La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux
**Actualités Droits-Libertés | 2020**

# Savoir resserrer les mailles du filet

## À propos de l'arrêt du 6 octobre 2020 de la Cour de Justice de l'Union européenne

**Vincent Sizaire**

OpenEdition Journals

**Electronic version**
URL: http://journals.openedition.org/revdh/10627
DOI: 10.4000/revdh.10627
ISSN: 2264-119X

**Publisher**
Centre de recherches et d'études sur les droits fondamentaux

**Electronic reference**
Vincent Sizaire, « Savoir resserrer les mailles du filet », *La Revue des droits de l'homme* [Online], Actualités Droits-Libertés, Online since 28 November 2020, connection on 02 December 2020. URL : http://journals.openedition.org/revdh/10627 ; DOI : https://doi.org/10.4000/revdh.10627

# Savoir resserrer les mailles du filet

## À propos de l'arrêt du 6 octobre 2020 de la Cour de Justice de l'Union européenne[1]

Vincent Sizaire

1 Si l'on s'en tient à la classification aristotélicienne des disciplines de l'esprit, le Droit est un art[2]. Mais un art particulier, dont la fonction éminemment démocratique requiert davantage de réalisme que de lyrisme, *a fortiori* lorsqu'il s'agit d'encadrer les atteintes les plus importantes à nos libertés. Depuis le début du siècle, le développement exponentiel des technologies de l'information et de la communication a conduit à la mise en place, par les services de renseignement de la plupart des États européens, de dispositifs de surveillance de masse des échanges informatiques de leurs citoyen-e-s. Face à l'atteinte considérable à la vie privée que constitue cette captation occulte, générale et indifférenciée de notre activité électronique, il n'est pas inutile de voir la Cour européenne des droits de l'homme rappeler que *« le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret »*, car il s'agit d'un *« domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière »*[3]. Toutefois, ces pétitions de principe apparaissent de bien faible portée lorsque, dans le même temps, la Cour considère que le choix de mettre en œuvre un dispositif de surveillance de masse des échanges informatiques relève de la marge d'appréciation des États[4]. Si le juge de Strasbourg veille à l'existence de garanties adéquates et effectives contre les abus, il admet qu'elles puissent être insuffisantes pour peu que *« dans l'ensemble »*, le risque d'arbitraire apparaisse réellement prévenu[5]. Une telle grille de lecture qui l'a conduit à valider sans aucune réserve le système de surveillance suédois – dont le cadre juridique est certes protecteur des libertés – et à ne censurer que marginalement son homologue britannique – lequel l'est beaucoup moins -[6].

2 C'est dans ce contexte que la Cour de Justice de l'Union européenne était conduite, sur questions préjudicielles du Conseil d'État français, de la Cour constitutionnelle belge et de *l'Investigatory Powers Tribunal* anglais, à se prononcer sur la conformité au droit européen des législations nationales permettant de conserver de manière généralisée ou indifférenciée les données des utilisateurs d'internet relatives au trafic et à la

localisation. Sa décision était d'autant plus attendue que si elle avait, en réalité, déjà jugé que les États membres ne pouvaient imposer aux fournisseurs de services de communications électroniques une telle obligation de conservation[7], la pression de certains gouvernements pour l'inflexion de sa jurisprudence était tout aussi grande[8]. Une pression à laquelle la Cour aura heureusement su, en grande partie, résister : en limitant rigoureusement les possibilités de surveillance massive des réseaux numériques (I) et en posant de solides exigences s'agissant du contrôle de cette surveillance (II), elle invite nombre d'États, dont la France, à renforcer significativement l'encadrement de l'activité de leurs services de renseignement.

## I/- La limitation de la surveillance de masse

3 Se retranchant derrière la marge de manœuvre laissée aux États, la Cour de Strasbourg est conduite à n'exercer qu'un contrôle restreint et, pour tout dire, approximatif sur l'atteinte à la vie privée qu'emporte la surveillance massive de nos échanges informatiques. C'est au contraire à un plein et entier contrôle de nécessité et de proportionnalité de l'atteinte que se livre la Cour de Luxembourg, au visa des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne – qui garantissent respectivement le droit au respect de la vie privée et familiale et des données personnelles – et de la directive n° 2002/58/CE 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 »*[9]. La Cour rappelle ainsi que *« la protection du droit fondamental au respect de la vie privée exige [...] que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause »*[10]. Comme il l'avait fait en 2016, le juge communautaire en déduit que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose en principe à une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée – ou la transmission généralisée et indifférenciée aux services de sécurité et de renseignement – des données relatives au trafic et à la localisation, et ce quel qu'en soit le motif[11].

