Surveillance de masse, liberté publique et état d'exception

Parsa, Saba; Van Gyseghem, Jean-Marc

Published in:
Bulletin social et juridique

Publication date:
2022

Document Version
le PDF de l'éditeur

Surveillance de masse, liberté publique et état d'exception : quand sécurité ne rime plus avec protection des données à caractère personnel et vie privée

Saba Parsa
Avocate au barreau du Brabant wallon
DPO certifiée
Assistante en droit à l'Université Saint-Louis – Bruxelles
Première vice-présidente du Conseil supérieur de l'audiovisuel
et
Jean-Marc Van Gyseghem
Avocat au barreau de Bruxelles
Directeur de recherche au Centre de recherche information, droit et société de l'UNamur

Introduction

En ce début de XXIe siècle, les situations dites d'urgence se multiplient et se succèdent : menaces terroristes, gestion des pandémies, crises migratoires, changement climatique, guerres, cyberattaques, voire cyberguerres d'envergure mondiale… Dans ce contexte, les gouvernements jouent pourtant régulièrement aux « pompiers pyromanes », sacrifiant sur l'autel de la sécurité les libertés fondamentales et particulièrement la protection des données à caractère personnel, par l'utilisation de solutions numériques de surveillance massive des citoyens. Pire encore, le citoyen semble s'en accommoder, de sorte que le conformisme et la surveillance deviennent les nouvelles normes au détriment de nos libertés fondamentales.

Pour comprendre ce phénomène et les garde-fous élaborés par le droit fondamental des droits de l'homme, nous définirons, dans un premier temps, la notion de « surveillance de masse » et examinerons les normes qui l'encadrent à l'échelle de l'Europe (I), avant de tirer les enseignements de la récente jurisprudence *Big Brother*[1] de la Cour européenne des droits de l'homme (ci-après, « Cour eur. D.H. ») (II).

1. Notion et contexte juridique

Le phénomène de surveillance de masse n'est pas nouveau. On en trouve une première forme organisée de service secret de surveillance sous l'Antiquité, au premier siècle avant notre ère, sous l'autorité de l'empereur Auguste : le *cursus publicus*[2]. Il s'agissait d'un service postal destiné en réalité à être un service de renseignement[3]. Plus tard, en France, on retrouve une autre institution de surveillance : le cabinet du secret des postes, couramment appelé « Cabinet noir », institué, semble-t-il, sous Louis XIV. Plus récemment, en février 1950, dans l'ancienne République démocratique allemande (en abrégé, « RDA »), l'un des systèmes de surveillance étatique les plus célèbres du XXe siècle, connu sous le nom de « Stasi »[4] était mis en place[5], remplaçant la terreur staliniste[6], afin d'assurer le contrôle social et éliminer toute forme de dissidence.

Si jusqu'alors la surveillance était essentiellement organisée par l'État, la fin du XXe siècle et le début du XXIe siècle amorcent une nouvelle ère pour la surveillance. Soutenue par de nouveaux moyens techniques de communication et par l'arrivée de nouveaux acteurs issus du développement d'Internet, la surveillance massive émerge à l'échelle globale, présentant plusieurs caractéristiques[7]. Premièrement, l'attention est désormais portée tant sur les métadonnées que sur les données elles-mêmes[8]. Deuxièmement, cette nouvelle surveillance opère sur un principe de « collecte en masse, accès en détail »[9], grâce à l'utilisation d'un ensemble de technologies appelé « *big data* », dont la notion n'est pas définie de manière unanime[10]. L'objectif poursuivi par l'utilisation de ces technologies d'analyse est la détection de relations qui seraient autrement restées imperceptibles. Troisièmement, cette surveillance fonctionne en coopération entre les acteurs privés et publics[11].

