www.coe.int/cybercrime

Strasbourg, version du 25 octobre 2018 T-CY (2018)26

Comité de la Convention Cybercriminalité (T-CY)

Préparation d'un Deuxième Protocole additionnel à la Convention de Budapest sur la cybercriminalité

Conditions d'obtention des informations sur les abonnés concernant les adresses IP dynamiques par rapport aux adresses IP statiques : vue d'ensemble des décisions judiciaires et des développements pertinents

Document de travail
préparé par le Secrétariat en coopération
avec les membres du Groupe de rédaction du Protocole du T-CY

Table des matières

Personne à contacter :

Alexander Seger
Secrétaire exécutif
Comité de la Convention Cybercriminalité (T-CY)
Direction Générale Droits de l'Homme et État de droit
Conseil de l'Europe, Strasbourg, France

Tél : +33-3-9021-4506
Fax : +33-3-9021-5650
Courriel : alexander.seger@coe.int

1 Objet

Le Comité de la Convention Cybercriminalité (T-CY) réfléchit depuis plusieurs années aux moyens effectifs d'obtenir les données relatives aux abonnés, compte tenu de l'importance de cette information pour les enquêtes pénales.

En 2014, le T-CY a réalisé une enquête sur les Règles concernant l'obtention de données relatives aux abonnés et, en 2017, le T-CY a adopté une Note d'orientation sur les injonctions de production concernant des informations sur les abonnés, conformément à l'article 18 de la Convention de Budapest.

Le Groupe du T-CY sur les preuves dans le Cloud a aussi recommandé en 2016 de distinguer les différents types de données recherchées :

- les « données relatives aux abonnés », c'est-à-dire les informations permettant d'identifier l'utilisateur d'une adresse IP spécifique ou, à l'inverse, les adresses IP utilisées par une personne précise. Les données relatives aux abonnés comprennent également les données tirées de bureaux d'enregistrement sur les déposants de noms de domaines ;
- les « données relatives au trafic », c'est-à-dire les fichiers où sont enregistrées les activités du système d'exploitation d'un ordinateur ou d'autres logiciels ou les communications entre des ordinateurs, en particulier lorsqu'il s'agit de l'expéditeur ou du destinataire de messages ;
- les « données relatives au contenu », par exemple les messages électroniques, images, films, musique et documents. Il y a lieu de faire la distinction entre les données relatives au contenu « conservées », c'est-à-dire les données déjà disponibles sur un système informatique, et les données relatives au contenu « futures », qui ne sont pas encore disponibles et qui devront être obtenues en temps réel.

De nouvelles solutions permettant d'obtenir des informations sur les abonnés via la coopération directe avec les fournisseurs de services et/ou par le biais d'une entraide judiciaire accélérée doivent être développées dans le cadre de la négociation d'un nouveau Protocole Additionnel à la Convention de Budapest.

Néanmoins, au vu de plusieurs décisions de justice concernant la nature de l'information sur les abonnés concernant les adresses IP dynamiques par rapport aux adresses IP statiques, en juillet 2018, la Plénière du T-CY sur la rédaction du Protocole :

> a pris note des développements nationaux et internationaux pertinents, notamment des décisions de justice et des règles de procédure concernant les informations relatives aux abonnés, et des difficultés que pose la délimitation des différentes catégories d'informations et de leurs relations réciproques, ainsi que des préoccupations exprimées par certains délégués au sujet des restrictions croissantes qui s'appliquent à l'obtention des informations sur les abonnés, et invité le Secrétariat à préparer en coopération avec les Parties intéressées un document de travail bref sur la question des informations sur les abonnées concernant les adresses IP dynamiques par rapport aux adresses IP statiques en vue de la réunion du Groupe de rédaction du Protocole qui aura lieu du 17 au 19 septembre 2018.

Le présent document de travail examine la question de savoir si les informations sur les abonnés concernant les adresses IP dynamiques doivent être considérées comme des données relatives au trafic – ou comme équivalentes à ces données – et si, par conséquent, les règles concernant l'obtention des données relatives au trafic (et non les règles concernant l'obtention des informations sur les abonnés) peuvent s'appliquer aux adresses IP dynamiques.

Cela est lié à la question plus générale de savoir :

- s'il serait justifié d'abaisser le seuil d'obtention des informations sur les abonnés concernant à la fois les adresses IP statiques et dynamiques ;
- si les restrictions s'appliquant à la conservation des données relatives au trafic et l'accès aux données conservées devraient s'appliquer également aux informations sur les abonnés ;
- si la divulgation d'informations sur les abonnés par un fournisseur de services porterait atteinte au droit à la protection des données, ainsi qu'au droit au secret des communications.

2 Données relatives au trafic et informations sur les abonnés dans la Convention de Budapest

2.1 Informations sur les abonnés concernant les adresses IP dynamiques par rapport aux adresses IP statiques

Les informations sur les abonnés constituent le type de données le plus fréquemment recherché par les organes de justice pénale dans les enquêtes sur la cybercriminalité et d'autres affaires impliquant des preuves électroniques.

Les données recherchées sont généralement les suivantes :

- les données concernant l'adresse IP associée à un compte particulier ou un site web, ou des données similaires utilisées pour commettre une infraction pénale. Les données concernant l'adresse IP comprennent l'adresse IP utilisée pour créer le compte, la dernière adresse IP de connexion ou l'adresse IP utilisée à un moment particulier ;

- les informations sur les abonnés liées à une adresse IP spécifique utilisée pour commettre une infraction pénale.

Une adresse IP statique est stable et attribuée à un abonné particulier pour la durée de la fourniture du service (comme un numéro de téléphone), et un fournisseur de services peut donc rechercher cette information dans la base de données de ses abonnés. Cependant, un fournisseur de services peut aussi attribuer une adresse IP à plusieurs utilisateurs de façon dynamique[1] et une marque temporelle est alors nécessaire pour déterminer à quel abonné l'adresse IP a été attribuée à un moment spécifique.

Pour ce faire, un fournisseur de services devra examiner ou analyser les données relatives au trafic de nombreux utilisateurs. En vertu de la jurisprudence de certains tribunaux, le fait d'examiner les données relatives au trafic peut en tant que tel être considéré comme une atteinte au droit au respect de la vie privée et, spécifiquement, au droit au secret des communications, et pas seulement comme une interférence avec les règles relatives à la protection des données.

[1] La raison de l'allocation dynamique des adresses IP est qu'avec la version 4 du Protocole Internet (IPv4), les numéros disponibles sont en nombre limité. Ce problème devrait être résolu lorsque le passage à la version 6 de l'IP sera plus avancé ou achevé.
Une autre complication est due à l'architecture à grande échelle Network Address Translator (NAT) qui permet d'attribuer une adresse IP à des centaines d'utilisateurs. Pour un résumé de ces questions, voir la section 5.4 du rapport du Groupe du T-CY sur les preuves dans le Cloud intitulé « Défis de l'accès de la justice pénale aux données stockées dans le nuage ».

Il convient de noter à cet égard que l'examen des données relatives au trafic pour identifier quelle adresse IP a été attribuée à un abonné à un moment particulier prendra généralement la forme d'une interrogation automatique des bases de données par le fournisseur de services et pas nécessairement celle d'une analyse des données relatives au trafic.

En outre, il serait erroné d'affirmer qu'une adresse IP dynamique – par opposition à une adresse IP statique – constitue nécessairement un élément d'une communication particulière et que l'obtention de cette adresse suffit à modifier le degré d'ingérence dans les droits d'un individu. En effet :

- Une adresse IP dynamique peut être attribuée à un abonné particulier non pas pour chaque nouvelle communication mais pour plusieurs jours ou plusieurs mois, par exemple, ou bien jusqu'à ce que l'abonné réinitialise le routeur.

- L'appareil utilisé par un abonné peut se connecter automatiquement et utiliser une adresse IP sans que l'abonné soit effectivement en train de communiquer, par exemple pour des mises à jour lorsque l'ordinateur est inactif ou pour se reconnecter à un nouveau site cellulaire en cas de déplacement. Par conséquent, les appareils communiquent les uns avec les autres sans intervention humaine et sans contenu concret.

L'obtention d'informations sur un abonné dans le cadre d'une enquête pénale – que ce soit une adresse IP dynamique ou une adresse IP statique – a un but identique, à savoir identifier l'abonné correspondant à un compte ou à un site particulier, ou l'abonné ayant utilisé une adresse IP en relation avec une infraction pénale particulière lorsque les autorités d'enquête ont déjà obtenu par d'autres moyens des informations pertinentes sur le contenu, le contexte ou la nature du délit en cause.

