. Maurice a donc clairement le pouvoir de mettre en œuvre les quatre éléments de l'article 19.3.<br><br>Les demandes de recherche et les ordonnances qui en découlent précisent les paramètres de la recherche envisagée. Si une extension de la recherche est nécessaire, une seconde ordonnance doit être obtenue. Il est peu probable qu'un tribunal autorise l'extension d'une recherche lorsque la localisation des données est inconnue. | Maurice applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3 |
| Monaco | Les autorités ont souligné que le droit interne prévoit des mécanismes spécifiques pour la saisie ou la sécurisation de données informatiques dans le cadre d'une enquête ou d'une instruction judiciaire (article 255 du CPP).<br><br>L'art. 255 fournit une base juridique pour la copie et l'effacement de données informatiques dont la possession ou l'utilisation est illégale ou dangereuse pour la sécurité des personnes ou des biens.<br><br>Les originaux des logiciels sont mis en sécurité et des copies exactes sont réalisées. Les logiciels peuvent également être confiés à un expert lorsque les enquêteurs ne sont pas en mesure de les traiter eux-mêmes. | Monaco applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Monténégro | Les dispositions relatives à la saisie provisoire du CPC s'appliquent. L'art. 85.4 étend l'application aux données enregistrées dans des dispositifs de traitement automatique ou électronique des données et aux supports dans lesquels ces données sont enregistrées. Les données enregistrées dans les appareils de traitement automatique ou électronique des données et les supports sur lesquels elles sont enregistrées doivent être remises à la demande du tribunal, sous une forme lisible et compréhensible. Le tribunal et les autres autorités doivent respecter les règles relatives au maintien du secret des données. Il n'est cependant pas clair comment l'Art. 19.3 d) de la Convention est mis en œuvre dans le droit national. | Le Monténégro applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Il serait souhaitable de clarifier davantage la mise en œuvre de l'article 19.3 d). 19.3 d) serait souhaitable. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les autorités n'ont pas indiqué comment elles procèdent en cas d'extension de la perquisition et dans les situations où il est impossible de déterminer où sont stockées les données recherchées. Toutefois, le mandat de perquisition doit préciser tous les détails concernant les objets de la perquisition et de la saisie. Parallèlement, un nouveau mandat de perquisition et de saisie peut être demandé en cas de nécessité de perquisitionner un autre système informatique. | |
| Maroc | Il convient de noter que le Maroc est en train de mettre à jour sa législation. Dans l'intervalle, ses mécanismes de procédure pénale sont proches, dans la pratique, des exigences de la Convention. Ainsi, les éléments a à d de l'article 19.3 peuvent être satisfaits par la procédure marocaine. Il y a des indications que le Maroc peut satisfaire au moins certains de ces éléments par le biais de ses lois actuelles - par exemple, l'article 104 du CPP mentionne l'inventaire et la protection des articles qui ont été saisis. Il n'y a pas de pouvoir apparent pour supprimer les données ou les rendre inaccessibles.<br><br>Les procédures habituelles d'autorisation et de conduite d'une perquisition s'appliquent, sans discrimination particulière pouvant correspondre à des preuves électroniques et à des données électroniques stockées.<br>Une expertise technique est disponible. | Le Maroc applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. Il serait utile de clarifier davantage la mise en œuvre des éléments spécifiques a à d de l'article 19.3. 19.3. pourrait être bénéfique. |
| Pays-Bas | Le code de procédure pénale ne contient pas de dispositions spécifiques sur la saisie de données informatiques, mais les dispositions générales en matière de saisie peuvent être utilisées pour saisir des dispositifs de stockage de données. L'art. 125i du code de procédure pénale introduit le pouvoir de perquisitionner et de conserver des données. Les données en tant que telles ne peuvent pas être saisies, car elles ne sont pas considérées comme des "biens", mais elles peuvent être copiées par les forces de l'ordre lors d'une perquisition.<br><br>Les autorités ont indiqué qu'elles disposaient de la législation suivante : Lorsqu'un suspect est arrêté ou détenu, les articles suivants s'appliquent : Art. 53-55b DCCP et 95-96 DCCP 19 para 3 CCC. Lorsqu'un lieu (autre qu'un domicile) est perquisitionné, les articles suivants s'appliquent : Art. 96 DCCP, Art. 96b DCCP, Art. 96c DCCP et Art. 110 DCCP 19 paragraphe 3 CCC.<br><br>Dans l'intérêt de l'ordre public ou de la protection des victimes, l'article 125p du code de procédure pénale permet au procureur d'ordonner à un fournisseur d'accès à Internet de rendre le contenu inaccessible et, dans certains cas, sur ordre judiciaire, de supprimer définitivement les données (article 354 du code de procédure pénale). | Les Pays-Bas appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Le pouvoir de piratage de l'art. 126nba, lid 1, sub e, DCCP, permet également de rendre des données inaccessibles, si les données se trouvent dans un travail automatisé concernant ou à l'aide duquel une infraction pénale a été commise. Dans ce cas, le procureur peut décider que ces données sont rendues inaccessibles dans la mesure où cela est nécessaire pour mettre fin à l'infraction pénale ou pour prévenir de nouvelles infractions pénales.<br>Les mesures décrites sont également applicables à l'extension des situations de recherche. | |
| Nigéria | Les procédures et exigences de l'article 45 de la loi sur la cybercriminalité, décrites précédemment, régissent les saisies comme dans l'article 19.3 de la Convention de Budapest. Les autorités d'autorisation et d'exécution sont les mêmes.<br>Les mêmes mesures sont appliquées lors de l'extension d'une recherche conformément à l'article 19, paragraphe 2, et dans les situations où la localisation des données ne peut être déterminée. | Le Nigeria applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Toutefois, la manière dont les pouvoirs de faire et de conserver une copie des données, de maintenir l'intégrité des données et de supprimer les données ou de les rendre inaccessibles en vertu de l'article 19, paragraphe 3, points b) et d), sont mis en œuvre au Nigeria n'est pas claire. Des dispositions spécifiques aux données et systèmes informatiques pourraient apporter plus de clarté et de sécurité juridique. |
| Macédoine du Nord | Les conditions, les étapes de la procédure et les autorités concernées par les saisies au titre de l'article 19.3 sont les mêmes que celles décrites ci-dessus pour l'article 19.1. Elles sont également les mêmes que pour l'extension des perquisitions en vertu de l'article 19.2 et lorsque la localisation des données est inconnue.<br><br>Les articles 194 et 198 du code de procédure pénale font référence à la conservation des objets saisis, y compris les données informatiques. Les articles 184, 194 et 198 du CPC prévoient la copie des preuves électroniques. Associés aux normes du laboratoire médico-légal du ministère de l'intérieur, ces articles du CPC permettent de protéger l'intégrité des | La Macédoine du Nord applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données. Cependant, les articles du CPC ne concernent pas l'un des autres éléments de Budapest 19.3 : supprimer les données ou les rendre inaccessibles. | sécurité juridique, notamment en ce qui concerne la suppression des données ou le fait de les rendre inaccessibles, ce qui ne semble pas possible. |
| Norvège | Deux articles du code de procédure pénale et l'article 7 de la loi sur la police satisfont aux éléments de l'article 19, paragraphe 3, points a) à d). En particulier, l'article 203 autorise l'enlèvement d'objets physiques et, implicitement, le fait de rendre inaccessibles ou d'enlever des données informatiques. En outre, le pouvoir légal de la police de prévenir ou de faire cesser des infractions peut être utilisé pour ordonner que des données soient rendues inaccessibles, par exemple pour empêcher la propagation de logiciels malveillants. La Norvège a fourni plus de détails et d'exemples concernant ce pouvoir.<br>En général, les mêmes dispositions s'appliquent dans les cas où la localisation des données est inconnue que dans les cas d'extension des recherches. La bonne foi, la proportionnalité et la coopération internationale sont prises en considération. Les autorités concernées sont les mêmes. | La Norvège applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Panama | La base juridique de la saisie est l'article 308 du code de procédure pénale. Le règlement ne fait pas spécifiquement référence aux systèmes informatiques ou aux dispositifs de stockage, mais il est suffisamment large pour atteindre cet objectif.<br><br>Il n'existe pas de règlement spécifique pour mettre en œuvre ce qui est établi dans l'article 19.3d.<br><br>Il convient de noter que les autorités ont mentionné que les règlements de procédure permettent la saisie de tout type d'instruments utilisés dans la commission d'un acte criminel. Le règlement ne fait pas spécifiquement référence aux systèmes informatiques ou aux dispositifs de stockage, mais il est suffisamment large pour atteindre cet objectif.<br><br>Le Panama applique les mêmes mesures lorsqu'il étend une recherche (conformément à l'article 19, paragraphe 2) et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées.<br><br>Les autorités qui autorisent une saisie sont le juge en tant qu'autorité judiciaire. Les autorités qui procèdent à une confiscation sont le ministère public, agissant par l'intermédiaire des différents bureaux des procureurs, en tant | Le Panama applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Il semble que l'article 19.3d doive être transposé en droit interne. 19.3d doit être transposé en droit interne. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | qu'autorité compétente. En ce qui concerne les expériences techniques, l'article 298 du code de procédure pénale établit les exceptions dans lesquelles une perquisition et une saisie peuvent être effectuées sans autorisation judiciaire, si elles sont nécessaires pour empêcher la commission d'un crime ou en cas de flagrant délit. Cet article s'applique également lorsque le procureur qui effectue la perquisition détermine qu'il y a un risque de perte de preuves ou si celles-ci proviennent d'une perquisition immédiatement antérieure. Dans ces cas, cette procédure de perquisition exceptionnelle doit être soumise au contrôle d'un juge des garanties (en tant que contrôle ultérieur). | |
| Paraguay | Le code de procédure pénale paraguayen contient des dispositions relatives à la saisie et à la sauvegarde des preuves, y compris des preuves numériques. Conformément à l'article 196 du code, la procédure d'enregistrement sera suivie. Les effets ou objets saisis seront inventoriés et conservés en toute sécurité dans des lieux désignés, sous la garde des tribunaux. S'il s'agit d'objets de valeur, ils peuvent être remis à des détenteurs légitimes agissant en tant que dépositaires judiciaires. Lorsque les objets saisis risquent d'être altérés, disparus ou difficilement conservés, des reproductions, des copies ou des certifications de leur existence et de leur état peuvent être ordonnées.<br><br>Selon les informations fournies par les autorités paraguayennes, le respect des dispositions de l'article 19.3 repose sur des interprétations analogiques permises par le principe de la liberté de la preuve.<br>Après toute perquisition ou saisie, le ministère public a l'obligation de signaler ce qui a été trouvé et ce qui n'a pas été trouvé, qu'il s'agisse de preuves traditionnelles ou numériques.<br><br>Les autorités compétentes qui autorisent une saisie : par ordonnance d'un juge pénal compétent, à la demande du ministère public, puis saisine du Secrétariat national des biens saisis. | Le Paraguay applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Pérou | En ce qui concerne l'application de la saisie de données informatiques stockées, elle est prévue aux articles 214°, 217°, 316° et 318° du code de procédure pénale, une mesure qui est exécutée au mérite d'une résolution judiciaire ou qui entraîne une extension de la perquisition par une validation judiciaire de la confirmation de la saisie de biens. Les dispositions du chapitre V, du chapitre VI, du chapitre VII, du chapitre VIII et du titre X du code de procédure pénale, la loi 27697 - loi qui confère au procureur le pouvoir d'intervenir et de contrôler les communications et les documents privés dans des cas exceptionnels s'appliquent par analogie.<br><br>À cet égard, les autorités péruviennes ont interprété que l'article 19, paragraphe 3, alinéa a) de la Convention de Budapest, peut être appliqué au moyen de la "saisie" conformément au code de procédure pénale, et qu'en ce qui | Le Pérou applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | concerne les alinéas b) et c), il est susceptible d'être appliqué au moyen de la mesure d'"inspection" prévue par le code de procédure pénale, entre autres, qui sera appliquée en fonction de chaque cas spécifique.<br><br>Les autorités péruviennes indiquent que les mêmes mesures sont appliquées dans le cadre d'une extension de la recherche par la validation de l'exigence relative à la confirmation de la saisie des biens, conformément à ce qui est indiqué dans la procédure établie au titre X du code de procédure pénale. En ce qui concerne les situations dans lesquelles il n'est pas possible de déterminer où sont stockées les données recherchées, le non-respect de cette obligation peut entraîner des conséquences pénales, civiles ou administratives, selon les circonstances. Si possible, les serveurs peuvent être saisis. Les autorités qui respectent la loi, comme les procureurs du ministère public par exemple, peuvent demander au juge l'autorisation et l'exécution de la mesure limitant le droit de "saisie" sur les données enregistrées, qui peuvent être soumises à validation si, pendant l'exécution de la mesure, une extension de la recherche a été effectuée, sans préjudice de la validité de l'exécution de la mesure de "saisie" même si les données ont été stockées dans un autre système informatique, comme le prévoient les articles 214°, 217°, 316° et 318° du code de procédure pénale.<br><br>L'exécution des mesures restrictives de saisie est requise par le procureur, autorisée par le juge par une résolution dûment motivée, et exécutée par le procureur et/ou la police nationale, le personnel qui exécute la mesure doit avoir des connaissances informatiques de base minimales pour mener à bien la procédure. Des mesures restrictives sont appliquées aux données informatiques et aux supports de stockage de données stockés sur le territoire, conformément aux dispositions du chapitre V, du chapitre VI, du chapitre VII, du chapitre VIII et du titre X du code de procédure pénale, de la loi 27697 - qui confère au procureur le pouvoir d'intervenir et de contrôler les communications et les documents privés dans des cas exceptionnels - et du code de procédure pénale en vigueur. Cette loi joue un rôle complémentaire dans les affaires impliquant la levée du secret des communications et, contrairement à l'article 230° du code de procédure pénale, elle énumère divers délits, y compris ceux liés aux délits informatiques décrits dans la loi n° 30096. Le procureur peut utiliser cette loi pour soutenir les mesures de limitation des droits lorsque cela est nécessaire pour lever le secret des communications et accéder aux données informatiques stockées. Toutefois, il souligne que cela ne modifie pas la base juridique établie à l'article 230° du code de procédure pénale, qui impose différentes exigences formelles plutôt que d'énumérer des crimes spécifiques. | |
| Philippines | Les procédures et les exigences relatives aux recherches en vertu de l'article 19, paragraphe 3, sont les mêmes que celles décrites précédemment, et les mêmes autorités et experts sont impliqués. Les mêmes mesures sont appliquées lorsque la localisation des données est inconnue que lorsqu'une recherche est étendue en vertu de l'article 19.2. | Les Philippines appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La loi sur la prévention de la cybercriminalité prévoit expressément la possibilité d'effectuer et de conserver des copies des données, de maintenir leur intégrité et de supprimer les données ou de les rendre inaccessibles :<br><br>SEC. 15. Perquisition, saisie et examen des données informatiques. - Lorsqu'un mandat de perquisition et de saisie est dûment délivré, les autorités chargées de l'application de la loi ont également les pouvoirs et les devoirs suivants.<br><br>Dans le délai spécifié dans le mandat, procéder à l'interception, telle que définie dans la présente loi, et :<br><br>(a) Sécuriser un système informatique ou un support de stockage de données informatiques ;<br><br>(b) de faire et de conserver une copie de ces données informatiques sécurisées ;<br><br>(c) maintenir l'intégrité des données informatiques stockées ;<br><br>(d) procéder à une analyse ou à un examen médico-légal du support de stockage de données informatiques ; et<br><br>(e) rendre inaccessibles ou supprimer ces données informatiques dans l'ordinateur ou le réseau d'ordinateurs et de communications consulté. | |
| Pologne | La réponse réfléchie et détaillée de la Pologne cite de nombreux articles du CPC et règlements de police pour satisfaire aux éléments de l'article 19.3. La législation applicable ne prévoit pas d'étape procédurale distincte pour la conservation des preuves numériques. Par conséquent, les dispositions indiquées se réfèrent également aux parties b et d de l'article 19. Dans les cas où il n'est pas nécessaire de sécuriser les données en même temps que le support, une copie intégrale du contenu d'un support donné est effectuée sous la forme d'une copie binaire.<br><br>Conformément à l'article 218 a § 4 du CPC, le tribunal ou le procureur peut ordonner la suppression d'un contenu si sa publication ou sa communication constitue un acte interdit. Toutefois, il semble que le pouvoir de suppression ne puisse être utilisé qu'à l'égard des bureaux, institutions et entités exerçant des activités de télécommunications ou fournissant des services électroniques et des fournisseurs de services numériques, et qu'il soit applicable aux données qui ont déjà été publiées ou auxquelles l'accès a été accordé. Cela ne couvre toutefois pas tous les scénarios dans lesquels les | La Pologne applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions plus spécifiques pour mettre en œuvre les alinéas b. et d. de l'art. 19.3.b. et d pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données sont stockées dans le système informatique du suspect (données non publiques) et sont consultées par les autorités compétentes.<br><br>Il semble que le pouvoir de copier soit régulièrement exercé dans la pratique, mais la base juridique exacte de cette mesure n'est pas suffisamment claire.<br><br>Les mêmes mesures sont utilisées lorsque la localisation des données est inconnue que lors de l'extension d'une recherche. Les autorités d'autorisation et d'exécution sont les mêmes. | |
| Portugal | L'article 16 de la loi sur la cybercriminalité inscrit dans le droit portugais tous les pouvoirs prévus à l'article 19.3 de la Convention de Budapest.<br>Les mêmes mesures sont appliquées dans les cas d'extension des recherches et de recherches pour lesquelles la localisation des données est inconnue. La doctrine et la jurisprudence concernant l'intégration de la possibilité d'extension des recherches dans la pratique juridique et judiciaire ne sont pas entièrement établies. Toutefois, l'accès à un système informatique distant n'est autorisé que dans le cadre d'une perquisition. Lors d'une telle perquisition, la procédure est la même que pour une perquisition "locale". L'une des formes de saisie prévues à l'article 16 de la loi sur la cybercriminalité sera utilisée. Elles sont équivalentes à celles décrites à l'article 19, paragraphe 3, de la Convention de Budapest.<br><br>Dans la pratique, les enquêteurs accèdent au système distant et, si nécessaire, font par exemple une copie des données pertinentes.<br><br>Les autorités impliquées dans le processus sont celles décrites ci-dessus. | Le Portugal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |
| République de Moldavie | Les procédures de saisie ou de sécurisation des données en vertu de l'article 19.3, et les autorités concernées, sont les mêmes que pour les perquisitions en vertu de l'article 19.1.<br><br>Les procédures d'extension d'une recherche en vertu de l'article 19.2 *et* lorsque la localisation des données ne peut être déterminée (et les autorités concernées) sont les mêmes que pour les recherches en vertu de l'article 19.1. | La Moldova applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La Moldavie ne dispose pas de dispositions législatives permettant de supprimer les données ou de les rendre inaccessibles. Toutefois, l'article 128 du code de procédure pénale, qui est une disposition générale, permet aux services répressifs et aux procureurs d'examiner les données et de les supprimer de tous les appareils saisis. | permettre une plus grande clarté et renforcer la sécurité juridique. |
| Roumanie | L'article 168 du CPP et les procédures standard de perquisition et de saisie prévoient les éléments a à c de l'article 19.3. En ce qui concerne l'article 19.3d, l'ordinateur ou les dispositifs de stockage internes ou autonomes sont considérés comme des corpus delicti au sens de la loi. Ils peuvent donc faire l'objet d'une ordonnance de saisie pendant l'enquête pénale et être confisqués à l'issue du procès. Le corps du délit peut être confisqué même si le procureur abandonne l'affaire pour cause de délit mineur.<br><br>Toutefois, le texte ne contient aucune indication concernant la saisie de données informatiques, le fait de rendre inaccessibles ou de supprimer des données informatiques dans l'ordinateur ou le dispositif recherché.<br><br>Les autorités habituelles sont impliquées dans les recherches relatives à l'article 19.3. | La Roumanie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.1. Il apparaît que l'article 19.3.d. n'a pas été mis en œuvre. 19.3.d. n'a pas été mis en œuvre. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Saint-Marin | La perquisition et la saisie de données informatiques se déroulent selon les mêmes procédures que pour les preuves matérielles. Bien que le droit applicable ne couvre pas suffisamment les éléments b-d de l'art. 19.3. de la CB, les autorités ont déclaré que les pouvoirs généraux du système juridique national peuvent englober ces pouvoirs<br><br>Plusieurs articles du code de procédure pénale prévoient l'intégrité des preuves. Les autorités ont déclaré que la suppression et l'inaccessibilité des données sont soumises à un ordre explicite délivré par l'autorité judiciaire compétente.<br><br>La loi n° 24 du 2 mars 2022, "Dispositions visant à mettre en œuvre les garanties et l'efficacité des procédures pénales" et les procédures opérationnelles pour l'exécution des saisies en général complètent le cadre juridique.<br><br>L'article 58-quinquies permet la saisie préventive de biens lorsqu'il y a des motifs raisonnables de croire qu'ils peuvent être utilisés pour aggraver ou étendre l'infraction en question, ou pour faciliter d'autres activités criminelles.<br><br>Il appartient au juge d'émettre un décret détaillé qui limite l'étendue de la saisie. Pour garantir l'extraction des données pertinentes, des mots clés sont souvent utilisés. La copie judiciaire des données est une entité indépendante, et toute | Saint-Marin applique des compétences générales pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | donnée superflue doit être restituée à son propriétaire légitime. La législation prévoit des garanties pour éviter les atteintes injustifiées à la vie privée. En cas de violation de ces protections, la saisie peut être annulée.<br><br>Il semble que Saint-Marin ne dispose pas de procédures établies pour traiter les cas où l'emplacement des données stockées est indéterminé.<br><br>La Cour accorde des pouvoirs délégués pour mener des enquêtes, des perquisitions et des saisies ; les forces de police exécutent ces pouvoirs délégués ou agissent de leur propre initiative dans le cas de crimes spécifiques.<br><br>Afin d'analyser les données, les fichiers et le matériel qui ont été saisis, les officiers des forces de police, toujours sur mandat du pouvoir judiciaire, collaborent avec des experts techniques spécialisés ou leur confient des tâches spécifiques. | |
| Sénégal | Les articles 90-1 à 90-14 du code de procédure pénale prévoient que les autorités peuvent saisir ou sécuriser de la même manière des données électroniques ou des systèmes d'information, copier et conserver les données saisies, préserver leur intégrité, les supprimer ou les rendre inaccessibles.<br><br>Les mêmes mesures sont appliquées lorsque les recherches sont étendues et dans les situations où la localisation des données ne peut être déterminée. Les autorités qui autorisent et effectuent les saisies sont les mêmes que celles décrites ci-dessus. | Le Sénégal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |
| Serbie | Les nombreux articles du code de procédure pénale examinés ci-dessus et les procédures opérationnelles standard des services répressifs concernés prévoient la mise en œuvre de l'article 19.3. Plusieurs articles prévoient que les "biens meubles" peuvent inclure des données, des appareils, des supports et des programmes informatiques qui peuvent être saisis temporairement pour être conservés à titre de preuve ou examinés par des experts en criminalistique. Les procédures opérationnelles normalisées des services répressifs et de la criminalistique numérique prévoient la copie des données à partir du dépôt d'origine. Les données électroniques accessibles via des réseaux informatiques ou d'autres moyens à distance peuvent être retirées ou rendues inaccessibles 1) par la saisie elle-même, conformément au code de procédure pénale et aux modes opératoires normalisés pour la sécurisation d'une scène de crime, ou 2) pour sécuriser les preuves et empêcher leur destruction, leur retrait ou leur altération, comme dans les modes opératoires normalisés pour la sécurisation d'une scène de crime. | La Serbie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19, paragraphe 3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique, en particulier en ce qui concerne l'article 19, paragraphe 3, point b). 19.3.b. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les mêmes mesures sont appliquées lors de l'extension d'une recherche et dans les situations où l'emplacement des données ne peut être déterminé.<br><br>Les procureurs demandent une saisie, les tribunaux l'autorisent ou l'ordonnent et la police l'exécute. Les unités spécialisées de la police disposent de l'expertise nécessaire. | |
| Sierra Leone | Pour permettre la saisie ou l'accès sécurisé à des données informatiques, l'agent d'exécution doit présenter une demande de mandat à un juge de la Haute Cour en vertu de l'article 10 (1). Ce mandat peut être utilisé comme une autorisation d'accès, de saisie ou de sécurisation d'un système informatique, d'un programme, de données ou d'un support de stockage de données informatiques qui peut être requis comme preuve d'une infraction dans le cadre d'une enquête ou d'une procédure pénale ou qui a été acquis par une personne en raison de la commission d'une infraction.<br><br>Un mandat délivré autorise un agent d'exécution à saisir ou à sécuriser un système informatique ou une partie de celui-ci ou un support de stockage de données informatiques et couvre également les éléments des lettres b-d de l'Art. 19 du BC.<br><br>La Sierra Leone a indiqué qu'elle appliquait les mêmes mesures lors de l'extension d'une recherche et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées.<br><br>Les autorités compétentes qui autorisent la mesure sont les juges et effectuent une saisie telle que décrite à l'article 19.3 sont les agents chargés de l'application de la loi, tels que la police et d'autres autorités compétentes. | La Sierra Leone applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.3. |
| République slovaque | La saisie du matériel informatique et des supports de stockage est possible en vertu des pouvoirs généraux de l'article 89a, qui prévoit l'obligation de "délivrer la chose". Sur la base d'une demande préalable, la personne doit être informée des conséquences du non-respect de cette obligation et du fait que cette chose, qui peut être utilisée à des fins de preuve, peut être confisquée et que l'article 90 - confiscation d'une chose - s'applique en cas de non-délivrance d'une chose qui peut être utilisée à des fins de preuve.<br><br>Pour obtenir des données informatiques à partir d'objets ainsi sécurisés ou de supports de stockage de données informatiques, aucun autre ordre n'est nécessaire. La Cour suprême de la République slovaque s'est déjà prononcée sur ce point dans le cadre de son activité décisionnelle. | La République slovaque applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'article 91.1 b) du CPC semble répondre aux exigences de l'art. 19.3 b) de la Convention. Les autorités peuvent ordonner à toute personne de retirer les données du système informatique.<br><br>L'intégrité des données informatiques est garantie par les valeurs de hachage (MD5 ou SHA-1) des données informatiques sécurisées. Cette opération est réalisée par un technicien ou un expert judiciaire lors de la sécurisation d'une trace ou de données informatiques.<br><br>Les autorités ont indiqué que les mêmes procédures sont utilisées dans les extensions de recherche et lorsque la localisation des données est inconnue - c'est-à-dire qu'une tentative est faite pour déterminer la localisation des données. | |
| Slovénie | Les articles 219 bis et 223 bis du CPC semblent couvrir les alinéas a à c de l'article 19.3. La Slovénie a le pouvoir de supprimer des données ou de les rendre inaccessibles en vertu de l'article 498 du CPC. L'article 498 est une disposition générale détaillée concernant la confiscation d'objets. Dans le cas des données électroniques, les objets saisis sont des supports de données. Toutefois, il semble que cette disposition ne s'applique pas aux données informatiques et il peut donc être problématique d'appliquer une telle règle lorsqu'il est nécessaire de "rendre inaccessibles ou d'enlever des données informatiques", mais pas le support de stockage sur lequel les données sont stockées.<br><br>Il semble que les mêmes mesures soient utilisées et que les mêmes autorités soient impliquées dans les cas de recherche étendue que dans les cas où la localisation des données ne peut être déterminée. L'accent est mis sur l'autorisation par un mandat initial ou un mandat ultérieur, en supposant que les systèmes ou dispositifs ultérieurs sont accessibles à partir de l'élément initial. Toutefois, les procédures ne sont pas claires dans les cas où la localisation des données est inconnue. | La Slovénie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Il apparaît que la Slovénie a mis en œuvre l'art. 19.3.d. uniquement par le biais de pouvoirs généraux de perquisition et de saisie. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Espagne | L'article 588sexies (c) du code de procédure pénale (LECrim) autorise la saisie et la copie de supports physiques susceptibles de contenir des données pertinentes, pour autant que les conditions appropriées soient réunies pour garantir l'authenticité et l'intégrité des données. Le juge chargé de l'enquête est responsable de l'autorisation de la perquisition et de la saisie des données et décide de la marche à suivre la plus appropriée. Le législateur espagnol confie à l'autorité judiciaire le soin d'établir les conditions nécessaires pour garantir l'intégrité et la conservation des données pour les expertises, qui seront évaluées au cas par cas en fonction des circonstances de l'enquête. | L'Espagne applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En résumé, le droit procédural espagnol prévoit que le juge est chargé de décider de la manière spécifique dont la saisie des données sera effectuée.<br><br>Les seules mesures visées à l'article 19.3 de la Convention expressément mentionnées dans le texte juridique espagnol sont la réalisation et la conservation de copies de données et la confiscation ou la saisie de l'appareil informatique.<br><br>En pratique, le juge peut également ordonner que les informations saisies soient stockées dans le système informatique soumis à enregistrement, mais que les mots de passe d'accès soient modifiés, avec l'autorisation du juge, afin que les informations soient préservées et ne puissent pas être consultées par l'enquêté lui-même ou par des tiers extérieurs à l'enquête.<br><br>Les mêmes normes sont appliquées dans les cas où les preuves se trouvent sur des serveurs étrangers ou sur des serveurs en nuage, mais le contexte est pris en compte. Si l'accès aux preuves est possible à partir de l'équipement initialement enregistré, mais que l'emplacement des preuves est inconnu, des garanties procédurales appropriées, conformément à la législation espagnole, et une autorisation judiciaire sont nécessaires pour y accéder. | |
| Sri Lanka | Les sections 18 et 20-22 de la loi sur la criminalité informatique (Computer Crime Act) sont utilisées pour mettre en œuvre les saisies prévues à l'article 19.3. En vertu de l'article 22 de la loi sur la criminalité informatique, le Sri Lanka a le pouvoir de supprimer des données ou de les rendre inaccessibles ("lorsqu'un élément ou des données ont été saisis ou rendus inaccessibles au cours d'une enquête, l'officier de police chargé de la perquisition doit remettre au propriétaire ou au responsable de l'ordinateur ou du système informatique une liste complète de ces éléments et données, y compris la date et l'heure de la saisie ou de l'interdiction d'accès à l'ordinateur"). Certains éléments du pouvoir de copier des données à l'usage des fonctionnaires de la justice pénale et d'en préserver l'intégrité peuvent être implicites dans la LCC (la LCC permet de faire des copies pour un tiers dans certaines circonstances).<br><br>Les mêmes mesures sont appliquées lorsque les recherches sont étendues conformément à l'article 19, paragraphe 2, et dans les situations où la localisation des données ne peut être déterminée.<br><br>La police est l'autorité qui exécute les saisies. Elle peut être assistée par le CERT du Sri Lanka et des experts nommés par le tribunal. | Le Sri Lanka applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Suède | Le CPC prévoit dans ses règles générales la saisie d'objets. Les règles générales prévoient le maintien de l'intégrité des données ainsi que la suppression des données ou le fait de les rendre inaccessibles. La copie de données électroniques est prévue par la section 17a, chapitre 27, du code.<br><br>Lorsque la localisation des données ne peut être déterminée, les mêmes mesures de copie peuvent être utilisées que pour les recherches étendues. Les autorisations et le déroulement des procédures sont les mêmes. | La Suède applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19, paragraphe 3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique, notamment en ce qui concerne l'article 19, paragraphe 3, point d). 19.3.d. |
| Suisse | Les autorités ont le pouvoir de rechercher, de saisir et de copier des données. Les réponses indiquent indirectement qu'il existe des procédures pour satisfaire à l'article 19, paragraphe 3, point c), c'est-à-dire pour protéger l'intégrité des preuves, notamment en les isolant des réseaux. En ce qui concerne l'article 19, paragraphe 3, point d), qui prévoit de supprimer les données ou de les rendre inaccessibles, l'article. 69 du code pénal prévoit que le tribunal ordonne, indépendamment de la responsabilité pénale de toute personne, la confiscation des objets utilisés ou destinés à être utilisés pour commettre une infraction ou qui ont été produits à la suite de la commission d'une infraction, si ces objets constituent un danger futur pour la sécurité publique, la morale ou l'ordre public. Le procureur peut également rendre une telle ordonnance lorsqu'il rend une ordonnance pénale.<br><br>Les mêmes procédures sont utilisées, et les mêmes fonctionnaires du système judiciaire sont impliqués, lorsque les recherches sont étendues et lorsque la localisation des données est inconnue. | La Suisse applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |
| Tonga | En vertu de l'article 9 de la loi sur les délits informatiques, la police peut perquisitionner et saisir des ordinateurs et des données, ainsi que copier et conserver des données. L'article 2 de la loi sur les délits informatiques précise que le terme "saisir" comprend également la suppression ou le fait de rendre les données inaccessibles. 2 précise que le terme "saisir" inclut également la suppression ou le fait de rendre les données inaccessibles.<br><br>Les mêmes mesures sont appliquées lorsque les perquisitions sont étendues et que la localisation des données ne peut être déterminée ; il n'existe pas de législation spécifique à ce sujet. L'extension d'une perquisition à la saisie ou à l'accès à des systèmes informatiques ou à des données dépend de ce que le mandat de perquisition stipule expressément, c'est- | Les Tonga appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | à-dire s'il inclut tout système informatique susceptible d'être connecté ou relié à l'appareil en question. De telles extensions ont été pratiquées et utilisées avec succès dans le cadre d'enquêtes policières.<br><br>Dans le passé, lorsque des données de localisation ont été perdues ou effacées et n'ont pu être déterminées, des experts informatiques de la police fédérale australienne et de la police néo-zélandaise, ainsi que des sous-traitants locaux, ont effectué un processus de récupération des données dans le cadre d'enquêtes sensibles et importantes uniquement. En outre, lorsque l'emplacement des données ne peut être déterminé, un soutien et une assistance technique seront recherchés auprès d'experts étrangers en collaboration avec le CERT.<br><br>Les magistrats autorisent les saisies conformément à l'article 19.3. Les saisies sont effectuées par des officiers de police, éventuellement en collaboration avec le CERT Tonga, et parfois avec l'aide d'experts médico-légaux étrangers. | |
| Tunisie | | |
| Türkiye | L'article 134 du CPC et l'article 17 du règlement relatif aux perquisitions judiciaires et préventives semblent prévoir les éléments a à c de l'article 19.3. La Turquie a fourni de nombreux détails sur sa législation et ses pratiques en matière de perquisition, en mettant l'accent sur la protection des preuves numériques. Par exemple, elle a mentionné le fait de se concentrer sur les particularités des systèmes informatiques, de s'assurer que seuls des spécialistes qualifiés (plutôt que des agents moins formés) travaillent sur les données électroniques, et d'utiliser des enregistrements vidéo, l'emballage médico-légal, le HASHing, la protection de l'écriture, etc. Il n'est pas certain que la Turquie ait le pouvoir de supprimer des données ou de les rendre inaccessibles.<br><br>Les procédures de perquisition et de saisie, ainsi que les fonctionnaires impliqués, sont les mêmes lorsque les perquisitions sont étendues et que la localisation des données est inconnue. | La Turquie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.3. Il serait souhaitable de clarifier davantage la mise en œuvre de l'article 19.3.d. 19.3.d. serait souhaitable. |
| Ukraine | L'article 159 du code de procédure pénale ukrainien prévoit un accès temporaire aux systèmes d'information électroniques, aux systèmes informatiques ou à des parties de ceux-ci, aux terminaux mobiles des systèmes de communication, qui s'effectue en prenant une copie des informations contenues dans ces systèmes d'information électroniques, systèmes informatiques ou à des parties de ceux-ci, terminaux mobiles des systèmes de communication, sans qu'il soit nécessaire de les retirer. | Il semble que l'Ukraine applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les questions liées au maintien de l'intégrité des données informatiques stockées, à l'inaccessibilité ou à la suppression de ces données dans le système informatique auquel l'accès est effectué ne semblent pas être réglementées par la législation ukrainienne.<br><br>Il semble que la mise en œuvre des éléments spécifiques décrits à l'article 19.3. nécessite une réglementation législative supplémentaire en introduisant les amendements appropriés au code de procédure pénale de l'Ukraine. | une plus grande clarté et renforcer la sécurité juridique, |
| Royaume-Uni | Les autorités britanniques ont indiqué que les pouvoirs conférés par l'APCE permettent de saisir ou de sécuriser de la même manière des données informatiques, tandis que l'activité elle-même sera menée à l'aide de processus opérationnels définis dans les procédures de formation de la police. Le pouvoir général de saisie est étendu par la législation pour couvrir les informations informatisées. C'est le cas en Angleterre, au Pays de Galles et en Irlande du Nord. En Écosse, il n'existe pas de mesures législatives séparées et distinctes pour saisir ou sécuriser les données informatiques. Lorsqu'il existe un pouvoir de perquisition, on considère qu'il existe un pouvoir de saisir ce qui est trouvé au cours de la perquisition.<br><br>Dans la pratique, les appareils électroniques sont souvent copiés ou "imagés" au lieu d'être saisis. Le pouvoir de copier les données électroniques des appareils est explicite dans la loi de 2001 sur la justice pénale et la police.<br><br>Il n'existe pas de dispositions régissant spécifiquement le traitement des données informatiques saisies dans le cadre d'un mandat de perquisition. Au lieu de cela, la manière dont ce matériel est traité est régie par les dispositions qui régissent le traitement du matériel en général. En outre, en vertu de l'APCE, les agents de police sont généralement habilités à conserver le matériel saisi ou produit aussi longtemps que nécessaire. Lorsque la saisie est effectuée aux fins d'une enquête criminelle, le matériel peut être conservé pour servir de preuve lors d'un procès pour une infraction, pour un examen médico-légal ou pour une enquête liée à une infraction.<br><br>Lorsque des informations électroniques sont accessibles depuis des locaux, un agent de police peut exiger la production de ce matériel "sous une forme qui peut être emportée et qui est visible et lisible ou à partir de laquelle il peut être facilement produit sous une forme visible et lisible". | Le Royaume-Uni applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3.<br><br>Le champ d'application de la mesure visant à rendre inaccessibles ou à supprimer les données informatiques d'un système informatique auquel on accède, tel qu'établi dans le droit interne, semble être limité aux situations où les autorités se trouvent sur les lieux et ne s'étend pas, par exemple, aux situations où un système informatique est perquisitionné dans les locaux des autorités chargées de l'application de la loi.<br><br>Des dispositions spécifiques aux données et systèmes informatiques créant un cadre juridique pour la perquisition et la saisie de données et systèmes informatiques applicables en |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les pouvoirs généraux de saisie étendus aux données informatiques (sections 19, 20 et 22 du PACE 1984) permettent aux forces de l'ordre de retirer physiquement les supports de stockage et de rendre ainsi les données inaccessibles lorsqu'un agent se trouve légalement sur les lieux.<br><br>Les autorités compétentes sont les mêmes que pour la recherche. L'expertise technique requise dépendra de l'affaire, mais des agents dûment formés des unités de lutte contre la cybercriminalité au niveau national, régional ou local peuvent être impliqués pour veiller à ce que le matériel soit géré correctement. | Angleterre, en Écosse, au Pays de Galles et en Irlande du Nord pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| États-Unis | Les mêmes mesures et procédures sont utilisées en cas d'extension des recherches et lorsque la localisation des données est inconnue. Les mêmes fonctionnaires du système judiciaire sont impliqués.<br><br>Les procédures décrites comprennent la possibilité de rechercher, de saisir et de copier des données. Les États-Unis ont le pouvoir de maintenir l'intégrité des données saisies. Cette obligation découle des droits constitutionnels de l'accusé à un procès équitable et à une procédure régulière, ainsi que (entre autres sources) des règles fédérales en matière de preuve, qui exigent que les données soient identifiées et authentifiées pour pouvoir être utilisées au cours du procès. Les forces de l'ordre ont des politiques concernant la "chaîne de possession" de toutes les preuves criminelles. Les données peuvent être rendues inaccessibles par l'exécution d'un mandat de perquisition, puisqu'elles sont généralement saisies et conservées en possession des forces de l'ordre. | Les États-Unis appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.3. |

# 7 ORDONNER A UNE PERSONNE DE PERMETTRE LA PERQUISITION ET LA SAISIE DE DONNEES INFORMATIQUES STOCKEES (EVALUATION DE L'ARTICLE 19.4)

Cette section évalue la mise en œuvre de l'article 19.4 :

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne ayant connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qu'il contient de fournir, dans la mesure du raisonnable, les informations nécessaires pour permettre l'application des mesures visées aux paragraphes 1 et 2.

