La collecte de données en matière de télécommunications

L'arrêt SpaceNet de la CJUE – une comparaison avec le droit suisse

Louis Wéry[1]*

Zusammenfassung: Der vorliegende Beitrag fasst zunächst eine Entscheidung des Gerichtshofs der Europäischen Union (EuGH) über die Vereinbarkeit des EU-Rechts mit einem deutschen Gesetz zusammen, das Telekommunikationsunternehmen dazu verpflichtet, dem Staat Daten über ihre Nutzer zur Verfügung zu stellen. Im Entscheid werden dann die Gründe für eine zulässige Verarbeitung dieser Daten analysiert, insbesondere im Zusammenhang mit der Bekämpfung von Straftaten und der Verhütung von Gefährdungen für die öffentliche Sicherheit. Der Autor überträgt im zweiten Teil seines Aufsatzes den vom EuGH behandelten Fall auf das Schweizer Recht und zeigt die Unterschiede zwischen den beiden Rechtsordnungen auf.

Résumé: La présente contribution résume, en premier lieu, une décision rendue par la Cour de justice de l'Union européenne (CJUE) portant sur la compatibilité entre le droit de l'Union et une loi allemande qui astreint des entreprises du secteur des télécommunications à fournir à l'État allemand des données sur leurs utilisateurs. À travers cette décision, la CJUE analyse les motifs permettant le traitement de ces données, en particulier dans un contexte de lutte contre la criminalité et la prévention des menaces contre la sécurité publique. La seconde partie de l'article transpose le cas analysé par la CJUE en droit suisse et relève les différences entre les deux ordres juridiques.

Inhalt:

I. Introduction

1

En 1989 éclatait en Suisse l'affaire dite « des fiches ». Il s'agissait de la découverte fortuite de 900'000 fiches qui consignaient des informations au sujet de personnes, d'organisations ou d'évènements recueillies par l'entremise des services cantonaux de renseignements ou des fonctionnaires de la Police fédérale[2]. Ces fiches constituées depuis les années 1930 en dehors de tout cadre légal étaient détenues par le ministère public de la Confédération.

2

La commission d'enquête parlementaire mise en place suite à ce scandale révéla, parmi une multitude de graves dysfonctionnements, qu'il n'y avait pas de critère de valeur générale concernant l'inscription d'une information sur une de ces fiches[3]. Une personne pouvait ainsi faire l'objet d'une fiche si elle avait une opinion politique divergente de la majorité, si elle adhérait à un certain parti politique, si elle exerçait des droits syndicaux ou même si elle était abonnée à un journal déterminé[4]. En d'autres termes, la collecte d'informations faite à travers ces fiches était exsangue de motif précis.

3

Bien qu'elle se soit déroulée en Allemagne, la décision rendue par le CJUE dont cet article fait l'objet nous ramène d'une certaine manière à ce scandale car elle discute des raisons pour lesquelles l'État peut collecter des informations sur ces concitoyens. L'analyse de la jurisprudence de la CJUE et sa comparaison avec le droit suisse nous permettra de voir si et dans quelle mesure la législation suisse a progressé depuis l'affaire dite « des fiches ».

II. La décision de la CJUE

1. Les faits

4

L'affaire[5] a été portée devant les tribunaux par SpaceNet AG, un fournisseur d'accès Internet, et Telekom Deutschland GmbH, un fournisseur d'accès Internet et un opérateur de téléphone. Ces deux entreprises sont actives en Allemagne. L'agence allemande pour l'électricité, le gaz, les télécommunications, la poste et les transports (« Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ») s'est fondée sur la loi sur les télécommunications (TKG)[6] pour exiger des deux entreprises qu'elles conservent les données relatives au trafic et des données de localisation à compter du 1er juillet 2017. Les deux entreprises ont contesté la demande en argumentant qu'elle était contraire au droit européen. Alors qu'en première instance SpaceNet AG et Telekom Deutschland ont obtenu, chacun à travers une décision, gain de cause, la République fédéral d'Allemagne a formé un recours en Revision contre ces deux décisions devant la Cour administrative fédérale. Cette dernière a formé un renvoi préjudiciel auprès de la CJUE qui a joint les deux affaires.