Dans ce contexte, définir la surveillance de masse semble laborieux. Jeremy Bentham, le père de l'utilitarisme, défi-

1 *Cour eur. D.H., Big Brother Watch et autres c. Royaume-Uni, 25 juin 2021.*

2 *H.-G. Pflaum, « Essai sur le cursus publicus dans le Haut-Empire », in Mémoires présentés par divers savants à l'Académie des inscriptions et belles-lettres de l'Institut de France, t. 14, 1re partie, Paris, Imprimerie nationale, 1940, p. 189, disponible sur : www.persee.fr/doc/mesav_0398-3587_1940_num_14_1_1120.*

3 *Ibid., p. 213.*

4 *Le terme est une contraction de l'allemand Staatssicherheit, le nom du ministère, littéralement traduit en « sécurité de l'État ».*

5 *S. Lorrain, Histoire de la RDA, Paris, P.U.F., 1994 ; voy. également « Stasi, histoire d'une police politique (RDA) », Histoire pour tous, 12 novembre 2019, disponible sur : www.histoire-pour-tous.fr/dossiers/3491- la-stasi-histoire-dune-police-politique-rda.html.*
La notion de panoptique renvoie au concept développé par Jeremy Bentham au XVIIIe siècle. Il va découvrir un moyen de surveillance qu'il considère comme sa grande invention, une solution universelle de gouvernance de l'homme économique.

6 *En ce sens, Amnesty International, « L'exemple de la Stasi – L'histoire de la surveillance de masse incite à la prudence », 31 mars 2015.*

7 *P. Bernal, « Data Gathering, Surveillance and Human Rights: Recasting the Debate », Journal of Cyber Policy, vol. 1, n° 2, 2019, p. 246.*

8 *Les métadonnées sont les données à propos des données, elles décrivent ou définissent une autre donnée et sont souvent générées automatiquement, voy. P. Bernal, « Data Gathering, Surveillance and Human Rights », op. cit., p. 8.*

9 *P. Bernal, « Data Gathering, Surveillance and Human Rights », op. cit., p. 246.*

10 *La CNIL, l'autorité française de protection des données, évoque un concept « encore flou et difficile à synthétiser » (CNIL, « Vie privée à l'horizon 2020, Paroles d'expert », Les cahiers IP, n° 1, 2012, p. 18).*

11 *C'est sur ce modèle que sont organisés la collecte et le traitement des données dans le cadre des applications Covid safe ticket. Les citoyens introduisent eux-mêmes leur données dans l'application, puis d'autres citoyens les contrôlent et les sanctionnent, en les privant pas exemple de vie sociale, d'accès aux lieux publics, etc.*

nissait en son temps la surveillance comme l'ensemble des mécanismes visant à faire agir les sujets dans un sens déterminé du seul fait d'être sous le regard d'autrui, qui analyse toutes les traces laissées par l'individu[12]. Aujourd'hui, la surveillance est organisée sous diverses formes avec des objectifs multiples, fait paraitre la nécessité de subdiviser le concept en plusieurs types : (i) la surveillance, (ii) la surveillance de masse et (iii) la surveillance dite diffuse[13].

Il s'ensuit que la surveillance « post-panoptique »[14] contemporaine dite « de masse », s'appuyant sur les prédictions des comportements humains, permises par l'utilisation des technologies des « *big data* », peut se définir comme :

> « Tout processus, centralisé ou non, d'acquisition systématique et à grande échelle d'informations relatives à l'individu et aux objets dont ils sont responsables, à l'aide de technologie de l'information, à l'occasion duquel l'individu est tour à tour agent et sujet de la surveillance, en vue de l'obtention d'un bénéfice extérieur à la simple collecte de l'information visant à prévenir, influencer, orienter, gérer, protéger ou sanctionner le sujet de la surveillance ».

Le cadre définitionnel posé, l'examen de l'équilibre entre la surveillance de masse et le respect des droits fondamentaux passe inextricablement par l'étude de la protection offerte au respect de la vie privée, mais également et surtout à la protection des données à caractère personnel à l'échelle supranationale. À ce titre, il est rappelé que la Convention européenne des droits de l'homme (ci-après, « CEDH » ou « Convention ») assure la protection des données à caractère personnel, par le biais de son article 8, mais également de la Convention n° 108[15]. Or, il existe une divergence majeure d'approche qu'il revient ici de souligner entre des garanties offertes, d'une part par l'article 8 de la CEDH et, d'autre part par la Convention n° 108. En effet, cette dernière, dès son intitulé, met au centre la protection de la personne concernée par le traitement et ses droits, de sorte que, dans un contexte de marchandisation des données à caractère personnel, l'individu et son intégrité physique et morale sont au cœur du discours juridique[16].