## 7.1 Mise en œuvre de l'article 19.4 : vue d'ensemble

### 7.1.1 Mesures législatives et autres - résumé

L'article 19.4 prévoit que les Parties ont le pouvoir d'ordonner à "toute personne ayant une connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qu'il contient" de fournir, dans la mesure du raisonnable, les informations nécessaires pour atteindre les objectifs de la perquisition. Il convient de noter que cette disposition est sans préjudice des garanties prévues par le droit interne, telles que le droit de ne pas s'incriminer soi-même (voir également le chapitre suivant). Il semble que le respect de cette exigence par de nombreuses Parties ne soit pas clair. Tel qu'il est mis en œuvre par de nombreuses Parties, ce pouvoir se concentre sur les propriétaires ou les utilisateurs de systèmes, souvent des administrateurs de systèmes, du personnel informatique ou des employés d'entreprise. Cette focalisation peut être suffisante la plupart du temps, mais elle n'est pas assez large pour englober des catégories de personnes moins attendues qui peuvent avoir des connaissances utiles. Les parties sont invitées à s'assurer qu'elles disposent des mêmes pouvoirs pour obliger des tiers à les assister lors de perquisitions dans des systèmes informatiques que pour obliger des tiers à les assister lors de perquisitions dans des lieux physiques.

Dans la pratique, les autorités qui effectuent des perquisitions peuvent être en mesure de faire face à de telles situations. Mais il semble qu'il y ait une tendance, en particulier dans les textes réglementaires, à limiter le "toute personne" de l'article 19.4 aux propriétaires ou utilisateurs de données. En outre, un certain nombre de Parties mettent en oeuvre cette disposition par le biais d'injonctions de produire qui habilitent les autorités compétentes à ordonner à une personne sur leur territoire de soumettre des données informatiques spécifiées en possession ou sous le contrôle de cette personne. Bien que, dans certains cas, la fourniture des "informations nécessaires" puisse couvrir la divulgation des données effectivement recherchées, l'article 19.4 n'exige la divulgation que des "informations nécessaires" qui sont "raisonnables". Dans certaines circonstances, lorsque cela est compatible avec les cadres juridiques nationaux, le caractère raisonnable peut inclure la divulgation d'un mot de passe ou d'une autre mesure de sécurité aux autorités chargées de l'enquête et non la divulgation des données en tant que telles. Par conséquent, les Parties qui ont mis en œuvre l'obligation prévue à l'article 19.4 de la Convention sur la cybercriminalité par le biais d'injonctions de produire doivent démontrer que les "informations nécessaires" peuvent comprendre différents types d'informations et pas seulement les données en tant que telles.

Certaines Parties ont également indiqué que les administrateurs de système ou d'autres personnes qui ont une connaissance particulière du système informatique peuvent fournir leur assistance volontairement mais ne peuvent pas être obligés de le faire. Toutefois, cela ne

répond pas suffisamment aux exigences de l'article 19.4, car la disposition exige l'établissement d'une obligation pour les personnes de fournir les informations nécessaires. Le fait d'obliger légalement un administrateur de système à prêter son concours peut également libérer l'administrateur de toute obligation contractuelle ou autre de ne pas divulguer les données. Il convient de noter que cela est sans préjudice des garanties prévues par le droit national, telles que le droit de ne pas s'incriminer soi-même (voir également le chapitre suivant).

Un certain nombre de Parties exigent des poursuites ou une décision de justice avant de pouvoir exiger l'assistance d'une personne. Dans certains cas, il semble que les autorités puissent demander une ordonnance d'assistance lorsqu'elles demandent un mandat de perquisition. (La nécessité d'un mandat ou d'une autorisation pour contraindre une personne à coopérer peut être importante en termes de garanties, en particulier dans les Parties où le refus de coopérer peut entraîner une inculpation pénale).

Une demande de mandat peut ne pas exiger des autorités qu'elles précisent qui elles devront contraindre au moment de la demande.

Mais si les autorités n'ont pas cette connaissance, ou si elles ont des surprises une fois la recherche commencée, il peut être nécessaire de retarder ou d'interrompre la recherche en vue d'une demande ultérieure d'ordonnance d'assistance.

Dans ce cas, une partie serait toujours en conformité avec l'article 19.4, car elle pourrait en fait contraindre l'assistance.

Exemples d'éléments pouvant être trouvés dans les législations ou pratiques nationales des parties :[60]

- Andorre : l'article 397 (désobéissance) et l'article 427.1 (entrave) du CC prévoient des sanctions pénales (en tant que délit mineur) pour quiconque ne suit pas l'ordre des autorités compétentes.

- Australie : L'article 3LA de la loi sur les infractions (Crimes Act) prévoit une ordonnance exigeant d'une personne déterminée qu'elle fournisse toute information ou assistance raisonnable et nécessaire pour permettre à un agent de police d'accéder aux données contenues dans un ordinateur ou un dispositif de stockage de données.

- Autriche : L'article 111, paragraphe 2, du Code de procédure pénale dispose que, si des informations enregistrées sur des supports de données doivent être sécurisées, toute personne doit permettre l'accès à ces informations.

- Belgique : L'article 88.1 quater oblige toute personne ayant une connaissance particulière des aspects pratiques et spécifiques de la technologie informatique à fournir des informations sur les possibilités d'accès, la configuration, la protection et les clés de cryptage. L'article 88.2 étend cette obligation aux personnes chargées d'effectuer certaines actions, lorsque cela est nécessaire (démarrage de l'ordinateur, recherche de fichiers, etc.).

- Brésil : Les tribunaux peuvent ordonner la suspension temporaire des activités des fournisseurs d'accès à Internet et le paiement d'amendes, afin de se conformer aux injonctions des tribunaux de fournir les informations demandées. En outre, selon

[60] Ces exemples peuvent ou non répondre aux exigences de l'article 19.4. Ils montrent l'éventail des réponses possibles.

l'art. 378 du code de procédure civile, personne n'est dispensé de l'obligation de collaborer avec le pouvoir judiciaire pour découvrir la vérité.

- Bulgarie : d'une manière générale, toute personne est tenue par la loi de coopérer avec les autorités chargées de l'enquête et de partager tout ce qu'elle sait lorsqu'elle est interrogée.

- Le Canada : La section 487(2.2) prévoit explicitement qu'une personne responsable d'un bâtiment ou d'un lieu peut être tenue d'autoriser l'accès aux données et leur extraction.

- Costa Rica : En vertu de l'article 7 de la loi organique du pouvoir judiciaire, un juge peut ordonner à toute personne d'aider à l'enquête en fonction de ses connaissances.

- Croatie : En vertu de l'article 257.2 du Code de procédure pénale, toute personne utilisant l'ordinateur ou ayant accès à l'ordinateur et à d'autres dispositifs, ou le fournisseur de services de télécommunications, doit immédiatement prendre des mesures pour empêcher la destruction ou la modification des données.

- Chypre : Les autorités peuvent demander la coopération des administrateurs de système ; cette coopération ne peut être imposée.

- République tchèque : Conformément à l'article 8 du code de procédure pénale, il est possible de demander la coopération des personnes physiques et morales et d'imposer une amende en cas de non-respect de cette demande.

- Danemark : En vertu de la section 747 de l'AJA, l'approbation du tribunal peut être demandée pour des mesures qui requièrent une assistance ou pour obtenir des preuves qui peuvent être perdues ou qui ne peuvent être obtenues qu'avec des inconvénients ou des retards importants.

- République dominicaine : L'article 54 de la loi 53-07 prévoit le pouvoir d'ordonner à toute personne qui a connaissance du fonctionnement d'un système d'information ou de l'un de ses éléments ou des éléments de protection des données ou des mesures de protection des données d'un tel système de fournir les informations nécessaires.

- Estonie : Si une personne peut être considérée comme un témoin, elle a l'obligation de fournir des informations. En vertu de l'article 95 du CPC, un expert est "une personne qui applique des connaissances spécialisées non juridiques lorsqu'elle procède à une expertise dans des situations et conformément aux règles prévues par le présent code".

- Finlande : La loi sur les mesures coercitives stipule qu'une personne qui possède ou maintient un système d'information ou toute autre personne a l'obligation de fournir les informations nécessaires (telles que le mot de passe) et d'aider les autorités en cas de besoin.

- France : 2 infractions visent spécifiquement le refus de prêter assistance aux autorités - Refus de remettre aux autorités ou de mettre en œuvre la convention secrète de déchiffrement d'un moyen de cryptologie (article 434-15-2 dal1 du CC) et Refus de remettre aux autorités judiciaires ou de mettre en œuvre une convention secrète de déchiffrement d'un moyen de cryptologie lorsque ce refus n'a pas permis d'éviter la commission d'une infraction (article 434-15-2 para 2 du CC).

- Géorgie : Conformément à l'article 112 du code de procédure pénale, les enquêteurs et/ou autres agents chargés de l'application de la loi qui exécutent un mandat de

perquisition doivent d'abord demander aux personnes responsables du site de perquisition (par exemple, les administrateurs de système) de fournir volontairement les informations pertinentes. En l'absence de réponse, l'enquête peut recourir à l'exécution forcée.

- Allemagne : En vertu de l'article 95, paragraphe 1, du code de procédure pénale, des personnes qui ne sont soupçonnées d'aucun délit peuvent être obligées de remettre des codes d'accès ou de parler de leurs connaissances sur le fonctionnement d'un système informatique.

- Hongrie : Les articles 267 et 271 du code de procédure pénale confèrent aux autorités le pouvoir général de recueillir des preuves pénales et de demander des informations pertinentes à toute personne, tandis que l'article 305 prévoit que les autorités peuvent exiger d'une personne qu'elle rende ses données électroniques accessibles.

- Islande : L'article 92 de la loi n° 70/2022 sur les communications électroniques oblige les entreprises de télécommunications à aider la police dans les enquêtes criminelles.

- Israël : L'article 45 de l'ordonnance de procédure pénale impose à l'occupant du lieu pour lequel un mandat de perquisition a été délivré d'autoriser l'entrée et de fournir toute assistance raisonnable.

- Japon : Les autorités peuvent exiger des personnes qu'elles participent à la perquisition ou à la saisie, en particulier qu'elles fassent fonctionner l'ordinateur, et qu'elles coopèrent d'une autre manière (articles 111-2 et 222 du code de procédure pénale). L'expression "faire fonctionner l'ordinateur ou coopérer d'une autre manière" visée à l'article 111-2 du code de procédure pénale peut comprendre, par exemple, (1) l'explication de la composition d'un système informatique et des rôles, fonctions et modes de fonctionnement des différents ordinateurs qui le composent, (2) la fourniture d'instructions sur l'emplacement des supports d'enregistrement à saisir, et (3) le décryptage d'enregistrements électroniques ou magnétiques cryptés.

- Lettonie : Conformément à l'article 190 du code de procédure pénale, les autorités peuvent obtenir des informations électroniques de la part des personnes concernées par les perquisitions et les saisies. Ce mécanisme ne prévoit pas de sanctions, les personnes peuvent coopérer volontairement.

- Liechtenstein : Plusieurs articles du code de procédure pénale prévoient la possibilité d'exiger des personnes qu'elles prêtent leur concours à une saisie et de les y contraindre en cas de refus.

- Lituanie : L'article 97 du code de procédure pénale dispose que les personnes physiques et morales doivent produire les objets et documents utiles à l'enquête. L'article 219a du CPC prévoit que le propriétaire ou l'utilisateur d'un appareil électronique doit en permettre l'accès, y compris le décryptage et des explications sur son utilisation, et faciliter l'enquête.

- Monténégro : L'article 75, paragraphe 2, du CPC oblige les utilisateurs à fournir les informations nécessaires, et l'article 83, paragraphes 3 et 4, oblige les personnes à remettre les éléments pertinents.

- Maroc : La loi oblige les réseaux et les fournisseurs de services de télécommunications publics titulaires d'une licence à aider les autorités judiciaires.

- Pays-Bas : L'article 125k du CPC permet aux autorités compétentes de contraindre une personne dont on peut raisonnablement présumer qu'elle a connaissance des

dispositifs de sécurité d'une œuvre informatisée à fournir l'accès à l'œuvre informatisée ou à des parties de celle-ci ainsi qu'à ses mesures de sécurité, et à en prendre connaissance. Une injonction similaire peut être adressée à la personne qui peut être raisonnablement soupçonnée d'avoir connaissance de la méthode de cryptage utilisée pour les données. Certaines limitations existent à l'égard de catégories spécifiques de personnes (par exemple, les personnes qui pourraient s'auto-incriminer).[61] En vertu de l'article 558 du DCCP, les personnes peuvent être contraintes de se soumettre à certaines "actions forcées" pour obtenir un accès biométrique à un dispositif verrouillé par empreinte digitale ou identification faciale (si l'action peut être effectuée sans obliger les personnes à faire volontairement quelque chose elles-mêmes). Le fait de poser le pouce sur le smartphone ou d'amener le smartphone devant le visage d'une personne peut être fait sans obliger la personne à donner l'identifiant.

- Norvège : Lors de la perquisition d'un système informatique, la police peut ordonner à toute personne ayant affaire au système informatique de fournir les informations nécessaires pour permettre l'accès au système informatique ou pour l'ouvrir au moyen d'une authentification biométrique. Si l'ordre d'authentification biométrique est refusé, la police peut procéder à l'authentification par la force.

- Panama : L'article 75 du CPC établit l'obligation de coopérer, applicable aux entités publiques et privées, de manière rapide, efficace et complète aux exigences formulées par les autorités compétentes.

- Pérou : Conformément à l'article 337.3 b) du Code de procédure pénale, les autorités compétentes peuvent demander des informations à toute personne. Le non-respect des exigences formulées peut entraîner la criminalisation de la résistance ou de la désobéissance à l'autorité.

- Portugal : L'article 14.1 de la loi sur la cybercriminalité prévoit l'obligation pour toute personne de communiquer ou d'autoriser l'accès à des données aux autorités de justice pénale, si elles en font la demande.

- Roumanie : La coopération volontaire est recherchée dans la pratique et rendue.

- Sénégal : Le code de procédure pénale prévoit que toutes les personnes ayant connaissance du fonctionnement du système ou des mesures de sécurité qui protègent les données doivent fournir toutes les informations nécessaires à l'exécution de la perquisition ou de la saisie. Le CPC permet également aux autorités d'exiger de toutes les personnes en possession ou sous le contrôle de données qu'elles en protègent l'intégrité.

- Slovénie : L'article 219a du CPC oblige les propriétaires ou les utilisateurs de dispositifs électroniques à fournir l'accès à l'objet, les clés d'accès au cryptage ou les mots de passe, ainsi que toutes les explications nécessaires sur le fonctionnement de l'objet.

- Espagne : L'article 588e(c) 5 du CPP permet aux autorités et agents chargés des enquêtes d'ordonner à une personne de fournir les informations nécessaires.

- Suisse : Certains tiers peuvent être tenus de fournir des informations à la demande des autorités. Un article du code pénal (art. 265) prévoit certaines obligations de remise d'objets ou de biens et prévoit des exceptions à cette règle.

---

[61] Traduction automatique des dispositions respectives par un service de traduction automatique neuronal.

- Tonga : la section 9 de la loi sur les délits informatiques permet à un magistrat d'émettre un mandat couvrant la fourniture de l'assistance nécessaire et la section 10 prévoit des sanctions.

- Türkiye : Le bureau du procureur est autorisé, en vertu de l'article 160-161 du code de procédure pénale turc, à ordonner la production ou la protection de données.

- Royaume-Uni : La partie III de la RIPA 2000 prévoit des pouvoirs permettant d'exiger que les informations électroniques protégées qu'ils ont obtenues légalement ou qu'ils sont susceptibles d'obtenir légalement soient mises sous une forme intelligible.

- États-Unis : les autorités compétentes peuvent obtenir des ordonnances judiciaires en vertu de la loi "All-Writs Act" (28 U.S.C. § 1651), afin d'ordonner à un tiers de prêter son concours à l'exécution d'un mandat de perquisition dans certaines circonstances, si nécessaire.

## 7.2 Mise en œuvre de l'article 19.4 - Évaluation

Les réponses à la question suivante du questionnaire ont été évaluées :

- 2.4.1 Veuillez résumer les mesures législatives ou autres prises par votre pays pour garantir que vos autorités sont en mesure d'ordonner à une personne de fournir les informations nécessaires décrites à l'article 19, paragraphe 4. Veuillez résumer les règles applicables à cette disposition.