5

La loi allemande sur la télécommunication (TKG) impose aux

opérateurs mobiles et aux fournisseurs d'accès internet de conserver les données de trafic et les données de localisation de leurs utilisateurs. Selon la TKG, les données de localisation doivent être conservées quatre semaines et les données de trafic dix semaines.

6

En matière de traitement de données personnelles, la TKG doit être conforme à la directive 2002/58[7] qui a pour but d'assurer la protection des droits et libertés fondamentaux lors de traitement de données à caractère personnel dans le secteur des communications électroniques (art. 1 de la directive 2002/58). Au regard de cette directive, les États membres sont notamment tenus de garantir par leur législation nationale la confidentialité des communications (art. 5 paragraphe 1 de la directive), l'effacement ou l'anonymisation des données relatives au trafic, c'est-à-dire les informations concernant l'acheminement d'une communication par un réseau (art. 6 paragraphe 1 et 2 de la directive) et enfin l'anonymisation des données de localisation (paragraphe 9 de la directive). Cependant, l'art. 15 de la directive permet aux États membres d'adopter des mesures législatives limitant la portée de la directive, en particulier des articles 5, 6 et 9, notamment lorsqu'il en va de *la sauvegarde de la sécurité nationale* ou *de la prévention, la recherche et la poursuite d'infractions pénales*.

7

Il est ainsi possible de conserver les données durant une durée limitée lorsque cela est justifié par un des deux motifs précédemment évoqués. À ce titre, la Cour rappelle que l'art. 15 de la directive doit faire l'objet d'une interprétation stricte, sauf à vider la directive de sa portée[8].

2. Les objectifs d'intérêt général

8

Selon la CJUE, la sauvegarde de la sécurité nationale est un objectif particulièrement important[9]. Il permet d'ordonner aux fournisseurs de service de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, pour autant qu'il s'agisse d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Cette conservation doit avoir lieu sur une période limitée au strict nécessaire, mais est renouvelable en cas de persistance de cette menace[10]. De plus, une telle injonction doit faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative.

9

S'agissant de prévention, de recherche, de détection et de poursuite d'infraction pénale, la Cour rappelle que des atteintes graves aux droits fondamentaux aux art. 7 et 8 de la Charte (telles que la conservation des données relatives au trafic et des données de localisation) ne sont proportionnelles que lorsqu'il s'agit de criminalité grave[11]. Et pour ce qui est de la lutte contre la criminalité grave, la Cour a jugé par le passé qu'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation excède les limites du strict nécessaire et ne peut être considérée comme étant justifiée[12]. En d'autres termes, ce second objectif ne permet pas une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

3. Le Telekommunikationsgesetz allemand

10

La Cour examine ensuite la loi allemande, tant sous l'angle du type de données conservées, des personnes visées et la durée de conservation que sous l'angle de l'objectif d'intérêt

général poursuivi et sa proportionnalité.

11

Dans un premier point, elle examine *la conservation généralisée et indifférenciée d'une majeure partie des données relatives au trafic et des données de localisation.* En effet, la loi allemande astreint les fournisseurs de services téléphoniques à conserver les données nécessaires pour identifier la source d'une communication ainsi que la destination, la date et l'heure du début et de la fin de la communication. Pour les fournisseurs d'accès Internet, l'obligation de conservation porte sur l'adresse IP attribuée à l'abonnée, la date et l'heure du début et de la fin de l'utilisation d'Internet à partir de l'adresse IP. Ces données permettent en outre de connaître la position géographique de l'utilisateur.

12

La Cour relève que la conservation des adresses IP permet d'effectuer le traçage exhaustif du parcours de navigation d'un internaute et ainsi de suivre son activité en ligne. Il est de ce fait possible d'établir le profil détaillé de l'utilisateur. La Cour juge dès lors qu'il s'agit *d'ingérences graves* dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte.