De son côté, l'Union européenne règle l'ingérence des États membres dans la mise en œuvre des mesures de surveillance par le truchement des articles 7 et 8 de la Charte[17], mais également par un ensemble de directives et de règlements visant à harmoniser les pratiques au sein de chaque État, et notamment le règlement général relatif à la protection des données (en abrégé, « RGPD »)[18], la directive relative aux communications électroniques (directive *ePrivacy*)[19] ou encore la directive relative au traitement des données à caractère personnel dans le secteur de la police et de la justice[20] (directive police-justice).

Reste maintenant à examiner la protection apportée par la Cour eur. D.H., particulièrement à l'occasion de son arrêt récent *Big Brother.*

2. Protection contre la surveillance de masse, enseignements tirés de l'arrêt *Big Brother*

Suite aux révélations d'Edward Snowden sur la surveillance massive des communications et les programmes de partage d'informations mis en œuvre par les services de renseignement des États-Unis et du Royaume-Uni, trois requêtes[21] ont été déposées devant la Cour eur. D.H. Lesdites requêtes dénonçait plus particulièrement le système de surveillance de masse mis en place par le *Regulation Investigatory Powers Act 2000* (ci-après, « RIPA »), instaurant différents régimes, à savoir : (1) l'interception massive des données de communications électroniques, (2) le partage des renseignements avec des gouvernements étrangers et (3) la demande de données aux fournisseurs de services de communication. Les requérants ont notamment fait valoir que ce régime britannique violait le droit au respect de la vie privée consacré à l'article 8 de la CEDH[22].

Il convient d'emblée de souligner que le terrain jurisprudentiel n'était pas vierge en matière de surveillance. Sollicitée de manière régulière sur la question relative à la conformité des mesures de surveillance avec la CEDH, la Cour eur. D.H. a développé une jurisprudence importante[23] au départ de l'affaire *Klass e.a. c. Allemagne* en 1978[24]. De manière générale, lors de l'examen de la conformité à la CEDH des restrictions aux libertés fondamentales, le contrôle de la Cour eur. D.H. se concentre en trois phases différentes. Premièrement, elle vérifie que la requête tombe dans le champ des droits protégés et établit la qualité de « victime » dans le chef des requérants. Deuxièmement, elle vérifie si l'État assume une obligation positive concernant

12 *G. Tusseau, « Sur le panoptisme de Jeremy Bentham », Revue Française d'Histoire des Idées Politiques, 2004/1, n° 19, p. 38.*

13 *S. Parsa, J.-M. Van Gyseghem, « Surveillance de masse, liberté publique et état d'exception. Quand sécurité ne rime plus avec protection des données à caractère personnel et vie privée », in S. Parsa et F. Tulkens (dir.), État de droit, état d'exception et libertés publique, Limal, Anthemis, 2022, pp. 89-147. Voy. p. 5 de ce numéro pour plus d'informations concernant cet ouvrage.*

14 *Z. Bauman et D. Lyon, Liquid Surveillance : A Conversation, Cambridge, Malden, Polity Press, 2013, p. 4967.*

15 *Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981, approuvée par la loi du 17 juin 1991, M.B., 30 décembre 1993, p. 29023; attentif à une protection internationale poussée des données à caractère personnel, le Conseil de l'Europe a adopté le 18 mai 2018 un protocole d'amendement qui modernise la Convention n° 108 pour donner naissance à la Convention n° 108+; Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signé à Elseneur (Danemark) le 18 mai 2018.*

16 *F. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », in Rev. trim. dr.h., n° 108/2016, pp. 872 et s.*

17 *Charte des droits fondamentaux de l'Union européenne, J.O.U.E., C-326, 26 octobre 2012.*