4 La Cour est en revanche amenée à préciser et, d'une certaine façon, à infléchir sa jurisprudence, en considérant qu'une telle surveillance de masse peut néanmoins être mise en œuvre dans certaines hypothèses restrictives. En premier lieu, elle reconnaît aux autorités nationales le pouvoir d'enjoindre *« aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation »* et de procéder à l'analyse automatisée de ces données, *« dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible »*[12]. En d'autres termes, si elle ne peut intervenir de façon permanente, la surveillance de masse peut, pour faire face à une menace effective, être ponctuellement mise en œuvre par les services de renseignement. En deuxième lieu, la Cour reconnaît également aux États la faculté de procéder *« aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique »* à une conservation non pas indifférenciée mais *« ciblée des données relatives au trafic et des*

*données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique* »[13]. En dernier lieu, elle les autorise à procéder au recueil systématique des données ne permettant pas, en soi, de retracer les échanges et dont la conservation est dès lors réputée n'emporter qu'une faible atteinte à la vie privée des usagers : les *« adresses IP attribuées à la source d'une connexion »*, ainsi que les *« données relatives à l'identité civile des utilisateurs de moyens de communications électroniques »*, c'est-à-dire les coordonnées de l'usager[14].

5 Si cette solution laisse aux États d'importantes marges de manœuvre, elle reste de nature à réduire sensiblement le risque d'arbitraire aujourd'hui associé à la mise en œuvre des activités de renseignement, en particulier en France. L'article L. 851-1 du Code de la sécurité intérieure autorise ainsi, en dehors de toute injonction circonstanciée des autorités, le recueil auprès des opérateurs de communications électroniques de l'ensemble *« des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques »*[15]. Soit très précisément le type dispositif de conservation générale et indifférenciée que prohibe l'arrêt de la Cour de Justice. Mais la contrariété du droit français au droit de l'Union européenne, apparait de façon plus encore manifeste encore dès lors qu'on le confronte aux modalités du contrôle des mesures de surveillance telles qu'elles ressortent des exigences du juge communautaire.

## II/- Le renforcement du contrôle des mesures de surveillance

6 Reprenant en cela sa jurisprudence antérieure, la Cour de Luxembourg rappelle qu'afin de garantir la nécessité et la proportionnalité de l'atteinte à la vie privée, la législation nationale *« doit prévoir des règles claires et précises régissant la portée et l'application de la mesure* [de surveillance] *et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données »*[16].

7 Loin de l'approche « impressionniste » du juge de Strasbourg, ce cadre suppose tout d'abord que les motifs pour lesquels la surveillance de masse est mise en œuvre soient définis de façon précise. À cet égard, la Cour souligne que seule *« une menace grave pour la sécurité nationale »* peut justifier le recours à une conservation indifférenciée des données et, outre ce motif, seules *« la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique »* peuvent justifier une conservation ciblée[17]. Si ces notions peuvent sembler insuffisamment définies, la Cour précise que les menaces pour la sécurité nationale se rapportent aux *« activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme »*, et qu'elles *« se distinguent, par leur nature et leur*

*particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique.* »[18]. En outre, elle indique que la menace doit être caractérisée par *« des circonstances suffisamment concrètes »*[19]. Et, de ce point de vue, force est de constater que le cadre juridique français manque singulièrement de rigueur, dès lors qu'il permet le recours à la conservation massive de données non seulement pour protéger *« l'indépendance nationale, l'intégrité du territoire et la défense nationale »*, mais également pour prévenir *« la reconstitution de groupements dissous »*, *« des violences collectives de nature à porter gravement atteinte à la paix publique »* ou *« la criminalité et la délinquance organisées »*[20].

8 Par ailleurs, la Cour juge qu'à l'exception de la conservation de l'identité civile des utilisateurs de moyens de communications électroniques, le recueil systématique des données ne peut être ordonné que *« pour une période temporellement limitée au strict nécessaire »*[21], même si la mesure peut être renouvelée. Surtout, elle est conduite à renforcer très sensiblement le contrôle juridictionnel ou quasi-juridictionnel des activités de renseignement. Ainsi, la décision enjoignant à un fournisseur de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données doit pouvoir *« faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant »*[22]. Le juge de l'Union profite en outre des questions qui lui étaient soumises pour souligner que cette exigence s'applique également à l'hypothèse, distincte, du *« recueil en temps réel (sic.) des données relatives au trafic et des données de localisation »* d'une personne soupçonnée d'être impliquée dans une activité terroriste. Auquel cas, le contrôle doit être systématique et préalable[23].