13

Pour ce qui est des *personnes visées* par la législation allemande, l'obligation de conservation prévue par la TKG s'étend même aux données d'utilisateurs soumis au secret professionnel tels que les avocats, les médecins et les journalistes. Sauf rares exceptions comme pour les associations religieuses, la réglementation concerne la quasi-totalité des personnes composant la population sans que celles-ci se trouvent même indirectement dans une situation susceptible de donner lieu à des poursuites pénales. Il ne s'agit donc manifestement pas d'une conservation ciblée des

données.

14

En ce qui concerne de la *durée de conservation*, l'art. 113b TKG prévoit une durée de quatre semaines pour les données relatives au trafic et une durée de dix semaines pour les données de localisation. Ces périodes sont sensiblement plus courtes que celles qui furent analysées par le passé par la Cour[13]. Cependant, indépendamment de la durée de conservation, les données en question sont susceptibles de fournir des conclusions très précises sur la vie privée des utilisateurs. Dès lors, il s'agit d'informations autant sensibles que le contenu même des communications. Ainsi, le simple fait de conserver ces données est déjà une ingérence grave.

15

La Cour rejette l'argumentation qui voudrait que la lutte contre la criminalité grave soit assimilée à une menace pour la sécurité nationale. En effet, la protection de la sécurité nationale vise la préservation des fonctions essentielles de l'État et les intérêts fondamentaux de la société. C'est le cas de la prévention et la répression des activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, ou qui menacent directement la société, la population ou l'État comme, typiquement, le terrorisme[14]. Une menace pour la sécurité nationale doit ainsi être réelle et actuelle, à tout le moins prévisible, et suppose donc la survenance de circonstances suffisamment concrètes. Une telle menace se distingue ainsi de par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent d'un risque général et permanent que représente la survenance de tensions ou de troubles mêmes graves à la sécurité publique ou d'infractions pénales graves[15]. Le risque constant de criminalité grave ne peut donc pas être assimilé à une menace pour la sécurité nationale.

16

La Cour arrive ainsi à la conclusion que la législation allemande viole le droit européen en prévoyant à titre préventif et aux fins de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique une conservation généralisée et indifférenciée des données relatives au trafic ainsi que des données de localisation.

III. Une conclusion intermédiaire

17

La sauvegarde de la sécurité nationale est un objectif d'un poids certain dans l'application de l'art. 15 de la directive 2002/58. L'État membre peut s'en servir pour faire injonction aux fournisseurs de procéder à une conservation généralisée et indifférenciée des données de trafic et des données de localisation. Cependant cette injonction doit s'étaler sur un temps limité.

18

Dans tous les cas, l'objectif de sécurité nationale, qui vise uniquement les cas d'atteintes aux fonctions essentielles de l'État, est à distinguer de celui de la lutte contre la criminalité grave, notion que la CJUE ne définit pas plus précisément. Il reste à émettre des conjectures sur cette notion : la criminalité grave représente les infractions pénales les plus graves du Code pénal d'un État membre, soit celles dont la peine menace est la plus lourde, comme l'assassinat par exemple.

19

Il existe ainsi une dichotomie entre la menace terroriste qui a pour objectif de déstabiliser l'État, et la criminalité grave qui ne cherche pas à déstabiliser l'État. Bien que les deux phénomènes criminels sous-entendent la commission d'actes particulièrement graves au regard du droit pénal, dans le cas

de la criminalité grave, l'intention du ou des auteurs n'est pas de déstabiliser l'État.

20

Cette frontière peut paraître particulièrement floue lorsqu'il s'agit de comparer la criminalité organisée, qui se caractérise au regard du droit pénal notamment par la répétition d'actes particulièrement graves, et le terrorisme. Alors que le premier phénomène naît d'une recherche de profit économique et d'acquisition de part de marché illégal, le second est motivé principalement par des buts idéologiques et par un désir de changement politique[16]. L'Histoire a cependant démontré que ces deux phénomènes peuvent converger. Ce fut au moins le cas dans les années '80 lorsque la promotion d'objectifs politiques de certains gouvernements et de certaines organisations terroristes était financée par le trafic de drogues : le « narco-terrorisme »[17].

