Surveillance de masse, liberté publique et état d'exception

Parsa, Saba; Van Gyseghem, Jean-Marc

Published in:
État de droit, état d'exception et libertés publiques

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
Assistante en droit à l'Université Saint-Louis – Bruxelles
Première vice-présidente du Conseil supérieur de l'audiovisuel
Rédactrice en chef de la revue *DPO News*

Jean-Marc Van Gysèghem

Avocat au barreau de Bruxelles
Directeur de recherche au Centre de recherche information, droit et société de l'Université de Namur

«They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.»

Benjamin Franklin, 1775[1]

Introduction

Depuis le début du XXIe siècle, les situations dites d'urgence ou d'exception se multiplient et se succèdent. Menaces terroristes, pandémies, crises migratoires, changement climatique, voire bientôt cyberattaques ou cyberguerres d'envergure mondiale, l'état dit d'exception semble prendre ses quartiers dans nos démocraties. Il entraîne dans son sillage la pérennisation des mesures liberticides et un nouveau rapport à la normalité.

Dans ce contexte, et alors que la sortie de la crise sanitaire mondiale causée par la pandémie Covid-19 semble s'éloigner, les réactions parfois impulsives des États, invoquant le bouclier de l'état d'exception pour mettre en œuvre des mesures et dispositifs contraignants et invasifs[2], se démultiplient. Parmi ces dis-

1 J. Bigelow, *The Works of Benjamin Franklin*, vol. VII (Letters and Misc. Writings 1775-1779), New York, G.P. Putnam's Sons, Knickerbocker Press, 1904.

2 Conseil de l'Europe, *Mass Surveillance – Who Is Watching the Watchers?*, Strasbourg, Éditions du Conseil de l'Europe, 2016, p. 5.

positifs, ceux visant la surveillance massive des citoyens se trouvent souvent mobilisés au premier rang[3].

Personne n'ignore les révélations faites en 2013 par Edward Snowden, ancien employé de la Central Intelligence Agency (ci-après C.I.A.) et de la National Security Agency (ci-après N.S.A.) du gouvernement américain et aujourd'hui «lanceur d'alerte», à propos de la surveillance mondiale d'Internet, des téléphones mobiles et autres moyens de communication par la N.S.A., avec la complicité de certains États membres de l'Union européenne, dont l'Angleterre. Qui ne connaît pas WikiLeaks, organisation non gouvernementale fondée par le lanceur d'alerte Julian Assange en 2006? Il y publiera le 7 mars 2017 plus de 8 761 documents confidentiels de la C.I.A. exposant une immense opération de surveillance. Le projet Pegasus[4] est un autre exemple de cette surveillance effectuée par des États. Le projet Pegasus est une enquête journalistique collaborative internationale placée sous l'égide du consortium de journalistes et l'expertise informatique de l'O.N.G. Amnesty International. Le projet révèle en juillet 2021 que onze États ont surveillé notamment des journalistes, opposants politiques, militants des droits de l'homme, chefs d'État au moyen du logiciel espion Pegasus édité par l'entreprise israélienne N.S.O. Group.

L'évolution des technologies de l'information consacre l'importance accordée aux données à caractère personnel tant dans le secteur privé et commercial que dans le secteur public. Il faut se rendre à l'évidence, à «l'ère du (presque) tout numérique», l'utilisation et l'exploitation des données à caractère personnel revêtent un caractère capital, menaçant les droits fondamentaux, entre services répressifs et opérations de renseignement.

Cependant, il faut savoir raison garder et reconnaître que la gestion de l'exceptionnel et de l'inattendu, qu'il s'agisse de la lutte contre le terrorisme, de la gestion des pandémies, ou des crises migratoires, poursuit des buts légitimes. Reste à déterminer les conditions assurant une telle légitimité et rendant les mesures de surveillance massive légales.

Pour répondre à cette question, dans un premier temps, une définition de surveillance de masse sera proposée au travers de l'examen des normes qui l'encadrent à l'échelon de l'Europe (I). Dans un second temps, seront examinés à la lumière de la jurisprudence de la Cour européenne des droits de l'homme (ci-après Cour E.D.H.) et de la Cour de justice de l'Union européenne (ci-après Cour de justice) les éléments essentiels visant à protéger nos libertés fondamentales face au danger de la normalisation de la surveillance de masse (II).

3 Amnesty International, «France. La prolongation de l'état d'urgence risque de normaliser des pouvoirs d'exception» 16 décembre 2016, disponible sur le site www.amnesty.org/fr/latest/press-release/2016/12/france-renewal-of-state-of-emergency-risks-normalizing-exceptional-measures/, consulté en dernier lieu le 4 décembre 2021.

4 Amnesty International, «Espionnage téléphonique à grande échelle: le projet Pegasus», 18 juillet 2021, disponible sur le site www.amnesty.be/infos/actualites/pegasus, consulté en dernier lieu le 4 décembre 2021.

I. Notion, contexte et cadre légal: de la surveillance à la surveillance de masse

Ambitionnant de défendre les valeurs démocratiques et l'état de droit, les gouvernements jouent aux «pompiers pyromanes» sacrifiant régulièrement sur l'autel de la sécurité les libertés fondamentales et particulièrement le respect de la vie privée et la protection des données à caractère personnel.

Il faut dès lors réinterroger le cadre juridique existant et réévaluer le recours à ces mesures de surveillance au risque de cautionner une normalisation inconsidérée de ces pratiques liberticides. Il est important, à l'échelle de l'Europe, de comprendre si la protection offerte notamment par la Convention européenne des droits de l'homme[5] (ci-après C.E.D.H. ou Convention) et la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[6] (ci-après Convention n° 108), ainsi que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[7] (ci-après Charte) et le règlement général sur la protection des données[8] (ci-après R.G.P.D.), est toujours adaptée aux défis contemporains liés à la protection de la vie privée et des données à caractère personnel au moment de la gestion de ce qu'il y a lieu d'appeler l'«exception».

Pour ce faire, il est important de définir la notion de «surveillance de masse» (A) avant de dessiner le cadre légal qui permet d'assurer l'équilibre fondamental entre nos droits et les besoins de sécurité des États friands de données quand il s'agit de gérer l'exception (B).

A. *De la petite histoire de la surveillance à la définition de la surveillance de masse*

Si le phénomène de surveillance de masse n'est pas nouveau, à l'heure du tout digital où les techniques de pointe offrent des possibilités inimaginables en termes de surveillance, les dangers liés à sa masse et son niveau d'acuité soulignent les risques de ces nouvelles pratiques. Leur développement incontrôlé pourrait généraliser un sentiment de surveillance permanent chez les citoyens et générer chez eux un phénomène d'accoutumance et de banalisation ou *a contrario* de paranoïa, portant atteinte au bon fonctionnement des démocraties[9].

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

6 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, entrée en vigueur le 1er octobre 1985, telle que modifiée par le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, 10 janvier 2018, S.T.C.E. n° 223.

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

8 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.

9 Conseil de l'Europe, *Mass Surveillance – Who Is Watching the Watchers?*, *op. cit.*, p. 5.

Les mesures de surveillance de masse ont détérioré la confiance des citoyens et constituent un nouvel objet de réflexion en prise directe avec la sociologie, la philosophie, la politique et le droit. La diffusion de la surveillance dans nos sociétés doit être comprise pour ce qu'elle est vraiment, à savoir un phénomène historique, social et politique (1) qui, par l'émergence du droit au respect de la vie privée et aux lois relatives à la protection des données à caractère personnel, est devenu progressivement une réalité appréhendée juridiquement (2).

1. De la surveillance à la surveillance de masse, histoire d'une affaire publique pour une collecte devenue privée

La surveillance des citoyens par leur État n'est pas un phénomène nouveau. On retrouve 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*[10]. Il s'agissait d'un service postal destiné en réalité à être un service de renseignement[11]. En effet, l'objectif poursuivi était d'être informé de toutes les communications dans chaque province afin de pouvoir prédire les rébellions.

Déjà en ce temps, la surveillance et les réseaux de communication étaient corrélés, de sorte que des moyens importants furent mis en œuvre, notamment la création de routes et de voies navigables[12] pour assurer cette surveillance.

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[13]. Ses activités auraient perduré jusqu'à la fin du XIX^{e} siècle, de sorte que le Cardinal Richelieu défloraît les courriers qu'il voulait surveiller avec la complicité d'Antoine Rossignol, mathématicien recruté pour son incroyable habileté à décrypter les écritures secrètes[14].

Il est également possible d'inscrire les systèmes de dénonciation dans cette optique dès lors que, ainsi que le décrit Amélie Lachapelle dans son ouvrage sur

10 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 le site www.persee.fr/doc/mesav_0398-3587_1940_num_14_1_1120, consulté en dernier lieu le 4 décembre 2021.

11 *Ibid.*, p. 213.

12 W. Smith, W. Wayte et G.E. Marindin, *A Dictionary of Greek and Roman Antiquities*, London, John Murray, 1890, disponible sur le site www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0063:entry=cursus-publicus-cn, consulté en dernier lieu le 4 décembre 2021.

13 P. Larousse, *Grand dictionnaire universel du XIXe siècle*, t. 3, Paris, Librairie classique Larousse et Boyer, 1867, disponible sur le site https://gallica.bnf.fr/ark:/12148/bpt6k507258, consulté en dernier lieu le 4 décembre 2021.

14 A. Belloc, *Les postes françaises : recherches historiques sur leur origine, leur développement, leur législation*, Paris, Librairie de Firmin-Didot et Cie, 1886, p. 504, disponible sur le site https://gallica.bnf.fr/ark:/12148/bpt6k94475s, consulté en dernier lieu le 4 décembre 2021.

les lanceurs d'alerte fiscale, « la dénonciation est intimement liée à l'exercice du pouvoir et à l'organisation de la cité »[15].

Avec le temps, l'invention de nouveaux moyens de communication profitera à une surveillance plus systématique. C'est ainsi que, lors des guerres mondiales du XX^{e} siècle, la surveillance intensive sera légitimée par l'état de guerre[16]. Les inventions technologiques de l'époque sont alors mises au service de l'État : le télégramme, la mise sur écoute des câbles téléphoniques et même la création du premier ordinateur par Alan Turing, célèbre pour avoir décrypté les communications codées de l'armée allemande en venant à bout d'Enigma, la machine de chiffrement utilisée par les nazis et réputée inviolable[17].

Cependant, le système de surveillance étatique le plus connu de la première moitié du XX^{e} siècle est mis en place, en février 1950, dans l'ancienne République démocratique allemande (R.D.A.) par le Ministère pour la Sécurité nationale sous le nom de Stasi[18]. La stratégie consiste à établir un système de surveillance panoptique discipliné[19] qui remplacerait la terreur staliniste[20] en se fondant sur le consentement de la population. L'objectif d'un tel système était d'assurer le contrôle social en éliminant toute forme de dissidence. Ce pari sur l'autorestriction plutôt que sur la coercition est, selon l'analyse de Foucault, celui fait par l'État moderne pour remplacer le pouvoir absolu et inefficace du monarque[21].

Si jusqu'alors, la surveillance était essentiellement organisée par l'État, avec une vocation de contrôle social et d'élimination de toute rébellion, la fin du XX^{e} siècle et le début du XXI^{e} siècle amorcent une nouvelle ère pour la surveillance. Elle devient plus massive grâce aux nouveaux moyens techniques de communication et à l'arrivée de nouveaux acteurs. Ainsi, dès les années 1980, l'enregistrement automatisé des transactions des consommateurs, telles que les

15 A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, coll. du Crids, Bruxelles, Larcier, 2021, p. 72, n° 38.

16 S.-Y. Laurent, *Le secret de l'État. Surveiller, protéger, informer. XVIIe-XXe siècle*, Paris, Nouveau Monde, 2015 ; A. Marklund, « Communications Surveillance during World War I », *Encyclopédie d'histoire numérique de l'Europe*, 2020, disponible sur le site https://ehne.fr/en/node/21294, consulté en dernier lieu le 4 décembre 2021.

17 A. Hodges, « Alan Turing – Le génie qui a décrypté les codes secrets nazis et inventé l'ordinateur », Paris, Michel Lafon, 2015, p. 600.

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

19 S. Lorrain, *Histoire de la RDA*, coll. Que sais-je ?, Paris, P.U.F., 1994 ; voy. également « Stasi, histoire d'une police politique (RDA) », *Histoire pour tous*, 12 novembre 2019, disponible sur le site www.histoire-pour-tous.fr/dossiers/3491-la-stasi-histoire-dune-police-politique-rda.html, consulté en dernier lieu le 4 décembre 2021. 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.

20 En ce sens, Amnesty International, « L'exemple de la Stasi – L'histoire de la surveillance de masse incite à la prudence », 31 mars 2015, disponible sur le site www.amnesty.org/fr/latest/news/2015/03/lessons-from-the-stasi/, consulté en dernier lieu le 4 décembre 2021.

21 M. Foucault, *op. cit.*, pp. 154-155.

achats par carte de crédit ou les appels téléphoniques, offre aux acteurs privés l'opportunité d'être un maillon important dans la surveillance de masse.

Ensuite, la bulle spéculative autour des entreprises liées à l'Internet au cours des années 1990[22] ayant éclaté lors du krach boursier en 2001, certaines technologies ont été recyclées pour assurer un rôle de surveillance dans le secteur privé, en vue de générer des revenus. Depuis lors, chaque clic, chaque courriel générant des données et des métadonnées devient une source de revenus[23].

À titre exemplatif, les *cookies*, aussi connus sous le nom français de « traceurs », conçus à l'origine pour permettre à un site de vente en ligne de se « souvenir » des éléments dans le panier d'achats d'un visiteur[24], sont aujourd'hui posés par des tiers ou par le propriétaire du site Internet lui-même pour tracer le visiteur d'un site Internet. Ces outils technologiques commerciaux feront également l'objet d'une reprise par l'État pour ses propres objectifs[25].

Force est de constater que l'ère des technologies de l'information et des communications permet le décentrement de la surveillance par dissémination des points d'observation. C'est l'émergence d'une surveillance massive à l'échelle globale qui fonctionne en partenariat, d'une part, entre les États, et de l'autre, entre les États et le secteur privé.

À l'aune de ce constat, le monde découvre en 2013 les divulgations d'Edward Snowden sur la surveillance de masse organisée par les gouvernements de certains États.