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Albanie | L'Albanie a indiqué que l'article 208/a du code de procédure pénale prévoit que le ministère public peut désigner un expert connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques, afin de permettre la mise en œuvre des mesures prévues par cet article.<br><br>L'Albanie a précisé que cette disposition ne devait pas être comprise comme se limitant exclusivement aux experts et qu'elle pouvait être interprétée comme signifiant que le procureur pouvait ordonner à toute personne ayant une connaissance spécifique du fonctionnement d'un système informatique de le faire. | L'Albanie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. Toutefois, une formulation plus spécifique dans le droit interne de l'Albanie contenant tous les éléments de l'article 19.4. pourrait permettre une plus grande clarté et renforcer la sécurité juridique. 19.4. pourrait permettre une plus grande clarté et renforcer la sécurité juridique. |
| Andorre | Deux articles du code pénal sanctionnent le fait de ne pas suivre l'ordre d'un juge ou d'autres autorités publiques. Les informations fournies par une personne connaissant le système ou ses protections seront transmises soit au juge, soit à la police spécialisée, selon le cas. | L'Andorre applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Argentine | Dans sa réponse, l'Argentine ne mentionne aucune disposition qui contienne expressément le pouvoir spécifique prévu à l'article 19.4 de la Convention. En outre, il est indiqué que cette disposition n'a pas été mise en œuvre en Argentine et que les autorités s'appuient sur les pouvoirs généraux prévus par le droit interne. Toutefois, étant donné que les provinces ont la capacité de réglementer leurs codes de procédure locaux, il a également été signalé que le code de procédure | L'Argentine applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | pénale de Neuquén prévoit que "toute personne physique ou morale qui fournit un service à distance par des moyens électroniques peut être tenue de remettre les informations en sa possession ou sous son contrôle concernant les utilisateurs ou les abonnés, ou leurs données. Les informations qui ne sont pas utiles à l'enquête ne peuvent pas être utilisées et doivent être restituées, avant d'être mises à la disposition de la défense, qui peut en demander la conservation. Les limitations applicables aux documents s'appliquent. | et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Arménie | L'Arménie a indiqué qu'elle avait mis en place des mesures législatives et autres permettant aux autorités d'ordonner aux personnes ayant connaissance du fonctionnement d'un système ou des mesures appliquées pour protéger les données de fournir les informations nécessaires.<br>L'Arménie cite l'art. 232 du CPC qui autorise les enquêteurs à demander à toute organisation des détails importants liés à l'affaire. Les autorités déclarent que, sous réserve de l'approbation du procureur superviseur, les enquêteurs peuvent également demander, par exemple, des détails tels que le moment et la durée de la connexion d'une personne à l'internet, son adresse de protocole internet (IP) et d'autres données de personnalisation liées à l'internet. | L'Arménie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Australie | Selon les deux lois applicables, les ordonnances judiciaires peuvent exiger d'une personne déterminée qu'elle fournisse toute information ou assistance nécessaire aux agents chargés d'effectuer la perquisition. | L'Australie applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'art. 19.4. |
| Autriche | L'article 111 du Code de procédure pénale impose aux personnes ayant des objets ou des actifs sous leur contrôle d'aider les autorités (avec certaines restrictions). L'article 93 du Code de procédure pénale précise les cas dans lesquels des mesures coercitives et des condamnations pour outrage peuvent être prononcées si les personnes concernées ne prêtent pas leur concours. | L'Autriche applique une combinaison de pouvoirs généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Azerbaïdjan | Il n'existe pas de dispositions spécifiques concernant l'obligation pour les personnes de prêter leur concours aux enquêtes, comme le prévoit l'article 19.4, mais, dans la pratique, les dispositions générales relatives à la collecte de preuves et aux procédures d'enquête s'appliquent pour satisfaire aux exigences de l'article 19.4. Les articles 245.6, .7 et .9 permettent aux enquêteurs de saisir ou de rechercher des objets qui ne sont pas remis volontairement. Les enquêteurs peuvent également ouvrir des bâtiments ou des entrepôts fermés s'ils ne sont pas ouverts volontairement. Ces dispositions fournissent un cadre juridique permettant de contraindre les personnes à fournir les informations nécessaires aux | L'Azerbaïdjan applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | enquêtes, notamment en ce qui concerne le fonctionnement des systèmes et les mesures appliquées pour protéger les données électroniques. Les autorités s'appuient généralement sur ces normes générales dans les affaires électroniques. | clarté et renforcer la sécurité juridique. |
| Belgique | L'article 88quater prévoit que le juge d'instruction peut ordonner la coopération nécessaire (autre que celle de la personne mise en cause et de ses proches) dans le cas d'un système d'information, notamment pour mettre en marche un système, localiser certains fichiers, révéler les méthodes d'accès, etc. | La Belgique applique des pouvoirs spécifiques pour mettre en œuvre l'article 19.4. |
| Bénin | En général, les demandes de la police ou les ordonnances du juge d'instruction conformément au CPP constituent la base pour obtenir les informations nécessaires. Les personnes qui fournissent ces informations bénéficient d'une protection juridique (si elles ne sont pas elles-mêmes impliquées dans l'infraction).<br><br>En outre, l'article 588 de la loi sur le code numérique impose aux personnes ayant connaissance des mesures de sécurisation du système d'assister les agents de recherche. Le défaut d'assistance est puni d'une amende.<br><br>Les art. 13, 14 et 40 du CPP, qui prévoient les pouvoirs de la police judiciaire et des procureurs, sont également applicables. | Le Bénin applique une combinaison de pouvoirs généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Bosnie et Herzégovine | La Bosnie-et-Herzégovine s'appuie sur les règles habituelles du code de procédure pénale - des formes juridiques de contrainte, telles que les citations à comparaître - pour obtenir des informations de la part des témoins, ainsi que sur des dispositions légales. Les articles 51 et 65 du code de procédure pénale obligent les utilisateurs du système à autoriser l'accès aux appareils, à les produire et à fournir des informations à leur sujet, sous peine de sanctions pénales potentielles, y compris une peine d'emprisonnement.<br><br>En revanche, les codes de la Fédération de Bosnie-et-Herzégovine, du district de Brcko et de la Republika Srpska stipulent que les personnes qui utilisent des appareils doivent en permettre l'accès et remettre ces supports de stockage. S'ils ne le font pas, ils s'exposent à des sanctions, des amendes ou des peines d'emprisonnement. | La Bosnie-Herzégovine applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4.<br><br>Il n'est pas certain qu'elle ait le pouvoir d'exiger l'assistance de toute personne (et pas seulement des utilisateurs du système). Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Brésil | Les tribunaux peuvent obliger toute personne à collaborer avec le pouvoir judiciaire pour découvrir la vérité. En cas de non-respect, le juge peut ordonner, outre l'imposition d'une amende, d'autres mesures inductives, coercitives, obligatoires ou de subrogation. La base juridique de cette mesure se trouve dans les articles 378 à 380 du code pénal. 378-380 du code de procédure civile.<br><br>Plus précisément, en vertu de l'art. 378 du code de procédure civile, "nul n'est dispensé du devoir de collaborer avec la justice à la découverte de la vérité". Cette disposition fournit une base juridique pour lapplication de l'article 19.4 en droit interne. 19.4 en droit interne.<br><br>À plusieurs reprises, le pouvoir judiciaire a répondu à des demandes de la police fédérale et a ordonné la suspension temporaire des activités des fournisseurs d'accès à Internet et le paiement d'amendes, afin de se conformer à des injonctions judiciaires de fournir les informations demandées nécessaires aux enquêtes criminelles en cours. En ce sens, si l'administrateur du système se montre récalcitrant à fournir l'accès ou à aider à la réalisation de la perquisition et de la saisie, cela peut être considéré comme une violation de l'ordre judiciaire qui a déterminé la mesure, ce qui peut même conduire à la responsabilité pénale de l'administrateur ou de quiconque détient les informations nécessaires et refuse de les fournir dans l'intérêt de l'exécution de la mesure de précaution.<br><br>En pratique, les autorités brésiliennes peuvent ordonner à toute personne ayant connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques de fournir les informations nécessaires. Toutefois, la fourniture de ces informations est limitée à ce qui est "raisonnable". Dans certaines circonstances, cela peut inclure la divulgation d'un mot de passe ou d'une autre mesure de sécurité. Toutefois, dans d'autres situations, cela peut ne pas être raisonnable, par exemple lorsque la divulgation menacerait la vie privée d'autres utilisateurs. Dans ces cas, les "informations nécessaires" pourraient être la divulgation des données réelles recherchées par les autorités compétentes, dans un format intelligible et lisible. | Le Brésil applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Bulgarie | D'une manière générale, toute personne est tenue par la loi de coopérer avec les autorités chargées de l'enquête et de partager tout ce qu'elle sait lorsqu'elle est interrogée. Selon l'article 4 de la loi sur le ministère de l'intérieur :<br><br>Les autorités de l'État, les organisations, les personnes morales et les citoyens sont tenus de prêter assistance aux autorités du ministère de l'intérieur et d'observer les ordres qu'elles émettent dans l'exercice de leurs fonctions statutaires ou dans le cadre de celles-ci. | La Bulgarie applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'article 64 de la même loi prévoit que les autorités de police peuvent donner des ordres écrits aux organisations, aux personnes morales et aux citoyens lorsque cela est nécessaire à l'accomplissement des fonctions de police. Ces ordres sont obligatoires à moins qu'ils n'exigent l'exécution d'un crime ou d'une violation évidente ou qu'ils ne mettent en danger la vie ou la santé de la personne concernée.<br><br>L'article 159 du code de procédure pénale peut également s'avérer pertinent, puisque (à la demande d'un tribunal ou de certaines autorités) tous les établissements, personnes morales, fonctionnaires et citoyens doivent produire des objets, des documents, des données informatiques et d'autres données susceptibles d'être importantes pour une affaire. | permettre une plus grande clarté et renforcer la sécurité juridique. |
| Cabo Verde | Le Cabo Verde a indiqué que l'article 16 de la CL permet d'adresser des injonctions à ceux qui ont le contrôle ou la disponibilité des données. Le législateur a prévu cette possibilité tout en restant dans le champ d'application de la loi. L'article stipule que S'il s'avère nécessaire de produire des preuves au cours du processus de découverte de la vérité et d'obtenir des données informatiques spécifiques stockées dans un système particulier, l'autorité judiciaire compétente peut ordonner à la personne qui a le contrôle ou la disponibilité des données de les rendre disponibles pour le processus ou d'en permettre l'accès. Le non-respect de cet ordre peut entraîner une sanction pour désobéissance. De même, quiconque a la disponibilité ou le contrôle de ces données doit se conformer à l'ordre décrit aux paragraphes 1 et 2. Il doit mettre ces données à la disposition de l'autorité judiciaire compétente ou permettre l'accès au système informatique où elles sont stockées, sous peine de sanction pour désobéissance. L'utilisation d'une telle injonction a toutefois des limites. Elle ne peut être appliquée aux systèmes informatiques utilisés dans le cadre d'activités juridiques, médicales, bancaires ou journalistiques. Au lieu de cela, le régime de secret pour les professionnels, les fonctions et les secrets d'État énoncé à l'article 247 du code de procédure pénale doit être appliqué avec les adaptations nécessaires. En outre, cette injonction ne peut être adressée à un suspect ou à une personne mise en cause dans l'affaire. | Le Cabo Verde applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4., mais il semble que le champ d'application de la mesure dans le cadre juridique national s'applique à une catégorie de personnes plus restreinte que celle visée par l'article 19.4". 19.4". |
| Cameroun | L'article 55 de la loi camerounaise sur la cybercriminalité permet aux autorités (le procureur de la République, le juge d'instruction ou la juridiction compétente) de demander à toute personne physique ou morale qualifiée d'effectuer des opérations techniques pour obtenir la version en clair des données saisies lorsqu'il apparaît que les données saisies ou obtenues au cours d'une enquête ou d'une instruction ont été cryptées. | Le Cameroun applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4., mais il semble que le champ d'application de la mesure en vertu du cadre juridique national couvre un type de situations et une |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | catégorie de personnes plus restreints que ceux prévus à l'article 19.4. de la CB. |
| Canada | L'article 487.02 du code pénal prévoit qu'un tribunal délivrant un mandat peut ordonner à une personne de prêter son concours à une perquisition, si l'on peut raisonnablement considérer que son concours est nécessaire. La section 487(2.2) prévoit explicitement (dans plusieurs alinéas) qu'une personne responsable d'un bâtiment ou d'un lieu peut être tenue de permettre l'accès à des données et leur extraction. | Le Canada applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Chili | Les réponses fournies par le Chili indiquent que la législation en la matière est constituée de l'article 12 de la loi 21.459, en liaison avec les articles 222 à 226 du code de procédure pénale. Le Chili cite également l'art. 190 du CPP, en vertu duquel le procureur peut citer différentes personnes comme témoins pour recueillir des déclarations. | Le Chili applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Colombie | La Colombie a indiqué qu'en vertu de la législation colombienne, les personnes qui connaissent le fonctionnement d'un système doivent se présenter et collaborer avec les autorités dans le processus d'évaluation et d'extraction des informations d'une manière efficace et simple.<br><br>À cette fin, la police judiciaire et le procureur de l'affaire peuvent les citer à comparaître en tant que témoins lors d'un entretien ou d'une déclaration sous serment ; leur connaissance du système et des données qui y sont stockées, ainsi que de leur structure, de leur format et de leur emplacement, est considérée comme un élément de conviction lors de l'établissement des motifs raisonnables pour l'obtention de preuves numériques et peut servir de témoin dans le cadre de la procédure.<br><br>D'autre part, en Colombie, il existe un devoir de coopération avec les autorités, comme le stipule l'article 4 de la loi 62 de 1993, qui est à son tour limité par l'article 33 de la Constitution politique de Colombie, qui stipule que "personne ne peut être contraint de témoigner contre lui-même, son conjoint, son partenaire permanent ou ses parents au quatrième | La Colombie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | degré de conscience, ses parents au quatrième degré de consanguinité, au deuxième degré d'affinité ou au premier degré de civilité". | |
| Costa Rica | Un juge, sur la base de l'article 7 de la loi organique du pouvoir judiciaire (loi 8 de 1937), peut ordonner à toute personne d'aider à l'enquête dans son domaine de connaissances et cette personne DOIT se conformer à l'ordre. Cette disposition ne s'applique pas si la personne disposant de connaissances ou d'informations spécifiques est le défendeur lui-même. Dans ce cas, il peut refuser la demande en vertu de son droit constitutionnel de ne pas être auto-incriminé. L'article qui le régit stipule ce qui suit : Article 7 : Afin d'exécuter les résolutions ou les actions qu'ils ordonnent, les tribunaux peuvent demander l'assistance des forces de police et d'autres moyens d'action appropriés. Les personnes sont tenues de fournir l'assistance qui leur est demandée et qu'elles peuvent fournir. | Le Costa Rica applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Croatie | L'article 257 du code de procédure pénale oblige toute personne utilisant des ordinateurs ou des appareils, toute personne y ayant accès ou tout fournisseur de services de télécommunications à donner accès à l'ordinateur, à l'appareil ou au support de données et à fournir les informations nécessaires à une utilisation sans perturbation et à la réalisation des objectifs de recherche.<br><br>Toutefois, il semble que le champ d'application de la mesure puisse être appliqué à une catégorie de personnes plus restreinte que l'article 19, paragraphe 4, qui ne se limite pas aux utilisateurs d'ordinateurs et aux personnes y ayant accès, mais s'applique à une catégorie plus large de personnes pouvant avoir des connaissances utiles. 19.4 qui n'est pas limité aux utilisateurs des ordinateurs et aux personnes y ayant accès, mais s'applique à une catégorie plus large de personnes susceptibles d'avoir des connaissances utiles.<br><br>Les autorités chargées de la recherche peuvent charger un assistant professionnel d'exécuter ces mesures.<br><br>Le non-respect de ces exigences est punissable (avec une exception pour le défendeur). | La Croatie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. Il apparaît que le cadre applicable est limité à une catégorie de personnes plus restreinte que celle prévue par l'article 19.4. 19.4. |
| Chypre | Il a été signalé que les officiers de police ont le pouvoir d'interroger toute personne détenant des informations pertinentes pour une affaire, y compris les personnes possédant les types de connaissances décrits à l'article 19.4. 19.4.<br><br>Toutefois, sur la base des réponses complémentaires de Chypre, il apparaît que l'article 19.4 de la Convention de Budapest n'est normalement pas mis en œuvre et que les recherches sont effectuées en s'appuyant sur d'autres mécanismes. En | Il apparaît que l'article 19.4 n'est pas transposé dans le droit interne de Chypre. 19.4 n'est pas transposé dans le droit interne de Chypre. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | général, lors de la perquisition d'un lieu, les forces de l'ordre ne coopèrent pas avec les administrateurs de systèmes privés ou, apparemment, d'autres catégories de personnes, et ne demandent pas leur assistance.<br><br>Les recherches de données électroniques sont généralement effectuées par des officiers de police et des membres du laboratoire de criminalistique numérique (LCN) de l'unité de lutte contre la cybercriminalité. Lors de l'exécution du mandat de perquisition, une recherche préliminaire peut être effectuée sur le lieu de la perquisition à partir des données électroniques trouvées, mais un examen plus approfondi des données est effectué au laboratoire de criminalistique numérique. Dans les affaires spéciales ou de grande envergure, les membres du LDF restent sur place pendant l'acquisition des données. Dans ces cas, les agents des services répressifs et le LDF effectuent les recherches sans l'aide d'administrateurs de systèmes externes. Cela s'explique par la nature stricte de la recherche et par les protections de la vie privée et de la communication privée prévues par la Constitution.<br><br>Si la recherche est effectuée dans des entreprises ou des organisations qui emploient un administrateur de système, les membres du LDF demanderont généralement la coopération de l'administrateur de système pendant la recherche. Le refus de coopérer n'est pas une infraction pénale et la coopération ne peut être imposée.<br><br>Il est possible de faire appel à des experts externes pour examiner les preuves après la perquisition et la saisie, mais cela se fait généralement dans des cas exceptionnels, lorsque le LDF ne peut pas examiner davantage les preuves collectées, par exemple des données électroniques très endommagées. | |
| République tchèque | En vertu de la disposition 8 du CPP, il est possible de demander la coopération des personnes physiques et morales et d'imposer une amende en cas de non-respect de cette demande (disposition 66 du CPP et 36 de la loi sur la responsabilité pénale des personnes morales). Cette obligation est limitée dans une certaine mesure par le droit de ne pas s'incriminer soi-même. | La République tchèque applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Danemark | Lorsque la Convention de Budapest a été transposée en droit danois, l'article 19.4 a été évalué comme étant satisfait par les règles danoises sur les témoins, y compris les moyens d'obliger les témoins à comparaître, et par l'article 747 de la | Il semble que le Danemark applique des pouvoirs généraux de |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | loi sur l'administration de la justice. Selon cette section, l'approbation du tribunal (par le biais d'une audience) peut être demandée pour des mesures qui requièrent l'assistance du tribunal ou pour obtenir des preuves qui risquent d'être perdues, qui ne seront pas disponibles sans inconvénient ou retard important, ou qui sont importantes pour l'affaire ou d'intérêt public. En vertu de l'article 804 de la loi, un tribunal peut ordonner à une personne ayant accès à des documents ou à des objets pouvant servir de preuves de les montrer ou de les remettre (sauf dans certains cas). Les règles relatives à l'interférence avec la correspondance peuvent également être utilisées pour obtenir l'assistance du prestataire de services. | perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| République dominicaine | La République dominicaine a informé que le ministère public a le pouvoir d'ordonner à la personne qui a connaissance du fonctionnement d'un système d'information ou de l'un de ses éléments ou des éléments de protection des données ou des mesures de protection des données d'un tel système de fournir les informations nécessaires pour mener à bien les enquêtes nécessaires (article 54 de la loi 53-07). | La République dominicaine applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. |
| Estonie | Le suspect et l'accusé jouissent de leurs droits procéduraux et ne peuvent être contraints d'apporter leur aide. Cependant, ces personnes coopèrent souvent avec les autorités et fournissent des informations, l'accès à des systèmes informatiques, etc. Si une personne peut être considérée comme un témoin, elle a l'obligation de fournir des informations.<br><br>Les autorités chargées de l'application de la loi peuvent également faire appel à leurs experts et les faire venir sur le lieu de la perquisition. Selon l'article 95 du code de procédure pénale, un expert est "une personne qui applique des connaissances spécialisées non juridiques lorsqu'elle procède à une expertise dans des situations et conformément aux règles prévues par le présent code". Lorsque des experts sont désignés, la préférence est normalement donnée à un employé d'une agence médico-légale gouvernementale, mais des experts privés ou étrangers peuvent également être sélectionnés. | L'Estonie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Fidji | En vertu des sections 20, 21(1) (2) (3) (4) du TCA, le juge délivrant le mandat autorisant la police ou une personne autorisée (avec assistance) à saisir ou sécuriser un système informatique, un programme, des données ou un support de stockage de données spécifiés ; inspecter et vérifier le fonctionnement de tout système informatique décrit dans le mandat ; demander à toute personne possédant des connaissances sur le fonctionnement du système informatique ou sur les mesures appliquées pour protéger les données informatiques qu'il contient de fournir, dans la mesure du raisonnable, les données ou informations informatiques nécessaires pour permettre à la police ou à la personne autorisée de mener les activités autorisées ; demander l'accès à toute information de décryptage nécessaire pour décrypter les | Les Fidji appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | données pertinentes pour le mandat et, enfin, obtenir une assistance technique ou autre raisonnable pour mener à bien les activités spécifiées dans le mandat.<br><br>Les dispositions de la loi de procédure pénale relatives à la signification des mandats de perquisition et aux pouvoirs des magistrats, ainsi que la Constitution des Fidji (article 24) et la loi sur la police sont également applicables à cet égard. | |
| Finlande | Le chapitre 8, section 23 de la CMA stipule l'obligation d'une personne qui possède un système d'information de fournir des informations. Une personne qui possède ou entretient un système d'information ou toute autre personne doit, sur demande, fournir à une autorité d'enquête criminelle les mots de passe et autres informations connexes nécessaires pour effectuer une recherche dans les données contenues dans un dispositif. Sur demande, un certificat écrit est fourni à la personne à laquelle la demande est adressée. Si une personne refuse de fournir les informations, elle peut être entendue par un tribunal de la manière prévue au chapitre 7, section 9 de la loi sur les enquêtes criminelles (805/2011). Les dispositions ci-dessus ne s'appliquent pas au suspect de l'infraction ou à une personne visée au chapitre 7, section 3, sous-section 1 ou 2, qui a le droit ou le devoir de refuser de témoigner.<br><br>Les modifications apportées à la LMC sont entrées en vigueur le 1er octobre 2023 (loi 452/2023). L'article 23 stipule désormais que les personnes possédant ou gérant des systèmes d'information doivent non seulement fournir les mots de passe et les informations nécessaires aux forces de l'ordre, mais aussi les aider à utiliser ces informations.<br><br>En outre, les dispositions du chapitre 8, sections 23 à 26, relatives à l'obligation d'information du détenteur d'un système d'information et à l'ordre de conservation des données s'appliquent à l'utilisation de mesures coercitives secrètes. | La Finlande applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| France | Le code de procédure pénale prévoit que la police peut demander l'assistance de personnes détenant des informations sur un système. En particulier, deux infractions créées ces dernières années visent spécifiquement le refus d'aider au décryptage. Il semble que le champ d'application de cette disposition soit plus restreint que celui de l'art. 19.4, car elles concernent des questions de décryptage, alors que l'article 19.4 couvre la fourniture des informations nécessaires. 19.4 couvre la fourniture des informations nécessaires. | La France applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. Toutefois, il semble que la disposition de droit interne applicable soit plus restrictive que l'article 19.4. 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Géorgie | Conformément à l'art. 112 du CPC, les enquêteurs et/ou autres agents des services répressifs qui exécutent un mandat de perquisition doivent d'abord proposer aux personnes responsables du lieu de la perquisition (généralement les propriétaires ou, dans le cas d'entreprises, les gestionnaires, les administrateurs de systèmes, etc. Sur la base d'une décision de justice fondée sur l'article 136 du code de procédure pénale, un administrateur de système ou toute autre personne concernée au sens de l'article 19.4 de la Convention de Budapest peut se voir ordonner de divulguer des informations pertinentes afin de faciliter une perquisition et une saisie. Le non-respect d'une telle ordonnance peut entraîner une responsabilité pénale en vertu du code pénal.<br><br>Les autorités se réfèrent également à l'art. 114 du CPP, qui peut être étendu aux gestionnaires ou administrateurs de systèmes non coopératifs, mais soulignent qu'il n'est pas souvent utilisé dans la pratique. | La Géorgie applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| Allemagne | L'Allemagne n'a pas de disposition qui contienne expressément le pouvoir prévu à l'art. 19.4. Toutefois, dans la pratique, il est entendu que les dispositions générales des articles 94 et 95 sont applicables.<br><br>Conformément à l'article 95, paragraphe 1, du code de procédure pénale, seules les personnes qui ne sont pas soupçonnées d'un délit peuvent être obligées de fournir des codes d'accès ou de parler de leurs connaissances sur le fonctionnement d'un système informatique. En revanche, les suspects ou les personnes ayant le droit de refuser de témoigner ne peuvent pas être obligés.<br><br>Dans de tels cas, les codes d'accès pourraient - s'ils sont disponibles - être collectés auprès des fournisseurs de services de télécommunications/télémédias conformément à l'article 100j (1), phrases 2 et 3 du code de procédure pénale. Les autorités chargées de l'application de la loi pourraient en outre tenter de décrypter les codes d'accès, si nécessaire, avec l'aide de spécialistes. | L'Allemagne applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Ghana | En vertu de l'article 99, paragraphe 2, de la LTA, les agents chargés de l'application de la loi qui exécutent des mandats en vertu de la loi peuvent demander à toute personne responsable du fonctionnement d'un ordinateur ou concernée par ce fonctionnement de fournir à l'agent ou à toute autre personne autorisée l'assistance technique et autre raisonnable nécessaire à l'enquête ou aux poursuites. En outre, une personne en possession d'informations de décryptage peut être tenue de fournir aux agents agissant en vertu de la présente section toute information nécessaire au décryptage d'un enregistrement requis pour l'enquête. Les personnes peuvent également être tenues de présenter des ordinateurs aux agents. | Le Ghana applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La section 98(1) de l'ETA permet aux forces de l'ordre d'utiliser les dispositions relatives aux perquisitions et saisies de l'ETA en plus des pouvoirs d'arrestation, de perquisition et de saisie d'une force de l'ordre prévus par d'autres lois. Par conséquent, l'assistance d'une tierce partie soutenue par l'ETA peut être utilisée en plus des pouvoirs prévus par d'autres lois.<br><br>Une personne qui refuse de fournir une assistance alors qu'un ordre légal a été émis peut être sanctionnée. | |
| Grèce | Il n'existe aucune disposition permettant d'exiger d'une personne qu'elle fournisse des informations sur un système informatique. | Il semble que l'article 19.4 n'ait pas été mis en œuvre par la Grèce. 19.4 n'a pas été mis en œuvre par la Grèce. |
| Grenade | L'article 22, lettre d), de la loi sur la criminalité électronique impose à une personne en possession d'informations de décryptage de fournir à la police l'accès à ces informations de décryptage nécessaires pour décrypter les données requises dans le cadre de l'enquête sur l'infraction. Ce pouvoir peut s'appliquer à toute personne chargée d'accéder au système ou disposant du code d'accès au système. Le fonctionnement ou l'exploitation du système n'est pas pris en considération. | La Grenade applique des pouvoirs spécifiques pour mettre en œuvre l'art. 19.4. Toutefois, il semble que le champ d'application du cadre juridique national applicable puisse s'appliquer à une catégorie de personnes plus restreinte que celles visées à l'article 19.4. 19.4. |
| Hongrie | Les articles 267 et 271 du code de procédure pénale confèrent aux autorités le pouvoir général de recueillir des preuves pénales et de demander des informations pertinentes à toute personne (tout en protégeant les droits fondamentaux de cette personne et en veillant à ce qu'ils ne soient affectés que dans la mesure nécessaire). L'article 305 du code de procédure pénale prévoit que les autorités peuvent exiger d'une personne qu'elle rende accessibles des données électroniques. Les personnes qui entravent les recherches sont passibles d'une amende. L'article 312 du code de procédure pénale prévoit que le possesseur ou le responsable du traitement d'un objet ou de données électroniques peut être contraint de révéler l'endroit où ils se trouvent ou de rendre les données électroniques accessibles. Le non-respect de cette obligation peut entraîner une amende (sauf pour les personnes appartenant à certaines catégories). | La Hongrie applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En vertu de l'article 261 du code de procédure pénale, certaines entités et organisations bénéficient d'une protection spéciale contre les demandes de données électroniques. Dans ces cas, l'autorisation du procureur doit être obtenue. Si une telle autorisation existe, ou si l'affaire est suffisamment urgente pour que la loi permette la demande sans cette autorisation, les données doivent être divulguées. Les demandes sans autorisation doivent être autorisées a posteriori et sans délai. Les données obtenues sans autorisation sont irrecevables lors d'un procès. | |
| Islande | L'article 92 de la loi n° 70/2022 sur les communications électroniques impose aux entreprises de télécommunications l'obligation d'aider la police dans les enquêtes criminelles lorsque celle-ci en fait la demande. | L'Islande applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. Toutefois, la disposition applicable du droit interne semble être plus restrictive que l'article 19.4, puisqu'elle ne couvre que les entreprises de télécommunications. 19.4. puisqu'elle ne couvre que les entreprises de télécommunications. |
| Israël | L'article 45 de l'ordonnance de procédure pénale prévoit que l'occupant du lieu pour lequel un mandat de perquisition a été délivré doit permettre l'entrée et toute assistance raisonnable. Cet article peut être interprété comme s'appliquant, avec les modifications appropriées, à une perquisition informatique. Il n'existe pas de jurisprudence en la matière.<br>Si la connaissance d'un système informatique se présente sous la forme d'un document, les autorités compétentes peuvent demander un mandat en vertu de l'article 43 de l'ordonnance de procédure pénale. Ce mandat oblige toute personne à fournir des documents utiles à l'enquête. | Israël applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Italie | **L'article 351, paragraphe 1,** est généralement appliqué.<br><br>Le code de procédure pénale italien comprend les articles suivants :<br><br>**Art. 256 - Ordre de production** : | L'Italie applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les personnes mentionnées **aux articles 200 et 201 sont tenues de** fournir rapidement à l'autorité judiciaire les documents, actes, données, informations, programmes informatiques et tout autre matériel pertinent lié à leur profession, leur emploi, leur ministère ou leur art. Ils doivent également fournir des copies originales si nécessaire, à moins qu'ils ne déclarent par écrit qu'il s'agit d'un secret d'État ou d'un secret professionnel ou lié à l'exercice de leurs fonctions. Si une déclaration concerne un secret officiel ou professionnel et soulève des doutes quant à sa validité, l'autorité judiciaire peut mener les enquêtes nécessaires. Si la déclaration est jugée infondée, l'autorité judiciaire peut ordonner la saisie. Dans le cas d'une déclaration liée à un secret d'État, l'autorité judiciaire informe le président du Conseil des ministres, en lui demandant de confirmer le secret. Si le secret est confirmé et que la preuve est cruciale pour le procès, le juge peut décider qu'il n'est pas nécessaire de procéder en raison de l'existence d'un secret d'État. Si le président du Conseil des ministres ne confirme pas le secret dans les soixante jours suivant la notification, l'autorité judiciaire peut ordonner la saisie. Les dispositions de l'article 204 s'appliquent.<br><br>**Art. 234-bis - Acquisition de documents et de données informatiques :**<br>L'acquisition de documents et de données informatiques stockés à l'étranger, même ceux qui ne sont pas accessibles au public, est toujours autorisée, à condition qu'il y ait consentement du propriétaire légitime dans le cas de données non publiques.<br><br>**Art. 248 - Demande de livraison**<br><br>Si une donnée informatique est recherchée par le biais d'une perquisition, l'autorité judiciaire peut exiger sa remise en vertu de l'article 248, qui prévoit la remise d'objets. 248 qui prévoit la remise d'objets.<br><br>Afin de repérer les données informatiques à saisir, l'autorité judiciaire ou les officiers de police judiciaire (délégués par l'autorité judiciaire) peuvent examiner les documents et la correspondance ainsi que les données, les informations et les logiciels dans les banques.<br><br>En outre, les autorités peuvent appliquer l'art. 351 qui prévoit d'autres types d'interrogatoires d'investigation. | clarté et renforcer la sécurité juridique. |
| Japon | Les articles du code de procédure pénale permettent aux autorités d'exiger des personnes qu'elles participent à la perquisition ou à la saisie, en particulier qu'elles fassent fonctionner l'ordinateur ou qu'elles copient et transfèrent des données, et qu'elles coopèrent d'une autre manière. | Le Japon applique une combinaison de pouvoirs de perquisition et de |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Kiribati | L'article 24 de la loi sur la cybercriminalité prévoit qu'un tribunal peut ordonner à des personnes ou à des fournisseurs ayant la possession ou le contrôle d'un système informatique d'aider les forces de l'ordre à effectuer une perquisition. Un officier de police doit convaincre le tribunal que les données ciblées sont nécessaires aux fins d'une enquête ou d'une procédure pénale. | Kiribati applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. Il n'est pas certain que Kiribati ait le pouvoir d'exiger l'assistance de toute personne ayant connaissance (plutôt que possession ou contrôle) d'un système. Les articles 23 et 24 ne semblent pas couvrir ce point, mais il se peut que ce pouvoir figure ailleurs dans la législation de Kiribati. |
| Lettonie | Conformément à l'article 190 du code de procédure pénale, les autorités peuvent obtenir des informations électroniques auprès des personnes concernées par les perquisitions et les saisies. Les autorités disposent de pouvoirs supplémentaires lorsqu'elles agissent en vertu de l'article 219 (mesures d'enquête spéciales). Toutefois, le code de procédure pénale ne prévoit pas de sanctions à l'encontre des personnes qui ne coopèrent pas lors de perquisitions et de saisies ordinaires (et les accusés potentiels bénéficient d'une protection contre l'auto-incrimination qui leur permet de refuser de coopérer). | La Lettonie applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19, paragraphe 4, mais le code de procédure pénale ne prévoit pas de sanctions à l'encontre des personnes qui ne coopèrent pas. |
| Liechtenstein | Plusieurs articles du code de procédure pénale prévoient d'exiger des personnes qu'elles prêtent leur concours à une saisie et de les y contraindre en cas de refus. Il est important de noter que ces personnes doivent remettre les supports de stockage et tout mécanisme d'accès et fournir des données dans un format commun si nécessaire. Le refus d'assistance peut être sanctionné par des amendes ou des peines d'emprisonnement. | Le Liechtenstein applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Lituanie | L'article 97 du code de procédure pénale stipule que les personnes physiques et morales doivent produire les objets et documents utiles à l'enquête. En vertu de l'article 155 du code de procédure pénale, une décision motivée du procureur, | La Lituanie applique des pouvoirs généraux de perquisition et de saisie |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | confirmée par un tribunal, permet au ministère public d'obtenir toutes les données raisonnablement nécessaires à une enquête pénale, y compris des informations sur le fonctionnement des systèmes informatiques. Les personnes qui ne se conforment pas à ces ordres peuvent être tenues pour responsables. | pour mettre en œuvre l'article 19, paragraphe 4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Luxembourg | L'article 66, paragraphe 4, du CPP autorise explicitement un juge d'instruction qui a rendu une "ordonnance motivée" à demander à toute personne (autre que la personne faisant l'objet de l'enquête) ayant connaissance du système ou de ses protections de donner accès 1) au système saisi et 2) aux données saisies dans ce système ou dans un autre système connecté, ainsi que de fournir une assistance pour comprendre les données saisies protégées ou cryptées. Cette disposition est soumise à certains autres articles. | Le Luxembourg applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Malte | Conformément au chapitre 9 de l'article 355AD du code pénal, *"toute personne considérée par la police comme étant en possession d'une information ou d'un document pertinent pour une enquête a l'obligation légale de se conformer à une demande de la police de se présenter à un poste de police pour fournir cette information ou ce document".* | Malte utilise des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Maurice | La section 28 fait double emploi avec l'article 19.4.<br><br>En outre, les fonctionnaires qui s'adressent aux juges pour obtenir des ordonnances incluent parfois les termes pertinents dans leurs demandes. | Maurice applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. |
| Monaco | Le procureur peut exiger de toute personne ayant connaissance du fonctionnement d'un système d'information qu'elle fournisse les informations nécessaires à l'accès aux données (article 255 du CPP).<br>En outre, la loi autorise les enquêteurs à demander l'assistance de témoins, d'experts ou de personnes ayant des connaissances spécifiques. Il peut s'agir, par exemple, de fournisseurs de services ou de personnel informatique (à l'intérieur ou à l'extérieur d'une entreprise). | Monaco applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Monténégro | L'art. 83.3 oblige toute personne en possession d'objets pouvant servir de preuves dans une procédure pénale à les remettre. L'art. 83.4 étend l'application aux données enregistrées dans des dispositifs de traitement automatique ou électronique des données et aux supports sur lesquels ces données sont enregistrées, qui doivent, à la demande du tribunal, être remises sous une forme lisible et compréhensible. | Le Monténégro applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Maroc | Les réseaux et fournisseurs de services de télécommunications publics titulaires d'une licence sont tenus d'aider les autorités judiciaires. Cependant, cette obligation ne semble pas s'étendre au-delà de ces réseaux et fournisseurs à d'autres personnes et entités. Il convient toutefois de noter que le Maroc est en train de mettre à jour sa législation. Dans l'intervalle, ses mécanismes de procédure pénale sont proches, dans la pratique, des exigences de la Convention. | Le Maroc applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. Il semble que la disposition applicable en vertu du cadre juridique national s'applique à une catégorie de personnes plus restreinte que celle visée à l'article 19.4. 19.4. |
| Pays-Bas | Aux Pays-Bas, l'article 125k DCCP permet d'ordonner la suppression d'une mesure de sécurité (art. 125k, paragraphe 1 DCCP) et d'ordonner le décryptage ou la remise d'une clé de décryptage de données cryptées (art. 125k, paragraphe 2 DCCP). Dans ce cas, si la demande lui en est faite, la personne à qui l'ordre est adressé doit s'exécuter en apportant son expertise en matière de sécurité. L'ordre de décryptage ne s'applique qu'aux mesures de sécurité mises en œuvre par la personne physique ou morale. Ces ordonnances ne peuvent pas être délivrées à des suspects en raison de l'interdiction de l'auto-incrimination.<br><br>Un élément d'information supplémentaire pourrait être de développer le pouvoir prévu à l'article 558 du DCCP Condamnation de la violation (involontaire) de la sécurité biométrique d'un dispositif informatique - article 558 du DCCP. 558 DCCP : les personnes peuvent être contraintes de tolérer certaines "actions forcées" pour l'accréditation biométrique afin d'ouvrir un appareil verrouillé par empreinte digitale ou identification faciale. Les personnes doivent accepter ces pouvoirs s'ils peuvent être exercés sans obliger les personnes à faire volontairement quelque chose elles-mêmes. Le fait | Les Pays-Bas appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | de poser le pouce sur le smartphone ou d'amener le smartphone devant le visage d'une personne peut être fait sans forcer la personne à donner l'accréditation | |
| Nigéria | Lorsque la demande ex parte est présentée à un tribunal pour obtenir une ordonnance, l'agent requérant peut demander au tribunal de prévoir que toute personne doit fournir les informations nécessaires à l'affaire. | Le Nigeria applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Macédoine du Nord | Plusieurs articles du CPP couvrent les personnes qui utilisent ou ont accès à des ordinateurs, des appareils, etc., et les obligent à "donner toutes les informations nécessaires pour que les objectifs de la perquisition puissent être atteints sans entrave". Cette définition couvre les personnes les plus susceptibles de détenir des informations utiles à la recherche, mais ne s'étend pas à toute autre personne qui pourrait, dans un cas donné, détenir des informations liées à la recherche - un ami de la cible, une personne qui travaille dans un bâtiment mais pas avec les ordinateurs, etc. | La Macédoine du Nord applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. Il apparaît que le droit interne applicable s'applique à une catégorie de personnes plus restreinte que celle visée par l'article 19.4. 19.4. |
| Norvège | L'article 199a du CPC prévoit la possibilité d'exiger l'assistance de toute personne impliquée dans le système visé. | La Norvège applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| Panama | L'article 75 du code de procédure pénale établit l'obligation de coopérer, applicable aux entités publiques et privées, de manière prompte, efficace et complète aux exigences formulées par les agents du ministère public. En outre, l'article 277 du même extrait juridique établit que, compte tenu de l'urgence et de l'objectif de la procédure, des informations peuvent être demandées à tout fonctionnaire, qui est tenu de les fournir et de collaborer à l'enquête. Il établit également que les informations détenues par des personnes physiques et morales peuvent être demandées.<br><br>Article 75. Obligation de collaboration. Les entités publiques et privées sont tenues de collaborer de manière prompte, efficace et complète aux exigences formulées par les agents du ministère public dans le cadre de leurs fonctions, sous peine d'encourir les responsabilités prévues par la loi. | Le Panama applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les agents du ministère public disposent des pouvoirs coercitifs qui leur sont conférés par le présent code, sa loi organique ou les lois spéciales.<br>Art. 277. Collaboration avec le ministère public. En dehors des cas qui requièrent l'autorisation du juge, le ministère public, compte tenu de l'urgence et des finalités de la procédure, peut demander des informations à tout agent public, qui est tenu de les fournir et de collaborer à l'enquête selon ses compétences. Il peut également demander des informations détenues par des personnes physiques ou morales. | |
| Paraguay | Il n'existe pas de disposition spécifique prévoyant expressément le pouvoir de l'article 19.4 et son application par les autorités résulte de la pratique. 19.4 et son application par les autorités découle de la pratique.<br><br>Les autorités ont indiqué qu'il n'existe que des bonnes pratiques et des demandes basées sur la recherche de preuves concernant les cybercrimes de la loi 4439/2011 et de la Convention de Budapest. | Il semble que les autorités s'appuient uniquement sur la pratique et sur les pouvoirs généraux pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Pérou | Le système juridique péruvien confère aux autorités le pouvoir d'exiger des informations nécessaires de la part des individus au cours d'une enquête. Le ministère public, conformément au point b) du numéro 3 de l'article 337 du code de procédure pénale, peut demander des informations à toute personne et même saisir des documents privés si nécessaire. Le non-respect de ces exigences peut entraîner des poursuites pénales pour résistance ou désobéissance à l'autorité, comme le prévoit l'article 368 du code pénal. En outre, le procureur et le juge, comme le stipule l'article 126 du code de procédure pénale, ont le pouvoir d'utiliser la force pour remplir leurs fonctions si nécessaire. | Le Pérou applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Philippines | La loi sur la prévention de la cybercriminalité prévoit expressément que toute personne ayant connaissance du fonctionnement d'un système informatique et des mesures de protection et de conservation de ses données peut se voir ordonner de fournir, dans la mesure du raisonnable, des informations pour faciliter les perquisitions, les saisies et les examens. | Les Philippines appliquent des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| Pologne | Conformément à l'article 175 du CPP, les suspects et les accusés ne peuvent être contraints d'apporter leur aide, bien qu'ils choisissent souvent de le faire. Toute personne susceptible d'être considérée comme un témoin peut être contrainte | La Pologne applique des pouvoirs généraux de perquisition et de saisie |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | de prêter son concours. Le responsable de la recherche décide qui sera considéré comme un témoin à interroger. Des sanctions peuvent être imposées à un témoin qui ne fournit pas d'informations. Il n'est pas clair si la possibilité d'interroger un "témoin" signifie qu'une personne se trouvant sur le site d'une perquisition peut être tenue de fournir des informations immédiatement. | pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Portugal | Il n'existe pas de disposition légale expresse permettant aux autorités d'ordonner l'assistance d'une personne. Toutefois, l'article 14, paragraphe 1, de la loi sur la cybercriminalité met effectivement en œuvre l'article 19.4 de Budapest. L'article 14 vise principalement à transposer l'article 18 de Budapest (injonctions de produire) en droit interne ; il crée donc une obligation pour tout citoyen de communiquer certaines données aux autorités de justice pénale, si elles en font la demande (à l'exception des personnes appartenant à certaines catégories protégées). En vertu de cet article, une personne peut être tenue d'"autoriser l'accès aux données" dans les cas de perquisition, si nécessaire. Le refus d'autoriser l'accès aux données peut être considéré comme un délit de désobéissance, avec une sanction pénale correspondante. | Le Portugal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| République de Moldavie | En vertu des articles 300 à 306 du code de procédure pénale, toute personne physique ou morale doit se conformer aux injonctions des tribunaux, y compris les injonctions de fournir des informations ou des éléments de preuve. Les données informatiques constituent des preuves. | La Moldova applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Roumanie | Il n'existe aucune disposition permettant d'obliger une personne à fournir une assistance technique avant ou pendant une perquisition informatique. Toutefois, dans la pratique, la coopération volontaire est recherchée et apportée.<br><br>L'objet de la perquisition ou le propriétaire, l'auteur, le témoin et les proches de l'auteur ont le droit de refuser de coopérer dans une affaire pénale, sur la base de différents principes, tels que le droit de ne pas s'incriminer soi-même. | La Roumanie n'a pas mis en œuvre l'art. 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Saint-Marin | Saint-Marin n'a pas de législation spécifique en la matière, mais il a été indiqué que si l'on soupçonne que des données ou des informations utiles à la conduite d'enquêtes pénales sont contenues dans un système informatique ou télématique, ou dans une partie de celui-ci, et qu'il existe des motifs raisonnables de croire que ces données peuvent être perdues ou effacées, le juge, par le biais d'une ordonnance motivée, peut ordonner à la personne qui contrôle ces données ou informations, ou qui les a à sa disposition, de prendre les mesures techniques nécessaires pour assurer la protection et la conservation immédiates des données d'origine.<br><br>En outre, le juge peut ordonner au destinataire du décret de prendre toutes les mesures nécessaires pour assurer la confidentialité des données.<br><br>Si l'on soupçonne que des données ou des informations utiles à la réalisation d'enquêtes pénales sont contenues dans un système informatique ou télématique, ou dans une partie de celui-ci, le juge peut, par une ordonnance motivée, ordonner à la personne qui contrôle ces données ou informations, ou à celle qui en dispose, de les transmettre à l'autorité judiciaire.<br><br>Les autorités ont également signalé la possibilité de demander la conservation des données utiles à l'enquête.<br><br>Le juge, par décret motivé, peut ordonner à la personne qui a la disponibilité ou le contrôle des données d'adopter les mesures techniques appropriées pour assurer la protection et la conservation des données dans leur état d'origine ; cependant, il n'y a pas de définition législative de l'"administrateur du système informatique". Il n'existe pas non plus de réglementation permettant à l'autorité judiciaire d'obliger une telle personne, qui a connaissance du fonctionnement du système ou des mesures de protection des données, à fournir l'assistance ou les informations nécessaires pour effectuer des perquisitions ou des saisies. | Saint-Marin applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Sénégal | Les articles du CPC cités ci-dessus prévoient que toutes les personnes ayant connaissance du fonctionnement du système ou des mesures de sécurité qui protègent les données doivent fournir toutes les informations nécessaires à l'exécution de la perquisition ou de la saisie. Ces articles permettent également aux autorités d'exiger de toutes les personnes qu'elles protègent l'intégrité des données en leur possession ou sous leur contrôle. | Le Sénégal applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| Serbie | Conformément au code de procédure pénale, à la loi sur le ministère public et, dans certains cas, à la loi sur les communications électroniques, toutes les personnes morales et physiques (à l'exception des suspects/accusés) sont tenues de participer aux enquêtes, comme indiqué à l'article 19.4. | La Serbie applique une combinaison de pouvoirs de perquisition et de |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |
| Sierra Leone | Le mandat prévu à l'article 10 peut autoriser un agent des services répressifs ou d'autres personnes possédant des connaissances sur le fonctionnement d'un système informatique ou sur les mesures appliquées pour protéger les données informatiques qu'il contient, à fournir les données informatiques ou les informations nécessaires pour permettre à un agent des services répressifs ou à une autre personne autorisée de mener à bien une activité autorisée par la loi. | La Sierra Leone applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. |
| République slovaque | La République slovaque cite les articles 91.5, 91.6 et 116 du CPP comme fondement de la capacité d'ordonner à des personnes d'assister à des perquisitions. Bien qu'il semble que les articles 91.5 et 91.6 puissent couvrir certains éléments de l'art. 19.4. de la Convention, le pouvoir national se concentre uniquement sur les propriétaires/utilisateurs de systèmes et les fournisseurs de services, mais il ne semble pas assez large pour englober des catégories moins attendues de personnes qui pourraient avoir des connaissances utiles, comme l'exige l'art. 19.4. | La République slovaque applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. Toutefois, il semble que le droit interne applicable soit plus étroit que l'article 19.4. 19.4. |
| Slovénie | En vertu de l'article 219a du CPP, les propriétaires ou les utilisateurs de dispositifs électroniques doivent fournir l'accès à l'objet, les clés d'accès au cryptage ou les mots de passe, ainsi que toutes les explications nécessaires sur le fonctionnement de l'objet. Les personnes qui refusent de coopérer peuvent être sanctionnées, y compris par une peine d'emprisonnement (sauf pour les personnes appartenant à certaines catégories, comme les prévenus). | La Slovénie applique des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. Toutefois, la disposition applicable en vertu du cadre juridique national semble s'appliquer à une catégorie de personnes plus restreinte que celle visée à l'article 19.4. 19.4. |
| Espagne | La loi espagnole de procédure pénale contient, à l'article 588e(c), une disposition similaire à celle décrite à l'article 19.4. Les autorités et les agents chargés des enquêtes sont habilités à ordonner à une personne de fournir les informations nécessaires. Ce pouvoir ne se limite pas à l'autorité judiciaire, mais s'étend également au ministère public et aux autorités chargées de l'application de la loi. Le fait de ne pas se conformer à la demande peut être considéré comme un délit de désobéissance. Toutefois, les personnes exemptées de l'obligation de témoigner pour des raisons de parenté ou de secret | L'Espagne applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | professionnel ne peuvent être poursuivies pour défaut de coopération dans les enquêtes liées à leur obligation de confidentialité. | |
| Sri Lanka | L'article 23 de la loi sur la criminalité informatique oblige les personnes à se conformer aux demandes légitimes des experts ou des officiers de police au cours des enquêtes. | Le Sri Lanka applique des pouvoirs de perquisition et de saisie spécifiques pour mettre en œuvre l'article 19.4. |
| Suède | Le code de procédure pénale prévoit que, dans le cas où une perquisition serait autrement entravée, une personne peut être tenue de fournir une authentification biométrique afin de pouvoir accéder à un système ou à un dispositif.<br><br>En outre, le code de procédure pénale prévoit qu'une personne peut être amenée à témoigner devant le tribunal pour fournir les informations nécessaires sur un système alors que l'enquête préliminaire est toujours en cours. Ce témoignage ne peut avoir lieu que lorsque l'enquête a suffisamment progressé pour qu'un suspect ait été identifié, et que ce dernier a le droit d'être présent lors du témoignage. | La Suède applique une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4., mais il semble que le cadre applicable soit limité aux identifications biométriques ou à l'audition de témoins, qui semblent être plus restreints et moins efficaces que les exigences énoncées à l'article 19.4. 19.4. |
| Suisse | Dans certains domaines, la loi oblige les tiers à fournir des informations à la demande des autorités. Un article du code pénal prévoit certaines obligations de remise d'objets ou de biens. Toutefois, cette disposition s'adresse principalement au propriétaire des objets ou des biens à saisir. En outre, un accusé a le droit de refuser de coopérer à une procédure pénale. D'autres personnes peuvent être autorisées à refuser de témoigner. Les personnes morales ne sont pas tenues de remettre des objets si elles risquent de s'incriminer elles-mêmes et d'être tenues pour responsables en vertu du droit pénal ou civil et si leur intérêt à être protégées l'emporte sur l'intérêt à être poursuivies. | La Suisse applique des pouvoirs généraux de perquisition et de saisie pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. Il apparaît également que le droit interne applicable est plus étroit que l'article 19.4 puisqu'il s'applique aux propriétaires des objets ou des biens à saisir. 19.4 |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | puisqu'il s'applique aux propriétaires des objets ou des biens à saisir et non à une catégorie plus large de personnes. |
| Tonga | L'article 9 de la loi sur la criminalité informatique (Computer Crimes Act) permet à un magistrat de délivrer un mandat qui couvre la fourniture de l'assistance nécessaire par d'autres personnes aux autorités chargées de l'application de la loi qui effectuent une perquisition. De manière peut-être plus directe, l'article 10 de cette loi prévoit des sanctions pénales pour les personnes en possession ou en contrôle de données qui n'autorisent pas les perquisitions autorisées par un mandat et n'y prêtent pas assistance.<br><br>En outre, si des données ou des informations sont nécessaires à une procédure pénale ou à une enquête, l'article 11 de la loi sur les délits informatiques permet à un magistrat d'ordonner à une personne ayant le contrôle d'un système informatique ou de données de les fournir. En outre, l'article 15 de la loi sur les délits d'abus de communication électronique (Electronic Communication Abuse Offences Act) prévoit que la Cour suprême peut délivrer un mandat de production pour permettre l'accès et la divulgation des données relatives au contenu et de toute information associée utilisée dans le cadre d'une infraction. Un juge de première instance peut délivrer un tel mandat de production si le juge de la Cour suprême n'est pas disponible. | Les Tonga appliquent des pouvoirs spécifiques de perquisition et de saisie pour mettre en œuvre l'article 19.4. |
| Tunisie | | |
| Türkiye | Bien qu'aucune disposition légale n'oblige une personne à prêter son concours, les autorités consultent fréquemment toute personne susceptible d'avoir des connaissances sur le système faisant l'objet de la perquisition. | Il semble qu'il n'y ait pas de disposition légale applicable dans le droit national pour mettre en œuvre l'article 19.4 et que la Turquie s'en remette à la pratique. 19.4 et la Turquie s'en remet à la pratique. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Ukraine | L'Ukraine a indiqué que la législation actuelle ne prévoit pas de règles de procédure spécifiques distinctes permettant aux autorités compétentes d'ordonner à toute personne ayant connaissance du fonctionnement d'un système informatique ou des mesures prises pour protéger les données informatiques qu'il contient de fournir, si cela est raisonnable, les informations nécessaires à la mise en œuvre des mesures visées aux paragraphes 1 et 2. Toutefois, les règles générales de procédure relatives à la collecte de preuves électroniques sont applicables. | L'Ukraine applique des compétences générales pour mettre en œuvre l'article 19.4. Des dispositions spécifiques aux données et systèmes informatiques pourraient permettre une plus grande clarté et renforcer la sécurité juridique. |
| Royaume-Uni | La partie III du Regulation of Investigatory Powers Act 2000 (RIPA 2000) semble fournir le cadre légal des pouvoirs généraux applicables aux crimes graves, permettant aux autorités publiques d'exiger que les informations électroniques protégées (clés/mots de passe) qu'elles ont acquises légalement ou qu'elles sont susceptibles d'obtenir légalement, soient mises sous une forme intelligible. Ces pouvoirs signifient que, dans des circonstances où il est nécessaire et proportionné de le faire, les enquêteurs peuvent exiger des entreprises et des individus qui ont une autorisation appropriée de fournir l'accès (ou les moyens d'accès) à des informations protégées qui peuvent ensuite être mises sous une forme intelligible.<br><br>La méthode d'obtention de l'accès aux informations protégées est réalisée par la signification d'un avis exigeant la divulgation (section 49, RIPA 2000). L'avis doit être fondé sur la conviction des enquêteurs.<br><br>Des dispositions obligeant les témoins à assister aux audiences et à témoigner au procès peuvent également être utilisées dans les différents pays. | Le Royaume-Uni applique une combinaison de pouvoirs généraux et spécifiques pour mettre en œuvre l'article 19.4. Toutefois, il semble que la mesure couvre un type de situations plus restreint (uniquement les clés/mots de passe après que l'objet a déjà été saisi, s'appliquant aux crimes graves) et une catégorie de personnes plus restreinte que celles visées à l'article 19.4. du Code de procédure pénale. |
| États-Unis | Bien que cela soit rarement nécessaire, un tribunal peut autoriser une ordonnance en vertu de la loi sur l'ensemble des écrits (après demande) pour imposer le type d'assistance requis par l'article 19.4. | Les États-Unis appliquent une combinaison de pouvoirs de perquisition et de saisie généraux et spécifiques pour mettre en œuvre l'article 19.4. |

# 8 CONDITIONS ET GARANTIES (EVALUATION DE L'ARTICLE 19.5)

Cette section évalue la mise en œuvre de l'article 19.5 :

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 5 Les pouvoirs et procédures visés au présent article sont soumis aux articles 14 et 15.

## 8.1 Mise en œuvre de l'article 19.5 : vue d'ensemble

### 8.1.1 Conditions et garanties - résumé

L'article 19.5 stipule que les mesures prévues dans l'article sont soumises aux conditions et garanties prévues par le droit interne des parties sur la base des articles 14 et 15 de la présente convention.

L'évaluation de la mise en œuvre de cette disposition comporte donc deux parties, l'une relative à l'article 14 et l'autre à l'article 15.

#### 8.1.1.1 Article 14

L'article 14 exige des Parties qu'elles appliquent le pouvoir de perquisition et de saisie des données informatiques stockées aux fins d'enquêtes ou de procédures pénales spécifiques aux infractions établies conformément à la Convention, aux autres infractions pénales commises au moyen d'un système informatique, ainsi qu'à la collecte de preuves sous forme électronique d'une infraction pénale.

La question de savoir si les pouvoirs de perquisition et de saisie de données informatiques stockées s'appliquent à toute infraction pour laquelle des éléments de preuve se trouvent sur un système informatique (question 1.1.2 du questionnaire) a déjà été abordée dans la section 3.2 du présent rapport et il est conseillé aux Parties de consulter cette partie pour une discussion plus détaillée. La conclusion la plus importante est que presque toutes les Parties appliquent le pouvoir de perquisition et de saisie des données informatiques stockées à toute infraction dont les éléments de preuve se trouvent sur un système informatique.

Exemple de mise en œuvre dans le droit interne d'une Partie :

Fidji : *"Tous les pouvoirs et procédures prévus par la présente loi sont applicables et peuvent être exercés en ce qui concerne (...) la collecte de preuves sous forme électronique d'une infraction pénale en vertu de la présente loi ou de toute autre loi écrite".*[62]

#### 8.1.1.2 Article 15

Conformément à l'article 15, les pouvoirs et les procédures de la Convention sont limités par des conditions ou des garanties prévues par le droit interne de chaque Partie, qui assurent un équilibre entre les exigences de la sécurité publique et la protection des droits de l'homme et des libertés. Ces conditions ou sauvegardes peuvent être prévues par voie constitutionnelle, législative, judiciaire ou autre.

La Convention ne précise pas en détail les conditions et les garanties pour chaque pouvoir ou procédure, car elle s'applique à des Parties ayant des systèmes juridiques et des cultures très différents.

---

[62] Article 15.c. de la loi sur la cybercriminalité.

D'autre part, le rapport explicatif de la Convention reconnaît qu'il existe des normes communes ou des garanties minimales auxquelles les Parties à la Convention doivent adhérer et qui découlent des obligations qu'une Partie a contractées en vertu des instruments internationaux relatifs aux droits de l'homme.[63] Toutefois, compte tenu du fait que des Parties de toutes les régions du monde sont parties à la Convention, les rédacteurs n'ont pas établi de liste exhaustive de ces normes communes ou garanties minimales ; ils se sont plutôt appuyés sur des citations/références à des traités relatifs aux droits de l'homme.

De même, la Convention prévoit que des garanties spécifiques, y compris un contrôle judiciaire ou autre contrôle indépendant, des motifs justifiant l'application et la limitation de la portée et de la durée d'un pouvoir ou d'une procédure, s'appliquent de manière appropriée compte tenu de la nature d'un tel pouvoir ou d'une telle procédure. Par exemple, la Convention exige de ses Parties qu'elles appliquent de telles conditions et garanties en ce qui concerne l'interception, compte tenu de son caractère intrusif. En même temps, il n'est pas nécessaire que ces garanties s'appliquent également à d'autres pouvoirs, et les Parties peuvent donc décider elles-mêmes de ce qu'elles considèrent comme "approprié" en ce qui concerne la perquisition et la saisie de données informatiques stockées. Néanmoins, il est incontestable que la perquisition et la saisie sont des mesures procédurales plus intrusives que la conservation des données et que les Parties devraient introduire des garanties plus strictes en ce qui concerne la perquisition et la saisie de données informatiques stockées que celles relatives à la conservation accélérée de données informatiques stockées.

Compte tenu de ce qui précède, lorsqu'il a évalué l'effet de l'article 15 sur la mise en œuvre de l'article 19.5, le T-CY a analysé les résumés des conditions et garanties prévues par le droit interne des parties pour les différentes mesures prévues à l'article 19. L'objectif était de déterminer si les pouvoirs de perquisition et de saisie de données informatiques stockées sont soumis à des conditions et à des garanties dans le droit interne de chaque Partie, et non d'évaluer en détail ces garanties ou leur absence.

Presque toutes les parties ont fourni des informations sur les conditions et sauvegardes applicables dans les différentes parties du questionnaire. Il est donc conseillé aux membres du T-CY de consulter également les sections précédentes du rapport[64] et la compilation des réponses, où figurent des réponses plus détaillées de chaque Partie.[65] La présente section contient donc un résumé des conditions et sauvegardes les plus courantes mentionnées par les parties.

Il convient de noter que presque toutes les Parties ont indiqué qu'elles incluaient des garanties et des protections en matière de droits de l'homme lors de la mise en œuvre de l'article 19. Parmi les garanties les plus fréquemment mentionnées figure le contrôle judiciaire ou autre contrôle indépendant, tandis que la plupart des Parties ont indiqué que les ordonnances des

---

[63] Voir le paragraphe 145 du rapport explicatif de la Convention.