21

La CJUE ne discute pas d'une possible convergence entre ces deux objectifs. Nous pouvons cependant supposer que dans une telle hypothèse, la Cour se tiendrait à la définition du terrorisme et analyserait dans quelle mesure le phénomène criminel menace effectivement la sécurité de l'État.

22

En ce qui concerne les motifs d'exceptions restants de l'art. 15 de la directive, à savoir l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, ils ne pourront pas justifier des ingérences graves dans les droits fondamentaux, telles que la conservation généralisée et indifférenciée de données relatives au trafic et de données de localisation.

IV. La situation en droit suisse

23

Nous chercherons dès lors à transposer en droit suisse la situation précédemment décrite, à savoir la conservation de données secondaires effectuée de manière généralisée au profit de l'État.

24

En premier lieu, il convient de faire un bref rappel de la base légale primaire en matière de traitement de données en Suisse : la Loi fédérale sur la protection des données (LPD). Cette loi a fait l'objet d'une révision totale qui entrera en vigueur le 1er septembre 2023[18]. La suite de notre analyse intègre donc cette nouvelle loi (nLPD) (a). Comme nous le verrons rapidement, la nLPD est une loi-cadre qui, dans notre hypothèse de comparaison, nous obligera à nous tourner vers une autre loi : la Loi fédérale sur la surveillance de la poste et des télécommunications (LSCPT) ainsi que son ordonnance (OSCPT) (b) qui, elles, procèdent de la même intention que la TKG.

1. La Loi fédérale sur la protection des données

25

En droit suisse, c'est la Loi fédérale sur la protection des données (nLPD) qui a pour but de protéger les droits fondamentaux des personnes qui font l'objet d'un traitement de données (art. 1 nLPD), en particulier la protection contre l'emploi abusif de données personnelles (art. 13 al. 2 Cst)[19].

26

À l'instar de la LPD, la nLPD, qui s'appliquera elle aussi tant dans le traitement fait par des personnes privées que des organes fédéraux (art. 2 al. 1 let. a et b nLPD), classe les données dans deux catégories. Les données personnelles sont toutes les informations se rapportant à une personne

identifiée ou identifiable (art. 5 let. a nLPD), alors que les données sensibles sont des données personnelles contenant des informations telles des opinions politiques, des informations sur la santé, la sphère intime ou encore des poursuites ou sanctions pénales et administratives (art. 5 let.c nLPD). La seconde catégorie de données est ainsi entièrement comprise dans la première. La différence entre les deux catégories s'exprime dans le fait que les données sensibles contiennent des informations relevant si étroitement de la personnalité que l'on peut supposer que la personne concernée désire que ces informations soient traitées avec des égards particuliers. Le traitement de telles données est ainsi soumis à des obligations supplémentaires telles qu'une analyse d'impact préalable en cas de traitement à grande échelle (art. 22 al. 2 let. a nLPD) ou un consentement pour pouvoir les traiter dans le but d'évaluer la solvabilité (art. 31 al. 2 let. c nLPD)[20].

27

La nLPD pose comme cadre l'article 34 al. 1, qui stipule que le traitement de données par un organe de l'État ne peut avoir lieu que s'il existe une base légale. Il s'agit dans cette première hypothèse du traitement de données personnelles ordinaires[21].

28

Dans les cas de traitement de données sensibles, de profilage ou lorsque la finalité ou le mode du traitement de données personnelles sont susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée, l'art. 34 al. 2 LPD exige que la base légale permettant le traitement soit contenue dans une loi au sens formel. En dérogation à l'art. 34 al. 2 nLPD, l'art. 34 al. 3 nLPD permet un traitement des données à travers une base légale prévue dans une loi au sens matériel si le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel et que la finalité du traitement ne présente pas de

risques particuliers pour les droits fondamentaux de la personne concernée.

29

Pour rappel, une loi au sens formel contient les dispositions importantes portant notamment sur la restriction des droits constitutionnels (art. 164 al. 1 let. b Cst.)[22] – le traitement de données personnelles sensibles étant au minimum une ingérence dans le droit de chacun à voir sa sphère privée protégée (art. 13 Cst.).

30

La LPD et ainsi conçue comme une loi-cadre qui renvoie à des bases légales spécifiques pour le traitement concret des données[23].