Il s'ensuit que la sortie de l'ère de la surveillance « traditionnelle » pour entrer dans l'ère de la surveillance « automatisée » n'est pas simplement inscrite dans l'utilisation de nouvelles technologies, elle est la combinaison de plusieurs caractéristiques[26]. Premièrement, l'attention est désormais portée tant sur les métadonnées que sur la donnée elle-même[27]. À titre exemplatif, les métadonnées peuvent être des données relatives à la provenance de données, le moment ou la durée de connexion, le volume d'une communication, le réseau de départ ou d'arrivée de la communication[28]… Deuxièmement, cette nouvelle surveillance opère sur un principe de « collecte en masse, accès en détail »[29], grâce à l'utilisation d'un ensemble de technologies appelé les « big data » dont la notion n'est pas définie de manière unanime[30]. Elle pourrait néanmoins être analysée comme « un ensemble de technologies et de méthodes consistant à analyser, à des fins généralement prédictives, le flot de données produites par les entreprises, les organisations, et les individus, mais aussi les objets s'ils sont connectés, dans des volumes et à une vitesse sans précédent ; […] et qui engloberait les mails, SMS, photos, vidéos, commentaires ou changements de statuts sur les réseaux sociaux, sessions de connexion, relevés d'étiquettes ou de capteurs électroniques, signaux de géolocalisation, envoyés à foison chaque minute partout dans le monde »[31].

Elle renvoie autant aux masses de données numériques qu'à l'ensemble des techniques logicielles d'analyse de ces données, au rang desquels on retrouve le *data mining*[32], le *machine learning*[33], le *social network analysis*, la *predictive analytics*[34].

L'objectif poursuivi par l'utilisation de ces technologies d'analyse est la détection de relations qui seraient autrement restées imperceptibles, de sorte que naîtront de ces interconnexions des données inconnues du sujet de la surveillance lui-même et émergeront des modèles ou des standardisations.

Troisièmement, cette surveillance fonctionne en coopération entre l'État et les collecteurs de données commerciales[35], ou entre les États lorsqu'il s'agit d'échanger des informations issues de la surveillance[36].

L'ère dite du « big data » sonne ainsi la fin de la prévisibilité pour les citoyens et permet, au détour d'un algorithme ou d'un autre, de collecter sans précaution une quantité massive de données et de faire des corrélations avec ces données alors même que la personne concernée par les données n'est pas en mesure de le faire elle-même. La surveillance induit ainsi une double intrusion

22 J. Ninet et D. Bourghelle, « De la Bulle Internet (1999-2000) à la bulle Internaute (2020-2021) ? Une ouverture vers une autre économie », *Institut Rousseau*, 10 mai 2021, disponible sur le site www.institut-rousseau.fr/de-la-bulle-internet-1999-2000-a-la-bulle-internaute-2020-2021-une-ouverture-vers-une-autre-economie/, consulté en dernier lieu le 4 décembre 2021.

23 Voy. en ce sens S. Myers West, « Data Capitalism: Redefining the Logics of Surveillance and Privacy », *Business & Society*, 2019/1, n° 58, p. 25 ; J. Schöpfel, « Mondoux André, Ménard Marc : Big Data et société. Industrialisation des médiations symboliques », *Études de communication*, 2019, n° 52, disponible sur le site https://journals.openedition.org/edc/8990, consulté en dernier lieu le 4 décembre 2021.

24 S. Myers West, « Data Capitalism: Redefining the Logics of Surveillance and Privacy », *op. cit.*, p. 27.

25 *Ibid.*, p. 28.

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

27 Les métadonnées sont les données à propos des données, elles décrivent ou définissent une autre donnée et sont souvent générées automatiquement.

28 P. Bernal, « Data Gathering, Surveillance and Human Rights », *op. cit.*, p. 8.

29 *Ibid.*, p 246.

30 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).

31 Définition proposée par D. Cuny, « "Big Data" is Big Business. Vraiment ! », *La tribune*, 3 avril 2013, disponible sur le site www.latribune.fr/technos-medias/internet/20130403trib000757290/-big-data-is-big-business.-vraiment-.html, consulté en dernier lieu le 4 décembre 2021.

32 Le *data mining* peut se définir comme étant de l'exploration de données, du forage de données, de la prospection de données ou encore de l'extraction de connaissance à partir de données.

33 Il s'agit d'une science moderne permettant de découvrir des patterns et d'effectuer des prédictions à partir de données en se basant sur des statistiques, sur du forage de données, sur la reconnaissance de patterns et sur les analyses prédictives.

34 Considérée comme un type d'exploration de données, la *predictive analytics*, en français l'analyse prédictive, est un domaine de l'analyse statistique qui extrait l'information à partir des données pour prédire les tendances futures et les motifs de comportement.

35 En ce sens, P. Bernal, « Data Gathering, Surveillance and Human Rights », *op. cit.*, pp. 246 et 247.

36 Les deux exemples les plus connus sont, d'une part, l'alliance des Five Eyes, créée par un accord entre le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, à l'origine secrète (son existence a été publiée par Edward Snowden en 2013), et de l'autre, l'alliance européenne Maximator dont les cinq membres sont l'Allemagne, le Danemark, la France, les Pays-Bas et la Suède.

dans la vie privée des individus, d'une part par une collecte déloyale décentralisée dans les mains des sujets de la surveillance qui en deviennent l'agent, et d'autre part par une traçabilité constante de sorte que notre société apparaît comme un espace de surveillance permanente et mutuelle[37]. De manière plus triviale et imagée, cela revient à dire que le pêcheur utilise un chaland afin de prendre le maximum de poissons (en l'occurrence de données) pour ensuite procéder à une sélection en fonction de ses besoins non spécifiés au moment de la pêche. Cette dernière n'est plus limitée aux besoins réels mais aux besoins potentiels de sorte que se retrouvent pris dans la nasse des poissons (ou dans notre cas des données) qui ne devraient pas s'y retrouver. Ainsi, la surveillance de masse réalisée par l'État ou les acteurs privés travaillant pour le compte de l'État viole le principe de la présomption d'innocence dès lors que des données sont traitées sans le moindre soupçon sur la masse des personnes surveillées.

C'est dans ce contexte que le cadre légal doit assurer la protection des droits fondamentaux lors des traitements des données et métadonnées par les États à l'occasion de la gestion de l'état d'exception.

2. De la définition de la surveillance de masse

La surveillance est partout et depuis toujours ! Elle existe et évolue sous l'impulsion de la globalisation pour devenir encore plus invasive et performante.

Elle interpelle le juriste, qui l'aborde au travers de référentiels, allant des libertés fondamentales en passant par le rôle de l'État, et de questionnements liés à la force de la loi, ou encore à l'État de droit[38]. Étonnamment, la notion de surveillance de masse n'a encore aucune définition juridique faisant l'objet d'un consensus réel, ni d'un point de vue international, européen ou national.

Or, si « surveiller » consiste à prévenir les dangers, réduire les risques et arrêter les bras criminels, la surveillance est naturellement corrélée à l'action de punir et donc intrinsèquement un objet d'étude du droit.

C'était à ce titre que Jeremy Bentham, le père de l'utilitarisme, définissait la surveillance comme l'ensemble des mécanismes visant à faire en sorte que les sujets agissent dans un sens déterminé du seul fait d'être sous le regard d'autrui, qui analyse toutes les traces laissées par l'individu. Dans sa vision utopique de la société sous surveillance, toute dangerosité sociale ou de délinquance et toute menace du crime organisé ou de terrorisme seraient bannies[39].

En vue de définir la notion de surveillance, il y a lieu de s'attarder sur les définitions établies par les chercheurs du Surveillance Studies Network. Selon eux,

37 Chr. LAVAL, « Surveiller et prévenir. La nouvelle société panoptique », *Revue du MAUSS*, 2012/2, n° 40, pp. 47-72, disponible sur le site www.cairn.info/revue-du-mauss-2012-2-page-47.htm, consulté en dernier lieu le 4 décembre 2021.

38 M. DELMAS-MARTY, *Libertés et sûreté dans un monde dangereux*, coll. La couleur des idées, Paris, Seuil, 2010, p. 7.

39 M. FOUCAULT, *op. cit.*

la surveillance de masse renvoie à l'idée que les données relatives aux activités personnelles des individus et à leurs déplacements sont enregistrées et traitées par des technologies pour le compte des organisations et des gouvernements qui structurent la société. Ces informations une fois passées au crible alimentent les décisions qui affectent l'existence même des individus, dès lors qu'elles touchent au droit et à l'accès aux prestations sociales, au travail, aux services administratifs, à la justice pénale, ainsi qu'à la santé et à nos mouvements dans les lieux publics et privés.

En ce sens, en 2001, David Lyon offrait la première définition de la surveillance, entendue comme « toute collecte et traitement de données personnelles, permettant d'identifier ou non une personne, aux fins d'influencer ou de gérer ceux dont les données ont été recueillies »[40].

En 2007, dans son ouvrage *Surveillance Studies: An Overview*, il affine sa proposition de définition comme suit :

> « La surveillance [...] est l'attention ciblée, systématique et régulière des détails personnels à des fins d'influence, de gestion de direction et de protection.
> La surveillance porte en effet son attention sur les individus [...]. Par le recours à la notion de systématique, je veux dire que cette attention aux détails personnels [...] est délibérée et dépend de certains protocoles et techniques. Au-delà de ces éléments, la surveillance est devenue routinière ; une partie "normale" de la vie quotidienne dans toutes les sociétés qui dépendent de l'administration bureaucratique et de certaines technologies de l'information. La surveillance quotidienne est endémique aux sociétés modernes »[41].

Ces définitions portent une attention particulière sur les objectifs spécifiques de la surveillance, à savoir : *influencer, gérer, protéger ou orienter*. Les objectifs varient mais restent majoritairement dans la lignée de ceux énoncés par Bentham, puis par Foucault, à savoir ceux liés au contrôle, de sorte que la société de surveillance la plus accomplie serait une société sûre, dans laquelle chacun pourrait vivre en toute tranquillité sous l'œil attentif et protecteur du gardien de l'ordre public représenté par l'État. David Lyon s'inspire en effet directement du concept de panoptique de Bentham et de l'application qui en est faite par Foucault.

40 D. LYON, *Surveillance Society: Monitoring Everyday Life*, Buckingham, Philadelphia, Open University Press, 2001, p. 2 ; traduction libre de l'auteur des propos suivants : « What is surveillance? In this context, it is any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered ».

41 D. LYON, *Surveillance Studies: An Overview*, Cambridge, Polity Press, 2007, p. 21, traduction libre tirée des mots suivants : « So what is surveillance? For the sake of argument, we may start by saying that it is the focused, systematic and routine attention to personal details for purposes of influence, management, protection direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, Surveillance is routine; it occurs as a "normal" part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. Everyday surveillance is endemic to modern societies ».

Néanmoins, la métaphore du panoptique, concept fondamental dans les études et rapports réalisés par les membres du Surveillance Studies Network, tend à être dépassée. Considérée comme obsolète au vu de la structure de la surveillance contemporaine, l'architecture originelle du panoptique[42], qui suggère un seul poste d'observation central, n'est plus parfaitement conforme à la réalité au regard de la multiplication des acteurs et de l'absence de liens systématiques d'autorité entre l'agent de la surveillance et les sujets de la surveillance.

Pour pallier cette représentation erronée, Kevin Haggerty et Richard Ericson[43] ont développé le concept de *surveillant assemblage*, développant l'idée d'un centre de surveillance unique substitué par une multitude d'éléments surveillants, organisés en rhizome et non hiérarchisés[44]. En ce sens, Sami Coll, en 2014, décrit la surveillance en rhizome, composée de flux de données captés par des points de contact multiples, par opposition à un modèle fondé sur un surveillant central orwellien[45].

Les études du Surveillance Studies Network sont également critiquées par une certaine doctrine en raison de l'attention portée aux effets négatifs de la surveillance[46]. Cette critique porte sur le postulat « technophobe » qui considère la surveillance comme quelque chose de dangereux en soi[47]. Elle appelle à une approche plus nuancée en précisant que la surveillance n'est pas dangereuse parce qu'elle est technologique[48].

Ainsi, dans une démarche qui vise à dépasser l'équilibre parfois précaire entre sécurité et liberté pour comprendre le phénomène de surveillance, on voit également émerger la notion de surveillance diffuse[49]. La surveillance diffuse n'est plus la simple activité de recherche de renseignements concernant un individu potentiellement dangereux. Elle s'inscrit plutôt dans la poursuite de ce que Hannah Arendt qualifie de « crise de la culture ». La surveillance diffuse est alors définie comme l'une des caractéristiques de la culture contemporaine dominée par la peur, la consommation et l'aliénation par les technologies.

42 Pour Bentham, le surveillant du centre pénitentiaire occupe la place centrale (G. Tusseau, « Sur le panoptisme de Jeremy Bentham », *Revue française d'histoire des idées politiques*, 2004/1, n° 19, pp. 3-38) ; pour Foucault, c'est l'État qui l'occupe (M. Foucault, *op. cit.*, p. 229).

43 K.D. Haggerty, R.V. Ericson, « The surveillant assemblage », *The British Journal of Sociology*, vol. 51/4, décembre 2000, pp. 608-610, disponible sur le site www.uio.no/studier/emner/matnat/ifi/INF3700/v17/bakgrunnsnotat/the_surveillant_assemblage.pdf, consulté en dernier lieu le 4 décembre 2021.

44 Fl. Castagnino, « Critique des *surveillances studies*. Éléments pour une sociologie de la surveillance », *Déviance et Société*, vol. 42, 2018/1, p. 29, disponible sur le site www.cairn.info/journal-deviance-et-societe-2018-1-page-9.htm, consulté en dernier lieu le 4 décembre 2021.

45 S. Coll, *Surveiller et récompenser. Les cartes de fidélité qui nous gouvernent*, Genève, Seismo, 2015, pp. 11-12.

46 *Ibid.*, p. 13.

47 Ces analyses concluent forcément au caractère liberticide des pratiques de surveillance ; voy. en ce sens Fl. Castagnino, « Critique des *surveillances studies* », *op. cit.*, p. 13.

48 *Ibid.*, p. 25.

49 C. Codron, *La surveillance diffuse : entre Droit et Norme*, thèse, Université de Lille, 2018, disponible sur le site https://tel.archives-ouvertes.fr/tel-01905217, consulté en dernier lieu le 4 décembre 2021.

Devenue la nouvelle norme sociale admise, elle désinstitue également le droit au profit de la norme et du libéralisme économique qu'elle porte en son sein[50].

La surveillance étant aujourd'hui organisée sous diverses formes avec des objectifs multiples, il paraît nécessaire de subdiviser le concept en plusieurs types : (a) la surveillance, (b) la surveillance de masse et (c) la surveillance dite diffuse.