[64] Par exemple, la section 3.4 sur la notification, la section 4.1.5 sur les autorités compétentes qui autorisent et exécutent une perquisition, la section 5.1.2 qui traite des motifs de croire que les données recherchées sont stockées dans un autre système sur le territoire de cette Partie ou la section 6.1.2 sur les autorités compétentes qui autorisent et exécutent une saisie.

[65] Les parties ont adopté des approches différentes à l'égard de cette question. Certaines ont donné des réponses très larges, en commençant par les traités et les documents fondamentaux nationaux et en poursuivant par des listes de droits procéduraux très spécifiques. D'autres Parties se sont concentrées plus étroitement sur les droits pratiques (qui doit être présent lors d'une perquisition ?) et les droits procéduraux. L'une ou l'autre approche répondait à la question ; les Parties ont simplement compris différemment le sens de la question. Pour cette raison, les lecteurs doivent garder à l'esprit que le silence sur les traités ou les droits constitutionnels ne signifie pas qu'un pays ne les respecte pas et ne les applique pas.

tribunaux ou les décisions d'autres autorités judiciaires constituaient une exigence pour l'autorisation du pouvoir.

Un certain nombre de Parties ont souligné que les pouvoirs procéduraux doivent respecter les obligations en matière de droits de l'homme inscrites dans leurs constitutions ou documents fondamentaux respectifs. En outre, il a été souligné que ces pouvoirs doivent être conformes aux obligations des Parties en vertu des instruments universels applicables en matière de droits de l'homme, tels que le Pacte international relatif aux droits civils et politiques, ou des instruments régionaux en matière de droits de l'homme, tels que la Convention américaine des droits de l'homme, la Convention européenne des droits de l'homme ou la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et ses protocoles.

Voici des exemples de garanties qui ont été fréquemment mentionnées par les parties :

- la légalité (l'utilisation de tous les pouvoirs doit être réglementée par la loi)
- limitation du champ d'application (par exemple, limitation à l'enquête ou à la procédure pénale spécifique, identification de la personne connue/inconnue dont les données doivent être consultées, identification du lieu ou des objets à perquisitionner/saisir, détails sur les avantages de l'enquête)
- limitation de la durée de la puissance[66]
- le droit à un procès équitable ;
- le droit à la vie privée ;
- la protection des données
- la nécessité, la subsidiarité, la proportionnalité[67] ou le caractère raisonnable de la mesure
- les privilèges et immunités (certaines catégories de personnes ou d'activités peuvent être protégées contre les pouvoirs de perquisition et de saisie : journalistes, sources journalistiques, conversations médecin-patient, conversations avocat-client, conversations prêtre-pénitent, diplomates) ;
- le droit de ne pas s'incriminer soi-même
- de l'oubli ;
- les mesures relatives aux voies de recours (droit de faire appel d'une décision, droit de recours) ;
- les mesures relatives à la conservation des données
- notification d'une personne concernée par la mesure et droit d'assister à la fouille.

Plusieurs parties ont souligné que la violation des conditions et des garanties peut entraîner l'interdiction d'utiliser des preuves en faveur de la personne concernée.

Conformément à l'article 15, paragraphe 3, les intérêts des tiers doivent également être pris en considération. En ce qui concerne cette exigence, la Slovénie a souligné que l'enquête doit être menée de manière à porter le moins possible atteinte aux droits des personnes qui ne sont pas des suspects ou des défendeurs, et qu'elle doit protéger le secret ou la confidentialité des données et ne pas causer de dommages disproportionnés.

---

[66] En ce qui concerne la limitation de la durée du pouvoir, la Hongrie a indiqué que si la saisie n'est plus nécessaire aux fins d'une procédure, des dispositions doivent être prises sans délai pour mettre fin à la saisie et libérer l'objet saisi, ou une demande de confiscation de l'objet saisi doit être présentée. Le Portugal a souligné que toutes les décisions de perquisition et de saisie sont limitées à 30 jours, c'est-à-dire qu'après la décision de l'autorité judiciaire, la police dispose d'un délai limité (jusqu'à 30 jours) pour exécuter la mesure. Passé ce délai, l'autorisation expire et ne peut plus être exécutée.

[67] Par exemple, en ce qui concerne la proportionnalité, la Géorgie a souligné que lorsque plusieurs alternatives sont disponibles, le pouvoir d'investigation le moins intrusif doit être choisi (par exemple, lorsque c'est possible, la production de données doit être effectuée au lieu de la perquisition et de la saisie).

D'autres garanties ont été signalées, comme le droit de la personne visée par la mesure d'être présente lors d'une perquisition ou l'obligation de procéder à la perquisition en présence d'un certain nombre de personnes n'ayant aucun lien avec l'enquête et considérées comme impartiales (principe des "quatre yeux").

Les garanties liées à l'intégrité des données ont également été mentionnées. Parmi elles, le traitement des données de manière sûre et confidentielle et les mesures visant à garantir que les données ne sont pas altérées ou modifiées de quelque manière que ce soit ont été les plus citées. Afin d'empêcher l'accès à distance aux appareils et l'effacement et/ou le verrouillage des données, les autorités sécurisent les ordinateurs portables et les appareils téléphoniques dans des cages de Faraday ou les mettent en mode avion. Pour ce faire, il faut disposer de l'expertise technique nécessaire pour effectuer la perquisition, l'extension de la perquisition et la saisie des données informatiques stockées d'une manière qui préserve l'intégrité des données et ne cause pas de dommages excessifs au système ou à d'autres données.

Quelques Parties ont initialement indiqué que, dans leur juridiction, il n'y a pas de conditions et de garanties applicables en matière de perquisition et de saisie de données informatiques stockées, mais certaines d'entre elles ont par la suite clarifié leurs réponses.

Voici quelques exemples de pratiques :

- Australie : obligation de déclarer le nombre de mandats

  Les agences doivent rendre compte chaque année du nombre de mandats demandés et délivrés au cours de l'année, ainsi que du nombre d'autorisations d'urgence. Des registres doivent également être tenus sur les mandats d'accès aux ordinateurs, notamment en ce qui concerne les décisions d'octroi, de refus, de retrait ou de révocation des mandats et la manière dont les informations contenues dans le mandat ont été communiquées. Cela permet de vérifier le respect des exigences prévues par le droit national applicable.

- Autriche : notification en cas de saisie

  Dans tous les cas de saisie, une confirmation de la saisie doit être remise immédiatement à la personne concernée ou envoyée dans les 24 heures au plus tard. La confirmation doit être faite par écrit et constitue un document (public). Dans tous les cas, la confirmation doit également contenir des mentions légales : Elle doit non seulement informer sur le droit de former une objection conformément à l'article 106, mais aussi sur le droit de la personne concernée de demander une décision judiciaire sur la levée ou le maintien d'une saisie (article 111, paragraphe 4, du code de procédure pénale). Conformément à l'article 106 para. 1 du CPC, toute personne affirmant que ses droits personnels ont été violés dans le cadre d'une procédure d'enquête par l'autorité de poursuite peut soulever des objections auprès du tribunal, notamment si une mesure d'enquête ou de coercition a été ordonnée ou exécutée en violation des dispositions du présent code. La personne concernée a également le droit de demander une décision judiciaire sur la levée ou le maintien d'une saisie conformément à l'article 115, paragraphe 2, du code de procédure pénale. Conformément à la section 115 para. 6 du CPC, si et lorsque les conditions préalables à la saisie ne sont pas réunies ou cessent d'exister, ou si la somme d'argent est payée, l'autorité chargée des poursuites ou, après le dépôt de l'acte d'accusation, le tribunal, doit lever la saisie. L'article 112 du CPC prévoit également un droit d'opposition dans le cas où une personne faisant l'objet d'une saisie bénéficie des privilèges prévus par le CPC (par exemple, le secret professionnel de l'avocat). De la même manière, l'article 112a du code de procédure pénale prévoit des conditions et des garanties pour certains types d'informations classifiées (renseignements). Il peut

s'agir, par exemple, d'informations qui ont été transmises sous une forme classifiée par des autorités de sécurité ou des organisations de sécurité étrangères.

- Danemark : traitement des données privilégiées

  Décision de la Cour suprême du 8 janvier 2015, affaire 154/2014 (UfR 2015.1249 H). Dans cette affaire, plusieurs ordinateurs et téléphones portables ont été saisis, ainsi que les données stockées sur ces appareils. Certaines parties des données étaient liées à l'affaire, tandis que d'autres étaient protégées par le privilège des informations fournies par les sources aux médias. Il a donc été décidé de dupliquer les données sur une copie de sauvegarde, et le tribunal a décidé quelles parties des données devaient être accessibles au cours de l'enquête. Cette procédure avait pour but de garantir que toutes les données pertinentes feraient partie de l'enquête tout en protégeant la confidentialité entre un média et ses sources, telle que protégée par la législation danoise.

- Pays-Bas : critères relatifs au niveau d'atteinte à la vie privée en ce qui concerne la fouille de l'appareil informatique confisqué (smartphone) :

  - Lorsque l'atteinte à la vie privée est limitée : L'agent des services répressifs peut effectuer des recherches sans autre autorisation (articles 95 et 96 du DCCP) (par exemple, numéros de téléphone récemment utilisés, recherche de messages ou d'images spécifiques) ;
  - Lorsque l'atteinte à la vie privée est plus que limitée : l'autorisation préalable d'un procureur est nécessaire (article 141 ou article 148 ou article 95 ou 96 du DCCP) (par exemple, l'analyse d'une copie ou d'une image du contenu de l'appareil) ;
  - Lorsque l'atteinte à la vie privée est très grave et prévisible, l'autorisation préalable d'un juge d'instruction est nécessaire. (Article 181 jo. 104 jo. Article 177 DCCP) (pas d'exemples clairs, mais la nature des données informatiques stockées est considérée comme décisive).

- Suède : Commission sur la sécurité et la protection de l'intégrité

  Une autorité spéciale, la Commission sur la sécurité et la protection de l'intégrité, est chargée de superviser l'utilisation par les forces de l'ordre de la surveillance secrète, y compris l'interception de données secrètes. Ce contrôle vise notamment à s'assurer que les activités sont menées conformément aux lois et autres réglementations. La Commission exerce son contrôle par le biais d'inspections et d'autres enquêtes. La Commission peut faire des déclarations sur des circonstances établies et exprimer son avis sur la nécessité de modifier les activités. Elle s'efforce de veiller à ce qu'il soit remédié à toute lacune dans les lois et autres réglementations. À la demande d'un particulier, la Commission est tenue de vérifier si celui-ci a fait l'objet d'une surveillance secrète et si le recours à la surveillance secrète et aux activités connexes a été conforme aux lois et autres règlements. La Commission notifie à l'intéressé que le contrôle a été effectué.

## 8.2 Mise en œuvre de l'article 19.5 - Évaluation

Les réponses aux questions suivantes questionnaire ont été évaluées :

- Les conditions et garanties applicables lors de l'application des différentes mesures de perquisition, d'extension de la perquisition et de saisie des données informatiques stockées ont été évaluées (réponses à la question 3.1.1 et autres questions correspondantes du questionnaire).