2. La Loi fédérale sur la surveillance de la poste et des télécommunications

a) L'autorisation de la surveillance

31

La loi fédérale sur la surveillance de la poste et des télécommunications permet de surveiller la poste et les télécommunications, notamment, dans le cadre d'une procédure pénale (al. 1 al. 1 let. a LSCPT), lors de l'exécution d'une demande d'entraide judiciaire (art. 1 al. 1 let. b LSCPT) ou en application de la Loi fédérale sur le renseignement (art. 1 al. 1 let. e LSCPT).

b) Les personnes obligées de collaborer

32

Comme la TKG allemande, la LSCPT oblige les fournisseurs de services de télécommunication (art. 2 let. b LSCPT) à la collaboration. Au sens de la LSCPT est « fournisseur de services de télécommunication » celui qui s'engage à

transmettre lui-même, pour le compte d'un tiers et au moyen de techniques de télécommunication, des informations[24]. Le Message du Conseil Fédéral donne à titre d'exemples les entreprises telles que Swisscom, Sunrise et Cablecom qui permettent aux usagers de téléphoner, au moyen d'un téléphone fixe ou mobile, ou d'accéder à Internet[25]. En termes d'activité, il s'agit donc d'entreprises comparables à SpaceNet AG et Telekom Deutschland GmbH.

c) Les types de surveillance

33

La LSCPT permet deux types de surveillance des télécommunications : la surveillance en temps réel et la surveillance rétroactive (art. 26 al. 4 LSCPT)[26]. Alors que dans le premier cas, il s'agit de transmissions d'informations en temps réel, soit le contenu de la correspondance entre les utilisateurs, dans le second, des données relatives au trafic sont préalablement enregistrées par les fournisseurs de service de télécommunication et les fournisseurs d'accès à Internet[27].

d) Les types de données

34

À la différence des données de contenu, soit celles qui peuvent faire l'objet d'une surveillance en temps réel, les données secondaires contiennent, notamment, les informations avec qui, quand et où les communications ont eu lieu[28]. L'OSCPT oblige ainsi les fournisseurs d'accès Internet à conserver les données de localisation au début, pendant et à la fin de la session (art. 60 let. g OSCPT) pour toute connexion à Internet via un téléphone mobile. En outre, les données secondaires de la messagerie électronique doivent aussi être conservées. Il s'agit notamment de la date, l'heure, les éventuels alias de messagerie, les adresses de

l'expéditeur et du destinataire lors de l'envoi ou de la réception d'un message mais aussi simplement lors de la connexion à la boîte de courrier électronique (art. 62 let. a OSCPT).

e) La durée de conservation

35

Une fois enregistrées, ces données sont conservées durant 6 mois (art. 26 al. 5 LSCPT) et peuvent, notamment, être obtenues, comme précédemment évoqué, dans le cadre d'une procédure pénale, avec l'autorisation de l'autorité compétente pour autoriser les surveillances[29].

V. Le droit suisse au vu de la jurisprudence européenne

36

À l'instar de la TKG, la LSCPT ne fait pas la différence entre la criminalité grave et la menace terroriste. En effet, autant une procédure pénale que la LRens permettent une mise en œuvre de la LSCPT. À ce titre, il convient encore de relever que ces deux catégories ne sont pas entièrement perméables en droit pénal suisse car le financement du terrorisme fait l'objet d'une disposition spécifique dans le Code pénal suisse (art. 260quinquies). De plus, et bien que l'acte terroriste à proprement parler ne fasse pas l'objet d'une disposition particulière dans le Code pénal suisse, l'acte terroriste peut être réprimé par les autres dispositions du Code pénal telles que l'assassinat ou la prise d'otage[30]. Ainsi une menace ou un acte terroriste pourraient être à l'origine d'une surveillance rétroactive de la LSCPT tant par le truchement d'une action pénale que par l'application de la LRens. Mais qui peut le plus, peut le moins : la LSCPT peut non seulement trouver application dans des cas de criminalité grave ou de terrorisme mais aussi pour tous les actes que le droit pénal réprime,

soit également de banales affaires de trafic de stupéfiants.