2.2 Dispositions de la Convention

La Convention de Budapest comprend une définition des « données relatives au trafic » et des « données relatives aux abonnés » :

> Article 1 d « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, *produites* par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;
>
> Article 18.3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
>
> a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
> b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
> c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

La Convention ne mentionne pas explicitement les adresses IP en tant qu'éléments des données relatives aux abonnés mais, compte tenu de la portée étendue de la définition figurant à l'article 18.3 (voir aussi le Rapport explicatif) et de la clause « tout autre numéro d'accès », on peut considérer que les adresses IP sont incluses dans ces données lorsque cela est nécessaire pour identifier un abonné.

En juillet 2018, le T-CY a adopté un formulaire type de demande d'entraide judiciaire en vue de l'obtention d'informations sur des abonnés. Ce document, qui vise à fournir des orientations, n'est pas contraignant mais il énumère en annexe les catégories d'informations

pouvant être demandées, en particulier « l'adresse IP utilisée pour l'enregistrement initial du compte », « l'adresse IP utilisée lors du dernier accès au compte » et « l'adresse IP utilisée pour accéder au compte pendant la période […] ».

La Convention ne mentionne pas non plus les adresses IP statiques et dynamiques et ignore cette distinction.

2.3 Règles concernant l'obtention de données relatives aux abonnés dans les Parties

Le T-CY a réalisé en 2014 une enquête sur les Règles concernant l'obtention de données sur les abonnés[2]. Initialement, le but était de préparer une note d'orientation sur cette question mais, au vu de la diversité des règles, conditions et procédures, l'information reçue des Parties a été recueillie dans un rapport séparé, qui a ensuite été adopté par le T-CY en décembre 2014.

Ce rapport montre que :

- Dans 12 Parties, les données sur les abonnés peuvent être obtenues sur demande officielle de la police. Cependant, dans trois d'entre elles (Autriche, Danemark et Slovénie), cela s'applique uniquement aux adresses IP statiques et une ordonnance du ministère public (Autriche) ou d'un juge (Danemark, Slovénie) est nécessaire pour obtenir les adresses IP dynamiques.

- Dans 8 Parties, les données sur les abonnés peuvent être obtenues sur ordre du ministère public.

- Dans 13 Parties, une ordonnance d'un juge est requise dans tous les cas (dans certains d'entre eux) ou seulement dans certains cas (par exemple pour obtenir les adresses IP dynamiques, des informations ne se limitant pas aux données de base sur les abonnés, des informations au sujet d'une communication particulière, et donc les données connexes couvertes par les règles de conservation des données).

Le rapport conclut :

> La plupart des Parties qui ont répondu au questionnaire font en effet la différence, dans leurs définitions et leurs concepts, entre « données relatives aux abonnés » et « données relatives au trafic ».
>
> Les conditions requises pour l'obtention des informations relatives aux abonnés varient toutefois selon les pays :
>
> – Dans la plupart des Parties ayant répondu au questionnaire, il apparaît que les conditions requises pour l'obtention d'informations relatives aux abonnés sont semblables ou similaires à celles requises pour l'obtention de données relatives au trafic, notamment si les données relatives aux abonnés sont associées à une adresse IP dynamique. Dans plus de la moitié des Parties en question, une autorisation judiciaire est nécessaire pour obtenir des informations relatives aux abonnés ; dans d'autres, le ministère public ou un haut responsable des services répressifs habilité peut ordonner la production de ces informations.
> – Dans d'autres Parties, les conditions requises pour l'obtention des informations relatives aux abonnés sont moins exigeantes que celles requises pour les données

[2] 28 Parties ont répondu au questionnaire.

relatives au trafic et la production d'informations relatives aux abonnés peut être ordonnée par la police ou le ministère public.

En conclusion :

- La plupart des Parties font la différence entre « données relatives aux abonnés » et « données relatives au trafic ».
- Dans certains pays, l'atteinte aux droits fondamentaux est considérée comme étant nettement différente selon qu'il s'agit de l'obtention de données relatives aux abonnés, y compris concernant une adresse IP, dans le cadre d'une enquête pénale spécifique d'une part, ou de données relatives au trafic d'autre part.
- En conséquence, dans ces pays, des règles différentes devraient-elles s'appliquer pour l'obtention des informations en question.
- Les conditions requises pour l'obtention des données relatives aux abonnés sont, à l'heure actuelle, relativement variées.
- Néanmoins, une plus grande harmonisation des règles en matière d'obtention des informations relatives aux abonnés faciliterait la coopération internationale.

Il est recommandé au T-CY :

- de favoriser une plus grande harmonisation entre les Parties concernant les conditions, les règles et les procédures d'obtention des données relatives aux abonnés ;
- d'encourager les Parties à tenir compte des observations du présent rapport lors de la refonte de leur législation interne.

3 Décisions de justice et développements internationaux pertinents

3.1 Cour constitutionnelle fédérale d'Allemagne (2012) : accès aux informations sur les abonnés aux termes de la loi sur les télécommunications

3.1.1 Résumé

Un arrêt rendu par la Cour constitutionnelle fédérale allemande en 2012 offre des aperçus utiles sur le traitement des adresses IP dynamiques par rapport aux adresses IP statiques, notamment sous l'angle de la proportionnalité. Cet arrêt, tout en distinguant entre les données relatives aux abonnés concernant les adresses IP dynamiques et les adresses IP statiques, n'assimile pas les données relatives aux abonnés concernant les adresses IP dynamiques aux données relatives au trafic. Il statue en outre que la conservation générale des données relatives aux abonnés par les fournisseurs de services n'est pas contraire à la constitution.

Suite à cet arrêt, l'Allemagne a développé un système « à double entrée » et la nouvelle disposition 100j du code de procédure pénale pourrait servir d'exemple de bonne pratique à cet égard. En vertu de cette disposition, les services répressifs peuvent exiger la production des adresses IP dynamiques et des adresses IP statiques, mais pour les adresses IP dynamiques est prévue une obligation supplémentaire de notification, qui peut être différée ou à laquelle il est possible de passer outre sous certaines conditions.

La loi sur les télécommunications a maintenant établi sur une base légale la divulgation de données aux services répressifs par les fournisseurs de services, et elle prescrit les

conditions légales sous lesquelles les services répressifs peuvent requérir des données relatives aux abonnés, y compris leurs adresses IP statiques et dynamiques.

3.1.2 Arrêt n° 1 BvR 1299/05

La Cour constitutionnelle allemande a adopté en janvier 2012 l'arrêt n° 1 BvR 1299/05 sur la constitutionnalité des articles 111 à 113 de la loi sur les télécommunications (TKG). Cette loi prévoit :

- à l'article 111 que les fournisseurs de services de télécommunication sont tenus de conserver les données relatives aux abonnés depuis le commencement d'un contrat avec un abonné jusqu'à un an après son expiration, afin de les rendre accessibles conformément aux articles 112 et 113 de la TKG ;

- à l'article 112 (accès automatisé) que les données relatives aux abonnés doivent être ouvertes à l'accès automatisé de l'Agence fédérale des réseaux (*Bundesnetzagentur*), qui peut communiquer ces données aux tribunaux, aux services répressifs, aux douanes, aux autorités de régulation financière et aux services de sécurité et de renseignement ;

- à l'article 113 (production manuelle des données) qu'un fournisseur de services de télécommunication est autorisé à divulguer des données relatives aux abonnés aux autorités chargées de l'application de la loi et de la sécurité publique et aux services de sécurité et de renseignement. Ces données incluent les adresses IP attribuées à un moment particulier, et un fournisseur de services de télécommunication peut à cette fin analyser les données relatives au trafic. Cette disposition prévoit également la production des codes d'accès (tels que mots de passe, codes PIN ou codes PUK) utilisés pour protéger l'accès aux appareils des utilisateurs finaux ou aux installations de stockage de données.

La Cour a statué que :

1. L'attribution de numéros de télécommunication aux usagers constituait une ingérence dans l'exercice du droit à l'auto-détermination informationnelle, garanti à l'article 2.1 (droit au libre développement de sa personnalité) en conjonction avec l'article 1.1 (caractère inviolable de la dignité humaine) de la Loi fondamentale[3]. Cependant, l'attribution d'adresses IP dynamiques constitue une atteinte au droit fondamental au secret des communications, garanti à l'article 10.1 de la Loi fondamentale.