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Albanie | Les autorités ont déclaré que ces pouvoirs procéduraux sont sans exception soumis à une autorisation judiciaire. Selon l'article 151 du code de procédure pénale, les preuves (en général) qui ne sont pas obtenues conformément aux dispositions du code de procédure pénale ne peuvent pas être utilisées dans le cadre d'une procédure pénale.<br><br>Il est important de noter que le paragraphe 1 de l'article 208/A du CPP stipule que cet article ne s'applique qu'aux crimes liés aux technologies de l'information. | L'Albanie est partiellement en conformité avec l'art. 19.5.<br><br>Les autorités doivent envisager d'étendre le champ d'application de la mesure à toutes les infractions pour lesquelles les preuves se trouvent sur un système informatique. |
| Andorre | Les autorités ont indiqué que la perquisition et la saisie de données informatiques peuvent être appliquées à toutes les infractions pénales graves correspondant à des délits majeurs (plus de deux ans d'emprisonnement), quelle que soit la nature de l'infraction, et aux délits mineurs de corruption ou de trafic d'influence.<br>Les perquisitions doivent être fondées sur une base juridique suffisante et être autorisées par un juge d'instruction. Ces autorisations peuvent faire l'objet d'un recours et être contestées devant la Cour constitutionnelle pour violation des droits fondamentaux. | L'Andorre est partiellement en conformité avec l'art. 19.5.<br><br>Les autorités doivent envisager d'étendre le champ d'application de la mesure à toutes les infractions pour lesquelles les preuves se trouvent sur un système informatique. |
| Argentine | Il existe plusieurs traités internationaux sur les droits de l'homme auxquels l'Argentine est partie. D'autre part, l'article 18 de la Constitution nationale prévoit l'inviolabilité du domicile, ainsi que l'inviolabilité de la correspondance épistolaire et des papiers privés.<br><br>Dans cette optique, l'article 19 du texte constitutionnel reconnaît que "les actions privées des hommes qui ne portent pas atteinte à l'ordre public et aux bonnes mœurs, ni ne nuisent à un tiers, sont réservées à Dieu seul et soustraites à l'autorité des magistrats...". D'autre part, l'Argentine dispose | L'Argentine est en accord avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'un régime de protection des données en vertu de l'article 43 de la Constitution nationale et de la loi n° 25 326 sur la protection des données à caractère personnel.<br><br>Il convient de noter qu'au niveau international, l'Argentine a approuvé la Convention 108+ par le biais de la loi n° 27.699. L'accès au contenu des téléphones portables et des ordinateurs doit être effectué en vertu d'un mandat judiciaire. La perquisition doit faire l'objet d'une ordonnance judiciaire qui indique et justifie expressément la nécessité d'accéder au contenu d'un appareil donné. Les preuves ne seront pas admises si elles ont été obtenues illégalement ou en violation des garanties fondamentales du processus pénal. Les règles et les formalités prévues dans un moyen de preuve expressément envisagé et pouvant lui être assimilé sont appliquées par analogie, à condition que les garanties constitutionnelles ne soient pas violées. | |
| Arménie | Les conditions générales et les garanties prévues par le CPC s'appliquent à tous les types de mesures, y compris la perquisition et la saisie de données informatiques stockées. Elles concernent le contrôle judiciaire des mesures, les actions menées par les autorités compétentes, les privilèges et immunités, etc. | L'Arménie est en conformité avec l'art. 19.5. |
| Australie | La loi sur les infractions prévoit de nombreuses voies de recours. Il s'agit notamment de l'exclusion de preuves lors du procès, de l'indemnisation pour les dommages causés au matériel et du contrôle des décisions et des pouvoirs par quatre entités : le médiateur du Commonwealth, l'Australian National Audit Office, le Parlement et le pouvoir judiciaire. En vertu de la loi sur le développement durable, la première garantie est que les mandats doivent être délivrés par un juge ou un fonctionnaire désintéressé. La loi prévoit également des exigences en matière de rapports et de contrôle, y compris des rapports au procureur général sur certains détails de chaque mandat d'accès à un ordinateur et des rapports périodiques sur les mandats délivrés, refusés, etc. | L'Australie est en accord avec l'art. 19.5.<br><br>Les autorités devraient envisager d'étendre le champ d'application de la mesure à toutes les infractions pour lesquelles des éléments de preuve se trouvent sur un système informatique. |
| Autriche | Plusieurs articles du code de procédure pénale garantissent les droits procéduraux des personnes concernées par une saisie. La notification écrite d'une saisie doit être faite en temps utile et inclure une déclaration relative à certains droits de recours. Les plaintes peuvent être adressées à l'autorité chargée des poursuites ou au tribunal compétent. Si des données spécialement protégées sont saisies - par exemple, des données soumises au secret professionnel - des dispositions détaillées s'appliquent, | L'Autriche est en accord avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | y compris la mise sous séquestre des données, des procédures de traitement spéciales, etc. Des procédures spéciales s'appliquent également lorsqu'il s'agit de renseignements classifiés. | |
| Azerbaïdjan | En vertu du CPC, les dispositions générales applicables à toute perquisition et saisie sont applicables aux perquisitions et saisies électroniques ainsi qu'aux prolongations de perquisition. Les articles pertinents du CPC sont soumis aux articles 14 et 15 de la Convention de Budapest. Les protections prévues par le CPP comprennent le fait que les perquisitions et certains autres actes d'enquête ne peuvent être effectués qu'en vertu du CPP et sur la base d'une décision de justice. En outre, au cours d'une procédure pénale, les droits à la vie privée, à la confidentialité des communications et à l'inviolabilité de la personne sont protégés. Toute dérogation à ces droits nécessite une décision de justice, sauf dans les cas de détention et d'arrestation. Tous les actes d'enquête doivent être consignés et enregistrés immédiatement ou dans la journée. Toutes les décisions de procédure sont des documents essentiels qui doivent être enregistrés sur des formulaires spécialement conçus à cet effet. Nul ne peut pénétrer dans une habitation sans le consentement de ses occupants, sauf dans certaines circonstances. | L'Azerbaïdjan est en ligne avec l'article 19.5. |
| Belgique | L'article 39bis incorpore par référence, et s'applique aux systèmes d'information, les règles générales de perquisition et de saisie du code. Les règles générales permettent à une personne concernée de déposer une plainte auprès du procureur. Ces plaintes peuvent être fondées sur de nombreux motifs, avec lesquels le procureur peut être d'accord ou en désaccord, en tout ou en partie. Il est possible de faire appel de la décision du procureur. | La Belgique est en accord avec l'art. 19.5. |
| Bénin | En règle générale, les appels au domicile et les perquisitions ne peuvent avoir lieu qu'entre 6 heures et 21 heures, selon le code de procédure pénale. En outre, la personne concernée doit consentir à la perquisition (voir ci-dessus) et les droits des personnes physiques doivent être respectés à cet égard.<br><br>Plus précisément, l'article 78 du CPC et l'article 592 de la loi sur le code numérique précisent les conditions et les garanties attachées aux perquisitions et aux saisies. La violation de ces règles est un motif d'annulation de la procédure, ce qui ne signifie pas pour autant que l'affaire est classée sans suite. Par exemple, le non-respect des heures de perquisition constitue une violation des droits du | Le Bénin est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | suspect par l'enquêteur. Généralement, la procédure est reprise et confiée soit à une autre unité de police judiciaire, soit à un autre enquêteur de la même unité de police. | |
| Bosnie et Herzégovine | Les autorités de Bosnie-Herzégovine doivent respecter de nombreuses garanties concernant les perquisitions et les saisies. Il s'agit notamment des exigences décrites précédemment, telles que les mandats, ainsi que la protection du droit à un procès équitable et au respect de la vie privée ; les exigences de nécessité, de proportionnalité et de notification ; le maintien de l'intégrité des données saisies ; et la non-divulgation des données à des personnes non impliquées. La Fédération de Bosnie-Herzégovine a mentionné spécifiquement les mesures techniques visant à préserver l'intégrité des données. | La Bosnie-Herzégovine est en conformité avec l'article 19.5. |
| Brésil | Les pouvoirs en matière de perquisition et de saisie s'appliquent aux infractions pénales relevant du droit national lorsque les preuves se trouvent sur un système informatique. Cela signifie que s'il existe des preuves d'une infraction pénale stockées sur un système informatique, qu'il s'agisse d'une cybercriminalité ou de tout autre type d'infraction, les autorités peuvent demander une perquisition et une saisie des données. Le cadre juridique ne limite pas l'application des pouvoirs de perquisition et de saisie à des types d'infractions spécifiques.<br><br>La recherche, l'extension et la saisie de données informatiques stockées sont soumises à des garanties visant à protéger les droits individuels et la vie privée tout en assurant l'efficacité de l'application de la loi. Les principales garanties prévues par la constitution brésilienne sont les suivantes : autorisation judiciaire fondée sur des soupçons raisonnables ; mesures proportionnées à l'infraction faisant l'objet de l'enquête ; limitation des données perquisitionnées ou saisies aux informations pertinentes ; autorités compétentes disposant d'une expertise technique ; notification à la personne dont les données sont perquisitionnées ; confidentialité des données obtenues uniquement à des fins d'enquête ; contrôle judiciaire de la légalité et de la proportionnalité des mesures. | Le Brésil est en accord avec l'art. 19.5 |
| Bulgarie | Les garanties pertinentes comprennent le contrôle judiciaire. Les perquisitions sont toujours effectuées en présence d'une personne qui utilise les locaux ou d'un représentant de la personne morale. Une perquisition requiert également toujours la présence de deux personnes qui ne sont liées d'aucune manière à l'enquête et qui sont considérées comme impartiales. L'article 137 du code de procédure pénale énonce explicitement les droits et les responsabilités de ces témoins : | La Bulgarie est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | (4) Les témoins d'actes de procédure ont les droits suivants : faire des remarques et des objections sur le caractère incomplet et les violations de la loi qui ont été admises ; demander des corrections, des modifications et des compléments au dossier ; signer le dossier sous avis spécial, en indiquant par écrit les raisons de cet avis ; demander l'annulation des actes qui portent atteinte à leurs droits et à leurs intérêts légaux ; obtenir une rémunération et la couverture des frais encourus. | |
| Cabo Verde | Le Cabo Verde a indiqué que l'autorité judiciaire compétente autorise les perquisitions informatiques pour une durée maximale de 30 jours - sous peine de nullité - et que l'autorité doit superviser l'enquête (article 17 de la loi sur la protection des données). Dans des cas exceptionnels, la police criminelle peut effectuer des recherches sans autorisation préalable, par exemple lorsque le consentement est fourni ou en cas d'imminence de terrorisme ou de crime organisé. Dans ce cas, l'enquête doit être détaillée dans un rapport comprenant les résultats et les preuves, qui doit être soumis à l'autorité judiciaire.<br><br>Dans le cas de l'extension de la recherche (article 17º, nº 5), les mêmes conditions et garanties que celles de l'article 17 s'appliquent, à savoir l'autorité compétente, la durée de validité de l'autorisation et les formalités d'exécution de l'autorisation. Une copie de l'ordre de perquisition est remise à la personne qui a la disponibilité ou le contrôle du système informatique dans lequel la perquisition doit être effectuée. - Article 18º, n° 6, en liaison avec l'article 237º du code de procédure pénale.<br><br>Dans le cas de la saisie de données informatiques (article 18 de la CL), si nécessaire, la saisie doit être autorisée ou ordonnée par une ordonnance de l'autorité judiciaire compétente.<br><br>L'organe de police judiciaire peut effectuer des saisies sans autorisation préalable de l'autorité judiciaire, mais dans ce cas, il doit s'agir d'une perquisition informatique légitimement ordonnée et effectuée conformément à l'article 17º (perquisition informatique), ainsi que lorsqu'il y a urgence ou danger dans le délai. Cette situation doit être validée dans les 72 heures.<br><br>Si les saisies révèlent des données personnelles ou intimes, elles doivent être présentées au juge. | Cabo Verde est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les saisies liées à des professions spécifiques sont personnellement supervisées par le juge, avec notification préalable aux organismes professionnels concernés. Les perquisitions peuvent être empêchées par le secret professionnel, le secret de fonction et le secret d'État, qui peuvent être invoqués par des personnes désignées conformément à la loi. | |
| Cameroun | Les conditions et les garanties applicables dans ce domaine découlent du CPC.<br><br>En outre, d'autres mesures seront prises concernant l'application en cours du cadre camerounais de lutte contre la cybercriminalité, notamment :<br>- la révision en cours de la loi camerounaise sur la cybercriminalité mentionnée ci-dessus ;<br>- le projet de loi sur la protection des données personnelles, déjà élaboré ;<br>- le projet d'un manuel de procédures d'investigation numérique. | Le Cameroun est en conformité avec l'article 19.5. |
| Canada | Deux sections du code pénal précisent les garanties relatives aux perquisitions et aux saisies. Ces garanties prévoient notamment qu'il doit y avoir des motifs raisonnables de croire que l'objet recherché est lié à une infraction ou sera utilisé pour la commettre, ou qu'il révélera l'emplacement d'un suspect. Si des données dont la saisie n'est pas autorisée par un mandat sont saisies, elles peuvent être exclues en tant que preuves au procès. Un mandat général ne peut être délivré que lorsqu'un juge est convaincu que (outre les exigences habituelles) les meilleurs intérêts de l'administration de la justice seront servis par sa délivrance. En outre, un mandat général ne sera délivré que si aucune autre forme de mandat ou d'ordonnance n'est applicable à la technique en question. Cette dernière exigence garantit que les autorités ne demandent pas de mandats généraux pour se soustraire à des demandes plus élaborées de mandats pour des techniques (électroniques) spécifiques. Les mandats généraux sont également limités à d'autres égards.<br><br>Des organes de contrôle indépendants peuvent examiner les pratiques et procédures des services répressifs, intervenir à leur sujet et établir des lignes directrices. Il s'agit notamment du Commissaire à la protection de la vie privée du Canada et des commissions parlementaires.<br><br>La Charte des droits et libertés est le principal garant des droits de l'homme dans ce contexte. | Le Canada est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Chili | Les garanties prévues par l'article 12 de la loi 21.459 comprennent les aspects suivants : Premièrement, l'exigence d'un soupçon raisonnable, basé sur des faits spécifiques, d'implication ou de participation à un acte criminel. Deuxièmement, l'autorisation du juge est subordonnée à une demande formelle du ministère public. Enfin, le ministère public est tenu de fournir au juge un rapport exhaustif et complet dans le cadre de la procédure. Les mesures prévues par le code de procédure pénale sont soumises aux garanties qui y sont prévues. Les garanties prévues par la Constitution du Chili sont également applicables. | Le Chili est en accord avec l'art. 19.5. |
| Colombie | La Colombie a indiqué que la législation reconnaît la protection de la vie privée et des données de l'habeas pendant l'exécution des activités de police judiciaire. Ils ont également suggéré que les dispositions et les pouvoirs d'enquête mentionnés dans les paragraphes précédents s'appliquent i) aux affaires dans lesquelles un comportement informatique caractérisé comparable aux articles 2 à 11 de la CB fait l'objet d'une enquête ; ii) aux comportements dans lesquels les technologies de l'information ont été utilisées comme support, y compris les dispositifs et les systèmes informatiques ; et iii) à toute autre affaire dans laquelle la collecte de preuves numériques est nécessaire. Pour assurer la protection de ces droits, elle prévoit que :<br><br>- L'ordre écrit doit être délivré par un procureur et doit être motivé, délimiter les espaces virtuels à perquisitionner, les données à extraire et leur relation avec les informations à extraire, les données à obtenir et leur relation avec l'hypothèse d'enquête.<br>- Comme pour les mandats de perquisition dans les espaces physiques, l'ordre écrit du procureur doit délimiter les espaces virtuels à perquisitionner, les données à extraire et leur relation avec l'hypothèse de l'enquête.<br>- Les preuves collectées peuvent être exclues par les tribunaux pour non-conformité avec les dispositions légales, et/ou pour atteinte au droit à la vie privée, à l'Habeas Data, à la non auto-incrimination et, en général, à tout autre droit fondamental.<br>- La preuve peut également être exclue pour cause de violation du secret professionnel et de la protection des autres professions libérales prévue par la Constitution.<br>- L'extraction d'informations doit être effectuée dans un délai maximum de 30 jours pendant la phase d'enquête et dans un délai maximum de 15 jours pendant la phase d'enquête ou après l'acte d'accusation. | La Colombie est en accord avec l'art. 19.5 |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | - La procédure effectuée par l'expert informatique et les résultats obtenus sont soumis au contrôle constitutionnel d'un juge du contrôle des garanties (Juez de Control de Garantías) dans les 36 heures suivant la fin de l'activité.<br>- Pendant l'audience de légalisation et le contrôle de la procédure, il est possible pour la défense de participer pour s'opposer à n'importe laquelle des phases épuisées à cette fin. | |
| Costa Rica | Cette mesure s'applique à toutes les enquêtes, quel que soit le type d'infraction.<br><br>Les autorités ont indiqué qu'il n'y avait pas de développements législatifs concernant les moyens d'obtenir des preuves numériques, comme une loi spécifique, et qu'il n'y avait donc pas de garanties concernant la recherche et la saisie de données numériques. Néanmoins, les conditions générales des garanties établies dans le code de procédure pénale s'appliquent à l'acquisition de tout moyen de preuve ordinaire.<br><br>En raison de l'absence de réglementation spécifique sur la preuve numérique, il n'existe pas de garanties spécialement conçues pour les mesures prévues à l'art. 19. Les garanties générales de la procédure pénale s'appliquent par analogie. | Le Costa Rica est en conformité avec l'art. 19.5. |
| Croatie | La Croatie applique un contrôle judiciaire et un certain nombre d'autres conditions, limitations et garanties générales à respecter avant, pendant et après une perquisition (dispositions communes), qui s'appliquent également à l'article 257.<br><br>Les articles 239, 242 et 243 du CPP établissent de nombreuses garanties pour les perquisitions en général. Ces garanties comprennent (selon l'article 239) le fait que le défendeur doit être informé des raisons pour lesquelles il est soupçonné, qu'il n'est pas tenu de répondre aux questions ou de présenter une défense, qu'il a le droit de voir les preuves et qu'il a le droit d'avoir un interprète et un avocat.<br><br>L'article 64 du code de procédure pénale dresse une liste exhaustive des droits du défendeur en ce qui concerne toutes les mesures d'enquête. Ces droits comprennent le fait d'être rapidement informé des motifs de l'accusation, de bénéficier des services d'un interprète si nécessaire et d'un avocat de la | La Croatie est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | défense (rémunéré par le gouvernement si nécessaire), et de pouvoir examiner les preuves, contre-interroger les témoins et garder le silence.<br><br>Les articles 244 et 245 du code de procédure pénale permettent de ne pas appliquer certains droits du défendeur dans des cas exceptionnels (article 244 : non-remise d'un mandat judiciaire, d'une déclaration de droits ou d'une demande de remise d'un objet de perquisition ; article 245 : substitution du mandat du procureur de l'État à un mandat judiciaire antérieur). | |
| Chypre | Des mandats peuvent être délivrés pour des perquisitions et des saisies électroniques concernant n'importe quel délit.<br><br>Chypre exige la délivrance d'un mandat de perquisition/d'une ordonnance judiciaire par un juge sur la base du serment écrit d'un officier de police. L'ordonnance doit être nécessaire pour faire avancer l'enquête et éviter la destruction des preuves. D'une manière générale, elle doit être nécessaire et proportionnée. Les personnes concernées peuvent contester le mandat ou l'ordonnance. | Chypre est conforme à l'art. 19.5. |
| République tchèque | Les mesures ne peuvent être appliquées que dans le cadre de procédures pénales, y compris pour d'autres infractions, lorsque les preuves se trouvent sur un système informatique, sous réserve d'un soupçon raisonnable que le système informatique contienne les preuves.<br>Les perquisitions à domicile et les perquisitions dans d'autres locaux et lieux nécessitent une décision de justice. Dans des circonstances limitées, les autorités policières peuvent également délivrer des ordres d'enlèvement d'objets.<br><br>Le tribunal doit toujours évaluer la proportionnalité et la nécessité d'une telle action (disposition 2, paragraphe 4, du CPC). L'ordonnance du tribunal doit être motivée et signifiée à la personne chez qui la perquisition est exécutée. La personne concernée doit être entendue avant la perquisition, sauf en cas d'urgence, et elle a le droit d'être présente pendant la perquisition. La perquisition à domicile et la fouille personnelle doivent être effectuées en présence d'une tierce personne n'ayant aucun lien avec l'enquête et la personne concernée. | La République tchèque est en conformité avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La législation prévoit également la protection des personnes contre la contrainte de s'incriminer elles-mêmes, ainsi que la protection du secret professionnel. | |
| Danemark | La réglementation applicable aux perquisitions et saisies contient de nombreuses exigences, limitations et protections. Outre celles déjà décrites, les exigences comprennent la notification, la présence de la personne fouillée ou d'un substitut, la représentation par un avocat avant la délivrance d'une ordonnance dans certains cas, la possibilité d'annuler une ordonnance du tribunal et, en général, l'obligation de procéder à des fouilles aussi délicates que possible. | Le Danemark est en conformité avec l'article 19.5. |
| République dominicaine | La législation interne de la République dominicaine combine les mêmes conditions et garanties établies dans la Constitution dominicaine et le Code de procédure pénale, stipulant que les perquisitions ne peuvent être effectuées qu'à la demande du Procureur général, avec un mandat de perquisition délivré par une décision judiciaire motivée. En cas d'urgence et en l'absence du procureur, la police peut faire une demande directe.<br>La loi 53/07 ne prévoit pas expressément que les règles de procédure qu'elle contient s'appliquent aux enquêtes sur tous les délits. Par conséquent, il est possible d'interpréter que les pouvoirs procéduraux de perquisition et de saisie de données ne s'appliquent pas aux enquêtes sur tous les délits, mais uniquement aux délits informatiques prévus par cette loi spéciale.<br><br>Nonobstant ce qui précède, les autorités de la République dominicaine ont indiqué que, dans la pratique et la jurisprudence, le chapitre II de la loi 53-07 sur les mesures procédurales, y compris les pouvoirs prévus à l'article 54, n'est pas lié aux infractions établies par la loi 53-07 et est donc applicable à toute infraction comportant des preuves électroniques. | La République dominicaine est en conformité avec l'art. 19.5, mais il est conseillé de modifier la législation pour préciser que les dispositions procédurales s'appliquent à l'enquête sur tous les crimes. |
| Estonie | Les mesures de perquisition et de saisie s'appliquent à toutes les infractions et sont limitées aux enquêtes criminelles. En ce qui concerne l'accès clandestin, qui est considéré comme une activité de surveillance, la loi prévoit une liste ou un catalogue de crimes graves pour lesquels les mesures de surveillance sont autorisées.<br><br>L'exécution des pouvoirs est soumise à un contrôle judiciaire. | L'Estonie est en conformité avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | En règle générale, les personnes peuvent contester tout acte ou mesure de procédure conformément aux règles générales sur les recours. Tant au cours de l'enquête préliminaire que du procès, les preuves obtenues et les mesures procédurales utilisées peuvent faire l'objet d'un contrôle judiciaire.<br>Une plus grande limitation est imposée en ce qui concerne les opérations secrètes.<br><br>En ce qui concerne la notification, il existe des règles générales concernant l'information de la personne concernée sur la mesure en question, les droits et obligations ainsi que les voies de recours. | |
| Fidji | Les autorités fidjiennes ont indiqué que l'article 24 de la Constitution fidjienne prévoit que le droit à la vie privée doit être pris en compte.<br><br>Dans le même temps, l'article 21 du TCA prévoit les garanties nécessaires à la mise en œuvre de l'article 24 de la Constitution. Il établit la règle et précise l'expertise technique nécessaire pour extraire les données tout en préservant la vie privée telle qu'elle est inscrite dans la Constitution.<br><br>Plus précisément, l'article 21 du TCA prévoit des garanties pour la procédure de recherche et de saisie des données informatiques stockées. La demande de recherche doit répondre à certaines exigences afin de protéger l'intégrité et la confidentialité des données. Elle doit indiquer les raisons pour lesquelles le matériel recherché est susceptible d'être trouvé dans le système informatique ou le support de stockage spécifié. Elle doit également préciser la nature des preuves susceptibles d'être trouvées et les mesures techniques à prendre pour effectuer la perquisition et la saisie, en donnant la priorité à des techniques telles que la mise en miroir ou la copie des données pertinentes et en évitant, dans la mesure du possible, la garde physique du système informatique ou du support de stockage. | Fidji est en conformité avec l'art. 19.5 |
| Finlande | L'article 21 de la loi sur la protection des données énonce les conditions à remplir pour effectuer une recherche de données contenues dans un dispositif, à savoir la suspicion d'une infraction passible d'une peine d'emprisonnement d'au moins six mois et la possibilité de découvrir des éléments de preuve pertinents. Une recherche de données contenues dans un dispositif et une recherche à distance de données contenues dans un dispositif peuvent être effectuées si la peine la plus sévère prévue pour l'infraction est une peine d'emprisonnement d'au moins six mois. La surveillance technique d'un dispositif peut être effectuée si la peine la plus sévère prévue pour l'infraction est une peine | La Finlande est en accord avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | d'emprisonnement d'au moins quatre ans ou si l'infraction est l'une des infractions énumérées dans la disposition.<br><br>Lors de l'application des dispositions relatives aux mesures coercitives dans un cas spécifique, le principe de proportionnalité doit être pris en compte. Ces mesures ne peuvent être utilisées que si elles peuvent être considérées comme justifiées, compte tenu de la gravité de l'infraction faisant l'objet de l'enquête, de l'importance de l'élucidation de l'infraction, de la mesure dans laquelle l'utilisation de la mesure coercitive viole les droits du suspect de l'infraction ou d'autres personnes, et des autres circonstances. Un fonctionnaire ayant le pouvoir d'arrestation décide d'une fouille des données contenues dans un appareil et d'une fouille des données contenues dans un appareil en tant que fouille à distance. Un officier de police peut prendre la décision dans les situations d'urgence.<br><br>Si une perquisition peut permettre de découvrir des informations protégées par le droit ou l'obligation de ne pas témoigner en justice, un tribunal décide de la perquisition et désigne un représentant de la perquisition. Si, au cours d'une perquisition, il apparaît que la perquisition vise le type d'informations susmentionné, ou s'il est nécessaire d'effectuer la perquisition d'urgence, un fonctionnaire ayant le pouvoir d'arrestation décide de la conduite de la perquisition et de la désignation du représentant de la perquisition.<br><br>Le tribunal décide de la surveillance technique d'un dispositif. Si l'affaire ne souffre aucun retard, un fonctionnaire ayant le pouvoir d'arrêter peut décider de la surveillance jusqu'à ce que la juridiction ait décidé de rendre la décision.<br>Si, lors d'une perquisition, un document a été copié pour servir de preuve, la juridiction décide, à la demande de la personne concernée par l'affaire, si la copie du document doit être conservée pour servir de preuve. | |
| France | Les garanties applicables en matière pénale, notamment les droits de recours, sont également applicables dans ces affaires. | La France est en conformité avec l'article 19.5. |
| Géorgie | Ces pouvoirs sont soumis à des garanties, notamment le contrôle judiciaire obligatoire, la proportionnalité, les motifs justifiant l'application (cause probable), le droit de recours, les limitations, | La Géorgie est en accord avec l'art. 19.5 |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | les notifications, les immunités, les exigences en matière de protection des données et le droit à des voies de recours. | |
| Allemagne | Les mesures sont soumises aux exigences et garanties du système juridique national. Plus précisément, toute personne concernée a droit à un procès équitable, dans le respect des principes de l'État de droit. Parmi les autres garanties figurent la nécessité, la proportionnalité, la légalité, le contrôle judiciaire et le réexamen. | L'Allemagne est en accord avec l'art. 19.5. |
| Ghana | L'article 18 de la constitution protège la vie privée des personnes en ce qui concerne leur domicile, leurs biens, leur correspondance ou leurs communications, sauf dans certaines circonstances, conformément à la loi d'une société libre et démocratique. Les perquisitions et les saisies doivent faire l'objet d'un mandat délivré par un tribunal, sauf lorsqu'elles sont effectuées dans le cadre d'une arrestation ou dans d'autres cas limités. D'autres protections potentielles incluent des exigences relatives à la chaîne de possession, à la photographie avec marquage, aux témoins, à la réalisation et à la conservation de copies des données informatiques pertinentes et au maintien de leur intégrité, et au retrait des données d'un système perquisitionné ou au fait de rendre les données inaccessibles uniquement si les exigences spécifiques de la loi sont satisfaites (voir par exemple les articles 98 et 99 de la LTA). | Le Ghana est en accord avec l'article 19.5. |
| Grèce | Plusieurs principes "visent à établir un équilibre entre les besoins d'investigation des services répressifs et la protection des droits individuels et de la vie privée, en veillant à ce que ces mesures soient mises en œuvre de manière légale et responsable". Ces principes comprennent le respect de l'autorisation légale, de la cause probable ou des motifs raisonnables, la protection des droits individuels, l'intégrité et la sécurité des données, la transparence et la responsabilité, ainsi que la préservation des données en prévision d'un procès. | La Grèce est en conformité avec l'article 19.5. |
| Grenade | Les autorités de la Grenade ont indiqué que les articles 26 à 32 de la loi sur la criminalité électronique prévoient des conditions pour la saisie des données stockées. Les garanties les plus importantes sont le contrôle judiciaire et l'utilisation limitée des données et des informations. | La Grenade est en conformité avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | D'autres garanties en matière de droits de l'homme sont couvertes par la Constitution pour tous les citoyens et résidents.<br><br>Les pouvoirs conférés par la loi sur la criminalité électronique s'appliquent à toute infraction visée à l'article 22, paragraphe 2, point c). | |
| Hongrie | L'article 2 du code de procédure pénale protège expressément la dignité humaine et le droit à la liberté et à la sécurité. Les droits fondamentaux ne peuvent être restreints que de la manière décrite en détail à l'article 271 du code de procédure pénale et dans la mesure la plus limitée possible.<br><br>Les saisies doivent être interrompues le plus rapidement possible.<br><br>La base juridique et le mode de saisie des données électroniques peuvent être contestés par les parties concernées. Les plaintes sont transmises au ministère public pour examen. | La Hongrie est en conformité avec l'article 19.5. |
| Islande | Les pouvoirs de perquisition et de saisie des données informatiques stockées s'appliquent également à d'autres infractions prévues par notre droit interne lorsque des éléments de preuve se trouvent sur un système informatique.<br><br>Les principales conditions et garanties appliquées en Islande sont le contrôle judiciaire, le droit de recours, la proportionnalité, les notifications, la représentation légale et la durée limitée des mesures. | L'Islande est conforme à l'art. 19.5 |
| Israël | Les perquisitions et les saisies de données informatiques ne peuvent être effectuées qu'en rapport avec des délits passibles d'une peine maximale de plus de trois mois.<br><br>Les perquisitions sont régies par les directives du procureur général et les arrêts de la Cour suprême dans l'affaire CrimFH Urich, incorporés dans les directives de la police. Les demandes de mandats de perquisition informatique doivent répondre à de nombreuses exigences spécifiques. Les mandats doivent être délivrés par un juge et contenir des détails sur l'objectif de la perquisition et ses contraintes. La perquisition doit être nécessaire et l'atteinte à la vie privée de la personne concernée doit être limitée. | Israël est partiellement conforme à l'article 19.5. 19.5, les autorités devraient envisager d'étendre le champ d'application de la mesure à tous les éléments de preuve se trouvant sur un système informatique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | | |
| Italie | Les pouvoirs de perquisition et de saisie des données informatiques stockées s'appliquent à toute infraction prévue par le droit national.<br><br>Les conditions et les garanties sont les mêmes que celles prévues pour le suspect par le code de procédure pénale italien, à savoir : 1) la présence d'un défenseur (art. 356, 365), 2) la rédaction d'un rapport spécial par la police (art. 357), et 3) la possibilité de contester le décret - après son exécution - devant un juge (art. 257). | L'Italie est en conformité avec l'art. 19.5. |
| Japon | La Constitution et le CPP prévoient tous deux des garanties et des conditions. La Constitution stipule que toute personne a droit à la sécurité de son domicile, de ses papiers et de ses effets et que les perquisitions et les saisies doivent faire l'objet d'un mandat délivré pour un motif suffisant. L'expression "motif suffisant" est définie et les mesures coercitives non prévues par la loi sont interdites. Les personnes lésées par une perquisition et une saisie effectuées sur la base d'un mandat peuvent déposer une plainte auprès du tribunal compétent, intenter une action civile ou demander des dommages-intérêts sur la base d'une autre loi. | Le Japon est en conformité avec l'article 19.5. |
| Kiribati | L'article 29 de la loi sur la cybercriminalité prévoit des garanties lorsque ces pouvoirs procéduraux intrusifs sont utilisés. En vertu de cette loi, l'exécution des pouvoirs prévus par la loi est soumise à des conditions et à huit garanties conformément à la Constitution et aux obligations en matière de droits de l'homme découlant des conventions internationales applicables. En outre, une procédure pour une infraction prévue par la loi ne peut être engagée qu'avec le consentement du procureur général si le défendeur avait moins de 18 ans au moment où il a prétendument commis l'acte constituant l'infraction. | Kiribati est en ligne avec l'article 19.5. |
| Lettonie | L'article 219, qui s'applique à l'extension des perquisitions, ne s'applique pas à toutes les catégories de perquisitions et de saisies.<br>Les perquisitions ne peuvent être effectuées qu'après une décision d'un juge d'instruction ou d'un tribunal ou, au minimum, avec l'autorisation d'un procureur dans certains cas. Les preuves recueillies de manière inappropriée sont irrecevables lors du procès. Les accusés potentiels bénéficient de | La Lettonie est partiellement en conformité avec l'article 19.5.<br>Les autorités devraient envisager d'étendre le champ d'application de la mesure à toutes les infractions pour lesquelles des éléments de preuve se trouvent sur un système informatique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | protections contre l'auto-incrimination qui leur permettent de refuser de coopérer. Les pouvoirs de perquisition et de saisie sont régis par de nombreuses dispositions légales. | |
| Liechtenstein | En général, les perquisitions et les saisies doivent faire l'objet d'une ordonnance judiciaire.<br><br>Concrètement, ces mesures sont mises en œuvre par au moins deux agents, et toutes les actions importantes sont discutées, approuvées et exécutées par au moins deux personnes. Ces actions sont ensuite documentées dans un protocole avec des photos. L'analyse des données est toujours effectuée à l'aide de copies exactes et non de données originales. | Le Liechtenstein est en conformité avec l'article 19.5. |
| Lituanie | Les perquisitions et les saisies sont régies et limitées par plusieurs articles du code de procédure pénale. Les ordonnances judiciaires autorisant ces mesures sont susceptibles de recours de la part des personnes concernées et des tiers affectés. | La Lituanie est en conformité avec l'article 19.5. |
| Luxembourg | En résumé, toute mesure doit répondre aux normes suivantes : elle doit être approuvée par le procureur ou le juge d'instruction selon les circonstances, être dûment motivée, ne pas aller au-delà de ce qui est nécessaire à la manifestation de la vérité et être limitée dans le temps. La personne concernée doit être informée de la mesure dans un certain délai et peut être présente lors de la perquisition. Toutes les données inutiles doivent être effacées.<br><br>Le Luxembourg a énuméré de nombreuses dispositions légales qui comportent des éléments spécifiques de protection des droits de l'homme. | Le Luxembourg est en conformité avec l'art. 19.5. |
| Malte | Conformément au chapitre 9, article 355I du code pénal *: "L'agent d'exécution remet une copie du mandat à la personne qui occupe le lieu perquisitionné et qui s'y trouve, ou à toute autre personne qui semble à l'agent d'exécution être responsable du même lieu et qui se trouve être présente lors de la perquisition. S'il n'y a pas de personne présente qui semble à l'agent d'exécution être responsable des lieux, la copie du mandat est laissée dans un endroit facilement visible sur les lieux".* | Malte est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Conformément au chapitre 9 de l'article 355J du code pénal, "*une perquisition effectuée en vertu d'un mandat ne peut l'être que dans la mesure où elle est nécessaire pour atteindre le but pour lequel le mandat a été délivré".*<br><br>Le matériel saisi est stocké en toute sécurité. Les appareils devant être analysés par des experts sont remis rapidement par la police à l'expert en question ou sont récupérés par les analystes de la police dans un lieu de stockage sécurisé avant le début de l'analyse. Le laboratoire de la police n'est accessible qu'à l'équipe de criminalistique numérique et un système de vidéosurveillance assure une sécurité supplémentaire. | |
| Maurice | L'application de l'article 28 est soumise à un contrôle judiciaire. En outre, le droit d'un accusé à un procès équitable est protégé par la Constitution.<br><br>Les demandes de perquisition et de saisie sont normalement faites ex parte, mais si le juge n'est pas satisfait de la demande, il peut demander à la partie intéressée de comparaître devant le tribunal s'il y a un risque sérieux de violation des droits de l'homme ou des droits à la vie privée ou à la propriété. Si une ordonnance a déjà été rendue, une démonstration suffisante de la part de la partie intéressée peut amener le juge à annuler l'ordonnance.<br><br>Maurice a déclaré que, bien que la loi énumère des infractions dans sa partie III, l'utilisation des pouvoirs d'enquête de l'article 28 n'est pas limitée à ces infractions.<br><br>L'article 14 de l'ancien Computer Misuse and Cybercrime Act 2003 (aujourd'hui abrogé) était formulé dans des termes similaires à l'actuel article 28 de la Cybersecurity and Cybercrime Act (loi sur la cybersécurité et la cybercriminalité). L'article 14 abrogé prévoyait l'accès, la perquisition et la saisie "aux fins d'une enquête ou de la poursuite d'une infraction". Dans l'affaire Lee Wai Chung & Anor v The Independent Commission Against Corruption [2021 SCJ 37], une ordonnance a été rendue en vertu de l'article 14 pour l'accès, la perquisition et la saisie de données électroniques. Apparemment, l'infraction faisant l'objet de l'enquête était une infraction à la loi sur la prévention de la corruption, et non à la loi sur la lutte contre la corruption. L'octroi de cette ordonnance confirme que l'actuelle section 28 de la CCA et la section 14 abrogée de la CMCA ont été rédigées de manière à englober n'importe | Maurice est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | quelle infraction. Ainsi, le champ d'application de l'article 28 n'est pas limité aux infractions prévues par la loi sur la prévention de la corruption.<br><br>En outre, la Commission des crimes financiers, créée en vertu de la nouvelle loi sur la Commission des crimes financiers, est mandatée, en vertu de l'article 60 de cette loi, pour pénétrer et perquisitionner dans tous les locaux et recueillir des preuves sous forme électronique dans le cadre d'une "enquête".<br><br>Enfin, il existe des affaires (Police v Chady & Maunthrooa [2019 INT 228]) dans lesquelles des "preuves électroniques" ont été recueillies et étaient admissibles devant le tribunal pour un délit de corruption. Cette affaire confirme également que les pouvoirs d'enquête peuvent être utilisés pour d'autres infractions prévues par la loi. | |
| Monaco | Les saisies et les examens de données doivent être ordonnés ou ratifiés par une autorité judiciaire (de différents types, en fonction de l'enquête). Les preuves peuvent être supprimées si la loi a été violée au cours de l'enquête ou leur fiabilité peut être mise en doute si elles n'ont pas été protégées contre la manipulation. Les cibles peuvent demander un complément d'enquête ou l'avis d'un expert. Les données peuvent être saisies en scellant le support physique ou en faisant une copie sécurisée en présence de la personne concernée. | Monaco est en conformité avec l'art. 19.5. |
| Monténégro | La Constitution du Monténégro et le code de procédure pénale prévoient des conditions générales et des garanties qui assurent une protection adéquate des droits de l'homme et des libertés.<br><br>Les mesures sont appliquées dans le cadre d'enquêtes sur des infractions pénales. L'exécution des pouvoirs est soumise à un contrôle judiciaire. | Le Monténégro est en conformité avec l'art. 19.5. |
| Maroc | Toute enquête est supervisée par le procureur général, et les perquisitions et saisies ne peuvent avoir lieu qu'avec l'autorisation du procureur général ou du juge d'instruction. La procédure doit se dérouler en présence de la personne concernée et avec son consentement explicite. De nombreuses autres conditions et prérequis s'appliquent, tels qu'énoncés avec précision dans les articles 103 à 116 du CPP. | Le Maroc est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| Pays-Bas | Les pouvoirs conférés par la loi pour la perquisition et la saisie de données informatiques stockées s'appliquent à toutes les infractions prévues par le droit national lorsque les preuves se trouvent sur un système informatique.<br><br>Pour tous les pouvoirs procéduraux, la loi exige le respect des droits de l'homme, inscrits dans la constitution des Pays-Bas, la Charte des droits fondamentaux de l'UE, la CEDH ou dans d'autres traités auxquels les Pays-Bas sont parties. Les compétences procédurales sont inscrites dans le DCCP (légalité). Dans la plupart des cas, ils nécessitent une prise en compte explicite de la proportionnalité et de la subsidiarité. L'exécution des pouvoirs est soumise à un contrôle et/ou à une décision judiciaire. | Les Pays-Bas sont en accord avec l'art. 19.5. |
| Nigéria | La Constitution nigériane prévoit des garanties en ce qui concerne la propriété et la confidentialité des données de ses citoyens. Voir les articles 144 de la CFRN et 37 respectivement.<br>La loi sur l'administration de la justice pénale (Administration of Criminal Justice Act) contient des dispositions relatives au processus et à la procédure lors d'une perquisition et d'une saisie. Voir respectivement les articles 143-153 et 333-338. Ces processus et procédures préservent les droits des citoyens.<br><br>La procédure de perquisition et de saisie prévue par les lois nigérianes, y compris la loi sur la cybercriminalité, tient le plus grand compte des droits de l'homme fondamentaux et des garanties constitutionnelles. Par conséquent, à l'exception des cas impliquant des mineurs, aucune procédure formelle ne peut être supprimée. Le juge qui rend une ordonnance en vertu de l'article 45 doit s'assurer que toutes les procédures formelles ont été suivies, y compris l'existence de "motifs raisonnables de croire". Voir l'article 45(3)(c) de la loi sur la cybercriminalité.<br>Les lois nigérianes prévoient l'arrestation sans mandat. Toutefois, dans le cas de perquisitions et de saisies, un agent ne peut agir sans mandat, sauf dans des circonstances limitées, par exemple lorsqu'un mineur est impliqué. L'article 45 de la loi sur la cybercriminalité prévoit la délivrance d'un mandat par une autorité judiciaire lorsqu'une enquête porte sur des infractions spécifiques ou dans certaines circonstances.<br><br>En règle générale, au-delà de l'article 45, certaines garanties peuvent être mises en place lors d'une perquisition et d'une saisie : | Le Nigeria est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | - Droit d'être informé de l'infraction présumée.<br>- Droit d'obtenir une copie du mandat de perquisition.<br>- Droit de garder le silence.<br>- Présomption d'innocence.<br>- Droit d'être présent et d'avoir des témoins lors d'une fouille.<br>- Droit d'obtenir un inventaire de tous les objets saisis lors d'une perquisition.<br>- Droit d'une femme à ne pas être fouillée par un homme, etc. | |
| Macédoine du Nord | Conformément aux articles 181.2, 186.2, 189, 190.1, 190.3 et 191 du CPC, un tribunal rendra une ordonnance à la demande du procureur, qui devra contenir une explication/justification. L'ordonnance visera un support de données, un sous-flux ou un transfert de données précisément défini, en particulier lorsque le système concerné dessert plusieurs utilisateurs ou systèmes. L'ordre peut également prendre en compte des questions de protection des données et de transfert efficace des données. Les recherches ne portent que sur les parties d'un système qui sont pertinentes pour l'affaire pénale en question. | La Macédoine du Nord est en conformité avec l'article 19.5. |
| Norvège | Le code de procédure pénale contient une disposition exigeant la proportionnalité en cas de recours à des mesures coercitives. D'autres sections traitent du devoir de confidentialité et de la protection du droit de ne pas s'incriminer soi-même. La Convention européenne des droits de l'homme s'applique en Norvège et est appliquée par les tribunaux norvégiens. | La Norvège est en accord avec l'article 19.5. |
| Panama | Les pouvoirs conférés par la loi pour la recherche et la saisie de données informatiques stockées sont utilisés pour les infractions contre les systèmes informatiques ou les ordinateurs, ainsi que pour d'autres infractions prévues par la législation nationale.<br>Aucune garantie n'est expressément prévue pour ces mesures. Ce qu'il faut considérer, c'est que pour que les données obtenues lors des perquisitions ou des recherches étendues soient valables au stade de la procédure ou du procès, il faut que le droit à la défense soit respecté et que le procureur respecte les contrôles constitutionnels respectifs des garanties, devant le juge, qu'ils soient préalables ou ultérieurs. | Le Panama est conforme à l'art. 19.5 |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Aucune garantie n'est expressément prévue pour ces mesures. Ce qu'il faut considérer, c'est que la procédure pénale panaméenne établit une série de contrôles précisément pour assurer le respect des droits de l'homme et des droits et garanties individuels de chaque personne.<br><br>Pour la saisie des données, par exemple, le règlement prévoit un contrôle a posteriori par un juge des garanties. Dans ce cas, le procureur procède à la saisie des données stockées dans un système informatique et doit soumettre ses actions au juge dans un délai de dix jours. Le juge vérifiera 1. que la défense a été informée de la procédure, ce qui garantit le droit à la défense 2. L'existence d'une enquête criminelle qui justifie les mesures prises par le juge.<br><br>Procureur (procédure régulière). Si les données concernent la correspondance ou des informations privées, la procédure est différente. Dans le strict respect de l'inviolabilité de la correspondance, une telle mesure doit être justifiée. Devant un juge au préalable, sauf circonstances particulières établies par la loi, qui doivent être justifiées par la suite. | |
| Paraguay | Les dispositions relatives à la recherche et à la saisie de données s'appliquent à l'enquête sur tout délit. Les conditions et garanties à appliquer dans les dossiers sont que les mandats doivent décrire les appareils électroniques ou autres objets à saisir, et les conditions à prendre en compte sont que seuls les objets autorisés doivent être saisis.<br><br>En ce qui concerne l'extension et la saisie des données informatiques, seules les données correspondant à la période des événements peuvent être saisies, de même que les données des utilisateurs impliqués et les données des événements liés aux délits signalés.<br>Dans une autre réponse au questionnaire, le rapport cite une disposition importante de la constitution qui réaffirme les garanties constitutionnelles, à savoir l'article 36 sur le droit à l'inviolabilité du patrimoine documentaire et de la communication privée | Le Paraguay est en conformité avec l'art. 19.5 |
| Pérou | Les mesures de restriction des droits prévues à l'article 217 du code de procédure pénale s'appliquent aux crimes commis contre ou par l'intermédiaire d'ordinateurs et à d'autres crimes définis dans le droit national lorsque la preuve est trouvée dans un système informatique. | Le Pérou est en accord avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Les garanties se réfèrent à ce qui a été répondu dans l'ensemble du rapport et ne concernent pas spécifiquement les preuves numériques. | |
| Philippines | Un tribunal délivre des mandats de perquisition, de saisie et d'examen des données. L'intervention de ce tribunal "garantit l'équilibre entre le droit du gouvernement à mener des enquêtes criminelles et le droit des citoyens à la vie privée et à la protection contre les perquisitions abusives". | Les Philippines sont en conformité avec l'article 19.5. |
| Pologne | Les conditions et garanties prévues par le code de procédure pénale qui s'appliquent aux règles générales en matière de perquisition et de saisie sont également applicables au monde électronique. Ces dispositions garantissent la protection des droits de l'homme et des libertés. De nombreux articles du code de procédure pénale sont pertinents (voir les observations détaillées de la Pologne). Les protections générales comprennent le fait qu'un accusé est présumé innocent jusqu'à ce que sa culpabilité soit reconnue par un jugement définitif et qu'un accusé a le droit d'être défendu par un avocat et doit être informé de ce droit. Des protections plus spécifiques incluent l'exigence de la présence de la personne concernée lors d'une perquisition ou d'un substitut approprié. Entre autres exigences, les perquisitions ou saisies d'objets doivent être effectuées "avec modération et dans les limites nécessaires" pour atteindre l'objectif, dans le respect de la vie privée et de la dignité des personnes concernées. | La Pologne est en conformité avec l'article 19.5. |
| Portugal | En dehors des circonstances limitées décrites, les perquisitions et les saisies doivent être autorisées par un procureur ou un juge. Les mesures sont soumises aux restrictions prévues par la loi sur la cybercriminalité. Les perquisitions doivent être notifiées à la personne concernée ou à un substitut approprié. Si des données particulièrement privées sont saisies, elles doivent être soumises à un juge, qui examinera si elles sont nécessaires à l'affaire. Des protections spéciales s'appliquent aux données utilisées dans certaines professions, telles que la médecine ou le journalisme. Les ordres de perquisition et de saisie doivent être exécutés dans un délai de 30 jours et les données saisies doivent être restituées dès qu'elles deviennent inutiles en tant que preuves. | Le Portugal est en conformité avec l'article 19.5. |
| République de Moldavie | La Moldavie cite cinq lois (articles 11 à 15 du code de procédure pénale, relatifs à l'inviolabilité de la personne, du domicile, de la correspondance (y compris les conversations téléphoniques) et des biens ; procédures relatives aux perquisitions et aux saisies). Ces articles interdisent les mesures telles que | La Moldavie est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | les perquisitions et les saisies, sauf lorsqu'elles sont effectuées en vertu du code de procédure pénale. Le code de procédure pénale exige des mandats préalables à l'action, la ratification a posteriori par les tribunaux des mesures prises sans mandat, la saisie de biens uniquement en vertu d'une décision de justice et sur la base du procès-verbal de la procédure, ainsi que d'autres restrictions et exigences détaillées en matière de perquisitions et de saisies. | |
| Roumanie | Les perquisitions et saisies considérées comme "nécessaires" sont normalement autorisées par un tribunal sur la base d'une demande qui doit fournir de nombreux détails. Des copies sont faites pour garantir l'intégrité des preuves et des rapports détaillés ainsi qu'une documentation sur la perquisition sont exigés. La recherche est effectuée sans rendre publics de manière injustifiée des aspects de la vie privée de la personne visée. Les données recherchées qui sont de nature secrète sont protégées. | La Roumanie est en accord avec l'art. 19.5 |
| Saint-Marin | Saint-Marin a déclaré que les mesures étaient soumises aux conditions et garanties de son droit interne. Plus précisément, divers principes de son cadre juridique national (proportionnalité, caractère approprié) et les droits constitutionnels (respect de la vie privée) des individus sont applicables. Toutefois, il a indiqué que, lors de la mise en œuvre des saisies, des mots-clés devraient être utilisés pour rechercher des données pertinentes sur les dispositifs saisis. | Saint-Marin est en conformité avec l'art. 19.5. |
| Sénégal | Comme indiqué ci-dessus, selon les articles 90-4 à 90-6 et 90-8 du CPP, les perquisitions sont autorisées et supervisées par le procureur de la République ou par un juge d'instruction. Elles sont exécutées par le juge d'instruction ou par la police judiciaire sous le contrôle du procureur ou du juge d'instruction. Les perquisitions ne sont autorisées que si les données visées sont absolument nécessaires à l'enquête, dans le strict respect du principe de légalité des preuves. Les données doivent être utiles à la manifestation de la vérité. Le responsable du système doit être informé de la recherche effectuée et des données copiées, supprimées ou rendues inaccessibles.<br><br>L'utilisation d'informations d'identification légalement acquises et de procédés techniques, programmes, etc., pour restaurer des données effacées ou pour les attribuer n'est permise que si elle est nécessaire pour obtenir des preuves et doit être autorisée et supervisée par le procureur ou le juge d'instruction. | Le Sénégal est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Sous réserve des accords internationaux applicables, le juge peut recueillir des données stockées dans un système autre que le système initial situé dans un autre lieu sur le territoire sénégalais ou en dehors de celui-ci, à condition que le système ultérieur soit accessible à partir du système initial. Cette extension doit être nécessaire à la manifestation de la vérité ou il doit y avoir des risques de perte de preuves sans cette extension. L'extension ne doit concerner que les systèmes auxquels ont accès les personnes autorisées à utiliser le système initial. Le juge doit informer le responsable du système, sauf si son identité ou son adresse est introuvable.<br><br>Les articles 90-1 à 90-14 du CPC prévoient la copie, l'entretien et la préservation de l'intégrité des données saisies. Les personnes qui possèdent ou contrôlent des données peuvent être tenues d'en protéger l'intégrité.<br><br>Outre les protections des droits de l'homme prévues par la législation sénégalaise, la loi n° 2008-12 protège les données à caractère personnel. | |
| Serbie | Les conditions et garanties prévues par le CPC s'appliquent à tous les éléments de l'article 19. En outre, la loi sur la protection des données à caractère personnel, la loi sur les communications électroniques (dans la mesure où les données électroniques ont des implications personnelles) et d'autres lois et règlements connexes sont tous applicables. | La Serbie est en conformité avec l'article 19.5. |
| Sierra Leone | Les autorités ont indiqué que l'agent chargé de l'application de la loi doit s'adresser à un juge de la Haute Cour en indiquant les raisons de la demande d'un mandat de perquisition et de saisie et que le juge peut ou non faire droit à la demande. Cette disposition est prévue à l'article 10(1-4). Cette garantie a pour but d'assurer l'équité et de prévenir les abus de pouvoir.<br><br>En outre, l'article 10(8) prévoit des sanctions pour un agent chargé de l'application de la loi ou toute autre personne autorisée qui abuse intentionnellement, par imprudence ou par négligence, des pouvoirs qui lui sont conférés en vertu de l'article 10. Il peut s'agir d'une amende ou d'une peine d'emprisonnement. | La Sierra Leone est en conformité avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | La proportionnalité des mesures est reflétée, par exemple, dans la section 10(7). Plus précisément, un agent d'exécution ne doit saisir un système informatique que s'il n'est pas possible de sécuriser les données informatiques ou s'il est nécessaire de s'assurer que les données ne seront pas détruites, modifiées ou altérées, ou d'exercer une diligence raisonnable pendant que le système ou le support de stockage des données informatiques est conservé, conformément à la section 10 (7a-b).<br><br>En outre, l'agent d'exécution doit dresser une liste de ce qui a été saisi ou rendu inaccessible, avec la date et l'heure de la saisie, et remettre une copie de cette liste à l'occupant des lieux ou à la personne qui contrôle le système informatique. | |
| République slovaque | Les principes de proportionnalité, de nécessité et de respect des droits fondamentaux, tels que réglementés par la Constitution, la Cour européenne des droits de l'homme et la Charte de l'Union européenne, sont respectés en ce qui concerne les perquisitions et les saisies. Ces mesures sont établies par le code de procédure pénale et des mandats conformes aux exigences doivent être obtenus. | La République slovaque est en conformité avec l'art. 19.5. |
| Slovénie | Le CPP réglemente étroitement les perquisitions et les saisies et établit de nombreuses exigences, dont les suivantes. Les demandes de mandat doivent répondre à plusieurs normes précises. Les perquisitions sont parfois effectuées sur la base d'un consentement, auquel cas d'autres conditions doivent être remplies. Lorsque les perquisitions sont effectuées sur ordre, une copie de l'ordre doit être fournie à la personne intéressée avant la perquisition. Les enquêtes électroniques sur les données des avocats nécessitent une ordonnance du tribunal. La demande et l'ordonnance doivent identifier les éléments à rechercher et justifier la recherche, ainsi que d'autres détails importants. Les personnes appartenant à certaines catégories - le propriétaire d'un appareil, par exemple, ou son avocat - ont le droit d'être présentes. Les enquêtes doivent porter le moins possible atteinte aux droits des tiers, protéger la confidentialité des données et, d'une manière générale, ne pas causer de dommages disproportionnés. La recherche fait l'objet d'une documentation détaillée et les preuves peuvent être irrecevables si elles ont été obtenues de manière irrégulière. | La Slovénie est en conformité avec l'article 19.5. |
| Espagne | Les mesures peuvent être utilisées/appliquées dans toute enquête criminelle - crimes commis dans des systèmes informatiques ou crimes commis dans un environnement physique - à condition que les | L'Espagne est en conformité avec l'art. 19.5 |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | hypothèses justifiant une telle intervention conformément aux critères de proportionnalité soient remplies.<br><br>L'article 18 de la Constitution espagnole garantit la protection des droits fondamentaux à la vie privée, à l'inviolabilité du domicile, au secret des communications et à la protection des données à caractère personnel, de telle sorte que toute mesure d'enquête impliquant une ingérence dans l'un de ces droits requiert le consentement de la personne concernée ou une autorisation judiciaire expresse et motivée.<br><br>L'Espagne a été renvoyée aux exigences établies par la convention de Budapest pour sauvegarder les droits des personnes au cours des enquêtes. Parmi ces exigences figurent l'intervention obligatoire de l'autorité judiciaire, la résolution motivée qui évalue les principes de spécialité, de nécessité, d'adéquation, d'exceptionnalité et de proportionnalité, la délimitation du contenu et de la portée de la perquisition, l'autorisation séparée des perquisitions prolongées et la décision de l'autorité judiciaire sur les mesures nécessaires pour garantir l'authenticité et l'intégrité des données. En outre, ils ont mentionné que le chapitre IV du titre VIII du livre II de la loi espagnole de procédure pénale régit les dispositions générales applicables à toutes les mesures techniques d'enquête, telles que le contrôle permanent de l'enquête par une autorité judiciaire et les règles spécifiques d'utilisation des informations dans différentes procédures judiciaires. | |
| Sri Lanka | Les articles 20, 22 et 24 de la loi sur la criminalité informatique fixent les conditions à respecter lors des perquisitions et des saisies. Ils prévoient d'éviter, dans la mesure du possible, de perturber les activités, d'inventorier les objets saisis et éventuellement d'en fournir des copies, et de préserver la confidentialité de la procédure. | Le Sri Lanka est en conformité avec l'article 19.5. |
| Suède | Les exigences spécifiques relatives aux perquisitions et aux saisies sont décrites ci-dessus. Au-delà de ces exigences, les principes généraux des droits de l'homme s'appliquent aux mesures coercitives (y compris les perquisitions et les saisies). Ces principes comprennent la proportionnalité, qui est explicitement mentionnée dans la législation pertinente, la légalité, la finalité et la nécessité. La Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe est directement applicable en Suède. En général, les mesures coercitives peuvent être contestées en justice par la personne concernée. | La Suède est en conformité avec l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | L'autorisation et l'exécution de la surveillance secrète, y compris l'interception de données secrètes, sont régies par des lois et règlements spécifiques, notamment la loi sur l'interception de données secrètes. Les autorisations d'interception de données secrètes doivent normalement être ordonnées par un tribunal.<br><br>La Commission pour la sécurité et la protection de l'intégrité supervise l'utilisation de la surveillance secrète, y compris l'interception de données secrètes, par les forces de l'ordre. Ce contrôle vise en particulier à garantir que ces activités sont menées conformément aux lois et autres réglementations. Le contrôle est exercé par le biais d'inspections et d'autres enquêtes. La Commission peut faire des déclarations sur les faits qu'elle établit et exprimer son opinion sur la nécessité de modifier les pratiques ; en outre, elle "s'efforce de veiller à ce qu'il soit remédié à toute lacune dans les lois et autres règlements". À la demande d'une personne, la Commission doit déterminer si elle a fait l'objet d'une surveillance secrète et si l'utilisation de cette surveillance et les activités qui y sont liées étaient conformes aux lois et autres règlements. La Commission doit notifier à la personne que l'examen a été effectué. | |
| Suisse | En vertu du code pénal, certains éléments sont des conditions préalables à l'adoption de mesures coercitives dans le cadre de la procédure pénale. Ces mesures ne peuvent être prises que si elles sont autorisées par la loi et s'il existe des soupçons suffisants de délit. En outre, ces mesures doivent être nécessaires et raisonnables. Une personne lésée peut s'opposer aux décisions et aux actes de procédure de la police, du procureur et d'autres autorités, et les décisions peuvent faire l'objet d'un appel. Il existe également des garanties spécifiques, telles que la mise sous scellés des preuves et certaines interdictions de saisie. | La Suisse est en conformité avec l'article 19.5. |
| Tonga | Les garanties tongiennes découlent de la pratique des perquisitions et des saisies en général, ainsi que de pratiques spécifiques aux recherches de données. Tout d'abord, les mesures prévues à l'article 9 de la loi sur les délits informatiques ne sont autorisées qu'après délivrance d'un mandat fondé sur une déclaration sous serment d'un agent qui remplit de nombreux éléments statutaires. Des dispositions prévoient la protection des preuves saisies (y compris au profit du défendeur). Les garanties normales prévues par la loi sur la police des Tonga s'appliquent également aux recherches de données. | Les Tonga sont en conformité avec l'article 19.5.<br><br>Les autorités pourraient envisager d'étendre le champ d'application de l'ACC pour couvrir explicitement toutes les infractions dont les preuves se trouvent sur un système informatique. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | Deuxièmement, les pratiques tongiennes font appel à des experts médico-légaux à différents stades, y compris avant la perquisition.<br><br>Les pouvoirs spécifiques de la loi sur les délits informatiques (Computer Crimes Act) en matière de perquisition et de saisie ne s'appliquent qu'aux délits commis contre ou au moyen d'ordinateurs. Les pouvoirs plus généraux de perquisition et de saisie prévus par d'autres lois peuvent toutefois être utilisés dans le cadre d'une enquête sur n'importe quelle infraction.<br><br>Les dispositions relatives à la perquisition et à la saisie prévues par la loi sur les tribunaux de première instance et la loi sur la police des Tonga peuvent être appliquées de manière générale à n'importe quelle infraction, mais la formulation et les spécificités du mandat sont essentielles pour couvrir tous les aspects de la preuve, y compris la preuve numérique et physique. | |
| Tunisie | | |
| Türkiye | Les perquisitions et les saisies sont régies par des dispositions légales ou réglementaires. Le procureur est chargé d'empêcher les agents chargés des perquisitions d'outrepasser leurs fonctions et doit donner les ordres et les instructions nécessaires. Les procureurs doivent également obtenir des mandats judiciaires pour les perquisitions ou des ratifications des perquisitions exécutées. Un suspect peut faire appel de la décision d'un juge à tout moment, et cet appel est lui-même susceptible de recours. | Türkiye est en conformité avec l'article 19.5. |
| Ukraine | Les procédures pénales doivent être menées conformément à la procédure et aux principes clairement définis par la loi, en ce qui concerne les personnes impliquées dans les activités de procédure pénale, afin d'assurer l'efficacité des procédures pénales (prévenir et mettre fin aux actions illégales, assurer la détection et la consolidation des preuves, etc.)<br><br>L'accès temporaire aux objets et documents consiste à donner à une partie à une procédure pénale par une personne en possession de ces objets et documents la possibilité d'en prendre connaissance, d'en faire des copies et de les saisir (les saisir).<br><br>L'accès temporaire aux systèmes d'information électroniques ou à leurs éléments, aux terminaux mobiles des systèmes de communication s'effectue en faisant une copie des informations contenues | L'Ukraine est en accord avec l'art. 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
|---|---|---|
| | dans ces systèmes d'information électroniques ou leurs éléments, aux terminaux mobiles des systèmes de communication, sans les retirer. | |
| Royaume-Uni | Les autorités britanniques ont indiqué que l'ensemble de la législation britannique relative aux enquêtes sur les infractions pénales répondait aux normes internationales en matière de protection des personnes. Dans le cas de l'APCE, un mandat ne peut être demandé que s'il répond aux critères définis dans la loi et le code de pratique B, et la décision est prise par un tribunal plutôt que par la police.<br><br>Le code B de l'APCE stipule que le droit à la vie privée et le respect des biens personnels sont des principes fondamentaux de la loi de 1998 sur les droits de l'homme. Les pouvoirs d'entrée, de perquisition et de saisie doivent être pleinement justifiés avant d'être utilisés car ils peuvent interférer de manière significative avec la vie privée de l'occupant.<br><br>Les pouvoirs de perquisition et de saisie doivent être utilisés de manière équitable et responsable, en respectant les personnes qui occupent les lieux perquisitionnés ou qui sont responsables des biens saisis, et sans discrimination illégale.<br><br>En outre, en Écosse, seuls des examens ciblés et proportionnés des dispositifs numériques (pour extraire des données) devraient être effectués et uniquement lorsque cela est nécessaire pour poursuivre une ligne d'enquête raisonnable. L'examen des appareils numériques ne sera pas effectué de manière routinière, et avant d'ordonner un tel examen, les procureurs doivent être convaincus qu'il est strictement nécessaire. Lorsqu'un mandat est délivré en Écosse, il ne peut l'être que par un juge de paix ou un shérif. Ils doivent avoir l'expertise appropriée pour remplir ce rôle et doivent également agir d'une manière compatible avec la CEDH lorsqu'ils décident d'accorder ou non le mandat. | Le Royaume-Uni est en conformité avec l'article 19.5. |
| États-Unis | Les protections et garanties applicables comprennent les dispositions de la Constitution, en particulier celles relatives aux perquisitions et saisies et à l'auto-incrimination. Les mandats de perquisition ne sont délivrés que par un juge indépendant et les demandes de mandats doivent répondre à des normes élevées. Les règles fédérales de procédure pénale et certaines lois limitent la portée des mandats, par exemple en restreignant la période d'exécution d'un mandat. Les preuves obtenues en violation des protections et des procédures peuvent être irrecevables lors du procès. | Les États-Unis se conforment à l'article 19.5. |

| Parti | Mesures législatives et autres | L'évaluation |
| --- | --- | --- |
| | | |

# 9 CONCLUSIONS ET RECOMMANDATIONS

Comme indiqué au début de ce rapport, l'article 19 est un pouvoir procédural important en vertu de la Convention. Le partage d'informations et d'expériences sur les pratiques et les mesures législatives et autres de mise en œuvre de l'article 19 facilitera la poursuite des réformes dans les Parties actuelles et futures, le cas échéant. En outre, la question de l'extension des perquisitions aux territoires d'autres Parties, qui est liée au traitement national de l'article 19.2, continue d'intéresser le T-CY, puisque plusieurs Parties ont mis en place des dispositions nationales qui permettent aux autorités de mener ce type de mesures procédurales. Le T-CY a donc procédé à une évaluation détaillée de la mise en œuvre de l'article 19 dans le droit national des Parties à la Convention.

L'évaluation a été basée sur les réponses de [74] Parties. Des discussions ont eu lieu lors de la 28e plénière (juin 2023), de la 29e plénière (décembre 2023), de la 30e plénière (18-20 juin 2024), et de la 31e plénière (11-12 décembre 2024) qui ont également adopté le présent rapport. Conformément aux obligations découlant du règlement intérieur du T-CY, toutes les Parties répondantes ont soumis des réponses riches et détaillées au questionnaire. La plupart d'entre elles ont également fourni rapidement toutes les clarifications nécessaires. Toutefois, le processus d'évaluation et le respect des délais fixés par le T-CY ont rencontré certaines difficultés en raison des retards dans la soumission des réponses initiales et des clarifications ultérieures de certaines Parties.

Le T-CY :

- considère que l'évaluation de la mise en œuvre de l'article 19 de la Convention renforcera l'efficacité de ce traité ;
- se félicite des réponses au questionnaire du T-CY reçues de 74 Parties et des clarifications supplémentaires fournies par la plupart de ces Parties ;
- regrette que seules des réponses partielles aient été reçues de la Tunisie et que, par conséquent, la Tunisie n'ait pas pu être évaluée
- invite toutes les parties à participer activement et en temps voulu aux évaluations futures, dans l'intérêt de l'efficacité de la Convention et du fonctionnement du T-CY ;

## 9.1 Conclusions

### 9.1.1 Conclusions générales

Concl 1 **Spécificité du pouvoir procédural dans la législation nationale** - Certaines des Parties qui ont mis en œuvre l'article 19 s'appuient largement sur des pouvoirs généraux (tels que les pouvoirs traditionnels de mandat de perquisition, par exemple, pour fouiller une maison ou saisir un objet tangible) pour satisfaire à tout ou partie des exigences de l'article 19. D'autres Parties utilisent des pouvoirs spécifiques qui peuvent viser des systèmes ou des données informatiques. Le T-CY encourage vivement à ce que les pouvoirs, qu'ils soient de nature générale ou spécifique, soient suffisamment détaillés pour garantir que les preuves électroniques puissent être collectées et utilisées efficacement dans le cadre des enquêtes et des poursuites menées par les services répressifs. Les lois qui s'appuient uniquement sur des dispositions relatives à la perquisition et à la saisie d'"objets" tangibles ne couvrent pas toujours tous les scénarios.[68] L'article 19 est plus efficace lorsque ces principes

[68] Il convient également de noter que des règles différentes peuvent s'appliquer si les pouvoirs de perquisition et de saisie des données informatiques stockées sont exercés sur le lieu où le système

généraux sont complétés par un texte législatif ou d'autres mesures spécifiques au monde numérique. Une spécificité appropriée peut également être importante pour la mise en œuvre adéquate des conditions et garanties de l'article 15 (voir la recommandation correspondante 1).