37

En ce qui concerne les types de données, alors que la législation allemande retoquée par la CJUE demandait aux fournisseurs de mettre à disposition les données secondaires de communications et de localisation, la loi suisse va plus loin en obligeant les fournisseurs à conserver également les données relatives à la messagerie électronique. Pour ce qui est de la durée de conservation, la loi allemande prévoyait une durée de quatre semaines pour les données de localisation et de dix pour les autres données (*supra* II./a). Le droit suisse prévoit quant à lui une durée de six mois, ce qui est substantiellement plus long.

38

Rappelons que la loi allemande était en contradiction avec le droit européen car elle prévoyait une conservation généralisée sans répondre à l'exigence de la directive européenne, à savoir qu'elle ne visait pas une menace terroriste concrète (*supra* II./c). Le simple risque abstrait de criminalité grave ne suffisait pas pour faire une exception (art. 15 par. 1 de la directive 2002/58). La LSCPT, au contraire, oblige sans motif aucun que les fournisseurs conservent les données secondaires de communication et de localisation ainsi que les données relatives à la messagerie électronique.

VI. Conclusion

39

La présente contribution a mis en lumière un arrêt récent de la CJUE sur l'obligation de conservation de données secondaires par les fournisseurs de télécommunication et d'Internet. L'arrêt a précisé la portée de l'art. 15 de la directive 2002/58. Ce dernier permet une conservation généralisée et indifférenciée sur une période limitée pour autant que la sécurité nationale soit en danger. La sécurité

nationale est en danger selon la Cour de justice de l'Union européenne lorsqu'il s'agit d'activités de nature à déstabiliser gravement les structures constitutionnelles politiques, économiques ou sociales fondamentales d'un pays, ou qui menacent directement la société, la population ou l'État, ce qui est typiquement le cas du terrorisme. Au contraire, la criminalité grave n'est pas un motif suffisant qui permet une conservation généralisée et indiscriminée de données.

40

À ce titre, la loi allemande a été jugée contraire au droit européen car elle obligeait les fournisseurs à conserver à titre préventif aux fins de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

41

De prime abord, le droit suisse semble contenir un cadre législatif solide en matière de protection des données. En effet, la nouvelle loi sur la protection des données, tout comme son ancêtre, permet le traitement de données sensibles seulement si une loi au sens formelle le permet. Il ne s'agit cependant que d'une exigence de *forme* car il faut encore déterminer ce que renferme la loi au sens formel. En l'occurrence, la LSCPT oblige les fournisseurs de télécommunication et d'accès à Internet à une conservation généralisée et indiscriminée en dehors de tout motif.

42

Ainsi, le constat que nous pouvons tirer suite à l'analyse de la législation suisse n'est pas très éloigné de l'affaire dite « des fiches ». En effet, dans les deux cas, les informations sont collectées sans motif. La différence réside dans le fait que les données collectes par application de la LSCPT ne peuvent être traitées que lorsque le Code pénal ou la LRens

trouvent application et dans un délai de 6 mois. Ce système de surveillance généralisé permet, à l'instar du panoptique décrit par Foucault, une surveillance permanente dans ses effets, mais discontinue dans son action car tributaire d'une action pénale ou de l'application de la LRens. Cependant, dans un panoptique, l'essentiel réside dans le fait qu'on se sache surveillé et non qu'on le soit effectivement. Le droit suisse atteint ce but aisément.

Notes de bas de page:

1. * Doctorant et assistant auprès de la Chaire de droit civil I de l'Université de Fribourg. L'auteur tient à remercier Madame la Professeure Christiana Fountoulakis, titulaire de la Chaire de droit civil I à l'Université de Fribourg, et Madame Milena Hendriks, LL.M (Heidelberg), assistante diplômée auprès de la Chaire de droit des obligations II à l'Université de Fribourg, pour leurs commentaires critiques lors de l'élaboration de cet article ↑

2. Événements survenus au DFJP – Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989 (FF 1990 p. 593 ss), p. 776. ↑

3. Événements survenus au DFJP – Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989 (FF 1990 p. 593 ss), p. 776. ↑

