www.coe.int/cybercrime

Strasbourg, le 13 novembre 2025 T-CY (2025)10

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 :

Questionnaire sur le suivi donné par les Parties aux recommandations relatives à la mise en œuvre de l'article 19 de la Convention de Budapest, adoptées en décembre 2024

Adopté lors de la de la 33ème session plénière du T-CY (13-14 novembre 2025)

Contexte :

Le présent questionnaire a pour objectif de permettre à la plénière du T-CY d'examiner les mesures de suivi prises par les Parties à la Convention de Budapest concernant les recommandations relatives à la mise en œuvre de l'article 19 de la Convention de Budapest, adoptées par le T-CY en décembre 2024. Le T-CY avait convenu que :

"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."

Les recommandations 1 à 16 ont été considérées comme "relevant principalement de la responsabilité des autorités nationales".

Mise en œuvre :

Les représentants du T-CY sont invités à préparer/compiler une synthèse des réponses à ce questionnaire provenant de leurs pays respectifs et à les soumettre au plus tard le **30 juin 2026** sous forme électronique, en anglais ou en français, à l'adresse T-CY.secretariat@coe.int.

Le Bureau fournira un aperçu initial lors la 35éme Plénière du T-CY (fin 2026) ainsi qu'un rapport provisoire complet pour le printemps 2027 pour examen par la 36éme Plénière du T-CY (mi-2027).

Question 1 : Veuillez fournir des informations sur les mesures prises, les initiatives ou les développements pertinents en rapport avec les recommandations suivantes. Vous pouvez également joindre des documents justificatifs illustrant les progrès réalisés, le cas échéant (par exemple, lois, politiques, documents d'orientation, jurisprudence, rapports, statistiques, etc.).

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.
Mesures prises/ développements pertinents:	
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[1] 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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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

[1] Ceci est sans préjudice du paragraphe 22 du Rapport explicatif.

	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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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).
Mesures prises/ développements pertinents:	
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.).
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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 : - les conditions à remplir ou les mesures à prendre pour acquérir légalement des titres conformément au droit interne d'une partie ; - 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.).
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	

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.
Mesures prises/ développements pertinents:	
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.
Mesures prises/ développements pertinents:	
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 oeuvre 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).
Mesures prises/ développements pertinents:	

Question 2 : Informations supplémentaires (le cas échéant)

Veuillez fournir toute autre information pertinente, tout développement, toute bonne pratique ou tout enseignement tiré depuis l'évaluation de l'article 19. Vous pouvez également joindre des documents justificatifs, s'ils sont disponibles (par exemple, lois, politiques, documents d'orientation, jurisprudence, rapports, statistiques, etc.).
Réponse de la partie :