Enfin, Stéphane Leman-Langlois identifie à son tour trois caractéristiques de la surveillance[51] :

1. elle peut être décrite de manière générale comme un processus d'acquisition d'information.
2. l'acquisition d'information porte sur des « objets sociaux », soit les individus et les objets dont ils sont responsables.
3. l'objectif est l'obtention d'un bénéfice extérieur à la simple collecte d'informations.

Dans ce contexte, la surveillance contemporaine, dite de masse, a pu être qualifiée de « post-panoptique »[52], pour désigner notamment une surveillance qui s'appuie sur la prédiction plutôt que sur l'observation[53]. Cette prédiction des comportements humains est permise par l'utilisation des technologies des « big data ».

Les gouvernements justifient souvent l'intensité de cette surveillance et la variété des moyens employés par la nécessité d'assurer la « sécurité nationale » et plus précisément la lutte contre le terrorisme du XXI^e siècle, la lutte contre la pandémie, la migration…

Dès lors que la présente contribution entend examiner les modalités d'un déploiement de la surveillance massive par les États à l'occasion de la gestion des situations qualifiées d'exception, la définition suivante de la surveillance de masse est proposée sur base des divers éléments et définitions repris ci-dessus :

> « Tout processus, centralisé ou non, d'acquisition systématique et à grande échelle d'informations relatives à l'individu et aux objets dont il est responsable, 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 ».

50 *Ibid.*, p. 382.

51 St. Leman-Langlois, *Sphères de surveillance*, coll. Régulation sociale, Montréal, Les Presses de l'Université de Montréal, 2011, pp. 10 et 11.

52 Z. Bauman et D. Lyon, *Liquid Surveillance: A Conversation*, coll. Polity conversations series, Cambridge, Malden, Polity Press, 2013, pp. 49-67.

53 K. Kubler, « State of Urgency: Surveillance, Power, and Algorithms in France's State of Emergency », *Big Data & Society*, vol. 4, n° 2, 2017, p. 7.

B. *Le cadre légal de la surveillance de masse : de la protection de la vie privée à la protection des données à caractère personnel*

À la lecture de ce qui précède, force est de constater que depuis que l'homme s'organise en société, l'utilisation et l'exploitation des informations à caractère personnel n'ont jamais revêtu une telle importance, et en perspective, ce phénomène est destiné à s'accroître dans le futur, au même rythme que les technologies de l'information.

À l'heure du « tout numérique », de la surveillance massive des États révélée par les lanceurs d'alerte tels qu'Edward Snowden et Julian Assange, alors que plane toujours la menace terroriste sur les démocraties libérales et que les données de santé des individus sont agglomérées dans de grandes bases de données en vue d'assurer le suivi de la pandémie de Covid-19 et le *tracing* des contaminations ou de la vaccination, les enjeux et les risques[54] pour les droits fondamentaux sont mis en lumière plus que jamais.

Partant, de nombreux instruments internationaux de protection des droits fondamentaux accordent une protection spécifique aux traitements de données à caractère personnel, comme, dans un premier temps, une extension du droit au respect de la vie privée[55] en vue d'assurer le respect des droits fondamentaux face à l'ingérence des États et, dans un second, un droit autonome tel que celui repris dans l'article 8 de la Charte. Les différents textes liés à la protection des données à caractère personnel sont issus de diverses organisations internationales telles que les Nations Unies[56], le Conseil de l'Europe, l'Union européenne ou encore l'O.C.D.E. ou Organisation de coopération et de développement économique[57].

Dans ce cadre, 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 surtout et également aux données à caractère personnel et à leurs traitements à l'échelle européenne. Depuis les années 1970-1980, le Conseil de l'Europe[58] comme l'Union européenne ont

54 C. Castets-Renard, « Introduction – Les enjeux et l'actualité de la protection des données personnelles en Europe », *in* I. De Lamberterie, A. Strowel et C. Castets-Renard (dir.), *Quelles protections des données personnelles en Europe*, Bruxelles, Larcier, 2015, p. 34.

55 C. Macq et S. Van Outryve, « Les droits fondamentaux à l'épreuve de la lutte contre le terrorisme », *in* Ligue des droits de l'homme A.S.B.L. (dir.), *État des droits de l'homme en Belgique – Rapport 2016-2017*, disponible sur le site https://www.liguedh.be/wp-content/uploads/2017/03/ldh_edh1617_web.pdf, p. 34, consulté en dernier lieu le 4 décembre 2021.

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

57 O.C.D.E., « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », 2013, disponible sur le site www.oecd.org/fr/numerique/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm, consulté en dernier lieu le 4 décembre 2021.

58 Conseil de l'Europe, Assemblée parlementaire, 4e sess., « La protection de la vie privée et des données à caractère personnel sur l'Internet et les médias en ligne », Doc. 12695, 29 juillet 2011.

régulièrement manifesté leur inquiétude envers des possibilités jusqu'alors impensables d'identifier les individus grâce à leurs données.

À ce titre, la protection des données à caractère personnel est assurée par le biais de l'article 8 de la C.E.D.H., mais également par la Convention n° 108.

De son côté, l'Union 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, mais également par un ensemble de directives et de règlements visant à harmoniser les pratiques au sein de chaque État, et notamment le R.G.P.D., la directive relative aux communications électroniques[59] (ci-après directive ePrivacy) ou encore la directive relative au traitement des données à caractère personnel dans le secteur de la police et de la justice[60] (ci-après directive police-justice).

Ainsi, les prochains paragraphes sont consacrés à la protection apportée au droit à la vie privée et à la protection de données d'une part par le Conseil de l'Europe (1), et d'autre part par l'Union européenne (2).

1. La protection offerte par le Conseil de l'Europe

À la suite des dérives de la Seconde Guerre mondiale en matière de droits de l'homme et pour prévenir tout nouveau conflit de ce type, le Conseil de l'Europe a très tôt marqué un intérêt certain pour la protection des données à caractère personnel. Il a, à ce titre, rédigé de nombreuses recommandations et résolutions sur ce thème, toutes fondées sur l'article 8 de la C.E.D.H., qui garantit le droit au respect de la vie privée[61]. L'article 8 énonce ce qui suit :

> « Droit au respect de la vie privée et familiale
> § 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
> § 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

59 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, *J.O.C.E.*, L 201, 31 juillet 2002.

60 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.

61 P. De Hert et S. Gutwirth, *Anthologie de la vie privée. Compilation d'articles, de législation et de jurisprudence concernant la protection de la vie privée et des données à caractère personnel pour la Belgique jusque 1998*, Bruxelles, Academic and Scientific Publishers, 2013, p. 9.

La jurisprudence de la Cour E.D.H. a élargi la portée de l'article 8, qui était initialement voué au respect de la vie privée et familiale, au point d'y inclure la protection des données à caractère personnel.

Sur le plan terminologique, la portée juridique de la notion de « vie privée » n'est pas entièrement délimitée, et a considérablement évolué au gré des arrêts[62] de la Cour E.D.H. Parmi ces décisions, en l'affaire *S. et Marper c. Royaume-Uni* du 4 décembre 2008, la Cour rappelle que « la notion de vie privée est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne »[63].

La Cour a également rappelé que ce droit à la vie privée est sous-tendu par une large part laissée à l'autonomie de l'individu. Ainsi, dans un arrêt du 11 juillet 2002, elle a rappelé que :

> « La dignité et la liberté de l'homme sont l'essence même de la Convention. Sur le terrain de l'article 8 de la Convention en particulier, où la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de cette disposition, la sphère personnelle de chaque individu est protégée, y compris le droit pour chacun d'établir les détails de son identité d'être humain (voir, notamment, *Pretty c. Royaume-Uni*, n° 2346/02, § 62, C.E.D.H. 2002-III, et *Mikulić c. Croatie*, n° 53176/99, § 53, C.E.D.H. 2002-I) »[64].

Par ailleurs, « la garantie offerte par l'article 8 de la Convention est principalement destinée à assurer le développement, sans ingérences extérieures, de la personnalité de chaque individu dans les relations avec ses semblables »[65]. En d'autres termes, « cette disposition protège également le droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur »[66].

De plus, ce droit fait partie intégrante de l'individu et il en bénéficie également dans d'autres sphères que celle privée. La Cour européenne des droits de l'homme n'a pas manqué de le rappeler à maintes reprises.

Il en va ainsi dans un arrêt rendu le 28 janvier 2003 dans lequel elle énonce que :

> « *La "vie privée" est une notion large,* qui ne se prête pas à une définition exhaustive. [...] *[Le droit à la vie privée] peut s'étendre à des activités professionnelles ou commerciales.* Il existe donc une zone d'interaction entre l'individu et autrui qui, *même dans un contexte public, peut relever de la "vie privée"* »[67].

62 Voy. en ce sens Cour eur. D.H, arrêt *Klass e.a. c. Allemagne*, 6 septembre 1978, req. n° 5029/71, § 28 ; arrêt *Malone c. Royaume-Uni*, 2 août 1984, req. n° 8691/79, § 95 ; arrêt *Leander c. Suède*, 26 mars 1987, req. n° 9248/81, § 116 ; arrêt *Gaskin c. Royaume-Uni*, 7 juillet 1989, req. n° 10454/83, § 160 ; arrêt *Niemietz c. Allemagne*, 16 décembre 1992, req. n° 13710/88 ; arrêt *Halford c. Royaume-Uni*, 25 juin 1997, req. n° 20605/92 ; gde ch., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95.

63 Cour eur. D.H. (gde ch.), arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n^{os} 30562/04 et 30566/04, § 66 ; voy. également Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 avril 2002, req. n° 2346/02, § 61 ; arrêt *Y.F. c. Turquie*, 22 juillet 2003, req. n° 24209/94, § 33.

64 Cour eur. D.H., arrêt *Christine Goodwin c. Royaume-Uni*, 11 juillet 2002, req. n° 28957/95, § 90.

65 Cour eur. D.H., arrêt *von Hannover c. Allemagne*, 7 février 2012, req. n^{os} 40660/08 et 60641/08, § 95.

66 Cour eur. D.H., arrêt *Peck c. Royaume-Uni*, 28 janvier 2003, req. n° 44647/98, § 57, nous soulignons.

67 *Ibid.*, nous soulignons.

En 2012, elle a également jugé que « la publication d'une photo interfère dès lors avec la vie privée d'une personne, même si cette personne est une personne publique » et que « dans certaines circonstances, une personne, même connue du public, peut se prévaloir d'une "espérance légitime" de protection et de respect de sa vie privée »[68].

En se référant à l'article 8, il a donc été possible pour la Cour de protéger de nombreux aspects de la vie privée de l'individu : de la protection de son domicile ou de la vie familiale en passant par la protection du droit à la correspondance jusqu'aux questions qui ont trait à la liberté sexuelle ou à la protection de l'environnement.

Eu égard à cette interprétation évolutive de la Cour, le Conseil de l'Europe s'est très rapidement préoccupé des risques et des enjeux liés au respect des droits de l'homme lors du traitement de données à caractère personnel. Il a, à ce titre et dès les années 1970, consacré deux résolutions importantes[69]. Puis par souci d'harmonisation, le 28 janvier 1981, l'Assemblée parlementaire du Conseil de l'Europe a consolidé ces résolutions en une seule convention, à savoir la Convention n° 108.

Attentif à une protection internationale poussée des données à caractère personnel, le Conseil de l'Europe[70] a adopté, le 18 mai 2018[71], un Protocole d'amendement qui modernise la Convention n° 108[72] pour donner naissance à la Convention n° 108+[73].

68 Cour eur. D.H., arrêt *von Hannover c. Allemagne*.

69 Conseil de l'Europe, Comité des ministres, 28^{e} sess., Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 1981, § 4(3) ; voy également la Résolution 22 de 1973 (Conseil de l'Europe, Comité des ministres, Résolution 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, 1973) qui énonçait les principes de la protection des données pour le secteur privé et la Résolution 29 de 1974 (Conseil de l'Europe, Comité des ministres, Résolution 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, 1974) qui a fait la même chose pour le secteur public.

70 Pour l'évolution des travaux législatifs, voy. également Conseil de l'Europe, CAHDATA, 3^{e} réunion, Document de travail : Convention 108 avec son Protocole additionnel et propositions de modernisation, 9 avril 2014, CAHDATA(2014)03.

71 Article 1er de la Convention n° 108 : « Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée ».

72 Eu égard à l'évolution des technologies de l'information, de la vidéosurveillance et au recours en hausse aux identifiants biométriques, le Comité conventionnel de la Convention n° 108 avait lancé en 2010 une étude recensant les déficiences de la convention, suivie d'une consultation publique en 2011, afin d'élaborer les pistes d'amélioration les plus adaptées possible, aboutissant ainsi à la dernière version de la Convention n° 108 adoptée en 2018 (S.T.C.E. n° 223). 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. Entre la version originelle et le protocole d'amendement qui est actuellement à l'étape de ratification, on peut remarquer plusieurs différences développées *infra*.

73 Afin d'assurer une facilité de lecture, les conventions n° 108 et 108+ sont reprises sous les termes de Convention n° 108.

La Convention n° 108 a toujours fait preuve de dynamisme, ayant été longtemps « le seul instrument international juridiquement contraignant dans le domaine de la protection des données et de par son caractère ouvert, elle a une vocation universelle, susceptible de pallier l'absence de convention mondiale »[74].

Les effets de la Convention n° 108 étant contraignants[75] pour les États signataires, ceux-ci ont adopté en interne les mesures nécessaires pour donner les effets utiles aux principes généraux énoncés dans la Convention visant à assurer la protection des données[76] et la justiciabilité de ce droit.

À cet égard, une nuance doit être apportée. Si une doctrine traditionnelle[77] utilise toujours la formule « protection des données à caractère personnel » pour indiquer une notion plus spécifique du droit à la protection à la vie privée couverte par l'article 8, § 1er, de la C.E.D.H., une autre partie minoritaire[78] préfère rester fidèle à la nomenclature de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, tel que défini par la Convention n° 108.

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 C.E.D.H., et d'autre part, par la Convention n° 108.

En effet, la Convention n° 108, dès son intitulé, met la personne concernée par le traitement au centre de la protection. Dans un contexte de marchandisation des données à caractère personnel, l'individu et son intégrité physique et morale sont au cœur du discours juridique[79].

Ainsi, la Convention n° 108, déjà dans sa version originelle de 1981, introduit des éléments novateurs qui permettent un exercice effectif du droit à la protection des données à caractère personnel dans le chef des personnes concernées

74 J.-P. Walter, « Modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », allocution présentée au Conseil de l'Europe, 7 octobre 2014, disponible sur le site https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/auditionlibe_/auditionlibe_en.pdf, p. 2, consulté en dernier lieu le 4 décembre 2021. La Convention n° 108 est une convention ouverte à l'adhésion d'États tiers.