Concl 2 **Jurisprudence et pratique en matière d'application de la loi** - De nombreuses Parties ont indiqué que les pouvoirs procéduraux de l'article 19 ont été appliqués dans le cadre d'enquêtes ou de procédures pénales en tenant compte des principes généraux du droit de la preuve, tels que le "principe de la liberté de la preuve" mentionné par certaines Parties dans leurs réponses au questionnaire. D'autres ont indiqué que ces principes ont été façonnés par la jurisprudence ou complétés par la pratique procédurale coutumière nationale et les manuels d'application de la loi pour informer la pratique d'application de la loi.

Cependant, l'exécution des pouvoirs procéduraux de perquisition et de saisie de données informatiques stockées est devenue plus complexe en raison des nouveaux défis technologiques (tels que la croissance du stockage des données, le cryptage, l'hébergement dans le nuage, etc.) La perquisition et la saisie de biens virtuels destinés à être utilisés comme éléments de preuve ont été mentionnées par certaines Parties comme l'un de ces défis technologiques.

Tous ces défis font qu'il est de plus en plus difficile de s'appuyer sur l'interprétation jurisprudentielle, les lignes directrices ou les pratiques acceptées pour combler les lacunes perçues dans les cadres législatifs ou les autres formes de droit interne établies à l'origine pour les preuves matérielles. Il est donc de plus en plus conseillé aux pays d'adopter des mesures législatives pour mettre en œuvre l'article 19 de la Convention de Budapest au lieu de laisser l'application à la seule jurisprudence, aux meilleures pratiques ou aux manuels. Cela pourrait également améliorer le respect de l'article 15 et garantir la sécurité juridique tant pour les services répressifs que pour les personnes accusées d'infractions (voir la recommandation correspondante n° 1).

Concl 3 **Définitions fondamentales de la Convention de Budapest** - Certaines Parties n'ont pas transposé dans leur droit interne la définition des données informatiques figurant à l'article 1er de la Convention. Bien que la Convention de Budapest n'oblige pas les Parties à copier dans leur droit interne ad verbatim les quatre concepts de l'article 1 de la Convention de Budapest[69] , il est essentiel que les mesures statutaires (telles que la législation interne) couvrent ces concepts afin de garantir en toute confiance que les pouvoirs procéduraux peuvent effectivement saisir des preuves électroniques, c'est-à-dire des données informatiques (voir la recommandation correspondante 2).

Concl 4 **Courriels stockés par le fournisseur de services et non ouverts par le destinataire** - Certaines Parties considèrent un message électronique non ouvert qui attend dans la boîte aux lettres d'un fournisseur de services jusqu'à ce que le destinataire le télécharge sur son système informatique comme une donnée informatique stockée à laquelle l'article 19 s'applique. D'autres Parties le considèrent comme des données en cours de transmission dont le contenu ne peut être obtenu qu'en appliquant le pouvoir d'interception. D'autres encore n'ont rien précisé. Ces questions peuvent être traitées dans des documents d'orientation adoptés au niveau national, mais toutes les Parties n'ont pas adopté de tels guides (voir la recommandation correspondante n° 3).

---

informatique ou les données sont trouvés, dans un autre lieu (par exemple dans des laboratoires d'informatique légale) après la saisie initiale du système informatique ou à partir d'un autre lieu dans le cas d'une extension des perquisitions.

[69] Voir le paragraphe 22 du rapport explicatif de la Convention de Budapest.

Concl 5 **Valeur de la formation et de l'orientation continues** - Un certain nombre de Parties ont indiqué que leurs autorités compétentes ne font que rarement ou jamais usage de certains pouvoirs de perquisition et de saisie (même dans les cas où ces mesures sont prévues par le droit interne). Le manque d'expérience pratique ou l'absence de formation permettant d'acquérir les connaissances nécessaires peuvent jouer un rôle à cet égard. Une formation et des conseils durables semblent être un élément important pour acquérir les compétences nécessaires et garantir que les mesures sont utilisées de manière appropriée et dans le respect des conditions et des garanties (voir la recommandation correspondante n° 4).

Concl 6 **Valeur du renforcement des capacités** - Un nombre considérable de Parties ont adopté des dispositions juridiques conformes à l'article 19 à la suite du soutien apporté par les projets de renforcement des capacités du Bureau du Programme sur la cybercriminalité du Conseil de l'Europe (C-PROC) et, en outre, ont reçu une formation et d'autres formes d'assistance pour appliquer ces dispositions. Ce soutien sera également disponible dans le cadre du suivi des conclusions et recommandations du présent rapport d'évaluation (voir la recommandation correspondante n° 18).

### 9.1.2 Conclusion sur la mise en œuvre de l'art. 19.2

Concl 7 **Extension d'une perquisition ou d'un accès similaire sur le territoire d'une Partie à un système informatique ou à une partie de celui-ci sur le territoire de cette Partie** - En règle générale, les Parties sont en mesure d'étendre leur perquisition ou leur accès similaire à un autre système informatique ou à une partie de celui-ci sur leur territoire, comme l'exige l'article 19.2.[70] Bien que certains pays ne prévoient pas expressément une telle situation dans leur législation, ils l'ont appliquée au cours d'enquêtes sans rencontrer de problèmes ou l'ont acceptée par le biais de décisions jurisprudentielles (voir la recommandation correspondante n° 5).

### 9.1.3 Conclusions sur la mise en œuvre de l'art. 19.3

Concl 8 **Copie de données informatiques stockées lors d'une perquisition et d'une saisie** - De nombreuses Parties ont indiqué qu'elles avaient le pouvoir de copier des données informatiques. Les Parties ont cependant des interprétations différentes de l'exercice de ce pouvoir. Certaines Parties n'utilisent ce pouvoir qu'après la saisie d'un système informatique afin de préserver l'intégrité des données. Bien qu'il s'agisse d'un aspect important, le pouvoir de copier devrait également couvrir les situations de copie sur place, car dans certains cas, la copie peut être préférable à la saisie. Il peut s'agir, par exemple, de situations où il est nécessaire de minimiser les dommages causés à une personne lorsque les droits, les responsabilités et les intérêts légitimes de tiers peuvent être en jeu. La copie sur place peut également contribuer à réduire les risques d'effacement involontaire ou intentionnel de preuves électroniques qui peuvent survenir avant qu'un système informatique saisi ne puisse être analysé par la police scientifique. La copie sélective au cours d'une perquisition peut également réduire le volume de données que les spécialistes de la police scientifique doivent analyser (voir la recommandation correspondante n° 6).

Concl 9 **Maintien de l'intégrité des données informatiques stockées pendant et après la saisie** - La plupart des Parties ont eu des difficultés à expliquer la source de leur pouvoir pour maintenir l'intégrité des données. Cette exigence pourrait peut-être être abordée dans le droit dérivé et les documents d'orientation (voir la recommandation correspondante n° 7).

---

[70] Par exemple, les forces de l'ordre d'une partie trouvent un ordinateur lors d'une perquisition et accèdent à un compte de messagerie basé sur un navigateur qui contient des courriels stockés à distance sur le serveur du service de messagerie qui est également situé sur le territoire de cette partie.

Concl 10 **Retirer ou rendre inaccessibles les données informatiques stockées** - La plupart des Parties n'avaient pas clairement le pouvoir de retirer les données d'un système perquisitionné ou de les rendre inaccessibles (sous réserve des garanties en matière de droits humains). Cette mesure ne semble pas non plus être utilisée très souvent dans la pratique.[71] Ces pouvoirs concernent les situations où les autorités ont accès aux données[72] et où les circonstances de l'affaire peuvent exiger que ces autorités suppriment immédiatement les données ou les rendent inaccessibles afin d'empêcher la poursuite de l'utilisation criminelle des données ou la poursuite de la victimisation des victimes. Par exemple, ces situations peuvent impliquer un danger ou un préjudice social, comme les logiciels malveillants. En outre, il est de plus en plus nécessaire de supprimer les contenus illicites (par exemple, les documents relatifs à l'exploitation et aux abus sexuels concernant des enfants ou les images intimes diffusées de manière non consensuelle)[73] (voir la recommandation correspondante n° 8)

### 9.1.4 Conclusion sur la mise en œuvre de l'art. 19.4

Concl 11 **Contraindre l'assistance d'un tiers pour accéder à des systèmes informatiques ou à des données informatiques stockées** - Les Parties ont donné un large éventail de réponses concernant leur capacité à contraindre toute personne ayant connaissance du fonctionnement d'un système informatique, ou des mesures appliquées pour protéger ses données, à fournir, dans la mesure du raisonnable, les informations nécessaires pour mener à bien les actions prévues à l'article 19.4. Le pouvoir de contraindre à l'assistance peut être crucial pour une recherche précise et complète de preuves. Pourtant, certaines Parties ne semblent pas avoir pleinement mis en œuvre cet aspect de l'article 19.[74] Souvent, un pays ne pouvait contraindre qu'une ou deux catégories de personnes ; les lois pouvaient supposer que les perquisitions ne seraient toujours effectuées que dans les bureaux des entreprises, de sorte que l'assistance de personnes telles que des amis ou des colocataires ne pouvait pas être contrainte ; souvent, les pays essayaient d'appliquer une loi plus ancienne à cette mesure clairement numérique. [75]

Comme l'indique le rapport explicatif de la Convention, ce pouvoir ne profite pas uniquement aux autorités chargées de l'enquête. Sans cette coopération, les autorités d'enquête pourraient rester dans les locaux perquisitionnés et empêcher l'accès au système informatique pendant de longues périodes lors de la perquisition. En l'absence de ce pouvoir, les droits et obligations des tiers, y compris des fournisseurs de services et de leurs clients, pourraient être affectés de manière

---

[71] Ce pouvoir ne couvre que les situations où les autorités accèdent aux données. Il ne couvre pas le fait de supprimer des données en ligne ou de les rendre inaccessibles par le biais d'une notification et d'un retrait ou par d'autres moyens visant à rendre un site web inaccessible en ordonnant à des tiers (par exemple des fournisseurs de services) d'exécuter la mesure.

[72] Les données peuvent être stockées sur un système informatique, sur un support de stockage de données informatiques ou être accessibles à distance depuis le système informatique faisant l'objet de la recherche (par exemple, des données hébergées dans le nuage et accessibles depuis l'appareil saisi).

[73] L'absence de mise en œuvre de l'article 19.3.d de la Convention de Budapest dans le droit national pourrait conduire à une situation où les autorités restituent au contrevenant un système informatique perquisitionné qui pourrait encore contenir un contenu illégal.

[74] Certaines Parties excluent normalement les cibles ou les défendeurs de l'obligation de prêter leur concours à une perquisition. Cette exception à la règle "toute personne" de l'article 19/4 est autorisée parce que l'article 19 est soumis aux garanties des droits de l'homme, y compris les droits fondamentaux des défendeurs.

[75] droit contre l'auto-incrimination s'applique dans certaines Parties, tandis que d'autres considèrent que l'exécution d'une telle mesure n'est pas soumise à ce droit.

négative. Les limites imposées aux tiers qui peuvent être contraints de prêter leur concours aux perquisitions informatiques peuvent conduire les Parties à recourir à des mesures plus intrusives telles que la saisie de l'ensemble du système informatique ou l'interception des données de contenu si les Parties ne peuvent pas contraindre une personne ayant connaissance d'un système informatique à fournir les informations nécessaires.

Une mise en œuvre raisonnable de ce pouvoir peut donc aider les autorités à mieux intégrer le principe de proportionnalité. Par exemple, fournir des informations nécessaires pour permettre l'exécution des mesures peut aider les autorités à obtenir les données nécessaires par la copie, qui est une mesure moins intrusive que la saisie de l'ensemble du système informatique ou l'interception des données relatives au contenu. La pleine mise en œuvre de l'article 19.4 constitue donc une garantie importante, à condition qu'elle soit appliquée conformément au principe de proportionnalité (voir les recommandations correspondantes 9 et 10).

### 9.1.5 Conclusions sur la mise en œuvre de l'art. 19.5

Concl 12 **Étendue des pouvoirs (valeur de la collecte de preuves électroniques pour toutes les infractions)** - Quelques Parties disposent de pouvoirs de perquisition et de saisie de données informatiques en vertu d'une loi limitée ou uniquement dans les affaires impliquant des infractions informatiques. D'autres pays s'appuient sur une combinaison de lois. Parfois, l'interaction complexe de ces lois semble signifier que les pouvoirs de perquisition et de saisie des données informatiques stockées ne s'appliquent qu'à certaines catégories d'infractions pénales. À l'heure actuelle, dans certains pays, il est possible de contourner ces lacunes dans les pouvoirs de perquisition et de saisie. Par exemple, les autorités peuvent utiliser ces pouvoirs principalement pour l'intrusion informatique, la fraude électronique et les cas étroitement liés. Mais la tendance irréversible est que les données informatiques seront pertinentes dans tous les types d'affaires, y compris les crimes hors ligne qui peuvent impliquer des preuves électroniques (voir la recommandation correspondante 11).

Concl 13 **Garanties et conditions applicables à l'article 19** - Toutes les Parties ont répondu que l'établissement, la mise en œuvre et l'application des pouvoirs en vertu de l'article 19 sont soumis aux conditions et garanties prévues par leur droit national. La Convention s'appliquant à des Parties ayant des systèmes juridiques et des cultures très différents, il n'est pas surprenant que les conditions et garanties mentionnées diffèrent d'une Partie à l'autre. En outre, les Parties ont adopté des approches différentes pour couvrir les garanties dans leurs réponses au questionnaire : certaines ont répondu par des discussions générales sur les textes nationaux fondamentaux, tandis que d'autres ont limité leurs réponses aux droits spécifiques des défendeurs au cours des enquêtes et du procès. Des travaux supplémentaires visant à identifier la manière dont les Parties mettent en œuvre certains éléments de l'article 15 de la Convention (tels que, par exemple, le droit de ne pas s'auto-incriminer, la question des privilèges et immunités, etc.) pourraient présenter un intérêt pour les Parties à la Convention (voir la recommandation correspondante 12).

Concl 14 **Demandes et contenu d'une ordonnance de perquisition et de saisie** - Les Parties ont fourni diverses réponses concernant le contenu d'une ordonnance autorisant une perquisition. On peut déduire des réponses de certaines Parties qui s'appuient sur la mise en œuvre de l'article 19 par le biais de pouvoirs généraux, que l'autorisation générique d'une perquisition à domicile inclut la perquisition d'un système informatique ou de données informatiques, même lorsqu'une perquisition électronique n'est pas mentionnée. D'autres Parties exigent une approche plus

spécifique, c'est-à-dire une ordonnance spécifiant qu'un système informatique ou des données informatiques identifiés au cours de la perquisition peuvent être perquisitionnés. Cette dernière approche peut constituer un argument plus solide pour démontrer qu'un pouvoir procédural interne spécifique peut faciliter les conditions et les garanties requises par l'article 15, y compris le principe de proportionnalité (voir la recommandation correspondante n° 12).

Concl 15 **Application des privilèges et immunités aux données informatiques perquisitionnées et saisies** - Certaines Parties ont souligné que les données informatiques obtenues peuvent être protégées par certains privilèges et immunités et ne pas servir de preuves au procès (communication avocat-client, secret médical, protection des sources journalistiques, etc.). Ceci est conforme aux exigences du cadre de la Convention[76] (voir la recommandation correspondante 12).

Concl 16 **Impact des pouvoirs procéduraux de perquisition et de saisie sur les tiers** - Dans la mesure où cela est compatible avec l'intérêt public, la Convention exige que ses Parties examinent l'impact des pouvoirs et des procédures sur les droits, les responsabilités et les intérêts légitimes des tiers.[77] Plusieurs Parties ont souligné que les mesures de perquisition et de saisie ne sont applicables que lorsque le préjudice causé aux droits et intérêts concernés n'est pas supérieur à l'avantage que leur utilisation procure à l'intérêt public et aux tiers (voir la recommandation correspondante n° 12).

### 9.1.6 Autres conclusions pertinentes

Les conclusions suivantes portent sur des questions qui se posent fréquemment en rapport avec les perquisitions et les saisies effectuées en vertu de l'article 19, mais qui ne sont pas abordées dans cet article. Les parties ayant fourni de nombreuses informations sur ces questions connexes, il a semblé important de les compiler et de les mettre à disposition :

Concl 17 **Procédure de perquisition et de saisie en cas d'urgence** - Les Parties ont échangé des informations sur la manière dont elles traitent les situations d'urgence ou d'autres situations urgentes dans lesquelles une perquisition ou une saisie peut s'avérer nécessaire. Certaines Parties n'ont pas d'avis sur les situations justifiant une fouille "d'urgence", tandis que d'autres définissent "l'urgence" au sens large, au-delà des urgences physiques. Pour d'autres, le risque de destruction de preuves justifierait une fouille d'urgence. En bref, certaines Parties n'avaient pas de mécanisme spécial pour réagir rapidement, tandis que d'autres pouvaient procéder à des fouilles d'urgence dans un large éventail de circonstances (voir la recommandation correspondante n° 13).

Concl 18 **Utilisation de références acquises légalement** - De nombreuses Parties ont habilité leurs autorités, en vertu du droit national, à utiliser des références acquises légalement dans le cadre d'une recherche (par exemple, en utilisant les données de connexion à un système informatique). Toutefois, les réponses de certaines autres Parties indiquent que l'utilisation d'identifiants acquis légalement n'est pas réglementée. Certaines Parties prévoient également la possibilité pour les autorités chargées de l'application de la loi de demander une ordonnance judiciaire pour contraindre ou aider une personne à fournir ces informations d'identification aux autorités chargées de l'application de la loi à l'appui d'une perquisition (voir la recommandation correspondante n° 10).

---

[76] Voir le paragraphe 147 de la RE de la Convention de Budapest.

[77] Voir l'art. 15.3. de la Convention de Budapest.

Concl 19 **Accès clandestin à distance à des systèmes informatiques par le biais d'activités licites d'exploitation informatique** - L'évaluation a montré que les Parties ont des interprétations différentes de la mesure de la perquisition clandestine à distance d'un système informatique. Un groupe de Parties a adopté des pouvoirs spécifiques permettant l'utilisation de pratiques d'exploitation informatique (telles que l'utilisation de logiciels spécialisés) pour perquisitionner légalement un système informatique à distance. D'autres Parties mettent en œuvre la mesure par le biais de pouvoirs généraux (surveillance des personnes, enquêtes sous couverture) ou d'autres mesures qui ressemblent à la mise en œuvre de l'article 21 de la Convention. Certaines Parties ne prévoient pas une telle mesure dans leur droit national (voir la recommandation correspondante 15).

Concl 20 **Extension d'une perquisition à partir du territoire d'une partie à des données informatiques dont on sait qu'elles se trouvent en dehors du territoire de cette partie** - En ce qui concerne l'extension des perquisitions à des données dont on sait ou dont on peut raisonnablement penser qu'elles se trouvent en dehors du territoire d'un État, il existe d'importantes différences d'approche. La Convention ne traite pas de ces extensions. Cependant, en raison des développements technologiques et de la nature de plus en plus transfrontalière du stockage des données, le stockage des informations et des données informatiques est souvent extérieur aux dispositifs trouvés lors des perquisitions et davantage lié aux nouvelles formes de services d'hébergement en ligne (cloud) avec des réseaux multinationaux. Comme l'a souligné le groupe de travail sur les enquêtes sous couverture et l'extension des perquisitions dans son rapport[78] , en l'absence de normes internationales, les États semblent rechercher de plus en plus des options unilatérales et étendre les perquisitions à des systèmes informatiques situés dans d'autres juridictions (comme l'ont déjà conclu les groupes de travail T-CY Transborder et Cloud Evidence) (voir les recommandations correspondantes 14 et 15).[79]

Concl 21 **Extension d'une perquisition à des données informatiques dont la localisation est inconnue** - De même, les Parties ont adopté des positions diverses sur la question de savoir si leur droit national leur permet d'étendre une perquisition à distance de leur propre territoire à une localisation inconnue ou dont on pense ou soupçonne qu'elle se trouve très probablement en dehors du territoire. Les Parties ont parfois indiqué que cela pouvait se faire dans la pratique mais qu'il n'y avait pas de base juridique claire. Certaines ont indiqué que les recherches pouvaient être étendues à un lieu inconnu si l'affaire était suffisamment urgente ou importante. Les réponses d'autres Parties n'ont pas abordé la complexité du problème, par exemple, en l'absence de norme juridique explicite ou de jurisprudence uniforme pour guider les actions des forces de l'ordre. Ou, parce que cette question peut être controversée, certaines Parties ont semblé hésiter à exprimer leur point de vue.

Comme l'ont reconnu les précédents rapports des groupes de travail T-CY, l'extension des perquisitions transfrontalières est susceptible d'avoir une série de conséquences ou d'implications politiques, juridiques et autres (y compris les droits des personnes et des tiers sur le territoire perquisitionné à distance) pour les enquêtes et les

---

[78] Un rapport contenant des projets d'options et des recommandations pour une action ultérieure du T-CY sur : 1. Enquêtes sous couverture au moyen d'un système informatique ; 2. Extension des perquisitions. Le groupe de travail a présenté le rapport lors de la 27e session plénière du T-CY (29-30 novembre 2022).

[79] Voir Comité de la Convention sur la cybercriminalité (T-CY), sous-groupe ad hoc sur l'accès et la compétence transfrontaliers : Accès transfrontière aux données et compétence - Options pour l'action future du T-CY. Adopté par la 12e plénière du T-CY (2-3 décembre 2014), p. 8. Voir également le Comité de la Convention sur la cybercriminalité (T-CY), T-CY Cloud Evidence Group : Accès de la justice pénale aux preuves électroniques dans le nuage : Recommandations pour examen par le T-CY (16 septembre 2016)

poursuites pénales[80] . L'augmentation du nombre de données informatiques stockées à distance et détenues en dehors du territoire d'une partie signifie que les lois sur les preuves relatives à ces données peuvent empêcher ou entraver leur utilisation dans le cadre de poursuites pénales lorsqu'elles n'ont pas été obtenues en vertu de cadres statutaires spécifiques (tels que les lois sur les preuves étrangères) (voir les recommandations correspondantes 14 et 15).

Concl 22 **Intérêt de développer une compréhension mutuelle internationale sur l'extension des perquisitions** - Bien que l'extension des perquisitions à un territoire différent soit une mesure qui dépasse le cadre de la présente évaluation, cet aspect intéresse le T-CY depuis de nombreuses années.[81] Les autorités compétentes peuvent ne pas être conscientes des incidences internationales et des questions soulevées par les perquisitions et les saisies effectuées en dehors de leur territoire. Elles peuvent même s'exposer à des risques juridiques vis-à-vis du pays ciblé. L'adoption de positions similaires ou compatibles entre différents pays pourrait être importante pour établir une pratique internationalement acceptée et améliorer la coopération internationale entre les Parties à la Convention. En même temps, des positions similaires ou compatibles pourraient protéger les intérêts des Parties et les intérêts des personnes se trouvant sur leur territoire contre un accès indu de la part d'autres États (voir les recommandations correspondantes 14 et 15).

[80] "La coopération internationale en matière pénale repose sur un certain nombre de principes, dont celui de la double incrimination ou la possibilité de refuser la coopération si elle est contraire à l'ordre public de l'État sollicité. L'accès transfrontalier peut être utilisé pour contourner ces principes". Accès transfrontalier et compétence : Quelles sont les options ? Rapport du groupe transfrontalier adopté par le T-CY le 6 décembre 2012, p. 12.

[81] Voir les travaux du T-CY sur l'accès transfrontalier aux données, sur les preuves en ligne (cloud), ou sur les enquêtes d'infiltration et l'extension des perquisitions. https://www.coe.int/en/web/cybercrime/tcy

## 9.2 Résumé de la mise en œuvre par les parties[82]

| Parti[83] | Article 19.1 | Article 19.2 | Article 19.3 | Article 19.4 | Article 19.5 |
|---|---|---|---|---|---|
| 1. Albanie | SP | SP | SP | SP | P (art. 14) |
| 2. Andorre | GP | GP | GP | GP | P (art. 14) |
| 3. Argentine | GP/SP | GP | GP/SP | GP | Y |
| 4. Arménie | SP | GP | SP | GP | Y |
| 5. Australie | GP/SP | GP/SP | SP | SP | Y |
| 6. Autriche | GP/SP | SP | GP/SP | GP/SP | Y |
| 7. Azerbaïdjan | GP | GP | GP | GP | Y |
| 8. Belgique | SP | SP | SP | SP | Y |
| 9. Bénin | GP/SP | SP | SP | GP/SP | Y |
| 10. Bosnie et Herzégovine | GP/SP | GP | GP/SP | GP | Y |
| 11. Brésil | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 12. Bulgarie | SP | SP | SP | GP | Y |
| 13. Cabo Verde | SP | SP | SP | SP | Y |
| 14. Cameroun [84] | GP/SP | N | GP/SP | | Y |
| 15. Canada | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 16. Chili | GP | GP | GP | GP | Y |
| 17. Colombie | GP | GP | GP | GP | Y |
| 18. Costa Rica | GP | GP | GP | GP | Y |
| 19. Croatie | SP | SP | SP | SP | Y |
| 20. Chypre | GP/SP | GP/SP | GP | N | Y |
| 21. République tchèque | GP | GP | GP | GP | Y |
| 22. Danemark | GP | GP | GP | GP | Y |
| 23. République dominicaine | GP/SP | GP | SP | SP | Y |
| 24. Estonie | GP | GP | GP | GP | Y |
| 25. Fidji | SP | SP | SP | SP | Y |
| 26. Finlande | SP | SP | GP/SP | SP | Y |
| 27. France | SP | SP | SP | SP | Y |
| 28. Géorgie | GP/SP | GP | GP/SP | SP | Y |
| 29. Allemagne | GP/SP | SP | GP | GP | Y |
| 30. Ghana | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 31. Grèce | GP/SP | GP/SP | GP/SP | N | Y |
| 32. Grenade | SP | GP | SP | SP | Y |
| 33. Hongrie | SP | SP | SP | GP/SP | Y |
| 34. Islande | GP | GP | GP/SP | SP | Y |
| 35. Israël | SP | SP | SP | GP | P (art. 14) |
| 36. Italie | GP/SP | GP | GP | GP | Y |

[82] Le tableau de synthèse de la mise en œuvre indique si les paragraphes 19.1 à 19.4 sont mis en œuvre par le biais des pouvoirs généraux ou spécifiques et si les parties sont en conformité avec l'article 19.5. Il est conseillé aux Parties de se référer aux tableaux d'évaluation pour plus de détails sur la mise en œuvre des paragraphes pertinents de l'article 19 dans chaque Partie. Des clarifications de la part de certaines parties sont attendues et le tableau de la section 9.2. pourrait être mis à jour avant la plénière T-CY si ces clarifications sont fournies.

[83] (GP = pouvoirs généraux
SP = pouvoirs spécifiques
Y = en ligne
P = Partiellement en ligne
N = Non mis en œuvre)

[84] Des clarifications sont en cours.

| Parti[83] | Article 19.1 | Article 19.2 | Article 19.3 | Article 19.4 | Article 19.5 |
|---|---|---|---|---|---|
| 37. Japon | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 38. Kiribati [85] | GP/SP | SP | | | Y |
| 39. Lettonie | GP/SP | SP | GP/SP | SP | P (art. 14) |
| 40. Liechtenstein | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 41. Lituanie | GP | GP | GP | GP | Y |
| 42. Luxembourg | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 43. Malte | GP/SP | GP | GP/SP | GP | Y |
| 44. Maurice | SP | SP | SP | SP | Y |
| 45. Monaco | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 46. Monténégro | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 47. Maroc | GP | GP | GP | GP | Y |
| 48. Pays-Bas | SP | SP | GP/SP | SP | Y |
| 49. Nigeria [86] | GP/SP | GP/SP | | GP/SP | Y |
| 50. Macédoine du Nord | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 51. Norvège | GP | GP | GP | SP | Y |
| 52. Panama | SP | SP | SP | GP | Y |
| 53. Paraguay | GP | GP | GP | GP | Y |
| 54. Pérou | GP | GP | GP | GP | Y |
| 55. Philippines | SP | SP | SP | SP | Y |
| 56. Pologne | GP/SP | GP/SP | GP/SP | GP | Y |
| 57. Portugal | SP | SP | SP | SP | Y |
| 58. République de Moldavie | GP | GP | GP/SP | GP | Y |
| 59. Roumanie | SP | SP | GP/SP | N | Y |
| 60. Saint-Marin | GP | GP | GP | GP | Y |
| 61. Sénégal | SP | SP | SP | SP | Y |
| 62. Serbie | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 63. Sierra Leone | SP | SP | SP | SP | Y |
| 64. République slovaque | GP | SP | SP | SP | Y |
| 65. Slovénie | SP | SP | GP/SP | SP | Y |
| 66. Espagne | SP | SP | SP | SP | Y |
| 67. Sri Lanka | GP/SP | GP/SP | GP/SP | SP | Y |
| 68. Suède | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 69. Suisse | GP/SP | GP/SP | GP/SP | GP | Y |
| 70. Tonga | GP/SP | GP/SP | GP/SP | SP | Y |
| 71. Tunisie [87] | | | | | |
| 72. Türkiye | SP | SP | SP | GP | Y |
| 73. Ukraine | GP/SP | GP | GP/SP | GP | Y |
| 74. Royaume-Uni | GP/SP | GP/SP | GP/SP | GP/SP | Y |
| 75. États-Unis d'Amérique | GP/SP | GP/SP | GP/SP | GP/SP | Y |

[85] Des clarifications sont en cours.

[86] Des clarifications sont en cours.

[87] Réponse partielle reçue. En conséquence, la Tunisie n'a pas pu être évaluée.

## 9.3 Recommandations

Les recommandations suivantes portent sur les mesures à prendre par les Parties au niveau national et/ou dans le cadre du programme T-CY et des programmes de renforcement des capacités :

### 9.3.1 Recommandations relevant principalement de la responsabilité des autorités nationales

| | |
|---|---|
| Rec. 1 | Les Parties devraient veiller à ce que les pouvoirs de perquisition et de saisie soient suffisamment détaillés et spécifiques pour répondre aux exigences de l'article 19 de la Convention. Dans la mesure où les éléments de l'article 19 ne peuvent pas être satisfaits en utilisant des pouvoirs de procédure généraux ou "traditionnels" (tels que ceux qui se rapportent aux perquisitions ou à la saisie d'objets tangibles), les Parties devraient dûment envisager d'établir des pouvoirs et des procédures spécifiques aux données informatiques stockées afin de satisfaire à ces obligations. De telles dispositions spécifiques pourraient également apporter une plus grande clarté et renforcer la sécurité juridique. Les Parties peuvent également prévoir (par exemple par des procédures opérationnelles standard ou des lignes directrices similaires) que les autorisations judiciaires de perquisition et de saisie concernent des systèmes informatiques ou des données spécifiques afin d'appliquer les conditions et garanties de l'article 15. |
| Rec 2 | Les Parties qui ne prévoient pas de définitions des données informatiques (couvrant les données informatiques, les données relatives au trafic, les informations sur les abonnés) dans leur législation nationale sont encouragées à le faire sur la base des définitions pertinentes contenues dans la Convention[88] et à appliquer les pouvoirs de perquisition et de saisie des données informatiques stockées à tous les types de données informatiques (informations sur les abonnés, données relatives au trafic et au contenu) sous leur forme stockée. |
| Rec. 3 | Les Parties sont encouragées à établir des lignes directrices claires à l'intention des autorités nationales sur la manière de traiter certaines situations spécifiques qu'elles peuvent rencontrer dans la pratique lorsqu'elles accèdent à des données informatiques et les sécurisent, afin d'assurer une approche cohérente, si possible, au niveau national pour des situations similaires. Ces situations pourraient inclure 1) un message électronique non ouvert qui attend dans la boîte de réception d'un fournisseur de services jusqu'à ce que le destinataire le télécharge, comme indiqué au paragraphe 190 du Rapport explicatif de la Convention, 2) la perquisition et la saisie de biens virtuels, ou 3) l'obtention de données dans la mémoire volatile ou les procédures de triage lorsque de multiples dispositifs physiques sont trouvés. |
| Rec. 4 | Les Parties devraient envisager de prévoir une formation continue et des conseils pour leurs autorités compétentes qui autorisent et effectuent des perquisitions et des saisies (y compris des formations conjointes pour les juges, les procureurs et les fonctionnaires chargés de l'application de la loi), en particulier compte tenu de la complexité croissante des technologies émergentes et de la manière dont les données peuvent être utilisées comme preuves électroniques d'un délit. Cette formation peut être complétée par l'adoption de documents d'orientation, le cas échéant. Ces activités de formation peuvent être soutenues, si la partie le souhaite, par les programmes de renforcement des capacités du Conseil de l'Europe. |

[88] Ceci est sans préjudice du paragraphe 22 de l'ER.

| | |
|---|---|
| Rec 5 | Les Parties sont encouragées à prévoir explicitement dans leur législation les différentes conditions et exigences énoncées à l'article 19.2 de la Convention. |
| Rec 6 | Les Parties devraient s'assurer qu'elles ont le pouvoir de copier les données lorsqu'elles accèdent à un système informatique. Cette mesure peut être préférable à la saisie d'un système informatique entier dans certaines situations (par exemple, lorsque les données faisant l'objet d'une recherche ou d'un accès similaire peuvent être stockées sur le système informatique d'un témoin qui n'est pas réellement impliqué dans l'acte répréhensible ou lorsque les données se trouvent sur le serveur d'un fournisseur de services). |
| Rec 7 | Dans leur droit national ou dans des procédures opérationnelles normalisées internes ou des lignes directrices similaires, les Parties devraient préciser les exigences relatives au maintien de l'intégrité des données et de la chaîne de possession afin de garantir que les données n'ont pas été altérées (protocoles d'action, création d'images, valeurs de hachage, stockage des données, périodes de conservation). Certains de ces éléments peuvent être trouvés dans l'article 14 du deuxième protocole additionnel (par exemple, la qualité et l'intégrité, les périodes de conservation, la sécurité des données, etc.) |
| Rec 8 | Les Parties devraient s'assurer qu'elles ont le pouvoir de retirer les données d'un système informatique perquisitionné ou de les rendre inaccessibles sous certaines conditions. |
| Rec 9 | Les Parties devraient s'assurer qu'elles ont le pouvoir d'ordonner à toute personne ayant connaissance du fonctionnement d'un système informatique, ou des mesures appliquées pour protéger ses données, de fournir, dans la mesure du raisonnable, les informations nécessaires pour mener à bien les actions prévues à l'article 19. Il est urgent de modifier les lois et les pratiques d'enquête à cet égard. Sans préjudice de certains droits prévus par leur législation nationale (par exemple, le droit de ne pas s'incriminer soi-même), les Parties sont encouragées à envisager d'établir des sanctions si la personne refuse de fournir la coopération nécessaire. Les Parties devraient limiter l'utilisation de ce pouvoir à la fourniture d'informations raisonnables. En particulier, les Parties devraient éviter d'utiliser ce pouvoir lorsque la divulgation du mot de passe ou d'une autre mesure de sécurité menacerait de manière déraisonnable la vie privée d'autres utilisateurs ou d'autres données dont la recherche n'est pas autorisée. Dans de tels cas, la fourniture des "informations nécessaires" pourrait consister à divulguer, sous une forme intelligible et lisible, les données réelles recherchées par les autorités compétentes. |
| Rec 10 | Dans le même ordre d'idées, les Parties sont encouragées à préciser dans leur législation nationale ou dans des procédures opérationnelles standard internes ou des lignes directrices similaires :<br>- les conditions à remplir ou les mesures à prendre pour acquérir légalement des titres conformément au droit interne d'une partie ;<br>- la manière dont les identifiants acquis légalement peuvent être utilisés par leurs autorités compétentes (par exemple, pour télécharger des données informatiques stockées, pour des activités d'infiltration lors du contrôle du compte, ou pour changer d'identifiant, etc.) |
| Rec 11 | Les Parties devraient veiller à ce que leurs pouvoirs de perquisition et de saisie de données informatiques s'étendent à tous les types d'infractions, conformément au champ d'application de la Convention en vertu de l'article 14. Dans les pays où ces pouvoirs découlent d'une combinaison de lois, l'interaction de ces lois devrait être examinée pour les cas qui ne relèveraient pas de toutes les lois. |

| | |
|---|---|
| Rec 12 | Conformément aux obligations découlant de l'article 15, les Parties doivent veiller à ce que les mesures de perquisition et de saisie soient appliquées dans le respect du principe de proportionnalité, conformément aux principes pertinents de leur droit interne. Les Parties doivent appliquer les conditions et garanties, que le pouvoir de perquisition et de saisie soit exercé sur le lieu où le système informatique ou les données sont trouvés, ou en un autre lieu, ou à partir d'un autre lieu. Les parties doivent veiller à ce que les privilèges et immunités juridiques applicables soient protégés. Cela peut inclure la possibilité de demander réparation pour les personnes qui se prévalent de cette protection. Lorsqu'elles appliquent les mesures prévues à l'article 19, les Parties devraient, dans la mesure où cela est compatible avec l'intérêt public, examiner leur impact sur les droits, les responsabilités et les intérêts légitimes des tiers, y compris les fournisseurs de services, et déterminer si des moyens appropriés peuvent être pris pour atténuer cet impact. |
| Rec. 13 | Certaines Parties n'ont pas de système en place pour effectuer des perquisitions et des saisies de systèmes conformément à l'article 19 dans des situations d'urgence, ou elles ont des systèmes rudimentaires, informels ou ad hoc. Ces Parties sont encouragées à examiner le présent Rapport d'évaluation pour savoir comment les autres Parties ont abordé ces situations avant qu'elles ne soient confrontées à une situation d'urgence réelle. Les Parties ayant mis en place des systèmes plus robustes sont également encouragées à examiner le présent rapport d'évaluation afin de déterminer si d'autres parties pourraient avoir des éléments utiles à incorporer dans leur propre système. Il est rappelé à toutes les parties que le deuxième protocole additionnel donne une définition de la notion d'"urgence" qui peut être utile. |
| Rec 14 | L'extension des recherches à un lieu connu comme étant étranger ou à un lieu inconnu est devenue une question urgente à laquelle les praticiens sont confrontés. Par conséquent, les Parties devraient préparer leur position sur l'extension des recherches à partir de leur propre territoire vers un lieu que l'on sait être étranger ou vers un lieu inconnu. En élaborant ces positions, les Parties devraient prendre en compte les implications possibles d'une extension des perquisitions transfrontalières (considérations politiques, juridiques et autres, y compris les droits des individus et des tiers ainsi que l'invalidation et la suppression potentielles de preuves). D'éventuelles secondes autorisations judiciaires, la consultation ou la notification du pays ciblé, la sensibilisation des autorités compétentes et des modifications du droit national pourraient être envisagées afin d'atténuer les risques. |
| Rec. 15 | Bien que les mesures d'extension des recherches en dehors du territoire d'une Partie ou dans un lieu inconnu et l'accès à distance secret ne soient pas spécifiquement prévus par la Convention, les Parties peuvent s'assurer que ces mesures sont soumises aux conditions et garanties prévues à l'article 15 de la Convention. |
| Rec 16 | Le cas échéant, les Parties sont encouragées à envisager de partager leurs procédures opérationnelles standards internes ou des lignes directrices similaires sur la mise en œuvre de l'article 19 avec le Secrétariat afin de les rendre disponibles avec un accès restreint sur la plateforme en ligne récemment développée pour l'échange de matériel, la formation et le partage de ressources sur la cybercriminalité et les preuves électroniques (CYBOX). |

### 9.3.2 Recommandation relevant principalement de la responsabilité du T-CY

| | |
|---|---|
| Rec 17 | Le T-CY invite le Bureau du T-CY à fournir à la plénière des options pour les travaux futurs sur la question des actifs virtuels et la pertinence de la Convention sur la cybercriminalité et de son deuxième protocole, comme décidé lors de la 30e plénière du T-CY en juin 2024.[89] |

### 9.3.3 Recommandations relevant principalement de la responsabilité du Conseil de l'Europe

| | |
|---|---|
| Rec 18 | Le Bureau du programme sur la cybercriminalité du Conseil de l'Europe (C-PROC) devrait soutenir les réformes de la législation, de la formation et de la spécialisation (y compris des autorités spécialisées) en matière de perquisition et de saisie de données informatiques stockées. |
| Rec. 19 | Le Conseil de l'Europe (Secrétariat T-CY et C-PROC) devrait mettre à disposition, avec un accès restreint, des documents sur la mise en œuvre de l'article 19 de la Convention partagés par les Parties sur la plateforme en ligne récemment développée pour l'échange de documents, la formation et le partage de ressources sur la cybercriminalité et les preuves électroniques (CYBOX). |

## 9.4 Suivi

Les parties sont invitées à informer le T-CY et son secrétariat des mesures prises et des exemples de bonnes pratiques à tout moment.