   La Cour a considéré à cet égard que :

   - l'article 10.1 de la Loi fondamentale protège la confidentialité d'événements de télécommunication spécifiques ; cette protection s'applique au contenu de la communication mais ne s'étend pas à la totalité de l'information, par exemple l'attribution par un fournisseur de services d'un numéro de télécommunication à certains abonnés. L'article 10.1 de la Loi fondamentale n'est pas enfreint si l'attribution d'un numéro spécifique à un abonné permet à une autorité publique de reconstituer le contenu ou les circonstances d'événements de communication spécifiques pour les rapporter à un individu particulier. Cela vaut aussi bien pour les adresses IP statiques que pour les numéros de téléphone ;

[3] La « Loi fondamentale » (*Grundgesetz*) désigne la constitution allemande.

- il n'en va pas de même pour les adresses IP dynamiques, non parce qu'elles sont attribuées pour une communication spécifique mais parce qu'il est nécessaire à un fournisseur de services d'analyser les données relatives au trafic pour identifier l'abonné à qui a été attribuée une adresse IP à un moment particulier. C'est pourquoi la procédure manuelle envisagée à l'article 13.1 de la TKG eu égard aux adresses IP dynamiques porte atteinte au secret des communications, tel que garanti à l'article 10.1 de la Loi fondamentale.

La Cour a également noté que la procédure manuelle prévue à l'article 113 s'appliquait non seulement aux prestataires de services de communication publics mais aux personnes et entités qui fournissent commercialement ces services ou y contribuent, en particulier les fournisseurs de réseaux d'entreprise ou de réseaux sans fil dans les hôpitaux, les hôtels ou autres. En 2004, environ 400.000 fournisseurs appartenaient à cette catégorie, alors que l'obligation de permettre l'accès automatisé prévue à l'article 112 s'appliquait à quelques centaines de fournisseurs seulement.

En outre, selon les informations fournies par le gouvernement dans cette affaire, la procédure d'accès automatisée prévue à l'article 112 était celle qui, en pratique, était le plus souvent appliquée. En 2008-2009, environ 1.000 autorités publiques ont émis 4,2 millions de requêtes de divulgation de données détenues par des fournisseurs de services : ces requêtes, qui portaient sur 26,6 millions de demandes de divulgation spécifiques, ont été adressées à 120 fournisseurs.

2. Une base juridique distincte était nécessaire pour l'extraction et la transmission de données. Le fait que la TGK autorisait les fournisseurs de services à divulguer des informations sur les abonnés ne pouvait être considéré comme suffisant à cet égard. Les demandes de données des autorités de justice pénale et d'autres autorités devaient reposer sur une base légale spécifique (système « à double entrée »).

3. La procédure d'accès automatisée prévue à l'article 112 de la TKG, y compris la conservation préalable d'informations sur les abonnés aux termes de l'article 111 de la TKG, était conforme à la Loi fondamentale.

Les spécialistes de la protection des données soutenaient que l'article 111 de la TKG, qui prévoit la conservation des données relatives aux abonnés par les fournisseurs de services, allait à l'encontre de l'interdiction générale de la conservation des données, alors que le gouvernement faisait valoir que la conservation des données relatives aux abonnés, telle qu'envisagée à l'article 111, n'entraînait qu'une interférence réduite.

La Cour a statué à cet égard que :

- la conservation de données relatives aux abonnés prévue à l'article 111 de la TKG était conforme à la constitution. Les données à conserver et donc l'interférence au regard de certains droits étaient limitées et proportionnées ;

- le but de cette disposition était de rendre possible la fourniture de l'accès aux données selon les modalités prévues aux articles 112 et 113 de la TKG. Le droit à l'auto-détermination informationnelle, garanti à l'article 2.1 en conjonction avec l'article 1.1 de la Loi fondamentale, n'interdisait pas

toute forme de conservation des données mais imposait seulement un seuil de nécessité plus élevé. Étant donné que l'article 111 de la TKG réglementait la conservation de seulement certaines données précisément identifiées dans un but clairement défini, cette disposition ne tombait pas sous le coup de l'interdiction de la conservation des données. Les données relatives aux abonnés à conserver ne permettaient pas d'inférer le contenu ou le contexte plus général des communications. En outre les adresses IP statiques étaient attribuées principalement aux abonnés institutionnels et moins fréquemment aux utilisateurs individuels, ce qui limitait l'impact de la disposition. Toutefois, il était possible que la situation change avec l'IPv6[4] ;

- cette disposition constituait un moyen approprié pour atteindre un but spécifique.

La Cour a également statué que la procédure automatisée prévue à l'article 112 de la TKG était conforme à la constitution.

4. La procédure d'accès manuel aux données prévue à l'article 113 de la TKG était également conforme à la constitution à condition d'être interprétée en conformité avec elle. Cependant, la procédure prévue à l'article 113.1 ne devait pas être utilisée pour obtenir la fourniture d'adresses IP dynamiques.

5. La production des codes d'accès ne pouvait être exigée qu'à condition que soient précisées les modalités de leur utilisation ultérieure. Sous sa forme actuelle, la disposition pertinente n'était pas proportionnée et, par conséquent, contraire à la constitution.

Pour des raisons d'intérêt public, la Cour constitutionnelle n'a pas invalidé les dispositions litigieuses mais donné au législateur jusqu'au 30 juin 2013 pour adopter de nouvelles dispositions.

3.1.3 Nouvelles dispositions adoptées suite à l'arrêt de la Cour constitutionnelle

S'agissant de l'obtention des données relatives aux abonnés concernant aussi bien les adresses IP statiques que les adresses IP dynamiques aux fins des enquêtes pénales, le nouvel article 100j du code de procédure pénale allemand constitue maintenant la première porte d'un système à « double entrée ».

L'article 100j stipule que les organes chargés de l'application de la loi et les autorités de justice pénale peuvent requérir la production des données relatives aux abonnés conservées au titre des articles 95 et 111 de la TKG, lorsque cela est nécessaire pour établir les faits ou localiser un accusé. Ces données comprennent les adresses IP attribuées à un abonné à un moment spécifique (c'est-à-dire les adresses IP dynamiques). Cependant, dans le cas des

[4] Voir *Arrêt n° 1 BvR 1299/05 du 24 janvier 2012*, par. 161 : « Cependant, l'empiètement résultant de l'article 112 de la TKG serait substantiellement accru si, à l'avenir, les adresses IP étaient plus largement utilisées comme base de la communication sur internet – notamment avec l'introduction de la version 6 du protocole internet (IPv6). En effet, le degré d'empiètement associé à l'identification d'une adresse IP ne dépend pas fondamentalement – même si un certain nombre de droits fondamentaux sont ici en jeu – de la question de savoir si une adresse IP est, d'un point de vue technique, dynamique ou statique, mais du sens effectif de l'introduction de l'obligation de fournir des données à cet égard. Mais si en pratique les adresses IP statiques sont aussi attribuées dans une large mesure à des personnes privées, cela pourrait signifier que l'identité des utilisateurs d'internet est généralement ou au moins le plus souvent connue et que les événements de communication sur internet sont dés-anonymisés non seulement pour une période de temps limitée mais de façon permanente. Une possibilité aussi étendue de dés-anonymisation des communications internet va bien au-delà de ce que permet un annuaire téléphonique classique ».

adresses IP dynamiques, la personne concernée doit être notifiée, sauf si cela met en danger le but de l'enquête. La personne concernée ne sera pas non plus notifiée si cela est contraire aux intérêts protégés de tiers ou à ses intérêts propres. En cas de décision de différer la notification ou de déroger à l'obligation de notification, cette décision doit être documentée. Pour obtenir la production des codes d'accès (mots de passe des appareils et codes PUK et PIN), une décision de justice est nécessaire[5].

3.2 Cour suprême du Canada (2014) : *R. c. Spencer*

3.2.1 Résumé

Dans l'affaire *R. c. Spencer* (2014 CSC 43), la police canadienne « a découvert l'adresse de protocole Internet (IP) de l'ordinateur qu'une personne avait utilisé pour accéder à de la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de fichiers. Elle a ensuite obtenu auprès du fournisseur de services Internet (FSI), sans autorisation judiciaire préalable, les renseignements relatifs à l'abonnée à qui appartenait cette adresse IP ».

La Cour suprême du Canada a considéré qu'en l'espèce « la fouille ou la perquisition n'avait pas simplement pour objet le nom et l'adresse d'une personne qui était liée par contrat au FSI. Il s'agissait plutôt de l'identité d'une abonnée aux services Internet à qui correspondait une utilisation particulière de ces services » [nous soulignons].