75 Conseil de l'Europe, Communiqué de presse, « Améliorer la protection des données au niveau mondial : le Conseil de l'Europe met à jour sa convention phare », Elseneur (Danemark), 18 mai 2018, disponible sur le site https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108, consulté en dernier lieu le 4 décembre 2021.

76 Article 4 de la Convention n° 108.

77 Fr. Sudre, *Droit européen et international des droits de l'homme*, 10e éd., Paris, P.U.F., 2011 ; A. Manzella *et al.*, *Riscrivere i diritti in Europa*, Bologne, il Mulino, 2001 ; Agence des droits fondamentaux de l'Union européenne, *Manuel de droit européen en matière de protection des données*, Luxembourg, Office des publications de l'Union européenne, 2014 ; Fr. Sudre *et al.*, *Les grands arrêts de la Cour européenne des droits de l'homme*, 6e éd., Paris, Thémis, 2011.

78 M. Gentot, « La protection des données personnelles à la croisée des chemins », *in* P. Tabatoni (dir.), *La protection de la vie privée dans la société de l'information*, t. 3, Paris, P.U.F., 2000.

79 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *Rev. trim. dr. h.*, 2016, n° 108.

par les traitements des données. Parmi ceux-ci, la définition des figures clefs intervenant dans les traitements des données permet d'appréhender plus clairement les rôles et responsabilités des parties. Au nombre de ces acteurs, on retrouve le « maître du fichier », appelé aujourd'hui le « responsable du traitement » dans un mouvement d'harmonisation avec les vocables utilisés dans la législation de l'Union.

Le responsable du traitement est, aux termes de l'article 2, alinéa 1er, b), de la Convention n° 108 :

> « La personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ».

La Convention n° 108 lui assigne des tâches particulières et des responsabilités spécifiques.

Ainsi, en son nouvel article 8 tel que modifié lors de la révision de 2018, à l'instar de l'obligation définie aux articles 12, 13 et 14 du R.G.P.D., il lui revient de procéder à une communication relative notamment à son identité et celle des tiers destinataires, aux finalités de ses traitements, et à la typologie de données traitées, comme suit :

> « 1. Chaque Partie prévoit que le responsable du traitement informe les personnes concernées :
> a. de son identité et de sa résidence ou lieu d'établissement habituels ;
> b. de la base légale et des finalités du traitement envisagé ;
> c. des catégories des données à caractère personnel traitées ;
> d. le cas échéant, des destinataires ou catégories de destinataires des données à caractère personnel ; et
> e. des moyens d'exercer les droits énoncés à l'article 9 ;
> ainsi que de toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel.
> 2. Le paragraphe 1 ne s'applique pas lorsque la personne concernée détient déjà l'information.
> 3. Lorsque les données à caractère personnel ne sont pas collectées directement auprès des personnes concernées, le responsable du traitement n'est pas tenu de fournir ces informations dès lors que le traitement est expressément prévu par la loi ou que cela lui est impossible ou implique des efforts disproportionnés ».

Ensuite, en son article 6, la Convention n° 108 met à charge du responsable du traitement des obligations et des garanties spécifiques s'agissant du traitement de données de catégories dites particulières, de données comme les données syndicales, génétiques, concernant les infractions pénales, l'origine raciale, l'orientation sexuelle, les opinions politiques, etc.

La Convention n° 108 définit également les notions de «sous-traitant» et de «destinataire des données». Le sous-traitant s'entend de la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement[80], alors que le destinataire est la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit la communication de données ou à qui des données sont rendues accessibles[81].

Enfin, et dans sa version amendée de 2018, la Convention n° 108 prévoit une «Autorité» indépendante, nationale, chargée de veiller au respect de ses dispositions, avec le «pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations des dispositions de la présente Convention»[82], et renforce aussi les pouvoirs du «Comité conventionnel» qui n'a plus seulement un rôle «consultatif», mais se voit également conférer des pouvoirs d'évaluation et de surveillance[83].

La création et l'évolution de la Convention n° 108 s'inscrivent dans la droite ligne de la jurisprudence novatrice et dynamique de la Cour en matière de protection des données à caractère personnel[84]. Cette jurisprudence sera également une source d'inspiration directe pour l'Union européenne qui a inscrit ce droit dans sa Charte, et pour de nombreuses constitutions nationales[85] des États parties au Conseil de l'Europe.

2. La protection offerte par l'Union européenne

L'Union européenne est également pionnière en matière de protection des données et de la vie privée. En effet, la Charte est la première charte à consacrer la protection des données à caractère personnel de manière distincte de la protection et du respect de la vie privée. Elle a créé un droit fondamental *per se*, comme suit:

> «Article 7
> Respect de la vie privée et familiale.
> Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

80 Article 2, alinéa 1er, f, de la Convention n° 108.

81 Article 2, alinéa 1er, e, de la Convention n° 108.

82 Article 12, de la Convention n° 108.

83 Selon l'article 23 de la Convention n° 108, le Comité conventionnel formulera un avis sur le niveau de protection des données assuré par un État ou une organisation internationale préalablement à leur adhésion à la Convention. Il peut aussi évaluer si le droit interne de la Partie concernée est conforme aux dispositions de la Convention et déterminer si les mesures prises ont été suivies d'effet (existence d'une autorité de contrôle, responsabilités, existence de voies de recours en vigueur).

84 R. Angrisani, «Données personnelles et surveillance massive: quelle protection face aux ingérences des autorités publiques?», *Revue québécoise de droit international*, Hors série, décembre 2020, p. 120, disponible sur le site www.erudit.org/en/journals/rqdi/2020-rqdi06138/1078532ar/, consulté en dernier lieu le 4 décembre 2021.

85 Par exemple l'Allemagne en 1971, la Suède en 1973 et la France en 1978.

> Article 8
> Protection des données à caractère personnel
> 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante».

Il est intéressant de constater que la note du Présidium[86] rattache ce droit tant à l'article 8 de la C.E.D.H. et à la Convention n° 108 qu'à la directive 95/46 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dont il sera question ci-dessous.

Cette filiation entre ces divers textes de base en matière de protection des données à caractère personnel est établie afin d'en renforcer l'ancrage dans le droit européen, d'autant plus que, en vertu de l'article 52.3 de la Charte[87], le sens du droit à la protection des données à caractère personnel ainsi que sa portée sont les mêmes que ceux conférés par la C.E.D.H.

À ce titre, le Présidium énonce ce qui suit:

> «Le paragraphe 3 vise à assurer la cohérence nécessaire entre la Charte et la C.E.D.H. en posant le principe que, dans la mesure où les droits de la présente Charte correspondent également à des droits garantis par la C.E.D.H., leur sens et leur portée, y compris les limitations admises, sont les mêmes que ceux que prévoit la C.E.D.H. Il en résulte en particulier que le législateur, en fixant des limitations à ces droits, doit respecter les mêmes standards que ceux fixés par le régime détaillé des limitations prévu dans la C.E.D.H., sans que ceci porte atteinte à l'autonomie du droit communautaire et de la Cour de justice des Communautés européennes. La référence à la C.E.D.H. vise à la fois la Convention et ses protocoles. Le sens et la portée des droits garantis sont déterminés non seulement par le texte de ces instruments, mais aussi par la jurisprudence de la Cour européenne des droits de l'homme et par la Cour de justice des Communautés européennes. La dernière phrase du paragraphe vise à permettre au droit de l'Union d'assurer une protection plus étendue.
> La liste des droits qui peuvent au stade actuel et sans que cela exclue l'évolution du droit, de la législation et des traités, être considérés comme correspondant à des droits de la C.E.D.H. au sens du présent paragraphe est reproduite ci-dessous. Ne sont pas reproduits les droits qui s'ajoutent à ceux de la C.E.D.H.»[88].

86 Note du Présidium sur le projet de Charte des droits fondamentaux de l'Union européenne, p. 11, disponible sur le site www.europarl.europa.eu/charter/pdf/04473_fr.pdf, consulté en dernier lieu le 4 décembre 2021.

87 Dans la mesure où la Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

88 Note du Présidium sur le projet de Charte des droits fondamentaux de l'Union européenne, p. 48.

Cela doit également être lu en parallèle avec l'article 6 du Traité sur l'Union qui prescrit que :

> « 1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités.
> Les dispositions de la Charte n'étendent en aucune manière les compétences de l'Union telles que définies dans les traités.
> Les droits, les libertés et les principes énoncés dans la Charte sont interprétés conformément aux dispositions générales du titre VII de la Charte régissant l'interprétation et l'application de celle-ci et en prenant dûment en considération les explications visées dans la Charte, qui indiquent les sources de ces dispositions.
> 2. L'Union adhère à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités.
> 3. Les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux ».

S'agissant de l'étendue de ce droit, la note du Présidium renvoie à l'article 52 de la Charte, mais également à la directive 95/46 relative à la protection des données, qui constitue le premier texte de droit dérivé de l'U.E. en la matière et qui est aujourd'hui remplacée par le R.G.P.D.

a. La directive 95/46 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

S'agissant du droit dérivé, dans un premier temps, dès les années 80, la Commission européenne travailla sur des recommandations adressées aux États membres[89] et le Parlement européen édita une série de résolutions visant à assurer la protection des données.

Partant en 1990, ambitionnant de préciser et d'amplifier les principes de la Convention n° 108, une proposition de directive comprenant les principes fondamentaux en matière de protection de données[90] fut présentée. Après cinq années de longues discussions et négociations, en 1995, la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement de leurs

89 Comme « la recommandation datant du 29 juillet 1981 concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, recommandant aux États membres de signer la Convention n° 108 dans le courant de l'année 1981 et de la ratifier avant la fin de l'année 1982 ». Voy. P. De Hert et S. Gutwirth, *Anthologie de la vie privée*, *op. cit.*, p. 12.

90 P. De Hert et S. Gutwirth, *ibid.*, p. 13.

données à caractère personnel et à la libre circulation de ces données[91] a enfin vu le jour.

Cependant, eu égard à l'évolution rapide des technologies, de la surveillance gouvernementale exacerbée par la menace terroriste, et au besoin d'harmonisation dans la mise en œuvre de la protection des données au sein des États membres, la Commission européenne proposa un projet de règlement dès le 25 janvier 2012.

Parallèlement, au cœur des négociations du projet de règlement, le Parlement européen, méfiant envers les États-Unis dans ce contexte d'hypersurveillance constante dénoncée par Edward Snowden, adopta le 12 mars 2014 une résolution[92] sur les organismes de surveillance américains élaborant ainsi toute une série de mesures renforçant le droit fondamental à la vie privée des citoyens européens.

Sur pied de cette résolution, le Parlement exigea la suspension des accords entre l'Union et les États-Unis, notamment s'agissant de l'usage illicite de l'accord SWIFT de 2010[93] qui autorisait le gouvernement américain à entrer en possession des données bancaires européennes dans le but de déjouer le terrorisme.

Il sollicita également la suspension immédiate du Safe Harbor, assurant la sécurité des transferts transatlantiques des données à caractère personnel des citoyens européens[94]. Enfin, il invita également à suspendre les négociations quant à un partenariat transatlantique de commerce et d'investissement (T.T.I.P.) insistant sur le fait que la lutte contre le terrorisme ne ne pouvait en aucune manière légitimer une surveillance de masse secrète et illégale[95].

Certes, cette résolution du Parlement n'était pas contraignante mais elle exprimait nettement la tendance suggérée[96] en faveur d'une protection accentuée des droits fondamentaux des citoyens européens lors du traitement de leurs

91 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281/31, 23 novembre 1995. Sa rédaction donna du fil à retordre aux États, faute d'accord unanime et de positions communes entre eux.

92 Parlement européen, Résolution sur le programme de surveillance de la N.S.A., les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, Résolution 2013/2188 (INI), 12 mars 2014.

93 L'accord Terrorist Finance Tracking Programme (T.F.T.P.) entre l'Union européenne et les États-Unis autorise un programme de surveillance gouvernemental américain à accéder aux transactions financières internationales sur le réseau « SWIFT ».

94 C'est finalement la Cour de justice qui, en octobre 2015, invalidera cet accord, qui sera remplacé dès 2018 par un nouvel accord, connu sous le nom de Privacy Shield, également invalidé par la Cour mais en 2020.

95 Parlement européen, Communiqué de presse, « N.S.A. : mettre fin à la surveillance massive ou faire face aux conséquences », 12 mars 2014.

96 Suivie par une très large majorité, avec un vote de 544 pour sur 682 voix.

données, contre la surveillance de masse, mais également l'émergence d'un climat de méfiance à l'égard des États tiers et particulièrement les États-Unis.

b. Le Règlement général sur la protection des données

C'est dans ce contexte, qu'après quatre années d'âpres négociations, le 25 mai 2016, le nouveau règlement a vu le jour pour entrer en vigueur le 25 mai 2018, date à laquelle il abrogea et remplaça la directive 95/46[97], annonçant une nouvelle ère pour la protection des données.

Premièrement, les principes généraux énoncés dans le règlement n'ont pas été fondamentalement modifiés par rapport à la directive 95/46, mais ont été étoffés en comparaison à ceux énoncés en l'article 6 de la directive 95/46. Si la transparence constituait déjà une des pierres angulaires de la protection des données, le R.G.P.D. la précise de manière plus complète en son considérant 39 afin d'assurer un meilleur contrôle pour les individus sur leurs données[98]. Corollaire de ce principe, un droit à l'information dans le chef de la personne concernée, portant sur la base de licéité du traitement[99], ses finalités, les transferts des données vers un pays étranger ou une organisation internationale[100], la durée de conservation[101], mais également l'existence et les modalités d'exercice de son droit, notamment de demander l'accès à ses données à caractère personnel, de rectification ou d'effacement, celui d'exiger la portabilité de ses données, ou une limitation des traitements, ainsi que de s'opposer au traitement ou de porter plainte à une autorité compétente.

Par ailleurs, le règlement renforce l'obligation d'information, qui était déjà présente dans la directive 95/46, lorsque les données ne sont pas collectées directement auprès de la personne concernée[102]. Il s'agit d'un aspect de transparence important dans le cadre de la présente contribution dès lors que la surveillance de masse procède régulièrement de manière secrète, indirecte et automatisée.

97 Enfin, précisons tout de même qu'en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires, il y aura lieu d'appliquer le règlement n° 45/2001/CE du Parlement européen et du Conseil datant du 18 décembre 2000 – actuellement en cours de révision – et non ce nouveau règlement.