Les parties sont invitées à faire le point sur le suivi des recommandations applicables relevant de la responsabilité des autorités nationales et à rendre compte au T-CY, au plus tard 18 mois après l'adoption du présent rapport, des mesures prises pour permettre au T-CY, conformément au règlement intérieur (article 2.1.g), d'examiner les progrès accomplis.

Le Secrétariat du Conseil de l'Europe est invité à assurer le suivi des recommandations relevant de sa responsabilité et à faire rapport au T-CY dans les 18 mois suivant l'adoption du rapport.

Le T-CY examinera ensuite les progrès accomplis.

[89] https://rm.coe.int/t-cy-2024-6-plen30-rep-v4final/1680b07f1c

# 10 ANNEXE

## 10.1 Exemples de dispositions juridiques nationales

### 10.1.1 Argentine

Les données peuvent être téléchargées ici.

### 10.1.2 Autriche

Les données peuvent être téléchargées ici et ici.

### 10.1.3 Canada

**"Agent de la paix**

***l'agent de la paix*** comprend

- **(a)** le maire, le gardien, le préfet, le shérif, le shérif adjoint, l'officier du shérif et le juge de paix,
- **(b)** un membre du Service correctionnel du Canada désigné comme agent de la paix conformément à la partie I de la *Loi sur le système correctionnel et la mise en liberté sous condition*, ainsi qu'un directeur, un directeur adjoint, un instructeur, un gardien, un geôlier, un garde et tout autre fonctionnaire ou employé permanent d'une prison autre qu'un pénitencier tel que défini dans la partie I de la *Loi sur le système correctionnel et la mise en liberté sous condition*,
- **(c)** un officier de police, un agent de police, un huissier, un agent de police ou toute autre personne employée pour la préservation et le maintien de la paix publique ou pour la signification ou l'exécution d'un acte de procédure civile,
- **(c.1)** un fonctionnaire désigné au sens de l'article 2 de la *loi sur les opérations transfrontalières intégrées de maintien de l'ordre*, lorsque
    - **(i)** participer à une opération transfrontalière intégrée, telle que définie à l'article 2 de cette loi, ou
    - **(ii)** **l'**exercice d'une activité accessoire à cette opération, y compris les déplacements effectués en vue de participer à l'opération et les comparutions en justice découlant de l'opération,
- **(d)** un fonctionnaire au sens de la *loi sur les douanes*, de la *loi sur les accises* ou de la *loi de 2001 sur les accises*, ou une personne ayant les pouvoirs d'un tel fonctionnaire, lorsqu'il exerce une fonction dans le cadre de l'application de l'une de ces lois,
- **(d.1)** l'agent autorisé en vertu du paragraphe 138(1) de la *Loi sur l'immigration et la protection des réfugiés*,
- (e) une personne désignée comme garde-pêche en vertu de la *loi sur la pêche* lorsqu'elle exerce des fonctions en vertu de cette loi et une personne désignée comme agent de pêche en vertu de la *loi sur la pêche* lorsqu'elle exerce des fonctions en vertu de cette loi ou de la *loi sur la protection des pêcheries côtières*,
- **(f)** le pilote commandant de bord d'un aéronef
    - **(i)** enregistrés au Canada en vertu des règlements d'application de la *loi sur l'aéronautique*, ou
    - **(ii)** loué sans équipage et exploité par une personne qui, en vertu des règlements pris en application de la *loi sur l'aéronautique*, est habilitée à être enregistrée comme propriétaire d'un aéronef immatriculé au Canada en vertu de ces règlements,

lorsque l'aéronef est en vol, et

- **(g) les** officiers et les militaires du rang des Forces canadiennes qui sont
    - **(i)** nommé pour l'application de l'article 156 de la *loi sur la défense nationale*, ou

**(ii)** employés à des tâches que le gouverneur en conseil, par règlement pris en vertu de la *Loi sur la défense nationale pour l'*application du présent alinéa, a prescrit comme étant de nature à nécessiter que les officiers et militaires du rang qui les exécutent aient les pouvoirs d'agents de la paix ; (*officer of the peace*)

### 10.1.4 République tchèque

Les données peuvent être téléchargées ici.

### 10.1.5 Estonie

**Extraits du code de procédure pénale**
https://www.riigiteataja.ee/en/eli/ee/504042023004/consolide/current
**§ Article 63 - Éléments de preuve**
(1) On entend par "élément de preuve" la déclaration ou le témoignage du suspect, de l'accusé, de la victime, du témoin ou du témoin spécialiste, le rapport d'un expert, la déclaration ou le témoignage d'un expert lorsqu'il apporte des éclaircissements sur son rapport, un élément de preuve matériel, le rapport d'une enquête ou d'une opération secrète, le procès-verbal ou l'enregistrement vidéo d'un procès ou d'une audience ou le rapport ou l'enregistrement vidéo d'une enquête ou d'une opération secrète, ainsi que tout autre document, de même que toute photographie, toute séquence ou tout autre enregistrement de données.
($1^1$) La présentation, à titre de preuve dans une procédure pénale, de toute information recueillie en vertu de la loi sur les autorités de sécurité est décidée par le procureur général, compte tenu des restrictions mentionnées au paragraphe 2 de l'article 1261 et au paragraphe 2 de l'article 1267 du présent code.
(2) Les éléments de preuve non énumérés au paragraphe 1 du présent article peuvent également être utilisés pour prouver les faits en cause dans une procédure pénale, sauf s'ils ont été obtenus par une infraction pénale ou par la violation d'un droit fondamental.

**§ 64. Conditions générales pour la collecte de preuves**
(1) Les preuves sont recueillies d'une manière qui ne porte pas atteinte à l'honneur et à la dignité des personnes qui participent à leur collecte, qui ne mette pas en danger la vie ou la santé de ces personnes et qui ne cause pas de préjudice pécuniaire injustifié. Il est interdit de recueillir des preuves en torturant une personne ou en la soumettant à la violence de toute autre manière, ou en utilisant des moyens qui affectent sa faculté de mémoire, ou en la traitant d'une manière qui porte atteinte à la dignité humaine.
(2) Si, au cours de la fouille ou de l'examen physique d'une personne, ou du prélèvement de matériel pour comparaison, il est nécessaire de révéler le corps de la personne, l'agent de l'autorité chargée de l'enquête, le procureur et tous les autres participants à l'opération procédurale correspondante, à l'exception des professionnels de la santé et des médecins légistes, doivent être du même sexe que la personne.
(3) Si des équipements techniques doivent être utilisés pour l'obtention des preuves, les participants à l'opération de procédure correspondante en sont préalablement informés et l'objectif de l'utilisation de ces équipements leur est expliqué.
(4) [Abrogé - RT I, 23.02.2011, 1 - entrée en vigueur 01.09.2011]
(5) Lorsque cela est nécessaire, les participants à une opération procédurale sont avertis que, conformément à l'article 214 du présent code, la divulgation d'informations relatives aux procédures préalables au procès n'est pas autorisée.
(6) L'obtention de preuves par des opérations secrètes est régie par le chapitre 31 du présent code.

**§ 83. But de l'inspection et objets de l'inspection**
(1) L'inspection a pour but de recueillir les informations nécessaires à la résolution de l'affaire pénale, de détecter les indices d'une infraction pénale et de saisir les objets qui serviront de preuves matérielles.
(2) L'inspection a pour objet

1) le lieu des événements ;
2) le cadavre ;
3) un document, un autre objet ou une preuve matérielle ;
4) en cas d'examen physique, la personne ou l'envoi postal ou télégraphique à examiner.
(3) Lorsque les explications du suspect, de l'accusé, du témoin, du témoin spécialisé ou de la victime sont de nature à garantir l'exhaustivité et l'objectivité de l'inspection, la personne est convoquée à l'inspection.

**§ 86 Inspection d'un document, d'un autre objet ou d'un élément de preuve matérielle**
(1) Lors de l'inspection d'un document ou d'un autre objet, les indices d'une infraction pénale et tout autre élément caractéristique nécessaire à la résolution de l'affaire pénale et justifiant l'utilisation de l'objet en question en tant qu'élément de preuve matérielle sont déterminés.
(2) Lorsqu'un examen complémentaire d'un document, d'une chose ou d'un autre objet apparaissant comme un élément de preuve matérielle est nécessaire, une inspection de l'élément de preuve matérielle est effectuée.

**§ 91. Recherche**
(1) La perquisition a pour but de trouver, dans un bâtiment, une pièce, un véhicule ou un espace clos, un objet à confisquer ou à utiliser comme élément de preuve matérielle, ou un document, une chose ou une personne nécessaire à la résolution de l'affaire pénale, ou un bien à saisir dans le cadre d'une procédure pénale, ou un cadavre, ou d'appréhender une personne déclarée fugitive. Une perquisition peut être effectuée s'il existe un soupçon raisonnable que ce qui est recherché se trouve à l'endroit à perquisitionner.
(2. Sauf disposition contraire du présent code, une perquisition peut être effectuée à la demande du ministère public en vertu d'un mandat du juge d'instruction ou du tribunal. L'ordonnance par laquelle le juge d'instruction ou le tribunal statue sur cette demande peut prendre la forme d'une note faite sur la demande.
(3) Une perquisition peut être effectuée sur la base d'un mandat du bureau du procureur, à l'exception d'une perquisition dans le bureau d'un notaire ou d'un cabinet d'avocats ou dans les locaux d'une personne traitant des informations à des fins journalistiques, à condition qu'il y ait des raisons de croire que le suspect utilise les locaux ou le véhicule à perquisitionner, ou qu'il a utilisé ces locaux ou ce véhicule, au moment de l'événement criminel ou au cours de la procédure préliminaire, et que la personne soit soupçonnée d'avoir commis une infraction pénale mentionnée au paragraphe 2 de l'article 1262 du présent code.
(4) Le mandat de perquisition indique :
1) le but de la recherche, c'est-à-dire l'objet de la recherche (ci-après "l'objet recherché") ;
2) les raisons de la recherche ;
3) le lieu où la recherche est effectuée.
(5) En cas d'urgence, s'il n'est pas possible de délivrer un mandat de perquisition en temps utile, une perquisition peut être effectuée, dans les conditions prévues au paragraphe 3 du présent article, sur la base d'une autorisation du ministère public fournie sous une forme reproductible par écrit.
(6. Lorsqu'une perquisition est effectuée pour les motifs prévus aux paragraphes 3 et 5 du présent article, elle doit être notifiée, par l'intermédiaire du ministère public, au juge de l'enquête préliminaire au cours du premier jour ouvrable suivant le début de la perquisition. Le juge décide, par une ordonnance qui peut être portée en note sur le mandat du ministère public, de déclarer ou non la perquisition autorisée.
(7) Lors de la préparation d'une perquisition, le mandat de perquisition est présenté à la personne chez qui la perquisition est effectuée, ou à un membre majeur de sa famille, ou à un représentant de la personne morale ou de l'autorité étatique ou municipale chez qui la perquisition est effectuée. La personne, le membre de la famille ou le représentant doit signer le mandat pour attester de cette présentation. Dans une situation visée au paragraphe 5 du présent article, les circonstances visées au paragraphe 4 du présent article et les raisons pour lesquelles la perquisition doit être effectuée d'urgence sont expliquées à la personne, au membre de la famille ou au représentant. La personne, le membre de la famille ou le

représentant signe le rapport de fouille pour attester de cette explication. Lorsque la personne concernée ou son représentant n'est pas présent, la participation d'un représentant de la municipalité doit être organisée.
(8) Lorsqu'une perquisition est effectuée dans l'étude d'un notaire ou d'un cabinet d'avocats, le notaire ou l'avocat chez qui la perquisition est effectuée doit être présent. Si le notaire ou l'avocat ne peut pas assister à la perquisition, la personne qui remplace le notaire ou un autre avocat qui fournit des services juridiques par l'intermédiaire du même cabinet ou, en cas d'impossibilité, un autre notaire ou un autre avocat, doit y assister.
(9) Lors de la préparation d'une perquisition, une invitation est faite à remettre l'objet recherché ou à indiquer l'endroit où un cadavre a été caché ou celui où se cache une personne déclarée en fuite. S'il n'est pas donné suite à l'invitation ou s'il y a lieu de penser qu'elle n'a été suivie que partiellement, les opérations de perquisition sont effectuées.
(10) Au cours d'une perquisition, les objets susceptibles d'être confisqués ou qui représentent manifestement des éléments de preuve dans une procédure pénale peuvent être saisis, à condition qu'ils aient été découverts en dehors de toute opération de perquisition, dans un endroit clairement visible, ou au cours d'opérations de recherche raisonnables entreprises pour trouver les objets recherchés.

**§ 126⁴. Octroi d'une autorisation pour une opération secrète**
(1) Une opération secrète peut être menée lorsqu'elle est autorisée par écrit par le ministère public ou par le juge de l'enquête préliminaire. Le juge de la mise en état décide de l'octroi d'une telle autorisation par ordonnance sur la base d'une demande motivée du ministère public. La demande motivée du ministère public est examinée sans délai par le juge de l'enquête préliminaire et l'autorisation de mener l'opération secrète en question est accordée ou refusée par une ordonnance.
(2) En cas d'urgence, une opération secrète nécessitant une autorisation du ministère public peut être menée, cette autorisation étant délivrée sous une forme reproductible. Une autorisation écrite est délivrée dans les 24 heures suivant le début de l'opération.
(3) En cas de danger immédiat pour la vie, l'intégrité physique, la liberté physique ou un bien de grande valeur d'une personne, et lorsqu'il n'est pas possible de demander ou de délivrer une autorisation pertinente en temps utile, une opération secrète nécessitant une autorisation du tribunal peut être menée, dans une situation d'urgence, avec une telle autorisation délivrée sous une forme reproductible. Une demande écrite est déposée et une autorisation correspondante est délivrée dans les 24 heures suivant le début de l'opération.
(4) L'autorisation délivrée en cas d'urgence sous une forme reproductible doit contenir les informations suivantes :
1) l'émetteur de l'autorisation ;
2) la date et l'heure de la délivrance de l'autorisation ;
3) l'opération secrète pour laquelle l'autorisation est délivrée ;
4) s'il est connu, le nom de la personne à l'égard de laquelle l'opération secrète doit être menée ;
5) le délai d'autorisation des opérations secrètes.
(5) Lorsque, pour **mener une opération secrète** ou pour placer ou retirer tout moyen technique nécessaire à une telle opération, il est nécessaire de **pénétrer secrètement** dans un bâtiment, une pièce, un véhicule, un espace clos ou un **système informatique**, le ministère public demande et obtient une autorisation distincte correspondante du juge de l'enquête préliminaire.
(6) La durée des opérations secrètes menées à l'égard d'une personne donnée pour les motifs prévus aux clauses 1, 2 et 4 de la sous-section 1 de l'article 126, paragraphe 2, du présent code, dans le cadre d'une même procédure, ne doit pas dépasser un an. Dans des situations exceptionnelles, le procureur général peut autoriser ou demander au tribunal l'autorisation de mener des opérations secrètes pendant plus d'un an. Dans une affaire pénale traitée en vertu du règlement (UE) 2017/1939 du Conseil, l'autorisation pertinente est accordée, ou la demande présentée, par un procureur européen ou un procureur européen délégué.

**§ 126[5]. Surveillance secrète, collecte secrète d'échantillons pour comparaison et conduite d'enquêtes initiales, examen secrète et substitution d'un objet.**
(1) Pour la surveillance secrète d'une personne, d'un objet ou d'une zone, pour la collecte secrète d'échantillons à des fins de comparaison et pour la conduite d'enquêtes initiales, ainsi que pour l'examen secrète ou la substitution d'un objet, le bureau du procureur accorde une autorisation pour une durée maximale de deux mois. Le bureau du procureur peut prolonger la durée de l'autorisation de deux mois au maximum.
(2) Au cours des opérations secrètes mentionnées dans la présente section, les informations collectées sont - si nécessaire - enregistrées par vidéo, photographiées, copiées ou enregistrées par toute autre méthode.

### 10.1.6 Finlande

Les données peuvent être téléchargées ici.

### 10.1.7 Géorgie

Les données peuvent être téléchargées ici.

### 10.1.8 Allemagne

Les données peuvent être téléchargées ici.

### 10.1.9 Hongrie

Attachment_Court_decisions.docx

### 10.1.10 Kiribati

Loi sur la cybercriminalité 2021

### 10.1.11 Lituanie

Entrée disponible ici, ici, ici et ici.

### 10.1.12 Norvège

Les données sont disponibles ici.

### 10.1.13 Paraguay

Les contributions sont disponibles ici et ici.

### 10.1.14 République de Moldavie

**Article 11. Inviolabilité de la personne (CPC)**
(1) La liberté individuelle et la sécurité de la personne sont inviolables.
....

(7) La perquisition, l'examen corporel et les autres actes de procédure portant atteinte à l'inviolabilité de la personne ne peuvent être effectués sans le consentement de la personne ou de son représentant légal que dans les conditions prévues par le présent code.
Article 12. Inviolabilité du domicile (CPC)
(1) L'inviolabilité du domicile est garantie par la loi. Au cours d'une procédure pénale, nul n'a le droit de pénétrer dans le domicile contre la volonté des personnes qui y résident ou y ont des locaux, sauf dans les cas et selon les modalités prévus par le présent code.
(2) Les perquisitions, visites domiciliaires et autres poursuites pénales à domicile peuvent être ordonnées et exécutées en vertu d'un mandat judiciaire, sauf dans les cas et selon les modalités prévus par le présent code. En cas d'exécution d'actes de procédure sans mandat judiciaire, l'organe autorisé à exécuter ces actes doit, immédiatement et au plus tard 24 heures après l'achèvement de l'acte, soumettre les documents correspondants au tribunal pour qu'il contrôle la légalité de ces actes.

**Article 13. Inviolabilité des biens (CPC)**
(1) Une personne physique ou morale ne peut être arbitrairement privée du droit de propriété. Nul ne peut être privé de sa propriété si ce n'est pour cause d'utilité publique et conformément au présent code et aux principes généraux du droit international.
(2) Les biens ne peuvent être saisis que sur la base d'une décision de justice.
(3) Les biens saisis au cours de la procédure sont décrits dans le procès-verbal de la procédure et une copie du procès-verbal est remise à la personne chez qui ils ont été saisis.

**Article 14. Secret de la correspondance (CPC)**
(1) Le droit au secret des lettres, télégrammes, autres envois postaux, conversations téléphoniques et autres moyens de communication légaux est garanti par l'État. Au cours d'une procédure pénale, nul ne peut être privé ou limité dans ce droit.
(2) La limitation du droit visé au paragraphe (1) n'est autorisée que sur la base d'un mandat judiciaire délivré dans les conditions prévues par le présent code.

**Article 15. Inviolabilité de la vie privée (CPC)**
(1) Toute personne a droit à l'inviolabilité de sa vie privée, au secret de sa vie intime et familiale et à la protection de son honneur et de sa dignité. Au cours d'une procédure pénale, nul n'a le droit de s'immiscer arbitrairement et illégitimement dans la vie privée d'une personne.
(2) Dans le cadre des actes de procédure, les informations relatives à la vie privée et intime de la personne ne peuvent être recueillies inutilement. À la demande de l'organe de poursuite et du tribunal, les participants aux actes de procédure sont tenus de ne pas divulguer ces informations et un engagement écrit est pris à ce sujet. Le traitement des données personnelles dans le cadre des procédures pénales est effectué conformément aux dispositions de la loi n° 133 du 8 juillet 2011 sur la protection des données personnelles.
(3) Les personnes auxquelles l'autorité de poursuite demande des informations sur leur vie privée et intime ont le droit d'être convaincues que ces informations sont administrées dans le cadre d'une affaire pénale spécifique. La personne n'a pas le droit de refuser de fournir des informations sur sa vie privée et intime ou celle d'autres personnes sous prétexte de l'inviolabilité de la vie privée, mais elle a le droit de demander à l'organe de poursuite une explication sur la nécessité d'obtenir ces informations, cette explication devant être incluse dans le procès-verbal de l'acte de procédure concerné.
(4) Les preuves confirmant des informations sur la vie privée et intime de la personne sont examinées, à la demande de celle-ci, à huis clos.
(5) Le préjudice causé à la personne au cours de la procédure pénale par la violation de sa vie privée et intime est réparé de la manière prévue par la législation en vigueur.

**Article 127. Personnes présentes lors de la perquisition ou de la saisie d'objets et de documents**
(1) Si nécessaire, l'*interprète ou le spécialiste* peut assister à la perquisition ou à la saisie d'objets et de documents.

(2) La présence de la personne à perquisitionner ou à saisir, des membres majeurs de sa famille ou des personnes représentant les intérêts de la personne concernée doit être assurée lors de la perquisition ou de la saisie d'objets et de documents. Si la présence de ces personnes est impossible, *le représentant de l'autorité exécutive de l'administration publique locale est invité*.
(3) La saisie d'objets et de documents ou la perquisition de locaux d'institutions, d'entreprises, d'organisations et d'unités militaires s'effectuent en présence du représentant concerné.
(4) Les personnes dont les objets et les documents sont perquisitionnés ou saisis, ainsi que les spécialistes, les interprètes, les représentants, les défenseurs, ont le droit d'assister à tous les actes de l'organe de poursuite ou d'application de la loi et de formuler des objections et des déclarations à ce sujet, qui sont consignées dans le procès-verbal.
(5) Pour assurer la sécurité, les autorités chargées des poursuites ou de l'application des lois peuvent faire appel à des subdivisions des institutions visées à l'article 56, paragraphe 1, ou à d'autres institutions. L'identité des personnes impliquées par les autorités chargées des poursuites ou de l'application des lois aux fins d'assurer la sécurité peut être dissimulée et/ou déguisée, ce qui est consigné dans le procès-verbal.
(6) La personne qui fait l'objet d'une perquisition ou dont les objets et documents sont saisis a le droit d'enregistrer ces actions par des moyens audiovisuels et d'en informer l'organe de poursuite ou les forces de l'ordre.
(7) Si la personne perquisitionnée demande la présence d'un *défenseur*, la procédure est interrompue jusqu'à ce que celui-ci soit présent, mais pour une durée maximale de deux heures. En cas d'urgence due au risque de perte, d'altération ou de destruction de preuves ou au danger pour la sécurité de la personne perquisitionnée ou d'autres personnes, la perquisition est poursuivie, les motifs étant indiqués dans le procès-verbal.

**Article 300. Champ d'application du contrôle judiciaire**

(1) Le juge d'instruction examine les demandes du procureur concernant l'autorisation d'exercer des poursuites pénales, les mesures spéciales d'enquête et l'application de mesures procédurales de contrainte limitant les droits et libertés constitutionnels de la personne, ainsi que les demandes d'achèvement de la procédure pénale en l'absence de l'inculpé.
...

**Article 301. Poursuites menées avec l'autorisation du juge d'instruction**
(1) Avec l'autorisation du juge d'instruction, les actes de poursuite pénale relatifs à la limitation de l'inviolabilité de la personne, du domicile, à la limitation du secret de la correspondance, des appels téléphoniques, des communications télégraphiques et autres, à l'achèvement de la poursuite pénale en l'absence de l'inculpé, ainsi que les autres actes prévus par la loi, sont exécutés
**(2)** Les actes de poursuite sous forme de perquisition, l'enquête sur place au domicile et la saisie de biens à la suite d'une perquisition peuvent être effectués, à titre exceptionnel, sans l'autorisation du juge d'instruction, sur la base d'une ordonnance motivée du procureur général, dans les cas de flagrant délit et dans les cas qui ne permettent pas d'ajourner l'enquête. Le juge d'instruction doit être informé de l'exécution de ces actes de poursuite *dans les 24 heures* et, aux fins de contrôle, il présente les pièces du dossier pénal dans lequel les actes de poursuite exécutés sont justifiés. S'il existe des motifs suffisants, le juge d'instruction déclare, par une décision motivée, que l'action publique est légale ou, le cas échéant, illégale.
...

**Article 306. Mandat de la Cour pour l'exécution de poursuites pénales, de mesures d'enquête spéciales ou pour l'application de mesures procédurales de contrainte**

La décision judiciaire relative à l'exercice de l'action publique, aux mesures spéciales d'instruction ou à l'application de mesures procédurales de contrainte indique : la date et le lieu de sa rédaction, les noms et prénoms du juge d'instruction, de la personne responsable et de l'organe qui a présenté la demande, de l'organe qui effectue les poursuites, les mesures spéciales d'enquête ou qui applique des mesures procédurales de contrainte, en indiquant l'objet de l'exécution de ces actions ou mesures et la personne

qu'elles visent, ainsi qu'une mention de l'autorisation de l'action ou de son rejet en cas d'objections de l'avocat de la défense, le représentant légal, le suspect, l'accusé, le prévenu, les raisons de leur admission ou de leur non-admission à l'application de la mesure de contrainte, la durée pour laquelle l'action est autorisée, la **personne responsable ou l'organe autorisé à exécuter le mandat (ordonnance du tribunal)**, la signature du juge d'instruction certifiée avec le cachet du tribunal.

**Article 540/2. Équipes communes d'enquête**
(1) Les autorités compétentes d'au moins deux États peuvent, d'un commun accord, créer une équipe commune d'enquête dans un but précis et pour une durée limitée, qui peut être prolongée avec l'accord de toutes les parties, afin de mener des procédures pénales dans un ou plusieurs des États qui créent l'équipe. La composition de l'équipe commune d'enquête est décidée d'un commun accord.

**- Chapitre IX (art.531-540[1] CPC)**
**ASSISTANCE JURIDIQUE INTERNATIONALE EN MATIÈRE PÉNALE**

**Article 533. Champ d'application de l'assistance judiciaire**
(1) L'entraide judiciaire internationale peut être demandée ou accordée pour l'exécution de certains actes de procédure prévus par la législation en matière de procédure pénale de la République de Moldova et de l'État étranger concerné en particulier :
...
3) mener l'enquête sur place, la **perquisition, la saisie d'objets et de documents et leur transmission à l'étranger**, la **saisie**, la confrontation, la présentation pour reconnaissance, l'identification des abonnés au téléphone, l'interception des communications, la **réalisation d'expertises médico-légales**, la confiscation des biens provenant de la commission de crimes et d'autres actions de poursuite pénale prévues par le présent code ;
...

**Art. 536 Commissions rogatoires**
(1) L'autorité ou la juridiction de poursuite, si elle estime nécessaire d'exercer des poursuites *sur le territoire d'un État étranger*, s'adresse par commission rogatoire à l'autorité ou à la juridiction de poursuite de cet État, ou à une juridiction pénale internationale conformément au traité international auquel la République de Moldova est partie ou par la voie diplomatique, dans des conditions de réciprocité.

**Art. 540/1. Perquisition, saisie, enlèvement d'objets ou de documents, saisie et confiscation**

Les commissions rogatoires demandant la perquisition, la saisie ou la remise d'objets ou de documents, ainsi que la saisie ou la confiscation, sont exécutées conformément à la législation de la République de Moldova.

### 10.1.15 États-Unis d'Amérique

**Règles fédérales de procédure pénale - Règle 17**
**(a) Contenu** - Une citation à comparaître doit mentionner le nom du tribunal et le titre de la procédure, inclure le sceau du tribunal et ordonner au témoin de se présenter et de témoigner à l'heure et au lieu spécifiés dans la citation. Le greffier doit délivrer une citation à comparaître en blanc - signée et scellée - à la partie qui la demande, et cette dernière doit remplir les blancs avant que la citation à comparaître ne soit signifiée.

**(b) Défendeur incapable de payer** - Sur demande ex parte du défendeur, le tribunal doit ordonner qu'une citation à comparaître soit délivrée pour un témoin nommé si le défendeur montre qu'il est incapable de payer les honoraires du témoin et que la présence du témoin est nécessaire pour une défense adéquate. Si le tribunal ordonne la délivrance d'une citation à

comparaître, les frais de procédure et les indemnités des témoins seront payés de la même manière que ceux payés pour les témoins que le gouvernement cite à comparaître.

**(c) Production de documents et d'objets.**
**(1) En général - Une** citation à comparaître peut ordonner au témoin de produire tout livre, document, donnée ou autre objet désigné par la citation à comparaître. Le tribunal peut ordonner au témoin de produire les éléments désignés devant le tribunal avant le procès ou avant qu'ils ne soient présentés comme preuves. Lorsque les pièces arrivent, le tribunal peut autoriser les parties et leurs avocats à les inspecter en tout ou en partie.
**(2) Annulation ou modification de la citation à comparaître - Sur** requête présentée rapidement, le tribunal peut annuler ou modifier la citation à comparaître si son respect est déraisonnable ou oppressif.
**(3) Citation à comparaître pour obtenir des informations personnelles ou confidentielles sur une victime - Après le** dépôt d'une plainte, d'un acte d'accusation ou d'une dénonciation, une citation à comparaître exigeant la production d'informations personnelles ou confidentielles sur une victime ne peut être signifiée à une tierce partie que sur ordonnance du tribunal. Avant de rendre l'ordonnance, et sauf circonstances exceptionnelles, le tribunal doit exiger que la victime soit avertie afin qu'elle puisse demander l'annulation ou la modification de la citation à comparaître ou s'y opposer d'une autre manière.

**(d) Signification : un** marshal, un marshal adjoint ou toute autre personne âgée d'au moins 18 ans peut signifier une citation à comparaître. Le serveur doit remettre une copie de l'assignation au témoin et doit lui offrir un jour de frais de présence et l'indemnité kilométrique légale. Le serveur n'est pas tenu de verser le droit de présence ou l'indemnité kilométrique lorsque les États-Unis, un fonctionnaire fédéral ou une agence fédérale ont demandé la citation à comparaître.

**(e) Lieu de signification ou de notification**
**(1) Aux États-Unis - Une** citation à comparaître obligeant un témoin à assister à une audience ou à un procès peut être signifiée en tout lieu sur le territoire des États-Unis.
**(2) Dans un pays étranger - Si** le témoin se trouve dans un pays étranger, l'article 28 U.S.C. §1783 régit la signification de l'assignation.

**(f) L'émission d'une citation à comparaître pour une déposition.**

**(1) Délivrance : une** ordonnance du tribunal autorisant une déposition autorise le greffier du district où la déposition doit être effectuée à délivrer une citation à comparaître pour tout témoin nommé ou décrit dans l'ordonnance.
**(2) Lieu - Après avoir** pris en compte la commodité du témoin et des parties, le tribunal peut ordonner - et la citation à comparaître peut exiger - que le témoin se présente à l'endroit désigné par le tribunal.

**(Le** tribunal (autre qu'un juge de première instance) peut condamner pour outrage un témoin qui, sans excuse valable, désobéit à une citation à comparaître émise par un tribunal fédéral de ce district. Un juge de première instance peut tenir pour coupable d'outrage un témoin qui, sans excuse valable, désobéit à une citation à comparaître délivrée par ce juge de première instance, conformément à l'article 28 U.S.C. §636(e).

**(Aucune** partie ne peut citer à comparaître une déclaration d'un témoin ou d'un témoin potentiel en vertu de la présente règle. La règle 26.2 régit la production de la déclaration.

**Règles fédérales de procédure pénale - Règle 41**
**(a) Champ d'application et définitions**
**(1) Champ d'application** - Cette règle ne modifie aucune loi régissant les perquisitions et les saisies, ou la délivrance et l'exécution d'un mandat de perquisition dans des circonstances particulières.

**(2) Définitions** - Les définitions suivantes s'appliquent à la présente règle :
**(A)** Les "biens" comprennent les documents, les livres, les papiers, tout autre objet tangible et les informations.
**(B)** On entend par "période diurne" les heures comprises entre 6 heures et 22 heures selon l'heure locale.
**(C)** "agent fédéral chargé de l'application de la loi" : un agent du gouvernement (autre qu'un avocat du gouvernement) chargé de l'application des lois pénales et appartenant à l'une des catégories d'agents autorisés par le procureur général à demander un mandat de perquisition.
**(D)** Les termes "terrorisme national" et "terrorisme international" ont le sens qui leur est donné au paragraphe 2331 du titre 18 du Code des États-Unis.
**(E)** "Dispositif de repérage" a la signification indiquée dans 18 U.S.C. §3117 (b).

**(A la** demande d'un agent fédéral chargé de l'application de la loi ou d'un avocat du gouvernement :
**(1)** un magistrate judge ayant autorité dans le district - ou, si aucun n'est raisonnablement disponible, un juge d'un tribunal d'État d'archives dans le district - a autorité pour délivrer un mandat de perquisition et de saisie d'une personne ou d'un bien situé dans le district ;
**(2)** un magistrate judge ayant autorité dans la circonscription est habilité à délivrer un mandat à l'encontre d'une personne ou d'un bien situé en dehors de la circonscription si la personne ou le bien se trouve dans la circonscription au moment de la délivrance du mandat mais pourrait se déplacer ou être déplacé en dehors de la circonscription avant que le mandat ne soit exécuté ;
**(3)** un magistrate judge - dans le cadre d'une enquête sur le terrorisme national ou international - ayant autorité dans tout district dans lequel des activités liées au terrorisme peuvent avoir eu lieu est habilité à délivrer un mandat à l'encontre d'une personne ou d'un bien à l'intérieur ou à l'extérieur de ce district ;
**(4)** un magistrate judge ayant autorité dans le district est habilité à délivrer un mandat pour l'installation d'un dispositif de localisation dans le district ; le mandat peut autoriser l'utilisation du dispositif pour suivre les mouvements d'une personne ou d'un bien situé dans le district, à l'extérieur du district, ou les deux à la fois ; et
**(5)** un magistrate judge ayant autorité dans tout district où des activités liées au crime peuvent avoir eu lieu, ou dans le district de Columbia, peut délivrer un mandat pour des biens situés en dehors de la juridiction de tout État ou district, mais dans l'une des zones suivantes :
**(A)** un territoire, une possession ou un commonwealth des États-Unis ;
**(B)** les locaux - quel qu'en soit le propriétaire - d'une mission diplomatique ou consulaire des États-Unis dans un État étranger, y compris tout bâtiment annexe, partie d'un bâtiment ou terrain utilisé aux fins de la mission ; ou
**(C)** une résidence et tout terrain attenant appartenant aux États-Unis ou loués par eux et utilisés par le personnel des États-Unis affecté à une mission diplomatique ou consulaire des États-Unis dans un État étranger.
**(6)** un magistrate judge ayant autorité dans tout district où des activités liées à une infraction peuvent avoir eu lieu est habilité à délivrer un mandat pour utiliser l'accès à distance afin de perquisitionner des supports de stockage électroniques et de saisir ou de copier des informations stockées électroniquement situées à l'intérieur ou à l'extérieur de ce district si :
**(A)** le district où se trouve le média ou l'information a été dissimulé par des moyens technologiques ; ou
**(B)** dans le cadre d'une enquête sur une violation de l'article 1030(a)(5) du 18 U.S.C., les supports sont des ordinateurs protégés qui ont été endommagés sans autorisation et qui sont situés dans cinq districts ou plus.

**(c) Personnes ou biens faisant l'objet d'une perquisition ou d'une saisie - Un** mandat peut être délivré pour l'une des raisons suivantes :
**(1) la** preuve d'un crime ;
**(2) la** contrebande, les fruits du crime ou d'autres objets détenus illégalement ;

**(3) les** biens conçus pour être utilisés, destinés à être utilisés ou utilisés pour commettre un crime ; ou
**(4)** une personne à arrêter ou une personne illégalement retenue.

**(d) Obtention d'un mandat.**
**(1) En général - Après avoir** reçu une déclaration sous serment ou d'autres informations, un magistrate judge - ou, si la règle 41(b) l'autorise, un juge d'une State Court of Record - doit délivrer le mandat s'il existe des motifs probables de rechercher et de saisir une personne ou des biens ou d'installer et d'utiliser un dispositif de repérage.
**(2) Demander un mandat en présence d'un juge.**
**(Lorsqu'**un agent fédéral chargé de l'application de la loi ou un avocat du gouvernement présente une déclaration sous serment à l'appui d'un mandat, le juge peut exiger que l'auteur de la déclaration se présente personnellement et peut interroger sous serment l'auteur de la déclaration et tout témoin qu'il produit.
**(B) Mandat sur la base d'un témoignage sous serment - Le** juge peut se dispenser totalement ou partiellement d'une déclaration écrite sous serment et fonder un mandat sur un témoignage sous serment si cela est raisonnable compte tenu des circonstances.
**(Les témoignages** recueillis à l'appui d'un mandat doivent être enregistrés par un sténographe judiciaire ou par un dispositif d'enregistrement approprié, et le juge doit déposer la transcription ou l'enregistrement auprès du greffier, ainsi que toute déclaration sous serment.
**(3) Demande de mandat par voie téléphonique ou par d'autres moyens électroniques fiables - Conformément** à la règle 4.1, un magistrate judge peut délivrer un mandat sur la base d'informations communiquées par voie téléphonique ou par d'autres moyens électroniques fiables.

**(e) l'émission du bon de souscription.**

**(1) Généralités - Le** magistrate judge ou le juge d'une state court of record doit délivrer le mandat à un officier habilité à l'exécuter.
**(2) Contenu du bon de souscription.-**
**(A) Mandat de recherche et de saisie d'une personne ou d'un bien - À l'exception d'**un mandat relatif à un dispositif de localisation, le mandat doit identifier la personne ou le bien à rechercher, identifier toute personne ou tout bien à saisir et désigner le magistrate judge à qui il doit être renvoyé. Le mandat doit ordonner à l'agent de :
**(i)** exécuter le mandat dans un délai déterminé ne dépassant pas 14 jours ;
**(ii)** exécuter le mandat pendant la journée, à moins que le juge n'autorise expressément, pour des raisons valables, l'exécution du mandat à un autre moment ; et
**(iii)** renvoie le mandat au magistrate judge désigné dans le mandat.
**(Un** mandat délivré en vertu de la règle 41(e)(2)(A) peut autoriser la saisie de supports de stockage électroniques ou la saisie ou la copie d'informations stockées électroniquement. Sauf indication contraire, le mandat autorise un examen ultérieur des supports ou des informations conformément au mandat. Le délai d'exécution du mandat prévu à la règle 41(e)(2)(A) et (f)(1)(A) se réfère à la saisie ou à la copie sur place du support ou de l'information, et non à une copie ou à un examen ultérieur hors site.
**(C) Mandat d'utilisation d'un dispositif de repérage - Un** mandat d'utilisation d'un dispositif de repérage doit identifier la personne ou le bien à repérer, désigner le magistrat à qui il doit être remis et préciser la durée raisonnable pendant laquelle le dispositif peut être utilisé. Cette durée ne peut excéder 45 jours à compter de la date d'émission du mandat. Le tribunal peut, pour des raisons valables, accorder une ou plusieurs prolongations pour une période raisonnable ne dépassant pas 45 jours chacune. Le mandat doit ordonner à l'agent
**(i)** réaliser toute installation autorisée par le mandat dans un délai déterminé ne dépassant pas 10 jours ;
**(ii)** effectuer toute installation autorisée par le mandat pendant la journée, à moins que le juge n'autorise expressément, pour des raisons valables, l'installation à un autre moment ; et
**(iii)** renvoie le mandat au juge désigné dans le mandat.