9 À cet égard également, la compatibilité du droit français avec le droit européen s'avère largement discutable. C'est en effet au seul premier ministre qu'est aujourd'hui reconnu le pouvoir d'ordonner les mesures de surveillance pouvant être mises en œuvre par les services de renseignement. S'il doit en principe recueillir l'avis préalable d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement, ledit avis n'est que consultatif – loin, donc, de l'exigence d'effet contraignant évoqué par la Cour de Justice[24]. Certes, depuis la réforme opérée par la loi n°2015-912 du 24 juillet 2015, le Conseil d'État peut être saisi par la commission, mais également par toute personne *« souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard »*[25]. Cependant, il est permis de douter qu'un tel contrôle puisse être considéré comme réellement effectif. D'une part, il n'intervient qu'autant qu'une personne saisisse la juridiction administrative. Par hypothèse, les activités de renseignement sont occultes et notre droit ne prévoit aucune obligation de notifier aux personnes surveillées l'existence de la mesure dont elles ont fait l'objet. Or, comme le rappelle la Cour, dès lors qu'elle peut être faite sans compromettre une surveillance en cours. *« cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits »*[26]. Le contrôle exercé par le Conseil d'État s'avère donc des plus hypothétiques. D'autre part, il n'intervient en tout état de cause qu'*a posteriori* alors que le juge communautaire exige, s'agissant du recueil de données « en temps réel », un contrôle préalable.

10 Les insuffisances du droit français méritent d'autant plus d'être soulignées que la Cour de Justice a tenu à préciser que *« le juge pénal national [est tenu] d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de*

*l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits »*[27]. Tel est notamment le cas de l'ensemble des informations qui, sous couvert de renseignement anonyme, sont à l'origine de nombre de procédures pénales ouvertes en matière de délinquance organisée et, singulièrement, de criminalité dite terroriste. C'est dire si, pour peu que le juge français s'en empare avec suffisamment de volontarisme, la décision de la Cour promet d'être à l'origine de nombreux autres bouleversements de notre ordre répressif.

*

**CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18.**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

## NOTES

**1.** CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18.

**2.** Michel Villey, « La philosophie du droit d'Aristote », *in* Michel Villey (dir.), *La formation de la pensée juridique moderne*, Presses Universitaires de France, Paris, 2013, pp. 78-99.

**3.** Cour EDH, 19 juin 2018, Centrum för Rättvisa c. Suède, Req. n° 35252/08, cons. 101 et 105.

**4.** Ibid., cons. 104.

**5.** Cour EDH, 13 septembre 2018, Big brother watch et a. c. Royaume-Uni, Req. n° 58170/13, 62322/14 et 24960/15, cons. 369.

**6.** Jean-Philippe Foegle, « La Cour Européenne des Droits de l'Homme procède à une condamnation en demi-teinte de la surveillance "de masse". », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 26 octobre 2018.

**7.** CJUE, 21 décembre 2016, Tele2 Sverige et Watson (C-203/15 et C-698/15).

**8.** Dans le résumé officiel de l'arrêt, il est ainsi indiqué, en termes diplomatiques, que sa jurisprudence *« a suscité les préoccupations de certains États, craignant d'avoir été privés d'un instrument qu'ils estiment nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité »*.

**9.** Dont l'article 15 dispose que tout atteinte à la vie privée des usagers, notamment la conservation de donnée, doit être *« 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 ».*

**10.** CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18, cons. 130.

**11.** Ibid., cons. 141 et 212

**12.** Ibid. cons. 168 et 192.

**13.** Ibid. cons. 147.

**14.** Ibid. cons. 155 et 157.

**15.** Le texte vise notamment *« les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».*

**16.** CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18, cons. 132.

**17.** Ibid., cons. 137 et 147.

**18.** Ibid., cons. 135 et 136.

**19.** Ibid. cons. 138.

**20.** Article L.811-3 du code de la sécurité intérieure.

**21.** CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18, cons. 168.

**22.** Ibid., cons. 139.

**23.** Ibid., cons. 192.

**24.** Article L. 821-4 du code de la sécurité intérieure.

**25.** Article L. 841-1 du code de la sécurité intérieure.

**26.** CJUE (grande chambre), 6 octobre 2020, Quadrature du Net et autres, C-511/18, C-512/18 et C-520/18, cons. 190.

**27.** Ibid., cons. 228.

## ABSTRACTS

Quatre ans après l'arrêt Tele2 Sverige et Watson par lequel elle a jugé que les États membres ne pouvaient imposer aux fournisseurs de services de communications électroniques une conservation générale et indifférenciée des données de navigation des usagers des réseaux numériques, la Cour de Justice de l'Union européenne confirme en grande partie sa jurisprudence. En limitant rigoureusement les possibilités de surveillance massive des réseaux et en posant de solides exigences s'agissant du contrôle de cette surveillance, elle invite nombre d'États – au premier rang desquels la France – à renforcer significativement l'encadrement de l'activité de leurs services de renseignement.

# AUTHOR

VINCENT SIZAIRE

Maître de conférences associé à l'Université Paris Nanterre