98 Article 5, § 1er, a, du R.G.P.D.: «Les données à caractère personnel doivent être: a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence); [...]»; cette disposition doit être lue en combinaison avec les articles 12, 13 et 14 du R.G.P.D. L'obligation de transparence et de loyauté implique que toute information adressée au public ou à la personne concernée doit être aisément accessible, facile à comprendre, et être formulée en termes simples et clairs, particulièrement en ce qui concerne les informations relatives à l'identité du responsable et aux finalités du traitement. Les obligations d'information à charge du responsable du traitement résultant du principe de transparence sont détaillées aux articles 12 et 13 et 14 du règlement. Cette obligation induit un droit à l'information et un droit d'accès dans le chef de la personne concernée.

99 Article 6 du R.G.P.D.

100 Articles 13 et 14 du R.G.P.D.

101 Lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.

102 Article 14 du R.G.P.D.

Plus spécifique, s'agissant du profilage, le responsable du traitement doit également fournir toutes les informations utiles relative à l'existence d'une prise de décision automatisée, et à tout le moins les informations concernant la logique sous-jacente, l'importance et les conséquences prévues pour la personne concernée, conformément aux dispositions de l'article 22, §§ 1er et 4, qui énonce ce qui suit:

> «§ 1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.
> [...]
> § 4. Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, à moins que l'article 9, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place.»

À cet égard le considérant 70 du R.G.P.D. énonce que:

> «En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.»

D'évidence, le droit à l'information revêt une importance capitale pour le législateur européen. Néanmoins, ce droit n'est pas absolu, notamment lorsque la collecte est indirecte, de sorte que le règlement précise, en son article 14, que l'information ne doit pas être délivrée si:

> «b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques [...] ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles;
> c) l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée [...]»[103].

Deuxièmement, le règlement amorce un changement de paradigme en matière de responsabilité, avec l'avènement de la notion d'*accountability*, ou de res-

103 Article 14, § 5, b, du R.G.P.D.

ponsabilisation en français. Elle constitue une forme de responsabilité renforcée[104] en ce qu'elle fait peser la charge de la preuve sur le responsable du traitement.

Si les obligations d'autorisations ou de notifications préalables ont disparu, le principe d'*accountability* impose aux acteurs des traitements d'être capables à tout moment de prouver la conformité de leurs traitements au R.G.P.D., induisant de nouvelles obligations documentaires. Ainsi tant le responsable du traitement que le sous-traitant doivent tenir un registre[105] des activités de traitement dans la grande majorité des cas. Ils ont l'obligation de mener une analyse d'impact sur les traitements présentant un risque important pour les droits et libertés des personnes concernées[106], ou encore de contractualiser leur relation[107] dans le cadre du traitement des données avec une attention particulière s'agissant des transferts hors de l'Union.

L'*accountability*, ou la responsabilisation, est donc caractérisée par un passage d'obligations générales à des obligations ciblées, notamment s'agissant des traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées. Le législateur européen espérait ainsi stimuler l'efficacité des mécanismes de protection en œuvre dans le règlement[108].

En ce sens, le R.G.P.D. suggère, en son considérant n° 91, la réalisation d'analyses d'impact dans les cas de surveillance de masse grâce au déploiement du « big data » via les réseaux sociaux, comme suit :

> « En particulier aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour es droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits [...] ».

104 Article 5, § 2, du R.G.P.D. : « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ». Son respect implique la mise en place de systèmes de contrôle et de documentation (mesures d'audit, politique interne...) pour garantir la conformité du traitement. Cette obligation conduit à une inversion de la charge de la preuve au profit des personnes concernées.

105 Article 30 du R.G.P.D.

106 Article 35 du R.G.P.D. La version finale du règlement a supprimé l'énumération non exhaustive des risques justifiant une analyse d'impact, à charge pour les États membres et le Comité européen de protection des données d'énoncer ces situations.

107 Articles 26 et 28 du R.G.P.D.

108 Au principe d'*accountability* le législateur européen a joint un mécanisme de sanction, avec des amendes pouvant atteindre un plafond de 20 000 000 euros (articles 77 et 84 du R.G.P.D.) sous le contrôle d'une autorité nationale indépendante (articles 51 et s. du R.G.P.D., à titre d'exemple : la CNIL en France, l'A.P.D. en Belgique, l'ICO en Angleterre, le C.N.P.D. au Luxembourg...) en vue d'assurer l'effectivité des dispositions du règlement.

S'agissant des transferts massifs vers les pays tiers ou une organisation internationale dans les cas où il n'existe pas de décision d'adéquation ou de garantie appropriée, le règlement démontre sa volonté de tenir compte des risques liés à la surveillance de masse en énonçant, en son article 49, que :

> « Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, *un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.* Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit » (nous soulignons).

Il y a lieu, néanmoins, de rester attentifs à l'interprétation faite *in concreto* de la notion d'« intérêts légitimes impérieux », qui ne fait l'objet d'aucune liste, qu'elle soit exemplative ou exhaustive.

Enfin, le règlement introduit, en son article 5, c), le principe de minimisation et proportionnalité[109], invitation explicite à la modération[110]. Ce principe de minimisation consiste, d'une part, à s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement, et d'autre part, à limiter le traitement des données au minimum, en ce qui concerne les catégories de données traitées, les données traitées, le volume ou la quantité de données traitées.

Il s'ensuit que seul le traitement nécessaire à la finalité déterminée peut être mis en œuvre et seules les données nécessaires peuvent être traitées en vue d'atteindre la finalité recherchée, et ce pour une durée minimale, à savoir limitée à l'état d'exception[111] dans le cadre de l'objet de la présente contribution.

109 Principe relatif au traitement des données à caractère personnel selon lequel celles-ci doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées », voy. article 5, § 1er, c, du R.G.P.D.

110 C. De Terwangne, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *in* I. De Lamberterie, A. Strowel et C. Castets-Renard (dir.), *Quelles protections des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, p. 94.

111 Article 5, § 1er, d), du R.G.P.D.

Les mesures de sécurité nécessaires doivent également être respectées en vue de protéger les données à caractère personnel[112], particulièrement quand il s'agit de données sensibles, telles que les données de santé.

Ces dispositions sont peu propices au déploiement par les autorités publiques ou le secteur privé de mesure de surveillance de masse. Si le R.G.P.D. apporte ainsi un cadre strict au déploiement des technologies de l'information à des fins de surveillance massive, s'agissant de communications électroniques, il doit être complété par la lecture de la directive ePrivacy relative aux communications électroniques[113].

c. La directive police-justice[114]

Ensuite, si le R.G.P.D. reste applicable au partage de données dans les secteurs privés et publics, il ne s'applique pas aux traitements des données de la police et de la justice. Il faut alors s'en remettre à la directive police-justice. Or ces autorités mobilisent de manière plus régulière la surveillance de masse.

La différence entre le R.G.P.D. et la directive police-justice se situe, outre son champ d'application matériel, surtout au niveau des droits des personnes concernées tels que le droit à l'information, le droit d'accès, le droit d'opposition, ou encore le droit à l'oubli, mais aussi dans le fait que la directive n'impose aucun système contraignant de sanctions administratives. En outre, s'agissant d'une directive, elle a dû être transposée dans le droit des États membres[115].

Par ailleurs, la directive police-justice ne prévoit pas de disposition spécifique relative aux tiers autres que les témoins ou les personnes susceptibles de pouvoir fournir des informations aux enquêteurs. Elle fera, à ce titre, l'objet de vives critiques du groupe de travail de l'article 29[116] (ci-après Groupe 29), qui

112 Article 32 du R.G.P.D.

113 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.C.E.*, L 201, 31 juillet 2002.

114 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.

115 En Belgique, elle a été transposée dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel entrée en vigueur le 5 septembre 2018. Cette loi implémente à la fois le R.G.P.D. et transpose la directive police-justice, et encadre les activités de traitement par les autorités hors champ d'application de l'U.E. telles que les services de renseignements, la défense et l'armée.

116 Le G29 ou Groupe de travail Article 29 sur la protection des données (en anglais, *Article 29 Data Protection Working Party*, abrégé en WP29) est un ancien organe consultatif de l'Union européenne indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE, dont il tire sa dénomination, et par l'article 14 de la directive 97/66/CE. À compter de l'entrée en vigueur du R.G.P.D., il est remplacé par le Comité européen de la protection des données.

précise que le traitement des données de ces tiers « ne devrait être autorisé que dans certaines conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité légitime, clairement définie » mais aussi « être limité à une période déterminée et l'utilisation ultérieure de ces données à d'autres fins devrait être interdite »[117]. De manière plus générale, le Groupe 29 préconise l'adoption de garanties supplémentaires à l'égard de la catégorie des personnes non suspectées compte tenu de l'évolution des techniques et des méthodes répressives[118].

À titre illustratif, le système « P.N.R. »[119] pour « Passenger Name Record » implique le traitement de données de personnes non suspectées d'avoir commis une infraction pénale, imposant aux transporteurs et opérateurs de voyage des différents secteurs de transport international (aérien, ferroviaire, routier et maritime) de transmettre les informations relatives à leurs passagers[120] à une banque de données gérée par les autorités publiques[121].

Ces données ont vocation à être analysées avant l'arrivée, le transit ou le départ d'une personne sur le territoire national des États membres[122] par l'Unité d'informations des passagers (ci-après U.I.P.)[123]. Cette méthode appliquée à des fins de « pre-screening »[124] permettrait de « faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services »[125].

117 Groupe 29, avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale, 26 février 2013, p. 3.

118 *Ibid.*

119 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (P.N.R.) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.U.E.*, L 119, 4 mai 2016, p. 132. Soulignons qu'avant l'adoption de cette directive, l'Union européenne a conclu en parallèle des accords bilatéraux avec des pays tiers, dont les États-Unis, le Mexique et le Canada ; transposée en Belgique par la loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017 (loi P.N.R.).

120 L'article 9 de la loi P.N.R. distingue les données A.P.I., à savoir les données d'enregistrement et d'embarquement, des données P.N.R., à savoir les données de réservation. Les données A.P.I. sont des données authentiques, par exemple des données biographiques figurant sur une carte d'identité. Les données P.N.R. comprennent davantage d'informations : il s'agit notamment de l'itinéraire complet pour le passager, l'agence de voyages, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre, poids et identification des bagages, numéro de transport, etc.), les modes de paiement et l'adresse de facturation, etc.

121 Article 3 de la loi P.N.R.

122 Article 24 de la loi P.N.R.

123 Article 24 de la loi P.N.R.

124 Le « pre-screening » consiste en « l'évaluation du risque représenté par les passagers » et s'effectue par le biais d'une corrélation entre les banques de données des services compétents ou par le biais de critères préétablis par l'U.I.P.

125 Exposé des motifs, *Doc. parl.*, Ch., 2015-2016, n° 54-2069/001, p. 29. En outre, les services compétents, à savoir les services de police, la Sûreté de l'État, le Service général de renseignement et de sécurité, de

Cette directive européenne est fortement critiquée au niveau européen tant par le Groupe 29[126] qu'ensuite par le C.E.P.D.[127] qui lui succède, invoquant notamment son manque de proportionnalité compte tenu de son caractère systématique et massif, celle-ci s'appliquant de manière générale et indifférenciée à l'égard des passagers.

De même, selon le Conseil de l'Europe, un tel mécanisme ciblant des personnes « qui n'ont commis aucune infraction » ne pourrait en aucun cas viser « un but légitime » au sens de la Charte et de la C.E.D.H. d'autant qu'il existe un risque d'erreur inévitable susceptible de mener à du profilage discriminatoire[128]. Dans le cadre de l'examen de l'accord P.N.R. conclu entre le Conseil de l'Union et le Canada[129], la Cour de justice a néanmoins validé cet outil de « renseignement en matière criminelle »[130] s'appliquant à des tiers non suspectés d'avoir commis une infraction, sous réserve de règles matérielles et procédurales strictes[131].

services d'enquêtes liées aux infractions douanes et accises (article 14, § 1er, 2°, de la loi P.N.R.), ont la possibilité de procéder à des recherches ponctuelles dans les limites de leurs missions et des finalités prévues par la loi, à savoir notamment la lutte contre le terrorisme, la recherche et la poursuite de certaines infractions et la lutte contre l'immigration illégale (article 8 de la loi P.N.R.).

126 Voy. notamment Groupe 29, avis 7/2010 sur la communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers passagers (P.N.R.) aux pays tiers, 12 novembre 2010 ; Groupe 29, avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 5 avril 2011.

127 C.E.P.D., avis n° 5/2015, deuxième avis sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 24 septembre 2015, pp. 4 et s.

128 Rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, « Passenger Name Records, data mining & data protection: the need for strong safeguards », 15 juin 2015, T-PD (2015)11.

129 Le 23 juin 2014, le Canada et le Conseil de l'U.E. signaient un accord concernant le transfert des données P.N.R. Le texte fut soumis pour approbation au Parlement en juillet 2014, lequel saisit la C.J.U.E. pour une demande d'avis (C.J.U.E., 26 juillet 2017, avis 01/2015).

130 Lors des négociations intraeuropéennes au sujet de la directive P.N.R., il y fut rappelé que même si les données des passagers sont liées aux déplacements, il s'agirait essentiellement d'un outil de « renseignement en matière criminelle » plutôt que d'un « instrument de contrôle aux frontières ». Voy. Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, COM(2011) 32 final.

131 La Cour, après avoir exclu le traitement des données sensibles, rappelle la nécessité de clarifier les catégories de données, de faire usage de modèles et critères « spécifiques et fiables » et « non discriminatoires » et de faire référence à des bases de données en lien avec l'objectif poursuivi. Puis, s'appuyant sur sa propre jurisprudence, la Cour rappelle que la période conservation des données devrait « toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi ». Partant, le stockage pendant cinq ans après le départ des passagers du territoire canadien pour lesquels aucun risque n'a été identifié ne semble présenter aucun lien « ne serait-ce qu'indirect » entre les données conservées et l'objectif poursuivi. De même, l'accès aux données devrait répondre à certaines conditions matérielles et procédurales basées sur des critères objectifs et être subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante sur demande motivée des autorités compétentes. En outre, les personnes concernées devraient bénéficier d'un droit à l'information individuelle. Par ailleurs, la communication des données P.N.R. à un pays tiers ne devrait être admise qu'à la condition qu'il existe soit un accord entre l'Union et ce pays tiers équivalent à l'accord envisagé, soit une décision d'adéquation de la Commission. Enfin, le contrôle du respect des règles précisées par l'accord devrait être assuré par une autorité de contrôle indépendante (C.J.U.E., 26 juillet 2017, avis 01/2015, considérants 158, 165, 172, 191, 199-202, 205, 208, 214, 220, 230).