**(f) Exécuter et renvoyer le mandat.**

**(1) Mandat de recherche et de saisie d'une personne ou d'un bien.**

**(L'**agent qui exécute le mandat doit y inscrire la date et l'heure exactes de l'exécution.

**(B) Inventaire - Un** agent présent lors de l'exécution du mandat doit dresser et vérifier un inventaire des biens saisis. Il doit le faire en présence d'un autre agent et de la personne dont les biens ont été saisis ou dont les locaux ont été occupés. Si l'un d'eux n'est pas présent, l'agent doit dresser et vérifier l'inventaire en présence d'au moins une autre personne crédible. En cas de saisie de supports de stockage électroniques ou de saisie ou de copie d'informations stockées électroniquement, l'inventaire peut se limiter à la description des supports de stockage physiques qui ont été saisis ou copiés. L'agent peut conserver une copie des informations stockées électroniquement qui ont été saisies ou copiées.

**(C) Reçu - L'**agent qui exécute le mandat doit remettre une copie du mandat et un reçu pour les biens saisis à la personne à qui les biens ont été pris ou dans les locaux de laquelle ils ont été pris, ou laisser une copie du mandat et du reçu à l'endroit où l'agent a pris les biens. Pour un mandat permettant d'utiliser l'accès à distance pour perquisitionner des supports de stockage électroniques et saisir ou copier des informations stockées électroniquement, l'agent doit faire des efforts raisonnables pour signifier une copie du mandat et du récépissé à la personne dont les biens ont été perquisitionnés ou qui possède les informations qui ont été saisies ou copiées. La notification peut être effectuée par tout moyen, y compris électronique, raisonnablement calculé pour atteindre cette personne. **(D) Renvoi - L'**agent qui exécute le mandat doit le renvoyer rapidement - avec une copie de l'inventaire - au magistrate judge désigné sur le mandat. L'agent peut le faire par des moyens électroniques fiables. Le juge doit, sur demande, remettre une copie de l'inventaire à la personne dont les biens ont été saisis ou dont les locaux ont été saisis, ainsi qu'au demandeur du mandat.

**(2) Mandat pour un dispositif de repérage.**

**(L'**agent qui exécute un mandat d'utilisation d'un dispositif de localisation doit y inscrire la date et l'heure exactes auxquelles le dispositif a été installé, ainsi que la période pendant laquelle il a été utilisé.

**(B) Restitution - Dans les** 10 jours suivant la fin de l'utilisation du dispositif de localisation, l'agent chargé de l'exécution du mandat doit le restituer au juge désigné dans le mandat. L'agent peut le faire par des moyens électroniques fiables.

**(C) Signification - Dans les** dix jours suivant la fin de l'utilisation du dispositif de localisation, l'agent chargé de l'exécution d'un mandat relatif à un dispositif de localisation doit signifier une copie du mandat à la personne qui a été localisée ou dont les biens ont été localisés. La notification peut être effectuée en remettant une copie à la personne qui a été suivie ou dont les biens ont été suivis, ou en laissant une copie à la résidence de la personne ou à son lieu de séjour habituel à une personne d'âge et de discrétion appropriés qui réside à cet endroit, et en envoyant une copie par la poste à la dernière adresse connue de la personne. À la demande du gouvernement, le juge peut retarder la notification conformément à la règle 41(f)(3).

**(3) Notification différée : à la** demande du gouvernement, un magistrate judge - ou, si la règle 41(b) l'autorise, un juge d'une state court of record - peut différer toute notification requise par cette règle si le délai est autorisé par la loi.

**(g) Requête en restitution de biens - Une** personne lésée par une perquisition et une saisie illégales de biens ou par la privation de biens peut demander la restitution des biens. La requête doit être déposée dans le district où les biens ont été saisis. Le tribunal doit recevoir des preuves sur toute question de fait nécessaire pour statuer sur la requête. S'il fait droit à la requête, le tribunal doit restituer le bien au requérant, mais il peut imposer des conditions raisonnables pour protéger l'accès au bien et son utilisation dans des procédures ultérieures.

**(h) Motion to Suppress - Un** défendeur peut demander la suppression d'une preuve devant le tribunal où se déroulera le procès, comme le prévoit la règle 12.

**(i) Transmission des documents au greffier - Le** magistrate judge à qui le mandat est renvoyé doit joindre au mandat une copie du rapport, de l'inventaire et de tous les autres documents connexes et les remettre au greffier du district où les biens ont été saisis.

**18 U.S.C. § 3103a**
**(a) En général -** Outre les motifs de délivrance d'un mandat visés à l'article 3103 du présent titre, un mandat peut être délivré pour rechercher et saisir tout bien constituant la preuve d'une infraction pénale commise en violation des lois des États-Unis.
**(b) Délai - En ce qui concerne** la délivrance d'un mandat ou d'une ordonnance judiciaire en vertu de la présente section, ou de toute autre règle de droit, pour rechercher et saisir tout bien ou matériel constituant la preuve d'une infraction pénale en violation des lois des États-Unis, toute notification requise ou pouvant être requise peut être retardée si

**(1)** le tribunal a de bonnes raisons de penser que la notification immédiate de l'exécution du mandat peut avoir des conséquences négatives (au sens de l'article 2705, sauf si ces conséquences négatives consistent uniquement à retarder indûment un procès) ;
**(2)** le mandat interdit la saisie de tout bien corporel, de toute communication par fil ou électronique (telle que définie à l'article 2510) ou, sauf disposition expresse du chapitre 121, de toute information par fil ou électronique stockée, sauf si le tribunal estime que la saisie est raisonnablement nécessaire ; et
**(3)** le mandat prévoit l'envoi d'une telle notification dans un délai raisonnable ne dépassant pas 30 jours après la date de son exécution, ou à une date ultérieure certaine si les faits de l'espèce justifient un délai plus long.
**(Toute** période de retard autorisée par la présente section peut être prolongée par le tribunal pour des motifs valables, sous réserve que les prolongations ne soient accordées que sur la base d'une démonstration actualisée de la nécessité d'un retard supplémentaire et que chaque retard supplémentaire soit limité à des périodes de 90 jours ou moins, à moins que les faits de l'affaire ne justifient une période de retard plus longue.
**(d) Rapports.**
**(1) Rapport du juge - Au plus tard** 30 jours après l'expiration d'un mandat autorisant une notification différée (y compris toute extension de celui-ci) délivré en vertu de la présente section, ou le refus d'un tel mandat (ou d'une demande d'extension), le juge qui a délivré ou refusé le mandat doit faire un rapport au bureau administratif des tribunaux des États-Unis...
**(A)** le fait qu'un mandat a été demandé ;
**(B) le** fait que le mandat ou toute extension de celui-ci a été accordé tel que demandé, a été modifié ou a été refusé ;
**(C)** le délai de préavis autorisé par le mandat, ainsi que le nombre et la durée des prorogations éventuelles ; et
**(D)** l'infraction spécifiée dans le mandat ou la demande.
**(2) Rapport du bureau administratif des** tribunaux des États-Unis : à compter de l'exercice fiscal se terminant le 30 septembre 2007, le directeur du bureau administratif des tribunaux des États-Unis transmet chaque année au Congrès un rapport complet résumant les données qui doivent être déposées auprès du bureau administratif en vertu du paragraphe (1), y compris le nombre de demandes de mandats et d'extensions de mandats autorisant une notification tardive, et le nombre de ces mandats et extensions accordés ou refusés au cours de l'exercice fiscal précédent.
**(3) Réglementation - Le** directeur de l'Office administratif des tribunaux des États-Unis, en consultation avec le procureur général, est autorisé à publier des réglementations contraignantes concernant le contenu et la forme des rapports devant être déposés en vertu du paragraphe (1).

## 10.2 Aperçu des réponses au questionnaire[90]

| | | |
|---|---|---|
| **1.1 Veuillez donner un aperçu de la base juridique de la perquisition et de la saisie de données informatiques stockées dans votre pays.** | Les pays qui ont adopté des pouvoirs spécifiques[91] pour la recherche et la saisie de données informatiques stockées, qui peuvent également compléter les pouvoirs généraux. | Albanie, Argentine, Arménie, Australie, Autriche, Belgique, Bénin, Brésil, Bulgarie, Cabo Verde, Cameroun, Canada, Chypre, Croatie, République dominicaine, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Israël, Italie, Japon, Kiribati, Lettonie, Liechtenstein, Luxembourg, Malte, Maurice, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Panama, Philippines, Pologne, Portugal, Roumanie, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Royaume-Uni, États-Unis. |
| | Les pays qui s'appuient largement sur les pouvoirs généraux[92] de leur législation mais qui peuvent, dans certains cas, avoir des pratiques ou des procédures opérationnelles pour appliquer ces pouvoirs à la perquisition et à la saisie de données informatiques stockées | Andorre, Azerbaïdjan, Bosnie-Herzégovine, , Chili, Colombie, Costa Rica, République tchèque, Danemark, Estonie, Islande, Lituanie, Maroc, Norvège, Pérou, Paraguay, République de Moldavie, Saint-Marin, Ukraine |
| **1.2 Les pouvoirs de perquisition et de saisie des données informatiques stockées s'appliquent-ils uniquement aux infractions commises à l'encontre ou au moyen d'ordinateurs ou** | Toutes les infractions pour lesquelles les preuves se trouvent sur un système informatique | Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Cameroun, Chili, Colombie, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Japon, Kiribati, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Moldavie, Monaco, Monténégro, Maroc, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Panama, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, |

[90] Le lecteur ne doit pas se fier à la matrice seule, car il n'a pas été possible de refléter les ambiguïtés et les nuances des législations nationales dans un simple tableau.

[91] Le "pouvoir spécifique" peut être une loi, une ordonnance, une règle ou un règlement ayant force obligatoire en vertu du droit national et prévoyant spécifiquement la perquisition et la saisie de données et de systèmes informatiques.

[92] Le "pouvoir général" peut être tout statut, loi, ordonnance, règle, règlement ayant une force contraignante qui ne mentionne pas spécifiquement la perquisition et la saisie de données et de systèmes informatiques.

| | | |
|---|---|---|
| **également à d'autres infractions prévues par votre droit interne lorsque les preuves se trouvent sur un système informatique ?** | | Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| | Certaines infractions pour lesquelles les éléments de preuve se trouvent sur un système informatique | Albanie, Andorre, Israël, Lettonie |
| | Uniquement les infractions commises à l'encontre ou au moyen d'ordinateurs | |
| **1.3 Qu'entendez-vous par "données informatiques stockées" ?** | Définition spécifique dans un texte | Australie, Bulgarie, Cabo Verde, Chili, Finlande, Allemagne, Lituanie, Malte, Moldavie, Pays-Bas, Sénégal, Sri Lanka, Suisse |
| | Pas de définition spécifique dans un texte | Andorre, Argentine, Arménie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cameroun, Canada, Costa Rica, Croatie, Chypre, Danemark, République dominicaine, Estonie, Fidji, France, Géorgie, Ghana, Grèce, Hongrie, Israël, Italie, Japon, Kiribati, Liechtenstein, Lituanie, Maroc, Maurice, Monaco, Nigeria, Macédoine du Nord, Norvège, Panama, Pérou, Pologne, Portugal, Roumanie, Saint-Marin, Sierra Leone, République slovaque, Espagne, Suède, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| | Définition tirée d'une autre source de droit | Albanie, Australie, Colombie, Liechtenstein, Pays-Bas, Paraguay, Philippines, Serbie, Suisse |

| | | |
|---|---|---|
| **1.4 Existe-t-il des exigences en matière de notification de l'exercice des pouvoirs en vertu de l'article 19 ? Dans l'affirmative, veuillez fournir un résumé (y compris la législation, les décisions de justice et les pratiques).** | Pays ayant des obligations de notification de quelque nature que ce soit [93] | Albanie, Andorre, Argentine, Australie, Autriche, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cameroun, Canada, Chili, Costa Rica, Croatie, République tchèque, Danemark, République dominicaine, Estonie, Finlande, France, Géorgie, Allemagne, Grèce, Islande, Israël, Italie, Japon, Kiribati, Liechtenstein, Lituanie, Luxembourg, Monaco, Monténégro, Pays-Bas, Macédoine du Nord, Norvège, Panama, Paraguay, Pérou, Pologne, Portugal, Saint-Marin, Sénégal, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Türkiye, États-Unis. |
| | Pays ayant ajouté des informations supplémentaires | Andorre, Australie, Bénin, Finlande, Géorgie, Norvège, Pays-Bas, Pologne, Portugal, Slovénie, Sri Lanka |
| **2.1.1 Veuillez résumer les mesures législatives et autres prises par votre pays pour garantir que les autorités puissent perquisitionner ou accéder de la même manière aux systèmes informatiques, aux données et aux supports de stockage de** | Une ordonnance judiciaire est nécessaire [94] | Albanie, Andorre, Argentine, Arménie, Australie, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde (dans la plupart des cas, bien que la législation prévoie des exceptions), Cameroun, Canada, Chili, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Israël, Italie, Japon, Kiribati, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Moldavie, Monaco, Monténégro, Maroc, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Sénégal, Serbie, Sierra Leone, République |

[93] La plupart des pays prévoient une notification traditionnelle pour les perquisitions et les saisies. Certains pays ont prévu des dispositions spéciales de notification pour la recherche et la saisie de données. Compte tenu de la diversité et de la sophistication des exigences en matière de notification, il est conseillé aux lecteurs d'examiner les réponses initiales des pays.

[94] Dans cette matrice, une décision de justice comprend une décision d'un juge d'instruction ou d'un juge similaire.

| | | |
|---|---|---|
| **données sur votre territoire, conformément à l'article 19.1. En réponse, veuillez résumer les conditions à remplir et les étapes de la procédure généralement suivies pour obtenir l'autorisation de procéder à une telle perquisition.** | | slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| | Aucune décision de justice n'est nécessaire | Autriche, Belgique, Bénin, Canada, Colombie, Danemark, Estonie, Finlande, Ghana, Grèce, Hongrie, Malte, Monaco, Maroc, Macédoine du Nord, Norvège, Pologne, Portugal, Sénégal, République slovaque, Suède, Suisse, Türkiye |
| **2.1.2 Des règles particulières s'appliquent-elles en cas d'urgence ou d'autres circonstances urgentes ? Dans l'affirmative, veuillez décrire ces règles et l'interprétation applicable de ce qui constitue une situation d'urgence.** | Pays qui définissent l'urgence dans un texte | Australie, Argentine, Autriche, Azerbaïdjan, Bosnie-Herzégovine, Canada, Croatie, République tchèque, République dominicaine, Estonie, France, Géorgie, Allemagne, Hongrie, Islande, Luxembourg, Malte, Moldavie, Monaco, Maroc, Macédoine du Nord, Norvège, Pologne, Saint-Marin, Serbie, Espagne, Sri Lanka, Suisse, Ukraine, Royaume-Uni, États-Unis. |
| | Pays qui s'appuient sur une autre source de droit pour gérer les situations d'urgence | Albanie, Andorre, Belgique, Bénin, Brésil, Bulgarie, Canada, Costa Rica, Chypre, Danemark, Estonie, Finlande, Ghana, Grenade, Israël, Japon, Lituanie, Maurice, Nigeria, Panama, Roumanie, Slovénie, Tonga, Türkiye |
| | Pays dont les autorités peuvent agir sans décision de justice dans une urgence | Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Croatie, Danemark, Estonie, Finlande, France, Géorgie, Ghana, Hongrie, Italie, Lituanie, Luxembourg, Malte, Moldavie, Maroc, Macédoine du Nord, Norvège, Pays-Bas, Pologne, Saint-Marin, Serbie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, États-Unis. |
| **2.1.3 Votre législation habilite-t-elle vos autorités compétentes à perquisitionner ou à accéder de la même** | Oui | Andorre, Arménie, Australie, Autriche, Belgique, Brésil, Bulgarie, Cameroun, Canada, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Ghana, Grèce, Grenade, Islande, Israël, Italie, Japon, Kiribati, Liechtenstein, Luxembourg, Maurice, Moldavie, Monaco, Monténégro, Pays-Bas, Nigeria, |

| | | | |
|---|---|---|---|
| **manière à un système informatique et aux données qu'il contient en utilisant des références d'accès légalement acquises ? En répondant à cette question, veuillez résumer les conditions à remplir et les mesures généralement prises pour exercer ce pouvoir.** | | Macédoine du Nord, Maurice, Panama, Philippines, Pologne, Roumanie, Saint-Marin, Sénégal, Serbie, Sierra Leone, Slovénie, Suisse,[95] Espagne, Suède, Tonga, Ukraine, États-Unis. | |
| | Non | Albanie, Azerbaïdjan, Bosnie-Herzégovine, Chili, Colombie, Hongrie, Lettonie, Malte, Norvège, Philippines, Portugal, République slovaque, Sri Lanka, Türkiye, Royaume-Uni | |
| **2.1.4 Votre législation habilite-t-elle vos autorités compétentes à perquisitionner ou à accéder de la même manière à un système informatique et aux données qu'il contient en utilisant un accès à distance secret ? Dans votre réponse, veuillez résumer les conditions à remplir et les mesures** | Non | Albanie, Arménie, Autriche, Azerbaïdjan, Bénin, Bosnie-Herzégovine (y compris l'entité de la Fédération de Bosnie-Herzégovine), Brésil, Bulgarie, Cabo Verde, Cameroun, Colombie, Costa Rica, Chypre, République dominicaine, Ghana, Grenade, Israël, Japon, Malte, Maurice, Monaco, Panama, Portugal, Sierra Leone, République slovaque, Sri Lanka, Suisse, Ukraine, Royaume-Uni. | |
| | Oui | Oui (sans plus de détails) | Bosnie-Herzégovine (applicable à l'Entité de la Republika Srpska), Italie, Liechtenstein, Luxembourg, Macédoine du Nord, Pologne, Roumanie, Saint-Marin |

[95] Cela relève non pas de la législation mais de la jurisprudence.

| | | | |
|---|---|---|---|
| **généralement prises pour exercer ce pouvoir.** | | | |
| | | Disponible pour toutes les infractions | |
| | | Disponible uniquement pour certaines infractions | Andorre, Argentine (dans certaines juridictions), Australie, Belgique, République tchèque, Danemark, Estonie, Finlande, France, Géorgie, Allemagne, Hongrie, Islande, Lettonie, Lituanie, Moldavie, Monaco, Monténégro, Pays-Bas, Norvège, Serbie, Slovénie, Espagne, Suède, Tonga, Türkiye. |
| | | Possible dans des circonstances particulières, telles que l'utilisation par la cible d'une technologie sophistiquée | Belgique, Croatie, France, Allemagne, Monténégro, Espagne, États-Unis |
| | | Ordonnance judiciaire requise | Andorre, Argentine, Australie, Belgique, Brésil, Canada, Croatie, République tchèque, Danemark, Estonie, Fidji, Finlande, Géorgie, Allemagne, Grèce, Hongrie, Islande, Kiribati, Lettonie, Lituanie, Moldavie, Monaco, Monténégro, Pays-Bas, Nigeria, Norvège, Saint-Marin, |

| | | | | |
|---|---|---|---|---|
| | | | | Serbie, Espagne, Suède, Tonga, Türkiye, États-Unis. |
| | | | Aucune décision de justice n'est nécessaire | Grèce, Moldavie, Sénégal |
| | | | La mesure inclut la possibilité de collecter des données en temps réel | Belgique, Danemark, Estonie, France, Géorgie, Hongrie, Lettonie, Moldavie, Monaco, Norvège, Espagne, Suède, Suisse, Tonga |
| | | | Exigences en matière de notification | Australie, Belgique, Danemark, Allemagne, Lituanie, Pays-Bas |
| | | | La mesure a une durée déterminée | Costa Rica, Danemark, Estonie, Finlande, Allemagne, Israël, Pays-Bas, Macédoine du Nord, Norvège, Espagne, Suède |
| | Pays qui ont également joint des informations supplémentaires sur les exigences et l'exécution de la mesure | | Australie, Belgique, Canada, Croatie, Danemark, France, Géorgie, Hongrie, Lettonie, Lituanie, Pays-Bas, Serbie, Tonga | |
| **2.1.5 Quelles sont les autorités compétentes qui autorisent et effectuent une recherche telle que décrite à l'article 19.1 ? Quel type d'expertise technique ou autre est requis et utilisé ?** | Autorités compétentes pour autoriser une perquisition | Juge d'instruction | Andorre, Belgique, Bénin, Cameroun, Croatie, Estonie, France, Lettonie, Liechtenstein, Luxembourg, Moldavie, Monténégro, Maroc, Sénégal | |
| | | Juge | Albanie, Arménie, Australie, Azerbaïdjan, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Israël, Italie, Japon, Kiribati, Lituanie, Malte, Maurice, Monaco, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. | |

| | | | |
|---|---|---|---|
| | | | |
| | | Procureur | Autriche, Belgique, Bénin, Cameroun, Colombie, Estonie, Finlande, Grèce, Hongrie, Luxembourg, Moldavie, Monaco, Maroc, Norvège, Panama, Pologne, Portugal, Sénégal, République slovaque, Suède, Suisse, Türkiye |
| | | Officier de police | Belgique, Danemark, Finlande, France, Ghana, Hongrie, Suède, Suisse [96] |
| | Autorités compétentes pour effectuer une recherche | Procureur | Allemagne, Argentine, Azerbaïdjan, Bosnie-Herzégovine, Brésil, Cameroun, Chili, Costa Rica, Espagne, France, Hongrie, Italie, Japon, Lituanie, Moldavie, Macédoine du Nord, Norvège, Panama, Pays-Bas, Pérou, Pologne, Portugal. |
| | | Officier de police | Albanie, Andorre, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Colombie, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Israël, Italie, Japon, Kiribati, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Moldavie, Monaco, Monténégro, Maroc, Nigeria, Macédoine du Nord, Norvège, Pays-Bas, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Sénégal, Serbie, Sierra Leone, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Royaume-Uni, États-Unis. |
| | | Autre autorité spécialisée | Albanie, Andorre, Arménie, Australie, Azerbaïdjan, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Croatie, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Israël, Kiribati, Lettonie, Lituanie, Maurice, Macédoine du Nord, Nigeria, Norvège, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Serbie, Sierra Leone, République |

[96] Pour la Suisse : uniquement dans les cas d'exception prévus par la loi.

| | | | |
|---|---|---|---|
| | | | slovaque, Espagne, Sri Lanka, Suède, Suisse, Tonga, Ukraine, Royaume-Uni. |
| **2.1.6 Vos autorités ont-elles adopté des procédures opérationnelles normalisées internes ou des lignes directrices similaires pour la recherche telle que décrite à l'article 19.1 ? Si possible, veuillez en donner un aperçu et indiquer les liens accessibles au public.** | Oui | | Argentine, Autriche, Bosnie-Herzégovine (certaines institutions), Brésil, Canada, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Israël, Japon, Malte, Maurice, Moldavie, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Roumanie, Saint-Marin, Serbie, Espagne, Suède, Tonga, Royaume-Uni, États-Unis. |
| | Non | | Andorre, Arménie, Australie, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine (en général), Bulgarie, Cabo Verde, Cameroun, Chili, Costa Rica, France, Islande, Kiribati, Liechtenstein, Lituanie, Luxembourg, Monaco, Portugal, République slovaque, Slovénie. |
| **2.1.7 Veuillez fournir des exemples de décisions judiciaires pertinentes relatives aux preuves obtenues par les perquisitions décrites à l'article 19.1.** | Cas/décisions fournis | | Andorre, Belgique, Bénin, Brésil, Canada, Danemark, France, Allemagne, Hongrie, Israël, Japon, Lituanie, Luxembourg, Moldavie, Nigeria, Norvège, Saint-Marin, Espagne, Suède, Suisse, Tonga, Royaume-Uni, États-Unis. |
| **2.2.1 Veuillez résumer les mesures législatives ou autres que vous avez prises pour garantir que vos autorités sont en mesure d'étendre la** | Prévu dans la législation | | Albanie, Allemagne, Arménie, Australie, Belgique, Bénin, Cabo Verde, Croatie, Fidji, France, Ghana, Grèce, Hongrie, Israël, Japon, Kiribati, Lettonie, Luxembourg, Maurice, Monaco, Monténégro, Maroc, Nigeria, Macédoine du Nord, Norvège, Pays-Bas, Philippines, Pologne, Portugal, Roumanie, Royaume-Uni, Sénégal, Sierra Leone, Slovénie, Espagne, Sri Lanka, Suède, Tonga, Türkiye, États-Unis. |

| | | | |
|---|---|---|---|
| **recherche telle que décrite à l'article 19.2.** | Peut obtenir des données à partir d'un webmail | Allemagne, Pays-Bas | |
| | Ordonnance judiciaire requise | oui | Albanie, Andorre, Arménie, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Allemagne, Grèce, Islande, Israël, Japon, Kiribati, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Paraguay, Pérou, Philippines, Pologne, Roumanie, Saint-Marin, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| | | non | Autriche, Danemark, Estonie, Ghana, Grèce, Hongrie, Luxembourg, Moldavie, Monaco, Norvège, Pologne, Suisse |
| **2.2.2 Veuillez résumer la procédure (y compris les autorisations requises et les techniques d'investigation appliquées) pour étendre une recherche ou un accès similaire à un autre système dans la pratique.** | Le pays utilise la même procédure que pour les autres recherches | Albanie, Andorre, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Ghana, Grèce, Grenade, Hongrie, Islande, Italie, Japon, Kiribati, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Monaco, Monténégro, Macédoine du Nord, Nigeria, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Portugal, Saint-Marin, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Sri Lanka, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. | |

| | | |
|---|---|---|
| | La mesure est appliquée à des données qui ne se trouvent pas sur le territoire du pays effectuant la recherche (à l'aide d'autorisations obtenues légalement ou autrement). | Andorre, Autriche, Azerbaïdjan, Belgique, Bénin, Brésil, Espagne, Estonie, Ghana, Islande, Luxembourg, Monaco, Nigéria, Pays-Bas, Pologne, Sénégal |
| **2.2.3 Veuillez résumer la manière dont votre cadre juridique applique l'élément "motifs de croire" de l'article 19, paragraphe 2, y compris la manière dont les autorités compétentes établissent généralement qu'elles ont des "motifs de croire" que les données recherchées sont stockées dans un autre système informatique ou une partie de celui-ci sur son territoire.** | Défini dans un texte traitant des perquisitions et saisies électroniques | Bénin, Bosnie-Herzégovine, France, Allemagne, Japon, Luxembourg, Monténégro, Espagne, Sri Lanka, Suède, Tonga |
| | 1) Exigences spécifiées dans une autre source de droit ou 2) source d'exigences non indiquée | Albanie, Andorre, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Costa Rica, Croatie, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, Géorgie, Ghana, Grèce, Hongrie, Israël, Italie, Japon, Kiribati, Liechtenstein, Luxembourg, Malte, Maurice, Monaco, Moldavie, Pays-Bas, Macédoine du Nord, Nigeria, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Suisse, Türkiye, Royaume-Uni, États-Unis. |
| **2.2.4 Veuillez résumer la manière dont votre cadre juridique applique l'élément "sur son territoire" de l'article 19.2, en indiquant notamment si votre cadre impose ou non une exigence positive selon laquelle le système** | Le cadre impose une exigence positive que le système connecté se trouve sur le territoire du pays qui exécute la mesure. | Arménie, Bosnie-Herzégovine (y compris entité de la Fédération de Bosnie-Herzégovine), Bulgarie, Canada, Costa Rica, Grèce, Grenade, Kiribati, Lettonie, Maurice, Macédoine du Nord, Paraguay, Philippines, Saint-Marin, Tonga, USA |
| | Le cadre n'impose pas que le système connecté se trouve dans le pays qui exécute la mesure. | Albanie, Andorre, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine (applicable à l'entité de la Republika Srpska et au district de Brcko), Brésil, Cabo Verde, Chili, Croatie, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, |

| | | |
|---|---|---|
| **connecté doit se trouver sur votre territoire.** | | Allemagne, Ghana, Hongrie, Islande, Israël, Italie, Japon, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Moldova, Monaco, Monténégro, Pays-Bas, Nigéria, Norvège, Pérou. Pologne, Portugal, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Suède, Suisse, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| **2.2.5 Comment procédez-vous lorsqu'il n'est pas possible de déterminer où les données recherchées sont stockées ("perte de (connaissance de) situations de localisation") ?** | Le pays continue à faire comme si les données se trouvaient sur son territoire | Allemagne, Australie, Autriche, Bénin, Bosnie-Herzégovine, Brésil, Croatie, Danemark, Espagne, Estonie, France, Grèce, Hongrie, Italie, Luxembourg, Moldavie, Monaco, Nigéria, Pays-Bas, Philippines, Pologne, Portugal, République dominicaine, République tchèque, Sénégal, Serbie, Slovénie, Suisse, Türkiye. |
| | Le pays cesse d'exploiter ces données | Canada, Chili, Costa Rica, Grenade, Kiribati, Paraguay, Pérou, Saint-Marin, Sierra Leone, République slovaque |
| | Décidé au cas par cas | Andorre, Belgique, Bulgarie, Finlande, Ghana, Israël, Japon, Lettonie, Maurice, Norvège, Saint-Marin, Sri Lanka, Suède, Royaume-Uni, USA |
| **2.2.6 Veuillez fournir des exemples typiques (cas d'utilisation) pour l'extension d'une recherche.** | Cas/décisions fournis | Andorre, Arménie, Autriche, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, République tchèque, Estonie, France, Allemagne, Ghana, Hongrie, Islande, Japon, Liechtenstein, Lituanie, Luxembourg, Pays-Bas, Norvège, Paraguay, Pérou, Pologne, Portugal, Serbie, République slovaque, Slovénie, Espagne, Suède, Tonga, Türkiye, États-Unis. |
| **2.2.7 Veuillez fournir des exemples de décisions judiciaires pertinentes relatives à l'extension d'une perquisition à un système informatique connecté.** | Cas/décisions fournis | Allemagne, Belgique, Bénin, Brésil, France, Hongrie, Israël, Lituanie, Macédoine du Nord, Norvège, Suède, Suisse |

| | | | |
|---|---|---|---|
| **2.3.1 Veuillez résumer les mesures législatives ou autres que votre pays a prises pour s'assurer que vos autorités sont en mesure de saisir ou de sécuriser de la même manière des données informatiques telles que décrites à l'article 19.3. Dans votre réponse, veuillez résumer les conditions à remplir et les étapes de la procédure généralement suivies pour obtenir l'autorisation d'une telle saisie.** | Les pays ayant des éléments spécifiques de l'art. 19.3 dans un texte spécifique | | Albanie, Argentine, Arménie, Autriche, Belgique, Bénin, Bosnie-Herzégovine (entité de la Fédération de Bosnie-Herzégovine), Bulgarie, Cabo Verde, Cameroun, Croatie, République tchèque, République dominicaine, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Israël, Italie, Japon, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Panama, Philippines, Pologne, Portugal, Sénégal, Sierra Leone, République slovaque, Espagne, Sri Lanka, Suède, Suisse, Tonga, . |
| | Les pays qui s'appuient sur une autre source de droit pour appliquer les éléments de l'Art. 19.3 | | Andorre, Azerbaïdjan, Belgique, Bosnie-Herzégovine (applicable au district de Brcko), Cameroun, Chili, Costa Rica, Brésil, Chypre, Danemark, Estonie, Allemagne, Ghana, Israël, Liechtenstein, Lituanie, Malte, Moldavie, Maroc, Nigeria, Norvège, Pérou, Paraguay, Saint-Marin, Serbie, Slovénie, Suède, Suisse, Ukraine, États-Unis. |
| | Les pays qui ne peuvent pas appliquer les éléments de l'Art. 19.3 | | Bosnie-Herzégovine (y compris l'entité de la Republika Srpska), Bulgarie, Canada, Danemark, Estonie, Géorgie, Ghana, Kiribati, Malte, Moldavie, Nigeria, Macédoine du Nord, Pologne, Roumanie, Suède, Suisse, Türkiye |
| **2.3.2 Appliquez-vous les mêmes mesures lors de l'extension d'une recherche (conformément à l'article 19, paragraphe 2) et dans les situations où il n'est pas possible de déterminer où les données recherchées sont stockées ?** | Oui | | Albanie, Andorre, Arménie, Australie, Belgique, Bénin, Bosnie-Herzégovine, Bulgarie, Cabo Verde, Canada, Chili, Costa Rica, Croatie, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Allemagne, Ghana, Grèce, Hongrie, Israël, Italie, Japon, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Moldavie, Monaco, Pays-Bas, Nigeria, Macédoine du Nord, Nigeria, Norvège, Panama, Pérou, Philippines, Pologne, Sénégal, Serbie, Sierra Leone, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Royaume-Uni, États-Unis. |
| | Non | | Kiribati, Grenade |
| **2.3.3 Quelles sont les autorités compétentes qui** | Autorités qui autorisent une saisie | Juge | Albanie, Argentine, Arménie, Australie, Azerbaïdjan, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Chili, Colombie, Costa Rica, Croatie, |

| | | | |
|---|---|---|---|
| **autorisent et effectuent une saisie telle que décrite à l'article 19.3 ? Quel type d'expertise technique ou autre est requis et utilisé ?** | | | Chypre, République tchèque, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Grenade, Hongrie, Islande, Israël, Italie, Japon, Kiribati, Lituanie, Malte, Maurice, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Roumanie, Saint-Marin, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Ukraine, Royaume-Uni, États-Unis. |
| | | Juge d'instruction | Andorre, Belgique, Bénin, Cameroun, Croatie, Estonie, France, Lettonie, Liechtenstein, Luxembourg, Moldavie, Maroc, Sénégal[97] |
| | | Procureur | Autriche, Belgique, Bénin, Cameroun, Chili, Estonie, Finlande, Grèce, Hongrie, Luxembourg, Moldavie, Monaco, Maroc, Norvège, Pays-Bas, Pologne, Portugal, Sénégal, République slovaque, Suède, Suisse, Türkiye |
| | | Officier de police | Belgique, Finlande, France, Ghana, Hongrie, Islande, Norvège, Suède |
| | Les autorités qui effectuent une saisie | Procureur | Allemagne, Argentine, Azerbaïdjan, Bosnie-Herzégovine, Brésil, Cameroun, Costa Rica, Espagne, Hongrie, Italie, Japon, Lituanie, Moldavie, Macédoine du Nord, Norvège, Panama, Paraguay, Pays-Bas, Pérou, Pologne, République dominicaine, Roumanie. |
| | | Officier de police | Albanie, Andorre, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Cameroun, Canada, Colombie, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Fidji, Finlande, France, Géorgie, Allemagne, Ghana, Grèce, Hongrie, Islande, Israël, Italie Japon, Kiribati, Liechtenstein, Lituanie, Luxembourg, Malte, Maurice, Moldavie, Monaco, Monténégro, Pays-Bas, Nigeria, Macédoine du Nord, Norvège, Pérou, Philippines, Pologne, Portugal, Roumanie, Saint-Marin, Sénégal, |

[97] Sénégal : un juge d'instruction peut également exécuter la perquisition.

| | | | |
|---|---|---|---|
| | | | Serbie, Sierra Leone, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Royaume-Uni, États-Unis. |
| | | Autre autorité spécialisée | Albanie, Andorre, Arménie, Australie, Azerbaïdjan, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Cabo Verde, Canada, Costa Rica, Croatie, Danemark, République dominicaine, Estonie, Fidji, Finlande, France, Géorgie, Ghana, Grèce, Grenade, Hongrie, Israël, Kiribati, Lituanie, Malte, Maurice, Monténégro, Nigeria, Macédoine du Nord, Norvège, Philippines, Pologne, Saint-Marin, Serbie, Sierra Leone, République slovaque, Espagne, Sri Lanka, Suède, Suisse, Tonga, Türkiye, Royaume-Uni. |
| **2.3.4 Veuillez fournir des exemples typiques (cas d'utilisation) et des décisions de justice pertinentes.** | Cas/décisions fournis | | Andorre, Arménie, Belgique, Bénin, Bosnie-Herzégovine, Brésil, République tchèque, France, Allemagne, Hongrie, Japon, Lituanie, Luxembourg, Maurice, Macédoine du Nord, Pérou, Suisse, Tonga, Türkiye, États-Unis. |
| **2.4.1 Veuillez résumer les mesures législatives ou autres prises par votre pays pour garantir que vos autorités sont en mesure d'ordonner à une personne de fournir les informations nécessaires décrites à l'article 19, paragraphe 4. Veuillez résumer les règles applicables à cette disposition.** | Défini dans un texte traitant des perquisitions et saisies électroniques | | Albanie, Andorre, Arménie, Australie, Autriche, Belgique, Bosnie-Herzégovine (applicable aux entités de la Fédération de Bosnie-Herzégovine, de la Republika Srpska et du district de Brcko), Cabo Verde, Canada, Croatie, République dominicaine, Fidji, Géorgie, Ghana, Grenade, Hongrie, Japon, Kiribati, Liechtenstein, Luxembourg, Maroc, Maurice, Monaco, Macédoine du Nord, Norvège, Pays-Bas, Philippines, Portugal, Royaume-Uni, Sénégal, Serbie, Sierra Leone, République slovaque, Slovénie, Espagne, Sri Lanka, Suède, Suisse, Tonga, États-Unis. |
| | Dérivé d'une autre source de droit | | Autriche, Azerbaïdjan, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Canada, Costa Rica, Chypre, République tchèque, Danemark, Estonie, Finlande, Géorgie, Allemagne, Ghana, Hongrie, Islande, Israël, Italie, Liechtenstein, Lituanie, Malte, Moldavie, Monténégro, Nigeria, Macédoine du Nord, Panama, Pologne, Portugal, Pérou, Paraguay, Saint-Marin, Serbie, Suède, Suisse, États-Unis. |

| | | |
|---|---|---|
| **2.4.2 Veuillez fournir des exemples typiques (cas d'utilisation) et des décisions de justice pertinentes.** | Cas/décisions fournis | Andorre, Belgique, Bénin, Brésil, République tchèque, France, Allemagne, Hongrie, Israël, Japon, Lituanie, Luxembourg, Pérou, Norvège, Slovénie, États-Unis. |
| **3.1.1 Veuillez résumer les conditions et les garanties applicables lors de l'application des différentes mesures de perquisition, d'extension de la perquisition et de saisie des données informatiques stockées décrites ci-dessus.** | Presque tous les pays ont indiqué qu'ils incluaient des garanties et des protections en matière de droits de l'homme lors de la mise en œuvre de l'article 19. Cependant, les réponses des pays à cette question étaient si nombreuses et diverses qu'il était impossible de les refléter dans la matrice - certains pays ont donné des réponses générales, faisant référence aux obligations conventionnelles et constitutionnelles ; d'autres pays ont fourni de longues listes spécifiques de recours disponibles (et il n'y a pas deux listes identiques). Pour ces raisons, seule l'évaluation contient une (brève) discussion sur l'approche de chaque pays en matière de protection et de sauvegarde des droits de l'homme vis-à-vis de l'article 19. Les lecteurs intéressés par les réponses des pays à cette question doivent consulter la compilation, où ces réponses apparaissent | |