> « En établissant un lien entre des renseignements particuliers et une personne identifiable, les renseignements relatifs à l'abonné peuvent compromettre les droits en matière de vie privée quant à l'identité d'une personne en tant que source, possesseur ou utilisateur des renseignements visés. Un certain degré d'anonymat est propre à beaucoup d'activités menées sur Internet et l'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives. En l'espèce, la demande de la police, dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée, visait en fait à établir un lien entre une personne précise et des activités en ligne précises [nous soulignons]. Ce genre de demande concerne, en ce qui a trait aux renseignements personnels, le droit à la vie privée relatif à l'anonymat puisqu'elle vise à établir un lien entre le suspect et des activités entreprises en ligne sous le couvert de l'anonymat, activités qui, comme on l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en matière de vie privée. »
>
> « Compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La demande faite par la police visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille. »

La Cour a jugé que cette fouille était illégale.

Néanmoins :

> « Les policiers se sont toutefois servis de ce qu'ils croyaient raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Par sa nature, la conduite des policiers en l'espèce ne serait pas susceptible de déconsidérer l'administration de

[5] On trouvera une traduction en anglais du code de procédure pénale allemand à l'adresse suivante : https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0677. Cette traduction, cependant, est en partie erronée. Par exemple, dans la version anglaise, l'article 100j porte le titre « Request for information », alors que, dans le texte original allemand, cet article est intitulé *Bestandsdatenauskunft*, c'est-à-dire « Fourniture de données relatives aux abonnés ».

> la justice. Bien que l'incidence de la conduite attentatoire sur les droits de l'accusé garantis par la Charte favorise l'exclusion de la preuve, les infractions reprochées en l'espèce sont graves. La société a un intérêt manifeste à ce que l'affaire soit jugée et à ce que le fonctionnement du système de justice demeure irréprochable au regard des individus accusés de ces infractions graves. Une mise en balance de ces trois facteurs permet de conclure que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice. L'admission de la preuve est donc confirmée. »

3.2.2 Analyse et conclusions

De même que la Cour constitutionnelle allemande qui, dans sa décision, a statué qu'une base légale distincte était nécessaire et que le fait que la divulgation était autorisée par la loi n'était pas en soi suffisant, la Cour suprême du Canada (CSC) a jugé que, bien que la loi canadienne régissant la conduite des entités commerciales au regard de la vie privée (Loi sur la protection des renseignements personnels et les documents électroniques, LPRPDE) permettait la divulgation de données, un pouvoir séparé était requis pour obtenir la divulgation de l'identité liée à l'adresse IP qui a conduit à M. Spencer (celui-ci utilisait le compte de sa sœur) dans la mesure où cette adresse permettait d'accéder à des renseignements confidentiels au sujet de ses activités sur internet. La CSC a statué qu'un autre pouvoir, fondé sur un texte de loi pertinent, était nécessaire et que cette condition aurait pu être satisfaite avec l'émission d'un mandat. Cependant, la CSC a également précisé que rien dans sa décision ne réduisait le pouvoir conféré par la *common law* aux policiers d'obtenir des renseignements sur les abonnés dans des circonstances contraignantes (sans pouvoir supplémentaire sous forme d'un mandat ou d'une autre base légale raisonnable), et que les renseignements sur les abonnés pouvaient être fournis si aucune règle de droit ne l'interdit et s'ils portent sur des éléments qui ne font pas l'objet d'une attente raisonnable en matière de vie privée.

En pratique, suite à l'arrêt rendu par la CSC dans l'affaire *R. c. Spencer*, et en l'absence de texte de loi portant spécifiquement sur l'accès aux renseignements sur les abonnés, la police cherche dans la mesure du possible à obtenir une ordonnance judiciaire, souvent une ordonnance de portée générale afin d'obtenir toute information pertinente, y compris les renseignements sur les abonnés, lorsqu'il existe des motifs raisonnables de penser qu'une infraction a été commise et que l'information pertinente est détenue ou contrôlée par la personne visée par cette ordonnance. Néanmoins, cette procédure pose à la police certaines difficultés. Le problème essentiel est que le seuil des « motifs raisonnables » ne peut toujours être atteint aux premières étapes d'une enquête où l'obtention de renseignements sur les abonnés peut être nécessaire alors que ces motifs ne sont pas encore établis.

Les problèmes qui se posent pour la police ont été examinés dans le cadre d'une consultation publique sur la sécurité nationale organisée dans l'ensemble du pays en 2016. Nombre des personnes qui ont participé à cette consultation ont fait part de leurs préoccupations au sujet des questions de protection de la vie privée que soulève l'accès de la police aux renseignements sur les abonnés. Beaucoup d'entre elles ont indiqué qu'elles pensaient que ces informations devraient bénéficier d'un haut niveau de protection et qu'une ordonnance judiciaire devrait être requise pour y avoir accès. Le domaine de préoccupation principal sous l'angle de la protection de la vie privée concernait la possibilité de mettre en relation les renseignements sur les abonnés avec d'autres données sur les activités ou la localisation des individus[6]. Cependant, le texte de loi sur la sécurité nationale soumis au parlement suite à cette consultation (Projet de loi C-59, Loi concernant des questions de sécurité nationale,

[6] Pur plus d'informations, voir le document *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*, disponible sur le site de Sécurité publique Canada (www.securitepublique.qc.ca), qui présente en détail les réponses à la consultation ; et, sur le même site, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016*, chapitre « Capacités d'enquête dans le monde numérique », ainsi que le Document de contexte, qui incluent le texte présenté au public en vue de la consultation.

2017) ne contenait aucune disposition concernant l'accès aux renseignements sur les abonnés.

3.3 Cour de Justice de l'Union européenne (2014 et 2016) : décisions relatives à la conservation des données

Les décisions préjudicielles rendues par la Cour européenne de justice (CJUE) en 2014 et 2016 au sujet de la conservation des données ne portent pas spécifiquement sur la question des données relatives aux abonnés. Ces décisions sont néanmoins pertinentes pour les raisons suivantes :

- la Directive 2006/24/CE de l'UE exige la conservation de diverses catégories de données, notamment les adresses IP attribuées aux abonnés et, par conséquent dans les États membres de l'UE, les normes concernant l'accès aux données relatives aux abonnés doivent être similaires aux normes s'appliquant à l'accès aux données relatives au trafic ;

- la conservation générale des différentes catégories de données « prises dans leur ensemble » est considérée comme une mesure disproportionnée. Cependant, la conservation ou l'accès à des catégories plus restreintes de données comme les données relatives aux abonnés dans le cadre d'une enquête pénale spécifique ne sont pas nécessairement soumis aux limites strictes établies par la CJUE.

3.3.1 Directive 2006/24/CE sur la conservation des données

En 2006, l'Union européenne a adopté la *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE* (Directive « Vie privée et communications électroniques »).

La Directive 2002/58/CE prévoit à l'article 15 que les États membres de l'UE doivent adopter des mesures pour assurer la conservation des données :

> Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la Directive /46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée [nous soulignons] lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

La Directive sur la conservation des données a pour but d'« harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de

poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne » (article 1.1 de la Directive 2006/24/CE).

L'article 1 stipule également que la Directive « s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques ».

L'article 2 définit les « données » comme suit : « les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur ».

Une distinction est donc établie entre les données relatives au trafic et les données relatives aux abonnés. Néanmoins, les catégories de données à conserver aux termes de l'article 5 incluent des données sur les abonnés :

(a) les données nécessaires pour retrouver et identifier la source d'une communication :
  (1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :
    (i) le numéro de téléphone de l'appelant ;
    (ii) le nom et l'adresse de l'abonné ou de l'utilisateur inscrit ;
  (2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :
    (i) le(s) numéro(s) d'identifiant attribué(s) ;
    (ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;
    (iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication.

En conséquence, lors de l'adoption des normes nationales sur la conservation des données et l'accès aux données, certains États membres de l'UE pourront être amenés à traiter de façon identique les données relatives au trafic et les données relatives aux abonnés.

3.3.2 Décisions préjudicielles de la CJUE (2014 et 2016)

Arrêt Digital Rights Ireland (2014)

La CJUE a invalidé en 2014 la Directive 2006/24/CE sur la conservation des données et statué en 2016 que le droit de l'Union européenne s'oppose à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Dans la décision préjudicielle rendue en 2014 au sujet des affaires jointes Digital Rights Ireland (C-293/12) et Seitlinger et autres (C-594/12), la CJUE a jugé la Directive 2006/24/CE sur la conservation des données invalide.

La CJUE a déclaré à ce propos :

> 26 (…) que les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, au titre des articles 3 et 5 de la Directive 2006/24, sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une

> communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.
>
> 27 Ces données, prises dans leur ensemble [nous soulignons], sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.