18 *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, J.O.U.E., L 119, 4 mai 2016.*

19 *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), J.O.U.E., L 201, 31 juillet 2002.*

20 *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, J.O.U.E., L 119, 4 mai 2016.*

21 *Req. nos 58170/13, 62322/14 et 24960/15.*

22 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950, entrée en vigueur le 3 septembre 1953.*

23 *En effet, la cour a développé ces dernières années une jurisprudence substantielle en la matière. Ainsi, dans l'arrêt Weber et Saravia c. Allemagne, la cour avait conclu l'État disposait d'une large marge d'appréciation en la matière ; Cour eur. D.H., Weber et Saravia c. Allemagne, 26 juin 2006, requête 54934/00. En revanche, dans l'arrêt Liberty et autres c. Royaume-Uni, elle a jugé que la loi nationale en vigueur relative aux interceptions de communications par téléphone ou courriel ne garantissait pas une protection suffisante contre les abus de pouvoir car l'étendue et les modalités du pouvoir d'appréciation des autorités n'était pas clairement définies ; Cour eur. D.H., Liberty et autres c. Royaume-Uni, 1er juillet 2008, requête 58243/00. Plus récemment, dans son arrêt Centrum för Rättvisa c. Royaume de Suède également rendu le 25 mai 2021, la grande chambre a conclu à la violation de l'article 8 de la Convention jugeant en particulier, que le régime en question souffrait de trois carences : (i) l'absence de règle claire concernant la destruction des éléments interceptés qui ne contiennent pas de données à caractère personnel, (ii) le fait que ni la loi relative au renseignement d'origine électromagnétique ni aucun autre texte n'énonce l'obligation de prendre en compte les intérêts liés à la vie privée lorsqu'une décision de partage de renseignements avec des partenaires étrangers est adoptée, et (iii) l'absence de contrôle a posteriori effectif; Cour eur. D.H., Centrum För Rättvisa c. Suède, (gde ch.), 19 juin 2018, requ. nos 58170/13, 62322/14 et 24960/15.*

24 *Cour eur. D.H., Klass e.a. c. Allemagne, 6 septembre 1978.*

les droits garantis, et enfin, troisièmement, si par ailleurs il s'en acquitte valablement. Autrement dit, une fois l'ingérence vérifiée et la qualité de « victime » établie, la cour procède à l'analyse de facteurs autorisant les restrictions au droit fondamental protégé par la CEDH, à savoir le critère de légalité, de légitimité et de nécessité (ou de proportionnalité).

2.1. Critère de légitimité

Ainsi dans l'arrêt *Big Brother Watch et autres c. Royaume-Uni* (ci-après, « l'arrêt *Big Brother* »), la Cour eur. D.H., dans un premier temps rappelle sa jurisprudence constante en matière de surveillance massive. Abordant la question de la légitimité, elle confirme sa position dans l'arrêt *Weber et Saravia*[25] de 2006, et dispose que « la décision d'utiliser un système d'interception en masse relève de la marge d'appréciation reconnue aux États »[26]. En effet, de manière constante depuis 1978, la cour accorde au législateur national un certain pouvoir discrétionnaire qui n'est toutefois pas illimité, examinant dès lors l'existence de garanties adéquates et suffisantes contre les abus et l'existence de recours adéquats.

Ce contrôle essentiel consiste en un examen in concreto des procédures et mécanismes de contrôle a priori ou a postiori à disposition des individus[27]. Ainsi, elle revient sur les six garanties minimales, appelées également « les six garanties Weber », de l'arrêt du même nom[28], et impose que le droit national indique clairement :

1. la nature des infractions susceptibles de donner lieu à un mandat d'interception ;
2. la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ;
3. la limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen ;
4. l'utilisation et la conservation des données recueillies ;
5. les précautions à prendre pour la communication des données à d'autres parties ;
6. les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.