II. La surveillance de masse comme clef de sortie de l'état d'exception : conditions posées par la jurisprudence de la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne

Sur Internet ou ailleurs, les individus et leurs données sont protégés contre leurs utilisations abusives, qu'il s'agisse du fait des autorités publiques[132] ou d'acteurs privés, comme les employeurs[133], les plateformes de partage de contenu, les vendeurs de chaussures ou les réseaux sociaux. La Cour de justice[134] tout comme la Cour E.D.H.[135] assurent cette protection et s'élèvent en rempart contre les excès de surveillance[136], clarifiant le contenu de la législation applicable.

Néanmoins, toute forme de surveillance n'est pas bannie pour autant. Bien au contraire, les interceptions sont admises devant les deux prétoires, mais au prix de strictes conditions protégeant la société contre les dérives de la surveillance étatique ou des entreprises privées[137]. L'examen de cette jurisprudence permet-

132 Parmi de nombreux arrêts, voy. notamment Cour eur. D.H., arrêt *Malone c. Royaume-Uni* ; Cour eur. D.H. (gde ch.), arrêt *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, req. nos 58170/13, 62322/14 et 24960/15.

133 Cour eur. D.H., arrêt *Copland c. Royaume-Uni*, 3 avril 2007, req. n° *62617/00* ; Cour eur. D.H. (gde ch.), arrêt *Barbulescu c. Roumanie*, 5 septembre 2017, req. n° 61496/08.

134 C.J.U.E., 8 avril 2014, *Digital Rights Ireland*, aff. jointes C-293/12 et C-594/12, EU:C:2014:238.

135 L'article 5, § 1er, de la directive 2002/58 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.C.E.*, L 201, 31 juillet 2002) prescrit la confidentialité des communications ainsi que des données relatives au trafic y afférentes, c'est-à-dire toutes les données traitées en vue de l'acheminement d'une communication ou de sa facturation.

136 Cour eur. D.H., arrêt *P.G. et J.H. c. Royaume-Uni*, 25 septembre 2001, req. n° 44787/98, § 42 ; C.J.U.E., *Digital Rights Ireland*. Voy. également Cour eur. D.H., arrêt *Sher et autres c. Royaume-Uni*, 20 octobre 2015, req. n° 5201/11, spéc. § 170 : « Les observations du tiers intervenant, Privacy International, portent essentiellement sur la perquisition d'appareils électroniques, pratique qui implique l'accès aux données personnelles et aux données de communication. Le tiers intervenant explique que les innovations technologiques offrent des possibilités de collecte, de stockage, de partage et d'analyse de données inimaginables auparavant. Selon lui, le contrôle par les forces de l'ordre des appareils électroniques d'un individu leur permet d'accéder à toutes les traces numériques laissées par celui-ci à quelque moment que ce soit, y compris les informations qui ne sont pas stockées sur ces appareils eux-mêmes mais sur des serveurs informatiques distants interconnectés. Le croisement de ces données serait extrêmement révélateur. La perquisition d'appareils électroniques revêtirait un caractère particulièrement intrusif, ce qui commanderait la fixation d'un seuil élevé d'exigence pour l'appréciation de la justification d'une atteinte aux droits protégés par l'article 8 ».

137 Cour eur. D.H., arrêt *Benedik c. Slovénie*, 24 avril 2018, req. n° 62357/14, § 132 : « La Cour estime que la loi dont la police s'est prévalue pour obtenir des informations sur l'abonné liées à l'adresse IP dynamique

tra de tirer les enseignements des décisions, d'une part, de la Cour E.D.H. (A), et d'autre part, de la Cour de justice (B).

A. *Enseignements tirés de la jurisprudence de la Cour européenne des droits de l'homme*

La Cour E.D.H., sollicitée de manière régulière sur la question relative à la conformité des mesures de surveillance avec la C.E.D.H., a développé une jurisprudence importante au départ de l'affaire *Klass e.a. c. Allemagne* en 1978[138].

Dans cette affaire, cinq ressortissants allemands se plaignaient de la violation de l'article 8 de la C.E.D.H. par l'Allemagne en cause de la législation dite « G 10 »[139] autorisant certaines autorités à adopter des mesures de surveillance sans que les individus en soient jamais avisés et sans qu'aucun recours judiciaire soit possible, même après la levée des mesures de surveillance.

Dans sa décision, la Cour commence par reconnaître aux requérants la qualité de « victimes » comme suit :

> « La législation incriminée institue un système de surveillance exposant chacun, en République fédérale d'Allemagne, au contrôle de sa correspondance, de ses envois postaux et de ses télécommunications, sans qu'il ne le sache jamais à moins d'une indiscrétion ou d'une notification ultérieure »[140].

Ensuite, la Cour établit les principes à suivre pour assurer la compatibilité d'un régime juridique de surveillance avec l'article 8 de la C.E.D.H.

De manière générale, lors de l'examen de la conformité à la C.E.D.H. des traitements de données à caractère personnel par une autorité publique, le contrôle de la Cour E.D.H. se concentre en trois phases différentes. Premièrement, elle vérifie que la requête tombe dans le champ des droits protégés par l'article 8, § 1er, de la C.E.D.H.[141] et établit la qualité de « victime » dans le chef des requérants. Deuxièmement, elle vérifie si l'État assume une obligation positive

manquait de clarté et n'offrait pas de garanties suffisantes contre une ingérence arbitraire dans l'exercice des droits du requérant découlant de l'article 8 ». Voy. également Cour eur. D.H., *Malone c. Royaume-Uni*; gde ch., arrêt *Amann c. Suisse*, 16 février 2000, req. n° 27798/95 ; gde ch., arrêt *Roman Zakharov c. Russie*, 4 décembre 2015, req. n° 47143/06 ; arrêt *Szabó et Vissy c. Hongrie*, 12 janvier 2016, req. n° 37138/14 ; gde ch., *Big Brother Watch et autres c. Royaume-Uni*.

138 Cour eur. D.H., *Klass e.a. c. Allemagne*.

139 *Ibid.*, §§ 10-17. La *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, appelé « la G 10 », est une loi du 13 août 1968 portant restriction du secret de la correspondance, des envois postaux et des télécommunications, permettant le contrôle de la correspondance et les envois postaux, la lecture des messages télégraphiques, l'écoute et l'enregistrement des conversations téléphoniques, contre des « dangers imminents » pour « l'ordre fondamental démocratique et libéral », pour « l'existence ou la sécurité de la fédération ou d'un Land », etc.

140 *Ibid.*, § 37.

141 Voy. en ce sens Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.* ; R. Angrisani, « Données personnelles et surveillance massive », *op. cit.* ; U. Kilkelly, « Le droit au respect de la vie privée et familiale : un guide sur la mise en oeuvre de l'article 8 de la Convention

concernant les droits garantis, et enfin, troisièmement, si par ailleurs il s'en acquitte valablement.

Une fois l'ingérence vérifiée et la qualité de « victime » établie, la Cour procède à l'analyse de facteurs autorisant les restrictions à l'article 8 de la C.E.D.H., à savoir le critère de légalité, de légitimité et de nécessité (ou de proportionnalité), comme suit.

1. Les critères de la Cour

a. Critère de légalité des mesures de surveillance

Pour que ce critère soit garanti, l'ingérence doit être prévue par une loi portant sur les mesures générales de surveillance, ce qui suppose l'adoption de la mesure par un parlement. S'agissant des mesures individuelles de surveillance, elles doivent se conformer aux conditions et procédures rigoureuses fixées par la législation elle-même[142]. En outre, dans la jurisprudence de la Cour, ce critère est étroitement corrélé à celui de nécessité[143], examiné ci-dessous.

b. Critère de nécessité des mesures de surveillance

La surveillance dénoncée doit, dans une société démocratique, être « nécessaire à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales »[144]. 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. La Cour vérifiera en deux étapes « 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 »[145].

c. Critère de légitimité

La Cour accorde une large marge d'appréciation aux États dans l'établissement du critère de légitimité. À titre d'exemple, elle a reconnu la légitimité de l'utilisation de mesures de surveillance à des fins de sécurité nationale dans le cadre de la prévention des actes de terrorisme, comme suit :

> « Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que

européenne des droits de l'homme », *in* Conseil de l'Europe, *Précis sur les droits de l'homme*, Allemagne, 2003, n° 1.

142 Cour eur. D.H., *Klass e.a. c. Allemagne*, § 43.

143 Voy en ce sens : les affaires Cour eur. D.H. (gde ch.), *Roman Zakharov c. Russie*, § 236 ; *Kennedy c. Royaume-Uni*, § 155 ; gde ch., *Big Brother Watch et al. c. Royaume-Uni*, § 334.

144 Cour eur. D.H., *Klass e.a. c. Allemagne*, § 46.

145 *Ibid.*

> l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales »[146].

Partant, de manière constante depuis 1978, la Cour reconnaît au législateur national un certain pouvoir discrétionnaire qui n'est toutefois pas illimité[147]. La Cour examine dès lors l'existence de garanties adéquates et suffisantes contre les abus et l'existence de recours adéquat, de sorte que s'agissant de la surveillance de masse, ce contrôle essentiel consiste en un examen *in concreto* des procédures et mécanismes de contrôle *a priori* ou *a posteriori* à disposition des individus[148].

À cet égard, elle précise que cette appréciation doit se faire compte tenu de toutes les circonstances de la cause, en particulier « l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne »[149].

En ce sens déjà, en l'affaire *Turek c. Slovaquie*[150], le juge de Strasbourg soulignait l'importance de l'obligation dans le chef des États parties d'adopter toutes les mesures pour un exercice effectif du droit à la protection des données, y compris le respect des garanties déjà énumérées, prévues dans la Convention n° 108.

Plus récemment, s'agissant de la surveillance de masse dénoncée par les révélations d'Edward Snowden, dans son arrêt *Big Brother* du 25 mai 2021, la Cour précise que :

> « [A]fin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré par des "*garanties de bout en bout*", c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori* »[151].

146 *Ibid.*, § 49.

147 *Ibid.*

148 R. Angrisani, « Données personnelles et surveillance massive », *op. cit.*, § 17.

149 Cour eur. D.H., *Klass e.a. c. Allemagne*, § 50.

150 Cour eur. D.H., arrêt *Turek c. Slovaquie*, 14 février 2006, req. n° 57986/00. Dans cette affaire, le requérant dénonçait à la fois le fait que l'ancien service de sécurité de l'ex-Tchécoslovaquie communiste conservait un dossier dans lequel il était inscrit sur la liste des agents de ce service, et le refus des autorités de lui délivrer un « certificat de sécurité » indispensable pour son avancement de carrière. Le juge slovaque avait considéré que ces informations étaient secrètes et donc inaccessibles à tous hormis aux autorités étatiques, c'est-à-dire le Slovenská informačná služba (SIS), soit le service de renseignements du gouvernement slovaque, la Cour a donc sanctionné, estimant « l'absence d'une procédure par laquelle le requérant aurait pu obtenir la protection effective de son droit au respect de sa vie privée » (§ 116) ; voy. également Cour eur. D.H., *S. et Marper c. Royaume-Uni*, § 96.

151 Cour eur. D.H. (gde ch.), *Big Brother Watch et autres c. Royaume-Uni*, § 350. Nous soulignons.

Ce nouveau principe d'encadrement de « bout en bout » sera alors renforcé par une grille d'examen offerte par la Cour, dont les critères permettant d'évaluer la conformité des mesures de surveillance massive vont au-delà des critères établis jusqu'alors dans sa jurisprudence plus traditionnelle. Dans ce dernier arrêt, la Cour E.D.H. procède un peu plus encore à une harmonisation de sa jurisprudence avec celle de la Cour de justice et les recommandations de l'ONU, au bénéfice d'une application de plus en plus autonome du droit à la protection des données.

2. Examen des critères et des exigences de la Cour E.D.H.

a. Exigence en matière de légalité : extension à la nécessité de surveillance

En son arrêt *Weber et Saravia c. Allemagne*[152] la Cour explicite la condition de légalité.

Prima facie, la légalité formelle suppose que les mesures de surveillance disposent d'un fondement légal, à savoir une loi, de sorte que si la mesure contestée ne remplit pas ce critère, elle est *ipso facto* assimilée à une violation « sans qu'il soit nécessaire d'examiner davantage l'affaire au fond »[153].

Ensuite, dans les affaires *Malone c. Royaume-Uni*, *Khan c. Royaume-Uni*[154], ou encore *Kennedy c. Royaume-Uni*[155], concernant l'interception de conversations téléphoniques, la Cour construit la portée de ce critère en précisant l'obligation de clarté, d'accessibilité et de prévisibilité de la norme, comme suit :

> « Les mots "prévues par la loi" [...] exigent l'accessibilité de celle-ci aux personnes concernées et une formulation assez précise pour leur permettre – en s'entourant, au besoin, de conseils éclairés – de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences pouvant résulter d'un acte déterminé »[156].

Par les termes « prévues par la loi », la Cour E.D.H. entend deux niveaux :

- Base en droit interne :
  - La loi doit être accessible au justiciable[157].

152 Cour eur. D.H., décision *Weber et Saravia c. Allemagne*, 29 juin 2006, req. n° 54934/00, §§ 93-94.

153 U. Kilkelly, « Le droit au respect de la vie privée et familiale : un guide sur la mise œuvre de l'article 8 de la Convention européenne des Droits de l'Homme », *op. cit.* ; I. Roagna, *La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme*, 1re éd., Série des précis sur les droits de l'homme du Conseil de l'Europe, Strasbourg, Conseil de l'Europe, 2012, p. 39.

154 Cour eur. D.H., décision *Khan c. Royaume-Uni*, 28 janvier 2014, req. n° 11987/11, § 303. Voy. aussi Cour eur. D.H., arrêt *Margareta et Roger Andersson c. Suède*, 25 février 1992, req. n° 12963/87, § 75.

155 Cour eur. D.H., arrêt *Kennedy c. Royaume-Uni*, 18 mai 2010, req. n° 26839/05, § 155. Voy. aussi R. Angrisani, « Données personnelles et surveillance massive », *op. cit.*, pp. 107-134.

156 Cour eur. D.H., *Margareta et Roger Andersson c. Suède*, § 75.

157 Cour eur. D.H., *Rotaru c. Roumanie*, § 52.

- La loi doit être prévisible, c'est-à-dire « rédigée avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite »[158].
- La loi doit être compatible avec la prééminence du droit[159].