La CJUE convient que, bien que la Directive constitue une ingérence au regard des articles 7 (respect de la vie privée et familiale) et 8 (protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne, elle répond à un objectif d'intérêt général :

> 43 À cet égard, il ressort du considérant 7 de la Directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil « Justice et affaires intérieures » du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.
>
> 44 Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la Directive 2006/24, répond effectivement à un objectif d'intérêt général.

Vérifiant la proportionnalité de l'ingérence constatée, la CJUE déclare que « la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi » par la directive.

Cependant, elle note la portée étendue de la directive (qui « couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves », ce qui constitue une ingérence dans les droits fondamentaux de « la quasi-totalité de la population européenne ») et conclut que cela n'est pas strictement nécessaire.

Bien que visant à contribuer à la lutte contre la criminalité grave, la directive ne requiert aucune relation entre les données dont la conservation est prévue, non plus que l'existence d'une menace pour la sécurité publique.

La CJUE note en outre l'absence générale de limites à l'accès aux données conservées par les autorités nationales.

En conclusion :

> 69 Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la Directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte.
>
> La Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE, est invalide

Arrêt Tele2 Sverige et Watson (2016)

Les demandes de décision préjudicielle adressées à la CJUE dans les affaires jointes Tele2 Sverige (C-203/15) et Watson (C-698/15) portaient sur l'interprétation de l'article 15(1) de la Directive 2002/58/CE « Vie privée et communications électroniques » et sur la question de savoir si la décision préjudicielle rendue par la CJUE en 2014 dans l'affaire Digital Rights Ireland, qui avait invalidé la directive sur la conservation des données, affectait également la validité de la législation nationale des États membres de l'UE, spécifiquement eu égard à la réglementation sur l'accès aux données conservées.

Dans son arrêt (paragraphe 99), la CJUE répète l'observation figurant dans la décision concernant Digital Rights Ireland, à savoir que « prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées » et que « ces données fournissent les moyens d'établir (…) le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications ».

La CJUE déclare que la réglementation nationale prévoyant la conservation générale des données « excède (…) les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique » (paragraphe 107). Elle évoque ensuite la possibilité pour les États membres d'adopter des mesures de « conservation ciblée » des données :

> 108 En revanche, l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

Il n'apparaît pas clairement ce qu'une telle « conservation ciblée » signifierait en pratique et en quoi elle serait différente de la collecte en temps réel des données relatives au trafic envisagée dans la Convention de Budapest, ou des mesures adoptées par les organes de renseignement et de sécurité nationale.

La CJUE définit en outre des critères rigoureux d'accès aux données conservées, en limitant cet accès aux affaires de criminalité grave et en exigeant qu'il soit soumis au contrôle d'une autorité judiciaire ou d'une autre autorité indépendante.

Enfin, la CJUE a statué :

> 1. L'article 15, paragraphe 1, de la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques), telle que modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.
>
> 2. L'article 15, paragraphe 1, de la Directive 2002/58, telle que modifiée par la Directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

3.4 Tribunal constitutionnel du Portugal (2017) : arrêt n° 420/2017 relatif à la conservation des informations sur les abonnés

Dans son arrêt n° 420/2017, le Tribunal constitutionnel du Portugal – tout en prenant en compte les décisions de 2014 et 2016 de la CJUE sur la conservation des données – a jugé que la conservation des données relatives aux abonnés et, en particulier, des adresses IP dynamiques était conforme à la constitution.

Cet arrêt portait sur une affaire de fichiers pédopornographiques dans laquelle la demande de communication de données émanant du ministère public pour identifier l'utilisateur à qui avait été attribué une adresse IP avait été rejetée par le Tribunal de district de Lisbonne en octobre 2016 au motif que la loi n° 32/2008 sur laquelle se fondait cette demande n'était pas conforme à la constitution.

La loi n° 32/2008 transposait la Directive 2006/24/CE de l'UE sur la conservation des données dans le droit interne du Portugal. Cette directive a été invalidée par la CJUE en 2014.

Bien que la loi n° 32/2008 exigeait la conservation de toutes les catégories de données énumérées dans l'ancienne directive, le Tribunal constitutionnel a abordé la question susmentionnée uniquement au regard des « données sources », c'est-à-dire des « données concernant le nom et l'adresse de l'abonné ou de l'utilisateur enregistré auquel une adresse IP était attribuée au moment de la communication, conformément à l'article 6 et à l'article 4(1)(a)(2), et 2(b)(iii), de la loi n° 32/2008 du 17 juillet 2008 ».

Le Tribunal constitutionnel du Portugal, en se référant aux arrêts de 2014 (Digital Rights Ireland) et de 2016 (Tele2 Sverige) de la CJUE, a conclu :

- « La Cour de Justice n'est pas compétente pour statuer sur la validité des textes de la législation nationale des États membres, puisque son analyse porte uniquement

sur le texte de la directive. La validité de la loi n° 32/2008 du 17 juillet 2008 ne peut être remise en cause simplement parce que ce texte réglementaire de l'UE a été déclaré invalide. »

- Le Portugal, lors de la transposition de la Directive sur la conservation des données dans le droit interne, a mis en place un cadre complexe et détaillé, notamment au sujet de l'accès et de la protection des données conservées[7].
- « Étant donné que les dispositions adoptées au niveau national diffèrent des normes de l'UE, une décision sur la constitutionnalité de ces dispositions doit tenir compte de ces différences ».

Le Tribunal constitutionnel a jugé que les dispositions exigeant des fournisseurs de services qu'ils conservent les « données sources » (c'est-à-dire les données relatives aux abonnés, y compris les adresses IP dynamiques) pendant une période d'un an étaient conformes à la constitution.

3.5 Cour européenne des droits de l'homme (2018) : *Benedik c. Slovénie*

3.5.1 Résumé

L'arrêt *Benedik c. Slovénie* est la première décision de la Cour européenne des droits de l'homme portant sur la nature des adresses IP.

Dans cette affaire, la Cour européenne des droits de l'homme a conclu à une violation de l'article 8 de la Convention européenne des droits de l'homme, principalement parce que la loi en cause sur l'accès aux données relatives aux abonnés associées à une adresse IP dynamique, ainsi que son application en l'espèce, manquaient de clarté – et aussi parce que, dans ses conclusions, la Cour constitutionnelle slovène avait jugé que M. Igor Benedek avait renoncé dans cette affaire à l'espérance légitime de voir sa vie privée protégée.

La Cour constitutionnelle avait jugé – contrairement aux instances slovènes inférieures – que les informations sur les abonnés associées aux adresses IP dynamiques demandées par la police dans cette affaire faisaient partie d'une communication particulière qui, en principe, est protégée par la constitution slovène et pour laquelle, par conséquent, une décision de justice est normalement requise. L'article 149b(1) du code de procédure pénale slovène exige une décision de justice pour l'obtention des données relatives au trafic (y compris sur les participants et les circonstances d'une communication), tandis que les données relatives

[7] « (…) lors de la transposition de la directive dans le droit interne, le législateur portugais a : (i) défini des règles d'accès aux données, qui sont soumises à des critères de nécessité, d'adéquation et de proportionnalité, dont l'application doit aussi être contrôlée eu égard à la définition des catégories de données (article 9(1) et (4)) et limitée à une liste restreinte de personnes concernées (article 9(3)) ; (ii) défini la notion de criminalité grave (article 2(1)(g)) ; (iii) exigé l'obtention préalable, sur la demande du ministère public ou de l'autorité de police judiciaire compétente, d'une ordonnance judiciaire d'accès aux données (article 9(2)) ; (iv) institué des obligations spécifiques quant à la protection et à la sécurité des données, notamment la création d'un outil logiciel appelé "système pour l'accès aux données et l'obtention de données des fournisseurs de communications » (SAPDOC) permettant la communication et l'accès aux données via un lien sûr, protégé par nom d'utilisateur et mot de passe, avec obligation d'enregistrer électroniquement les demandes de données envoyées, en indiquant la personne qui a effectué la demande et la date et l'heure à laquelle celle-ci a été effectué, et d'enregistrer également chaque ouverture des fichiers reçus, en indiquant les personnes qui ont ouvert ces fichiers et la date et l'heure de chaque consultation de fichier (article 7(3) de la loi n° 32/2008 et décret n° 469/2009) ; et (v) adopté des dispositions exigeant expressément que la décision judiciaire de communication de données respecte dûment le secret professionnel conformément à la loi, sans pour autant empêcher leur conservation (article 9(4)) (...) » *[traduction non officielle de l'arrêt du Tribunal constitutionnel]*.

aux abonnés concernant les moyens de communication auraient pu être demandées par la police sans qu'une décision de justice soit nécessaire, conformément à l'article 149b(3) du code de procédure pénale.