4. Événements survenus au DFJP – Rapport complémentaire de la commission d'enquête parlementaire (CEP) du 29 mai 1990, (FF 1990 p. 1469 ss) p. 1497. ↑

5. Arrêt du 20 septembre 2020, SpaceNet, C-793/19 (Affaires

jointes C-793/19, C-794/19), EU :C :2022 :702.. ↑

6. « Telekommunikationsgesetz » du 22 juin 2004 (BGBl. 2004 I, p. 1190). ↑

7. 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. ↑

8. Arrêt du 5 avril 2022, Commissioner of An Garda Siochana e.a., C-140/20, EU :C :2022 :258, point 40. ↑

9. Arrêt du 20 septembre 2020, SpaceNet, C-793/19 (Affaires jointes C-793/19, C-794/19), EU :C :2022 :702, point 72. ↑

10. Arrêt du 5 avril 2022, Commissioner of An Garda Siochana e.a., C-140/20, EU :C :2022 :258, point 58. ↑

11. Arrêt du 20 septembre 2020, SpaceNet, C-793/19 (Affaires jointes C-793/19, C-794/19), EU :C :2022 :702, point 73. ↑

12. Arrêt du 5 avril 2022, Commissioner of An Garda Siochana e.a., C-140/20, EU :C :2022 :258, point 65. ↑

13. Arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258). ↑

14. Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 61. ↑

15. Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 62. ↑

16. Bovenkerk Frank/Abou Chakra Bashir, *Terrorisme et criminalité organisée*, Nations Unies : Office contre la drogue et le crime – Forum sur le crime et la société, Volume 4, numéro 1 et 2, décembre 2004, p. 3 ss, 3. ↑

17. Bovenkerk Frank/Abou Chakra Bashir, *Terrorisme et criminalité organisée*, Nations Unies : Office contre la drogue et le crime – Forum sur le crime et la société, Volume 4, numéro 1 et 2, décembre 2004, p. 3 ss, 3. ↑

18. RO 2022 491. ↑

19. Bondallaz Stéphane, *La protection des personnes et de leurs données dans les télécommunications*, Fribourg 2007, N 532 ; ATF 143 I 253 c. 3.3. ↑

20. Métille Sylvain, *La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations*, in : Epiney Astrid/Moser Sophie/Rovelli Sophia (édit.), *La révision de la Loi fédérale sur la protection des données*, Zurich Bâle Genève 2022. ↑

21. Mund, art. 34 N 5 LPD, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (édit.), Datenschutzgesetz, 2ème éd., Berne 2023. ↑

22. La loi au sens formel est la source par excellence des règles de droit qui régit les rapports sociaux ou au moins leurs principaux contours, par opposition à la loi au sens matériel, qui, bien qu'elle contienne aussi des règles de droit, a pour but de préciser la loi au sens formel. La différence majeure entre ces deux formes est que la première est soumise de manière quasiment systématique au référendum, au contraire de la seconde. (Gonin Luc, *Droit constitutionnel suisse*, N 3907, 3941). ↑

23. Mund, art. 17 N 1 LPD (note de bas de page 16). ↑

24. Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013 (FF 2013, p. 2379 ss), p. 2403. ↑

25. Message LSCPT, p. 2403 (note de bas de page 19). ↑

26. Macaluso Alain/Piquerez Gérard, *Procédure pénale suisse*, 3ème éd., Zurich 2011, N 1459. ↑

27. Macaluso Alain/Piquerez Gérard, N 1459 ss (note de bas de page 21). ↑

28. Message LSCPT 2013, p. 2393 (note de bas de page 19). ↑

29. Message LSCPT 2013, p. 2394 (note de bas de page 19). ↑

30. Perrin Bertrand/Gafner Julien, *Droit pénal – Pénal law / Le droit de la lutte antiterroriste / 1. -2.*, in : Heckendorn Urscheler Lukas (éd.), *Rapport suisses présentés au XIXe Congrès international de droit comparé / Swiss Reports Presented at the XIXth International Congress of Comparative Law*, 2014 p. 351 ss, 353. ↑