– Contenu de la loi[160] :
- La loi doit fixer le genre d'informations pouvant être traitées.
- La loi doit fixer les catégories de personnes auprès desquelles les données peuvent être collectées.
- La loi doit fixer les circonstances précises dans lesquelles les données peuvent être collectées.

Eu égard au caractère généralement secret de la surveillance opérée à l'insu des personnes surveillées, les conditions d'accessibilité et de prévisibilité prennent une dimension particulière[161]. Dans ce contexte, la Cour, dans l'affaire *Weber et Saravia c. Allemagne*, précise :

> « Quant à [l']exigence [de] [...] prévisibilité de la loi, la Cour rappelle que dans le contexte particulier des mesures de surveillance secrète, telles que l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même d'escompter quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence. [Cependant], le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes. [...] En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire »[162].

La Cour impose dès lors à la loi organisant le régime du renseignement un certain nombre de précisions et de définitions minimales de la manière suivante :

> « [...] (i) la nature des infractions susceptibles de donner lieu à un mandat d'interception, (ii) la définition des catégories de personnes susceptibles d'être mises sur écoute, (iii) la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, (iv)les précautions à prendre pour la communication des données a d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[163].

Partant, dans cette même affaire, la Cour a jugé que la loi allemande du 28 octobre 1994 sur la lutte contre la criminalité qui était mise en cause satisfaisait à l'exigence de légalité. Elle contenait une définition claire et précise des infractions pour la prévention desquelles l'interception de télécommunications pouvait être ordonnée[164] ainsi que la procédure à suivre pour l'examen et l'utilisation des données collectées. Elle indiquait les catégories de personnes susceptibles de faire l'objet d'écoutes téléphoniques, la durée maximale des écoutes[165] et les modalités détaillées de la destruction des données obtenues.

A contrario, en l'affaire *Liberty e.a. c. Royaume-Uni*[166], la condition de légalité n'était pas satisfaite par la loi britannique, en ce que la loi de 1985 sur l'interception de communications[167] permettait d'intercepter les communications à destination ou en provenance de l'étranger sur pied d'un mandat, sans prévoir aucune restriction quant aux catégories de communications pouvant y figurer[168]. De plus, la loi autorisait le ministre de l'Intérieur, en se fondant sur sa seule appréciation, à écouter ou lire les données, en cas de nécessité pour la protection de la sécurité nationale, la prévention d'infractions graves ou la sauvegarde des intérêts de l'économie britannique. Au regard de l'absence de prévisibilité et de la très grande marge de manœuvre laissée au ministre de l'Intérieur, la Cour a estimé que le régime normatif britannique ne répondait pas à l'exigence de légalité, précisant que :

> « En définitive, la Cour considère que, faute d'avoir défini avec la clarté requise l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable conféré à l'État en matière d'interception et d'analyse des communications à destination ou en provenance de l'étranger, la loi en vigueur à l'époque pertinente n'offrait pas une protection suffisante contre les abus de pouvoir. En particulier, au rebours de ce qu'exige la jurisprudence de la Cour, aucune précision sur la procédure applicable à l'examen, la diffusion, la conservation et la destruction des données interceptées n'y figurait sous une forme accessible au public »[169].

158 *Ibid.*, § 55.
159 Cour eur. D.H., *Malone c. Royaume-Uni*, § 67.
160 Cour eur. D.H., *Rotaru c. Roumanie*, §§ 52 et s. ; Cour eur. D.H., *S. et Marper c. Royaume-Uni*, § 95.
161 Cour eur. D.H., arrêt *Liberty e.a. c. Royaume-Uni*, 1er juillet 2008, req. n° 58243/00, § 68 : « Le gouvernement avance que la divulgation d'informations sur les mesures relatives à l'examen, l'utilisation, la conservation et la destruction de renseignements interceptés prises par le ministre de l'Intérieur à l'époque pertinente aurait pu nuire à l'efficacité du dispositif de collecte de données ou créer un risque pour la sécurité. Toutefois, [la Cour] observe que les autorités allemandes ont considéré que l'insertion, dans la loi G10 en cause dans l'affaire *Weber et Saravia* (précitée), de dispositions expresses sur le traitement de données obtenues au moyen d'interceptions stratégiques pratiquées sur des lignes téléphoniques non allemandes ne présentait pas de danger. »
162 Cour eur. D.H., *Weber et Saravia c. Allemagne*, § 93.
163 *Ibid.*, § 95 ; voy. également Cour eur. D.H., arrêt *Huvig c. France*, 24 avril 1990, req. n° *11105/84*, § 34 ; arrêt *Kruslin c. France*, 24 avril 1990, req. n° 11801/85, § 35 ; arrêt *Valenzuela Contreras c. Espagne*, 30 juillet 1998, req. n° 27671/95, § 46 ; arrêt *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, 28 juin 2007, req. n° 62540/00, § 76 ; gde ch., *Big Brother Watch et autres c. Royaume-Uni*, § 115.
164 Cour eur. D.H., *Weber et Saravia c. Allemagne*, § 97.
165 *Ibid.*, §§ 98 et 99.
166 Le recours avait été introduit par trois associations de défense des libertés civiles, dont les communications entre Dublin et Londres avaient été interceptées.
167 Interception of Communications Act 1985.
168 Cour eur. D.H., *Liberty e.a. c. Royaume-Uni*, § 64.
169 *Ibid.*, § 69.

Il s'ensuit que les mesures de surveillance doivent être encadrées par un système légal qui en définit de manière suffisamment précise les contours, dépassant l'exigence purement formelle pour offrir une définition comprenant une série de conditions substantielles concernant les modalités de prise de décisions et de mise en œuvre de mesures de surveillance, qu'elles soient ciblées ou massives.

b. Exigence en matière de nécessité : proportionnalité au regard des buts légitimes de la surveillance

Par la suite, dans sa jurisprudence relative à la surveillance massive, la Cour procédera à un élargissement de son test de légalité, en y intégrant le critère de nécessité qui est un élément essentiel dans 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" »[170].

Depuis lors, cette dernière vérifie simultanément si la mesure est « prévue par la loi » et si elle est « nécessaire » et elle stipule que :

> « La "qualité de la loi" en ce sens implique que le droit national doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont "nécessaires dans une société démocratique", notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus »[171].

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[172].

Dès lors qu'il est établi qu'une ingérence est prévue par la loi, la Cour examine cette loi. Lors de son examen, elle se demande si cette loi poursuit un but légitime au sens de l'article 8, § 2, de la C.E.D.H. et évalue la proportionnalité de la mesure au regard de ce but.

i. Le but légitime

La Cour laisse aux États une marge d'appréciation plus ou moins large, s'agissant de la détermination du but légitime, de sorte que la surveillance de communications et de correspondances ou encore de données à caractère personnel peut être légitime quand elle est rendue nécessaire à la défense de la « sécurité

170 Cour eur. D.H., *Kennedy c. Royaume-Uni*, § 155.

171 Voy. en ce sens les affaires Cour eur. D.H. (gde ch.), *Roman Zakharov c. Russie*, § 236 ; *Kennedy c. Royaume-Uni*, § 155 ; gde ch., *Big Brother Watch et autres c. Royaume-Uni*, § 334.

172 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, p. 863.

nationale » et de « l'ordre », à « la prévention des infractions pénales », à la « protection de la santé ou de la morale » et « des droits et libertés d'autrui », ou encore au « bien-être économique du pays »[173].

Force est de constater que ces buts offrent un large pouvoir d'appréciation dans le chef de l'État dans la détermination des objectifs permettant de mener des activités de surveillance. À cet égard, la Cour rejette rarement le ou les buts légitimes identifiés, même lorsqu'ils sont contestés[174].

Toutefois, la nature du but invoqué pour justifier la surveillance devrait influencer l'analyse de la proportionnalité des mesures de surveillance[175]. À titre d'exemple, la lutte contre le terrorisme autoriserait des ingérences plus intrusives que la protection du bien-être économique, ou que la gestion d'une pandémie et la sécurité sanitaire.

ii. Le test de proportionnalité

Ensuite, le principe de proportionnalité s'examine au regard des objectifs publics poursuivis, à savoir les finalités de la surveillance. Il s'ensuit que les activités de surveillance ne peuvent s'ingérer dans les droits fondamentaux des individus que dans la mesure nécessaire à la protection de certains intérêts reconnus comme légitimes.

Le test de proportionnalité est réalisé à partir de différents critères mis en évidence par la jurisprudence de la Cour[176], en particulier la nature du but poursuivi, la portée de la mesure de surveillance, les conditions d'utilisation des données récoltées et les mécanismes de contrôle et de recours existants. Or, les moyens de surveillance ont évolué de manière extraordinaire ces dernières années, principalement en corrélation avec le développement des technologies numériques et d'Internet. Les mesures ciblées, consistant principalement en l'interception de conversations téléphoniques fixes et du courrier, en l'utilisation de balises ou encore en l'observation directe, ont cédé la place à des techniques beaucoup plus perfectionnées permettant de tracer le comportement et les habitudes d'un individu sans limites dans le temps ou dans l'espace, par

173 La loi britannique mentionnait comme motifs permettant la mise en place d'opérations de surveillance : « la sécurité nationale », « la prévention et la détection d'infractions graves », « la sauvegarde du bien-être économique du Royaume-Uni » sans renvoyer nécessairement à des impératifs de sécurité ni à la commission d'infractions pénales. La Cour, dans l'affaire *Liberty e.a. c. Royaume-Uni*, n'a toutefois pas jugé utile d'examiner ce point de manière spécifique (§ 28) ; voy. également U. Kilkelly, « Le droit au respect de la vie privée et familiale », *op. cit.*, p. 31.

174 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.* ; R. Angrisani, « Données personnelles et surveillance massive », *op. cit.*, p. 125 ; U. Kilkelly, « Le droit au respect de la vie privée et familiale... », *op. cit.*, p. 8.

175 Cette question n'a, jusqu'à présent, pas été abordée de manière directe par la Cour. En ce sens M. Milanovic, « Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age », *Harvard International Law Journal*, 2015, vol. 56, pp. 133 et s.

176 Cour eur. D.H. (gde ch.), *Big Brother Watch et autres c. Royaume-Uni*.

l'entremise de son téléphone, son smartphone, son ordinateur, sa consommation et sa navigation sur Internet.

Cette surveillance sophistiquée est complétée par une faculté grandissante de récoltes, de traitements et de stockages massifs de données à des fins stratégiques, en vue d'identifier parmi celles-ci des comportements suspects, de retrouver des informations concernant des infractions commises ou plus simplement de connaître les centres d'intérêt ou les accointances politiques ou religieuses des individus.

Cette évolution entraîne des ingérences plus intrusives dans la vie privée, susceptibles de concerner des personnes qui n'ont commis et qui ne commettront aucun délit. Les récentes révélations sur le projet Pegasus ne sont que le sommet de l'iceberg et démontrent que la surveillance 2.0 est une réalité, dure certainement, mais réalité quand même ! On constate que la présomption d'innocence est en danger et qu'apparaît de plus en plus un raisonnement qui tend à considérer tout individu comme étant potentiellement coupable donc sujet de surveillance.

Pourtant, pendant longtemps, la Cour ne voyait aucune raison de soumettre les dispositifs de surveillance plus généraux ou massifs à des critères d'accessibilité et de clarté différents de ceux de la surveillance plus ciblée[177]. Faisant fi de l'évolution des technologies de l'information jusqu'en 2015, elle se bornait à rappeler sa jurisprudence établie depuis 1978 en l'affaire *Klass e.a. c. Allemagne*, dans laquelle elle avait déjà reconnu un certain pouvoir discrétionnaire quant au choix des modalités du système de surveillance aux États parties[178].

Ainsi, en 2015, dans l'affaire *Roman Zakharov c. Russie*, la Grande Chambre a réitéré le principe selon lequel « les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale »[179].

En cette affaire, portée par une O.N.G. de défense des droits fondamentaux, la Cour devait apprécier le régime légal russe de surveillance visant à assurer « la sécurité nationale, contre les faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie »[180].

Dans ce cadre, elle a confirmé que le système de surveillance non ciblé, donc susceptible de viser « une personne non soupçonnée d'une infraction », n'appelait pas à un traitement particulier en raison du caractère stratégique ou indifférencié de la surveillance[181]. Dès lors, elle porte son analyse sur la légalité, à savoir la prévisibilité et la nécessité des mesures dans une société démocratique, et l'existence de garanties procédurales[182] comme suit :

> « La Cour déduit de ce qui précède que les recours évoqués par le gouvernement sont ouverts uniquement aux personnes qui disposent d'informations relatives à l'interception de leurs communications. L'effectivité de ces recours est donc compromise par l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception, et par l'inexistence d'une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations sur les interceptions. La Cour estime en conséquence que le droit russe n'offre pas de recours judiciaire effectif contre les mesures de surveillance secrète dans les cas où une procédure pénale n'a pas été engagée contre le sujet de l'interception »[183].

Comme dans sa jurisprudence précédente, la Cour n'a guère pris en considération la portée générale des mesures dénoncées, se bornant au caractère « secret » des mesures. Elle évalue la proportionnalité du régime de surveillance à l'examen de l'existence « des garanties et des garde-fous suffisants »[184].

iii. Le test de « la stricte nécessité »

Néanmoins, quelques semaines après cette décision, la Cour revient sur sa position, remise en question tant par la jurisprudence de la Cour de justice de l'Union européenne[185] que par les rapports des instances de l'ONU[186], de sorte que, dans *l'arrêt Szabó et Vissy c. Hongrie*, elle adopte pour la première fois une approche différente, malgré la forte similarité des deux affaires[187].

---

177 Cour eur. D.H., *Liberty e.a. c. Royaume-Uni*, § 28. Voy également Cour eur. D.H., *Weber et Saravia c. Allemagne*, §§ 111, 114-117 ; la Cour y tient une position similaire concernant des communications susceptibles d'être interceptées sur la base de mots clés, dans le cadre de ce qui constituait une activité de surveillance générale, ne ciblant pas des individus préalablement repérés comme présentant un risque pour la sécurité nationale.

178 Cour eur. D.H., *Klass e.a. c. Allemagne*, § 49.

179 Cour eur. D.H. (gde ch.), *Roman Zakharov c. Russie*, § 232.

180 *Ibid.*, §§ 31 et 32.

181 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, p. 880.

182 Elle a également procédé à un examen conjoint des critères de légalité et de nécessité, sans les distinguer. Elle précise que « [l]a "qualité de la loi" en ce sens implique que le droit interne doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont "nécessaires dans une société démocratique", notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus » (Cour eur. D.H. (gde ch.), *Roman Zakharov c. Russie*, § 236).