La Cour constitutionnelle a conclu que, même si une décision de justice était normalement requise, dans cette affaire, M. Igor Benedik avait renoncé à l'espérance légitime de voir sa vie privée protégée en téléchargeant et en échangeant des fichiers pédopornographiques via un réseau pair à pair et que, par conséquent, la procédure appliquée par la police pour obtenir des informations sur les abonnés d'un fournisseur de services en l'absence d'une décision de justice était légale.

3.5.2 Décision de la Cour

Dans cette affaire, la police slovène avait reçu en 2006 des autorités suisses des renseignements sur une adresse IP utilisée pour échanger des contenus pédopornographiques via un réseau de partage de fichiers. La police slovène avait ensuite obtenu d'un fournisseur de services slovène des informations sur les abonnés associés à cette adresse IP dynamique au titre de l'article 149b(3) du code de procédure pénale, qui exige des fournisseurs de services la divulgation de données relatives aux abonnés sans qu'une décision de justice soit nécessaire[8] :

> Article 149b(3). Lorsqu'il existe des motifs de soupçonner qu'une infraction pénale pour laquelle un auteur est poursuivi d'office a été commise ou est en cours de préparation, et qu'il est nécessaire d'obtenir des informations sur le propriétaire ou l'utilisateur de certains moyens de communication électronique [nous soulignons], dont les coordonnées ne sont pas accessibles dans l'annuaire pertinent, ainsi que des informations sur le moment où les moyens de communication ont été ou sont utilisés, pour détecter cette infraction pénale ou son auteur, la police peut exiger par écrit de l'opérateur du réseau de communication électronique la fourniture de ces informations en l'absence du consentement des personnes auxquelles se rapportent ces informations.

Dans un deuxième temps, la police peut exiger au moyen d'une décision de justice obtenue par le ministère public la production d'autres données relatives à l'abonné et au trafic associées à une adresse IP. Dans un troisième temps, la police peut procéder sur la base d'une autre décision de justice à la perquisition du domicile de l'abonné. C'est ainsi que, dans l'affaire en question, des fichiers pédopornographiques (images et vidéos) et des logiciels utilisés pour télécharger et échanger ces fichiers ont été trouvés sur l'ordinateur du fils du propriétaire, M. Igor Benedik (le requérant).

Le Tribunal de district de Kranj a ensuite condamné le requérant à une peine de prison avec sursis de huit mois. La Haute-cour de Ljubljana a rejeté l'appel du requérant en statuant que les informations concernant l'utilisateur de l'adresse IP avaient été obtenues de manière légale et qu'aucune décision de justice n'était requise à cet égard.

Le requérant a déposé un nouveau recours en faisant valoir une nouvelle fois qu'une adresse IP dynamique devait être considérée comme faisant partie des données relatives au trafic et que celle-ci avait donc été initialement obtenue illégalement par la police. La Cour suprême a rejeté cet appel au motif que la police n'avait pas obtenu de données relatives au

[8] En revanche, si les données recherchées portent sur une communication et non sur des *moyens de communication*, l'article 149b(1) exige l'obtention préalable d'une décision de justice : « (1) Lorsqu'il existe des motifs de soupçonner qu'une infraction pénale pour laquelle un auteur est poursuivi d'office a été ou est en train d'être commise, ou bien est en cours de préparation ou d'organisation, et qu'il est nécessaire d'obtenir des informations sur des communications via un réseau de communication électronique afin de détecter cette infraction pénale ou son auteur, le juge d'instruction peut (…) ».

trafic « mais seulement les données concernant l'utilisateur d'un ordinateur particulier au moyen duquel était effectuée la connexion à l'internet ».

L'affaire a ensuite été portée devant la Cour constitutionnelle slovène qui, en 2014, contrairement aux tribunaux précédents, a considéré que l'article 37 de la constitution protégeait les données relatives au trafic et que les adresses IP faisaient partie des données relatives au trafic.

Néanmoins, la Cour constitutionnelle slovène a conclu que :

> le requérant, qui n'avait en aucune manière dissimulé l'adresse IP dont il se servait pour se connecter à l'internet, s'était délibérément exposé au public et avait donc renoncé à l'espérance légitime de voir sa vie privée protégée. En conséquence, les données concernant l'identité de l'utilisateur de l'adresse IP n'étaient pas protégées au titre du secret des communications en vertu de l'article 37 de la constitution, mais seulement au titre de la protection des informations à caractère personnel en vertu de l'article 38 de la constitution, et une décision de justice n'était pas requise en l'espèce pour la divulgation de ces informations[9].

M. Benedik a ensuite déposé une requête auprès de la Cour européenne des droits de l'homme, en se référant notamment à l'arrêt rendu en 2012 par la Cour constitutionnelle fédérale allemande.

D'après l'analyse de la Cour européenne des droits de l'homme :

- « une adresse IP est un numéro unique attribué à chaque appareil connecté à un réseau et permettant aux appareils de communiquer entre eux. Contrairement à une adresse IP statique, qui est attribuée de façon constante à l'interface de réseau particulière d'un appareil particulier, une adresse IP dynamique est attribuée par le fournisseur de services Internet (FSI) temporairement à un appareil, en général chaque fois que l'appareil se connecte à l'internet »[10] et « pour obtenir le nom et l'adresse de l'abonné qui utilise une adresse IP dynamique, le FSI est normalement obligé de rechercher cette information, en examinant à cette fin les données de connexion pertinentes de ses abonnés »[11] ;

- les informations personnelles concernant l'utilisation du téléphone, du courrier électronique et de l'internet entrent dans le champ de l'article 8 de la Convention européenne des droits de l'homme, tel qu'interprété par la Cour européenne des droits de l'homme dans des arrêts antérieurs[12] ;

- « les informations sur les abonnés associées à des adresses IP dynamiques particulières attribuées à certains moments ne sont pas publiquement accessibles et ne peuvent donc être comparées aux informations figurant dans un annuaire téléphonique classique ou dans une base de données publique comportant les numéros d'immatriculation des véhicules (…) Il semblerait en effet que, pour pouvoir identifier un abonné auquel une adresse IP dynamique a été attribuée à un moment donné, le FSI doit consulter des données stockées liées à des événements de télécommunication particuliers »[13] ;

[9] Citation tirée du paragraphe 28 de l'arrêt de la Cour européenne des droits de l'homme *[traduction non officielle]*.
[10] Remarque : cela semble inexact. Une adresse IP dynamique n'est pas attribuée lors de chaque communication nouvelle et peut être attribuée pour une très longue période de temps. Une adresse IP dynamique n'est donc pas nécessairement associée à une communication particulière.
[11] Arrêt *Benedik c. Slovénie*, paragraphe 96 *[traduction non officielle]*.
[12] Arrêt *Benedik c. Slovénie*, paragraphe 104.
[13] Arrêt *Benedik c. Slovénie*, paragraphe 108 *[traduction non officielle]*.

Dans son arrêt, la Cour européenne des droits de l'homme procède à une analyse de droit comparatif, en examinant notamment les arrêts de la Cour constitutionnelle de l'Allemagne[14] et de la Cour suprême du Canada mentionnés plus haut[15], et suit une approche contextuelle.

Elle souligne que les informations sur les abonnés sont liées aux contenus spécifiques échangés par un individu :

> 109. En outre, la Cour ne peut ignorer le contexte particulier où étaient recherchées les informations sur les abonnés dans l'affaire présente. L'obtention des informations sur les abonnés avait pour seul but d'identifier l'individu particulier qui se trouvait derrière les données recueillies de façon indépendante révélant les contenus qu'il avait échangés. La Cour note à cet égard qu'il existe une zone d'interaction de l'individu avec autrui qui relève de la « vie privée » (voir plus haut paragraphe 100). Les informations concernant de telles activités engagent cet aspect de vie privée dès lors qu'elles sont liées ou attribuées à un individu identifié ou identifiable (sur cette question d'identification, bien que dans un contexte assez différent, voir *Peck c. Royaume-Uni*, n° 44647/98, paragraphe 62, CEDH 2003-I, et *J.S. c. Royaume-Uni* (déc.), n° 445/10, paragraphes 70 et 72, 3 mars 2015). Par conséquent, ce qui semblerait être des informations périphériques recherchées par la police, à savoir le nom et l'adresse d'un abonné, doit dans une situation telle que la présente être traité comme indissolublement lié aux données préexistantes pertinentes qui révèlent le contenu de communications (voir les avis divergents des juges de la Cour constitutionnelle cités aux paragraphes 31 et 34 ; comparer également le point de vue de la Cour suprême du Canada, cité plus haut aux paragraphes 69 et 72, et celui de la Cour constitutionnelle fédérale de l'Allemagne, cité plus haut aux paragraphes 64 et 65). Soutenir le contraire reviendrait à nier la nécessaire protection des informations susceptibles de révéler de nombreux éléments sur les activités en ligne d'un individu, y compris des détails sensibles au sujet de ses intérêts, de ses convictions et de sa vie intime[16].