Cependant, dans un second temps, la cour constate les limites de cette jurisprudence antérieure en soulignant que : « […] depuis, les progrès technologiques ont significativement modifié la manière dont on communique. On vit de plus en plus en ligne, ce qui génère un volume bien plus important de communications électroniques que celui qui pouvait être généré il y a dix ans, et les communications ont nettement évolué dans leur nature et leur qualité […] »[29]. Ainsi, elle distingue la protection à octroyer à la surveillance ciblée de celle à octroyer à la surveillance de masse. Elle remarque à ce titre que le régime d'interception en masse par les services de renseignement de communications transfrontalières dénoncé en l'arrêt *Big Brother* soulève des difficultés spécifiques, eu égard à l'évolution technologique de l'ère numérique[30].

Elle définit dès lors l'interception en masse comme « un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance. Les régimes d'interception en masse ne sont pas forcément tous conçus exactement sur le même modèle, les différentes étapes du processus ne sont pas nécessairement distinctes et ne répondent pas toujours à un ordre chronologique strict. »

Ensuite, la cour décrit les étapes du processus d'interception ou de la surveillance en masse comme suit :

> « a) interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées) ;
>
> b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées ;
>
> c) examen par des analystes des communications sélectionnées et des données de communication associées ; et
>
> d) rétention subséquente des données et utilisation du "produit final", notamment partage de ces données avec des tiers »[31].

2.2. Critère de légalité et de nécessité des mesures de surveillance

Ensuite, examinant le critère de légalité, la Cour eur. D.H. rappelle que l'ingérence doit être prévue par une loi s'agissant des mesures générales de surveillance. De manière spécifique, dans sa jurisprudence relative à la surveillance, ce critère est étroitement corrélé à celui de nécessité. En effet, la Cour eur. D.H. a procédé à un élargissement de son test de légalité en y intégrant le critère de nécessité, comme un élément essentiel à assurer la légalité de toute ingérence. La cour a ainsi jugé que : « […] la question de la légalité de l'ingérence est étroitement liée à celle de savoir si le régime institue par la [loi] satisfait au critère de la "nécessité", raison pour laquelle la Cour doit examiner conjointement les critères de la "prévisibilité au regard de la loi" et de la "nécessité". »[32]

Dès lors cette dernière vérifie simultanément si la mesure était « prévue par la loi » et si elle est « nécessaire »[33]. S'agissant de la surveillance de masse, à savoir non ciblée et à grande échelle, ce principe de nécessité fera l'objet d'un examen plus strict encore, en deux étapes afin de vérifier si les moyens prévus par la législation en cause pour atteindre ce but restent à tous égards à l'intérieur des bornes de ce qui est nécessaire dans une société démocratique[34]. Premièrement, la cour va évaluer la proportionnalité de

25 *Cour eur. D.H., Weber et Saravia c. Allemagne, 26 juin 2006, req. n° 54934/00.*
26 *Cour eur. D.H. (gde ch.), Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021, req. nos 58170/13, 62322/14 et 24960/15, § 275.*
27 *R. Angrisani, « Données personnelles et surveillance massive : quelle protection face aux ingérences des autorités publiques ? », in Revue québécoise de droit international, 2020, § 1er.*
28 *Cour eur. D.H., Weber et Saravia c. Allemagne, op. cit.*
29 *Cour eur. D.H. (gde ch.), Big Brother Watch et autres c. Royaume-Uni, op. cit., §§ 341-343.*
30 *Ibid., § 322.*
31 *Ibid., § 342.*
32 *Cour eur. D.H., Kennedy c. Royaume-Uni, op. cit., § 155.*
33 *Il s'ensuit que la question de la « légalité » doit être combinée avec la condition de « nécessité » et appelle à une analyse conjointe des deux conditions qui consiste à évaluer la proportionnalité du régime de surveillance au regard des buts légitimes poursuivis, voy. en ce sens F. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », op. cit., p. 863.*
34 *Ibid.*

la mesure de surveillance dans sa nature, compte tenu de sa portée et de ses caractéristiques technologiques. De la sorte, l'État devra être à même de justifier en quoi une telle méthode est nécessaire à la préservation de l'objectif légitime défini, ce qui implique de pouvoir démontrer que seule une collecte massive de données permet d'assurer une protection contre les menaces soulevées (test de nécessité au sens strict)[35]. Deuxièmement, elle vérifie que le choix de la surveillance massive se justifie pour recueillir des informations essentielles à la préservation de l'intérêt légitime poursuivi, notamment la sécurité nationale, à l'exclusion de voies alternatives moins intrusives (test de subsidiarité).