La Cour note en outre que :

> (…) l'article 149b(3) du code de procédure pénale (voir plus haut paragraphe 36), sur lequel se sont appuyées les autorités nationales, prévoit la possibilité de requérir des informations sur le propriétaire ou l'utilisateur d'un certain moyen de communication électronique. Il n'établit pas de lien spécifique entre l'adresse IP dynamique et les informations concernant un abonné. La Cour note en outre que l'article 37 de la constitution slovène requiert une décision de justice pour toute ingérence dans la confidentialité des communications (…) de plus, la loi sur les communications électroniques (…) qui régit spécifiquement le secret et la confidentialité des communications électroniques, ne prévoyait pas à l'époque la possibilité d'avoir accès et de transférer les informations sur les abonnés et les données associées relatives au trafic aux fins d'une procédure pénale[17].

La Cour mentionne l'article 15 de la Convention de Budapest mais sans préciser le sens de la clause « lorsque cela est approprié » :

> 126. Eu égard au contexte particulier de l'affaire, la Cour souligne que la Convention sur la cybercriminalité oblige les États à prendre des mesures telles que la collecte en temps réel des données relatives au trafic et à mettre en place les dispositions requises pour permettre aux autorités d'émettre des injonctions à produire des données, notamment afin de combattre

[14] Arrêt *Benedik c. Slovénie*, paragraphes 63 à 67.
[15] Arrêt *Benedik c. Slovénie*, paragraphes 68 à 72.
[16] Remarque : cette déclaration de la Cour soulève certaines questions. Lorsqu'un organe d'application de la loi cherche à obtenir des informations sur les abonnés, que ce soit des adresses IP dynamiques ou statiques ou de simples numéros de téléphone ou d'immatriculation d'un véhicule, n'est-ce pas toujours dans le but d'établir un lien entre un numéro ou une adresse – et donc un abonné – et un acte criminel particulier, y compris en ayant accès au contenu des communications ?
[17] Arrêt *Benedik c. Slovénie*, paragraphe 127 *[traduction non officielle]*.

> les délits associés à la pédopornographie (voir plus haut paragraphes 47 à 51). Cependant, aux termes de l'article 15 de la Convention, ces mesures doivent être « soumises aux conditions et sauvegardes prévues par [le] droit interne » des États Parties qui, « lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné » doivent inclure entre autres « une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question ».

La Cour observe en particulier que :

> (…) la seule raison pour laquelle la Cour constitutionnelle a rejeté la demande du requérant – en approuvant la divulgation d'informations sur l'abonné en l'absence d'une décision de justice – est la présomption que le requérant avait « renoncé à l'espérance légitime de voir sa vie privée protégée » (voir le paragraphe 18 de l'arrêt de la Cour constitutionnelle cité plus haut au paragraphe 29). Cependant, la Cour, au vu de ses conclusions concernant l'applicabilité de l'article 8, est d'avis que la position de la Cour constitutionnelle sur ce point n'est pas compatible avec la portée reconnue dans la Convention au droit à la protection de la vie privée (voir plus haut paragraphes 115 à 118). Gardant à l'esprit l'avis de la Cour constitutionnelle selon lequel l'« identité de l'individu communiquant » relève du champ d'application de la protection instituée à l'article 37 de la constitution (voir plus haut paragraphe 128) et la conclusion de la Cour selon laquelle le requérant pouvait raisonnablement s'attendre à ce que son identité eu égard à ses activités en ligne resterait confidentielle (voir plus haut paragraphes 115 à 118), une décision de justice était en l'espèce nécessaire[18].

La Cour européenne des droits de l'homme a statué par conséquent qu'il y avait eu violation de l'article 8 de la Convention européenne des droits de l'homme.

Suite à cette affaire et à l'arrêt rendu antérieurement par la Cour constitutionnelle slovène, la pratique en ce domaine a été modifiée et les services répressifs slovènes cherchent dorénavant à obtenir une décision de justice pour accéder aux adresses IP statiques et dynamiques en relation avec des communications particulières. Des amendements au code de procédure pénale sont encore en instance.

3.6 Cour de Justice de l'Union européenne (2018) : affaire C-207/16 Ministerio Fiscal

Dans l'affaire C-207/16, la demande de décision préjudicielle portait sur la question de savoir si la possibilité d'accéder aux données relatives aux abonnés – dans le cas d'espèce pour identifier les utilisateurs de numéros de téléphone activés avec un téléphone volé – doit être limitée à la lutte contre la criminalité grave. La CJUE a statué en octobre 2018 que l'accès aux données relatives aux abonnés « ne saurait être qualifié d'ingérence "grave" dans les droits fondamentaux des personnes dont les données sont concernées » et que cet accès ne peut donc être limité à la lutte contre la criminalité grave.

L'affaire en question concernait les faits suivants :

> Dans le cadre de l'enquête sur un vol avec violences d'un portefeuille et d'un téléphone mobile, la police judiciaire espagnole a demandé au juge d'instruction responsable de l'affaire de lui accorder l'accès aux données d'identification des utilisateurs des numéros de téléphone activés depuis le téléphone volé durant une période de douze jours à compter de la date du vol. Le juge d'instruction a rejeté cette demande au motif, notamment, que les faits à l'origine

[18] Arrêt *Benedik c. Slovénie*, paragraphe 128 *[traduction non officielle]*.

> de l'enquête pénale n'auraient pas été constitutifs d'une infraction « grave » – c'est-à-dire, selon le droit espagnol, une infraction sanctionnée d'une peine de prison supérieure à cinq ans –, l'accès aux données d'identification n'étant en effet possible que pour ce type d'infractions. Le Ministerio Fiscal (ministère public espagnol) a interjeté appel de cette décision devant l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne)[19].

De même que les décisions de la CJUE sur la conservation des données examinées plus haut, l'affaire C-207/16 portait sur l'interprétation de l'article 15(1) de la Directive 2002/58/CE sur la vie privée et les communications électroniques au regard d'autres textes de loi de l'Union européenne. Et, bien que cette affaire concernait l'accès aux données conservées au titre de la législation espagnole sur la conservation des données, dans sa décision préjudicielle, la CJUE n'a pas cherché à examiner la validité du règlement sur la conservation des données mais seulement la question de l'accès des autorités publiques à ces données.

Dans cette décision, la CJUE déclare :

> 60 Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.
>
> 61 Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées.
>
> 62 Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la Directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves ».
>
> 63 Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

En bref, sous l'angle de la présente étude, la CJUE a statué dans cette affaire que :

- les informations sur les abonnés « ne permettent pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées » ;

[19] Extrait du communiqué de presse publié le 2 octobre 2018.

- par conséquent, l'accès aux informations sur les abonnés « ne saurait être qualifié d'ingérence "grave" dans les droits fondamentaux des personnes dont les données sont concernées » ;

- enfin, bien que l'accès aux informations sur les abonnés « comporte une ingérence dans les droits fondamentaux », cette ingérence « ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave ».

3.7 Proposition de Règlement de l'UE relatif aux injonctions européennes de production et de conservation de preuves électroniques

Le 17 avril 2018, la Commission européenne a publié une proposition de Règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

La proposition de règlement vise à permettre aux autorités de justice pénale des États membres de l'UE d'adresser des injonctions de production aux fournisseurs de services offrant dans un État membre un service basé dans un autre État membre. Un projet de directive complémentaire exige des fournisseurs de services offrant des services à l'intérieur de l'UE qu'ils disposent d'un représentant légal dans au moins un des États membres de l'UE à qui adresser ces injonctions.

La proposition de règlement distingue entre les demandes concernant les « données relatives aux transactions » (qui sont similaires aux données relatives au trafic) et les données relatives au contenu, d'une part, et les données relatives aux abonnés et une nouvelle catégorie de « données relatives à l'accès », d'autre part. Une injonction de production de données relatives au contenu et aux transactions doit être émise ou validée par un juge, tandis qu'une injonction de production de données relatives aux abonnés et à l'accès peut être émise ou validée par un procureur.

Aux termes de l'article 2 (8) :

> « données relatives à l'accès » [désigne] les données relatives au début et à la fin d'une session d'accès utilisateur à un service, strictement nécessaires aux seules fins d'identification de l'utilisateur du service, telles que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service, ainsi que l'adresse IP attribuée par le fournisseur de service d'accès à l'internet à l'utilisateur d'un service, les données identifiant l'interface utilisée et l'identifiant de l'utilisateur. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point g), du [Règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques] ;

Selon le Rapport explicatif :

> Il y a donc lieu de distinguer les données relatives à l'accès par une catégorie de données spécifique utilisée dans le présent règlement. Les données relatives à l'accès au sens de la présente sont recherchées dans le même but que les informations relatives aux abonnés, c'est-à-dire pour identifier l'utilisateur, et leur niveau d'interférence avec les droits fondamentaux est similaire. Elles doivent donc être soumises aux mêmes conditions que les informations relatives aux abonnés. C'est la raison pour laquelle cette proposition introduit

> une nouvelle catégorie de données qu'il faudra traiter comme des informations relatives aux abonnés si le même objectif est visé.

L'inclusion des métadonnées, telles que définies dans le futur Règlement concernant le respect de la vie privée et des données à caractère personnel dans les communications électroniques, pourrait être source de confusion entre les « données relatives à l'accès » et les catégories de données relatives au trafic (ou de métadonnées) pour lesquelles un seuil plus élevé est souvent requis suite aux décisions de la CJUE et d'un certain nombre de tribunaux constitutionnels des États membres de l'UE. Aux termes de l'article 4, paragraphe 3, point c)[20] de ce projet de Règlement :

> « métadonnées de communications électroniques » : les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.

4 Remarques finales

Cette brève analyse des décisions judiciaires et développements nationaux et internationaux concernant les données relatives aux abonnés permet de formuler plusieurs thèses en vue d'un examen ultérieur :

1. L'obtention d'informations sur les abonnés dans un contexte de justice pénale – que ce soit en relation avec les adresses IP statiques ou dynamiques (ou même les numéros de téléphone) – a toujours le même but, à savoir identifier l'abonné d'un compte ou site web particulier, ou l'abonné lié à une adresse IP en relation avec une enquête pénale spécifique. L'obtention des données relatives aux abonnés permet, en particulier, aux autorités d'enquête de déterminer le lien entre un abonné et une communication concrète, ou inversement. Cependant, les informations sur les abonnés ne permettent pas en elles-mêmes de tirer des conclusions précises au sujet de la vie privée des individus. Par conséquent, la conservation et la production d'informations sur les abonnés ne risquent pas en tant que telles de conduire à une ingérence dans le droit au secret des communications, mais il est probable qu'elles pourront interférer avec d'autres droits.

2. La divulgation d'informations sur les abonnés dans le cadre d'enquêtes pénales spécifiques constitue, en principe, une ingérence moins grave dans les droits des individus, notamment le droit au secret des communications ou le droit à l'auto-détermination informationnelle, que la divulgation des données relatives au trafic ou au contenu. Certaines Parties ou leurs tribunaux jugent par conséquent proportionnée l'existence d'un seuil moins élevé pour la divulgation des informations sur les abonnés que pour la divulgation des données relatives au trafic ou au contenu. Dans d'autres États, la jurisprudence semble indiquer que ces questions doivent être résolues de façon contextuelle et que, la divulgation des informations sur les abonnés pouvant impliquer des enjeux plus importants de protection de la vie privée dans tel ou tel contexte, une évaluation au cas par cas est nécessaire.

[20] Il semble y avoir une erreur dans la Proposition de Règlement ; la référence exacte est : article 4, paragraphe 3, point m).

3. Les autorités de justice pénale peuvent requérir l'accès aux informations sur les abonnés dans certaines enquêtes pénales particulières portant sur des infractions qui sont en fait en-deçà du critère de « criminalité grave ». Limiter l'accès ou la divulgation des informations sur les abonnés aux enquêtes portant sur la criminalité grave pourrait empêcher les États de remplir leurs obligations de protection des individus et de leurs droits contre la criminalité, comme dans l'affaire K.U. c. Finlande examinée par la Cour européenne des droits de l'homme. En outre, au stade initial d'une enquête, la « gravité » des délits en jeu n'est pas toujours évidente.

4. Les informations sur les abonnés peuvent inclure les numéros d'accès, y compris les adresses IP qui sont absolument nécessaires pour identifier un abonné comme la première adresse IP de connexion, la dernière adresse IP de connexion ou l'adresse IP de connexion utilisée à un moment particulier[21]. Cela devra être précisé dans le Deuxième Protocole additionnel ou dans le rapport explicatif correspondant. L'introduction de nouvelles catégories de données, comme les « données relatives à l'accès », pourrait conduire à de nouveaux malentendus au sujet des règles applicables à la conservation et à l'accès à ces données et compliquer leur application par les praticiens.

5. Les États Parties pourraient envisager d'introduire dans la législation nationale l'obligation légale de conserver les données relatives aux abonnés, afin que ces données soient disponibles aux fins d'enquêtes pénales particulières. Plusieurs décisions de justice suggèrent qu'une telle mesure est appropriée et proportionnée dès lors qu'elle porte sur un ensemble limité de données ne permettant pas d'inférer le contenu des communications, les habitudes de la vie quotidienne ou les relations sociales d'un individu.

6. Certaines jurisprudences et réglementations nationales établissent une distinction entre les adresses IP statiques et les adresses IP dynamiques attribuées à un abonné particulier et considèrent que la production d'informations sur les abonnés telles que les adresses IP dynamiques constitue une ingérence dans le droit au secret des communications. Il est donc nécessaire de poursuivre la discussion à ce sujet :

   – D'une part, en effet, l'argument selon lequel une adresse IP dynamique – par opposition à une adresse IP statique – est toujours liée à une communication particulière est inexact :

      - une adresse IP dynamique peut être attribuée à un abonné pendant plusieurs jours ou plusieurs mois ou jusqu'à la réinitialisation d'un routeur, par exemple ;
      - l'appareil d'un usager peut se connecter automatiquement à l'internet sans participation active ou sans communication effective de l'usager ;
      - dans le cas des adresses IP statiques et des numéros de téléphone également, le but recherché dans une enquête est d'établir un lien entre un abonné et une communication ou un événement particulier.

   – D'autre part, les fournisseurs de services sont parfois obligés d'examiner ou d'analyser les données relatives au trafic pour déterminer l'adresse IP attribuée à un abonné à un moment particulier. Même si le fournisseur de services ne divulgue pas les données relatives au trafic à l'autorité de justice pénale, et même si le travail d'examen ou d'analyse qu'il effectue

[21] Voir l'annexe au Template for MLA for subscriber information adopté par le T-CY en juillet 2018.

ne constitue pas une analyse du contenu ou du contexte d'une communication et ne permet pas de tirer des conclusions précises sur la vie privée d'un individu, un tel examen des données par le fournisseur de services n'est pas nécessaire pour les adresses IP statiques. Néanmoins, la gravité de l'impact de cet examen sur le droit au respect de la vie privée et d'autres droits des individus est discutable, étant donné qu'il reposera probablement sur l'interrogation automatisée de bases de données.

7. L'accès aux informations sur les abonnés, aussi bien les adresses IP statiques que les adresses IP dynamiques, doit s'appuyer sur une base légale, par exemple en transposant dans le droit interne les injonctions de production envisagées à l'article 18 de la Convention de Budapest[22]. La mise en place de dispositions spécifiques sur les injonctions de production permettrait aussi de clarifier le fait que cette mesure est différente et que son application requiert un seuil moins élevé que les pouvoirs de perquisition et de saisie. Cette base légale pourra être renforcée en mentionnant ou en incluant spécifiquement les adresses IP attribuées à un moment particulier, c'est-à-dire les adresses IP dynamiques. Une réglementation « à double entrée » ou d'autres mesures législatives prévoyant (1) la possibilité pour un fournisseur de services de divulguer ces données, par exemple dans un texte de loi sur les télécommunications, et (2) la possibilité d'émettre des injonctions de production des deux catégories de données relatives aux abonnés, en précisant les conditions sous lesquelles les autorités de justice pénale peuvent requérir ces données, seraient à même, grâce à leur effet combiné, d'instituer de meilleures sauvegardes et d'assurer la sécurité juridique.

[22] La transposition complète de l'article 18 dans le droit interne a également été recommandée par le Groupe du T-CY sur les preuves dans le Cloud dans son rapport final, dont les recommandations ont été adoptées par le T-CY en novembre 2016.