Ensuite, selon la cour, au niveau national, la nécessité et la proportionnalité des mesures prises doivent être appréciées à chaque étape du processus par une autorité indépendante du pouvoir exécutif, et ce, dès la définition de l'objet et de l'étendue du processus de surveillance de masse jusqu'au contrôle opéré *ex post*. Ces facteurs sont « des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 »[36]. Par là même, elle va outre sa jurisprudence classique dont elle a énoncé plus tôt les limites et souligne qu'un tel régime doit être encadré par des garanties procédurales dites « de bout en bout »[37].

3. Les garanties procédurales de « bout en bout »

Cette nouveauté, introduite par l'arrêt Big Brother, consiste en la vérification de l'existence de garanties procédurales et la mise en place de mécanismes de contrôle effectif. Eu égard au caractère secret de la surveillance et aux impératifs de sécurité nationale impliquant de maintenir ce secret dans le cadre de mesures de surveillance menées par l'État, la cour a dégagé une solution assurant un équilibre délicat entre les exigences d'efficacité des mesures de sécurité et la garantie des droits des individus. La cour examinera dès lors si le cadre juridique national définit clairement les éléments suivants :

> « 1. Les motifs pour lesquels l'interception en masse peut être autorisée ;
>
> 2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
>
> 3. La procédure d'octroi d'une autorisation ;
>
> 4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
>
> 5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;
>
> 6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
>
> 7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
>
> 8. Les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement. »[38]

Il s'ensuit que la surveillance de masse doit être encadrée par des « garanties de bout en bout »[39] de sorte que la légalité, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus.

Compte tenu de ce qui précède, en l'arrêt *Big Brother Watch c. Royaume-Uni*, la grande chambre a jugé à l'unanimité que le régime d'interception massive des données violait l'article 8 de la CEDH.

Conclusion

En somme, la Cour eur. D.H. opère ainsi un nouveau tournant dans sa jurisprudence en matière de surveillance de masse, en soulignant le développement d'obligations procédurales positives. Ces dernières visent notamment à garantir la transparence des traitements de données et l'accès à un recours effectif à charge des États, sous l'impulsion des obligations découlant du droit à la protection des données. Cette évolution jurisprudentielle témoigne d'un développement autonome du droit fondamental à la protection des données à caractère personnel. Elle semble tendre vers une logique plus managériale visant essentiellement à encadrer de manière optimale l'usage d'informations personnelles[14]. Cependant, paradoxalement, cette approche du risque d'abus pourrait être effectuée au détriment de l'article 8 de la CEDH, en ce qu'elle présente un risque significatif de perte de sens du droit à la vie privée au profit de cette approche managériale ou processuelle des mesures restrictives de libertés fondamentales. Ainsi, au nom de la « lutte contre le terrorisme » ou contre les « épidémies », des atteintes toujours plus larges à la vie privée des personnes pourraient être admises voire même, a fortiori, normalisées, au motif de l'existence de garanties procédurales adéquates. L'article 8 peut-il se satisfaire d'une telle approche ?

Force est de constater que le déploiement du numérique pousse les droits de l'homme tels que nous les connaissons dans leurs retranchements pour, éventuellement, reconnaître de nouveaux droits subjectifs afin de préserver l'État de droit et l'individu dans son intégrité et son altérité.

35 *Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, n° A/69/397, 23 septembre 2014, § 52.*

36 *La cour fait référence au rapport de la Commission de Venise, selon lequel deux des garanties majeures dans un régime d'interception en masse sont l'autorisation et le contrôle du processus ; Cour eur. D.H. (gde ch.), Big Brother Watch et autres c. Royaume-Uni, op. cit., § 197.*

37 *Ibid., § 350.*

38 *Ibid., § 361.*

39 *Ibid., § 350.*