183 Cour eur. D.H. (gde ch.), *Roman Zakharov c. Russie*, § 298.

184 *Ibid.*, § 237.

185 Voy. notamment C.J.U.E., *Digital Rights Ireland*.

186 Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, A/69/397, 23 septembre 2014, § 50. Voy. également le rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », A/HRC/27/37, 30 juin 2014, §§ 39-41.

187 En effet, dans les deux occurrences, la requête était introduite par des O.N.G. actives dans le domaine des droits humains et mettait en cause le régime législatif permettant l'adoption de mesures d'interception des communications à l'égard de personnes qui n'étaient pas soupçonnées d'avoir commis une infraction pénale par des services de renseignement susceptibles de porter atteinte au droit à la vie privée des requérants, en violation de l'article 8 de la C.E.D.H. De manière plus spécifique en l'affaire *Szabó et Vissy c. Hongrie*, les requérants se plaignaient de la création en 2011 d'une unité spéciale en matière de lutte contre le terrorisme au sein des forces de police par le gouvernement hongrois. Les intéressés ont porté

En cette affaire, à l'étape de l'examen de la légalité au sens strict, la Cour procède à l'examen de la proportionnalité en prenant pour la première fois pleinement en considération les spécificités de la surveillance à grande échelle, en ce qu'elle énonce que :

> « [I]l ne peut être exclu que les dispositions générales de la loi sur la sécurité nationale puissent être considérées comme permettant des interceptions dites stratégiques et à grande échelle, ce qui constitue un sujet de grave préoccupation.
> La Cour ajoute que la possibilité offerte aux gouvernements d'acquérir un profil détaillé des aspects les plus intimes de la vie des citoyens peut entraîner des ingérences particulièrement envahissantes dans la vie privée.
> Il est fait référence dans ce contexte aux points de vue exprimés par la Cour de justice de l'Union européenne et le Parlement européen. Cette menace pour la vie privée doit faire l'objet d'un examen très attentif tant au niveau interne que sous l'angle de la Convention »[188].

La Cour fait ouvertement référence à la décision de la Cour de justice de l'Union européenne, notamment en l'affaire *Digital Rights Ireland*, dans laquelle les juges avaient mené une réflexion sur l'impact de l'utilisation des métadonnées[189].

Ensuite, la Cour, mettant fin à sa jurisprudence constante, ne procède plus au test de proportionnalité traditionnel mais inclut celui de la « stricte nécessité » dès lors qu'elle est confrontée à la surveillance de masse[190]. Il s'ensuit que l'examen de la « stricte nécessité » des mesures de surveillance massive doit être réalisé à la lumière de deux critères, comme l'énonce la Cour :

> « Toutefois, compte tenu du caractère particulier de l'ingérence en question et du potentiel des technologies de surveillance de pointe à porter atteinte à la vie privée des citoyens, la Cour estime que l'exigence de "nécessité dans une société démocratique" doit être interprétée dans ce contexte comme exigeant une "stricte nécessité" sous deux aspects. Une mesure de surveillance secrète ne peut être jugée conforme à la Convention que si elle est strictement nécessaire, à titre de considération générale, à la sauvegarde des institutions démocratiques et, en outre, si elle est strictement nécessaire, à titre de considération particulière, à l'obtention de renseignements vitaux dans une opération individuelle. De l'avis de la Cour, toute mesure de surveillance secrète qui ne répond pas à ces critères sera sujette à des abus de la part des autorités qui disposent de technologies redoutables à leur disposition »[191].

Le contrôle de stricte nécessité est effectué en deux temps. Premièrement, la Cour E.D.H. évalue « la proportionnalité de la mesure de surveillance dans sa nature, compte tenu de sa portée et de ses caractéristiques technologiques »[192]. Dès lors que la surveillance devient massive (non ciblée), 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[193] (test de nécessité au sens strict). Deuxièmement, elle vérifie, dans le cadre de l'opération spécifique portée à son attention, que le choix d'une 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).

c. Exigence de mécanismes de contrôles et de recours suffisants et effectifs

Le dernier élément pertinent pour évaluer la conformité des mesures de surveillance avec la Convention consiste en l'existence de garanties procédurales et la mise en place de mécanismes de contrôle effectifs. 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 doit dégager un équilibre délicat entre les exigences d'efficacité des mesures de sécurité et la garantie des droits des individus.

L'effectivité des mécanismes de contrôle mise en balance avec le caractère secret des surveillances soulève le problème de l'existence d'une procédure de notification en amont ou en aval de la surveillance. La notification est, en effet, le seul moyen pour les individus placés sous surveillance de prendre connaissance des mesures dont ils font l'objet et d'exercer le cas échéant les recours à leur disposition.

leur recours à la Cour constitutionnelle hongroise, qui a estimé que les opérations secrètes se justifiaient à des fins de sécurité nationale. Les requérants ont ensuite porté leur recours devant la Cour européenne des droits de l'homme en violation de l'article 8 (Cour eur. D.H., *Szabó et Vissy c. Hongrie*, § 11).

188 Cour eur. D.H., *Szabó et Vissy c. Hongrie*, §§ 69-70. Traduction libre de : « it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern. 70. The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile (see the CDT's submissions on this in paragraph 49 above) of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. »

189 Voy. *infra* B. Enseignement de la Cour de justice de l'Union européenne – 1. L'arrêt *Digital Rights Ireland*.

190 Test élaboré par la Cour de justice.

191 Cour eur. D.H., *Szabó et Vissy c. Hongrie*, § 73. Traduction libre de : « However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement 'necessary in a democratic society' must be interpreted in this context as requiring 'strict necessity' in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal ».

192 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, p. 282.

193 Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, précité, § 52.

Dans sa jurisprudence, la Cour n'a pas manqué d'aborder la question, considérant que l'absence de notification ne rendait pas nécessairement l'ingérence dans la vie privée abusive, même si elle reste souhaitable. Elle précise à cet effet ce qui suit :

> « La Cour rappelle que la question de la notification ultérieure de mesures de surveillance est indissolublement liée au caractère effectif des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance ; si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice.
> Toutefois, l'absence de notification ultérieure aux personnes touchées par des mesures de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'était pas "nécessaire, dans une société démocratique", car c'est précisément cette absence d'information qui assure l'efficacité de la mesure constitutive de l'ingérence. En effet, pareille notification risquerait de révéler les méthodes de travail des services de renseignements et leurs champs d'observation [...]. Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction [...] »[194].

Enfin, la Cour a également jugé qu'une absence totale de système de notification pouvait rester compatible avec les exigences de la Convention, à la condition qu'un organe de contrôle indépendant puisse être saisi sur recours à partir d'un simple soupçon de surveillance, sans que la compétence de cet organe soit subordonnée à une notification de l'interception.

Ainsi, s'agissant du recours effectif et nécessaire, la Cour se satisfait du mécanisme de contrôle non judiciaire et n'adapte pas son analyse des garanties procédurales à l'extension de la portée des mesures de surveillance. Néanmoins, elle précise l'importance de l'indépendance de l'organe de contrôle.

Enfin, s'agissant de l'exigence de mécanismes de contrôle et de recours suffisant, l'arrêt *Big Brother* marque un tournant important en ce que la Cour y considère que, afin de réduire autant que possible le risque d'abus, la surveillance de masse doit être encadrée par des « garanties de bout en bout »[195], de sorte que la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus.

3. Examen des derniers arrêts : « Big Brother » sous la loupe

Enfin, les derniers arrêts majeurs de la Cour européenne des droits de l'homme en matière de surveillance massive sont les arrêts *Big Brother Watch c. Royaume-Uni*[196] ainsi que *Centrum för rättvisa c. Suède*[197], faisant suite aux révélations d'Edward Snowden. Il s'agit de deux arrêts rendus le même jour dans deux dossiers distincts mais ayant des objets similaires, à savoir « l'interception, par les services de renseignement, de grandes quantités de communications et de données de communication associées transitant à travers les frontières nationales, et leur filtrage ultérieur au moyen de termes de recherche destinés à détecter des informations pouvant présenter un intérêt pour le renseignement »[198].

Les deux dossiers ont connu des parcours différents :

- Celui opposant Centrum för Rättvisa à la Suède a été introduit le 14 juillet 2008 et visait les interceptions par voie électronique auprès de fournisseurs de services de communication des communications entre la requérante et des particuliers, des organisations et des entreprises en Suède et à l'étranger par courrier électronique, par téléphone et par télécopie, souvent sur des sujets sensibles, dans le cadre d'activités de renseignement. Par un arrêt du 19 juin 2018, une chambre de la Cour avait conclu, à l'unanimité, à la non-violation de l'article 8. Le 19 septembre 2018, la requérante a demandé le renvoi de l'affaire devant la Grande Chambre conformément à l'article 43 de la C.E.D.H. qui a fait droit à cette demande par un arrêt du 19 septembre 2019.
- Celui opposant des organisations et personnes militant pour la défense des libertés civiles au Royaume-Uni a été introduit devant la Cour via trois requêtes, respectivement le 4 septembre 2013, le 11 septembre 2014 et le 20 mai 2015. Ces requêtes, faisant suite aux révélations d'Edward Snowden sur l'existence de programmes de surveillance et de partage de renseignements entre les États-Unis et le Royaume-Uni, portaient sur trois régimes de surveillance mis en place au Royaume-Uni, à savoir : (i) l'interception massive de communications, (ii) la réception d'éléments interceptés obtenus auprès de gouvernements et de services de renseignement étrangers, et enfin (iii) l'obtention de données de communication auprès des fournisseurs de services de communication[199]. Par un arrêt du 13 septembre 2018, une chambre de la Cour a conclu, par cinq voix contre deux, que le régime d'interception en masse emportait violation de l'article 8 parce que, d'une part, le processus de sélection des

194 Cour eur. D.H., *Weber et Saravia c. Allemagne*, § 135.
195 Cour eur. D.H. (gde ch.), *Big Brother Watch et autres c. Royaume-Uni*, § 350.
196 *Ibid.*
197 Cour eur. D.H. (gde ch.), arrêt *Centrum för rättvisa c. Suède*, 19 juin 2018, req. n° 35252/08.
198 Cour eur. D.H., « Questions-réponses sur les arrêts *Big Brother Watch et autres c. Royaume-Uni* et *Centrum för rättvisa c. Suède* », 25 mai 2021, disponible sur le site www.echr.coe.int/Documents/Press_Q_A_Big_Brother_Watch_Others_Centrum_for_rattvisa_FRA.pdf, consulté en dernier lieu le 4 décembre 2021. « Dans l'affaire dirigée contre le Royaume-Uni, les requérantes se plaignaient aussi de la réception de renseignements obtenus auprès de gouvernements et/ou de services de renseignement étrangers et de l'obtention de données de communication auprès des fournisseurs de services de communication » (*ibid.*).
199 À l'époque des faits, le régime d'interception en masse et d'obtention de données de communication auprès des fournisseurs de services de communication avait pour base légale une loi de 2000 portant réglementation des pouvoirs d'enquête (Regulation of Investigatory Powers Act 2000). Depuis lors, cette loi a été remplacée par la loi de 2016 sur les pouvoirs d'enquête (Investigatory Powers Act 2016). Les conclusions auxquelles la Grande Chambre est parvenue concernent uniquement les dispositions de la loi de 2000, qui formaient le cadre juridique en vigueur à l'époque des faits litigieux.

canaux de transmission Internet visés par les interceptions ainsi que le filtrage, la recherche et la sélection pour examen des communications interceptées faisaient l'objet d'une supervision insuffisante et, d'autre part, parce que les garanties applicables à la sélection pour examen des « données de communication associées » étaient inadéquates. Néanmoins, l'arrêt n'a pas rencontré la satisfaction des requérantes de sorte que le 12 décembre 2018, ils ont demandé le renvoi de l'affaire devant la Grande Chambre conformément à l'article 43 de la C.E.D.H., demande à laquelle il a été fait droit par arrêt du 4 février 2019.

Dans la cause *Centrum för rättvisa c. Suède*, la Grande Chambre a, par quinze voix contre deux et au terme d'un arrêt amplement motivé, conclu à la violation de l'article 8 de la C.E.D.H., en ce que le régime en cause ne satisfaisait pas à l'exigence de « garanties de bout en bout ». Il excédait la marge d'appréciation accordée aux autorités de l'État défendeur et n'offrait pas une protection adéquate et effective contre l'arbitraire et le risque d'abus. La Cour a jugé, en particulier, que même si les caractéristiques principales du régime suédois d'interception en masse répondaient aux exigences de la Convention relatives à la qualité de la loi, le régime en question souffrait néanmoins 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[200].

En son arrêt *Big Brother Watch* également du 25 mai 2021, la Cour rappelle sa jurisprudence en matière de surveillance massive issue d'un arrêt rendu en 2006, étant l'arrêt *Weber et Saravia* dans une affaire d'interception en masse de communications, considérant que « la décision d'utiliser un système d'interception en masse relève de la marge d'appréciation reconnue aux États »[201]. Elle relève que sa jurisprudence avait identifié six garanties minimales, appelées également les six garanties Weber de l'arrêté du même nom[202] et reformulées par la Chambre dans son arrêt du 13 septembre 2018, à savoir[203] :

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 ;

200 J.-Ph. Foegle, « L'État de surveillance au régime sec : la CJUE renforce la prohibition de la surveillance "de masse" », *La Revue des droits de l'homme*, 8 février 2017, disponible sur le site https://journals.openedition.org/revdh/2966, consulté en dernier lieu le 4 décembre 2021.

201 Cour eur. D.H. (gde ch.), *Big Brother Watch et autres c. Royaume-Uni*, § 275.

202 Cour eur. D.H., *Weber et Saravia c. Allemagne*.

203 Cour eur. D.H. (gde ch.), *Big Brother Watch et autres c. Royaume-Uni*, § 274.

3. la limite à la durée de l'exécution de la mesure et 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.

Elle explique également sa jurisprudence classique en rappelant que « tant dans la décision *Weber et Saravia* que dans l'arrêt *Liberty et autres* [...], la Cour a appliqué les six garanties minimales [...] énoncées dans sa jurisprudence relative aux interceptions ciblées [...] »[204].

Après avoir rappelé ces éléments, la Cour constate les limites de cette jurisprudence en relevant que :

> « [M]ême si les régimes d'interception en masse qu'elle y a examinés étaient à première vue similaires à celui contesté dans le cas d'espèce, ces deux affaires remontent à plus de dix ans et, 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 [...]. Par conséquent, l'étendue de l'activité de surveillance examinée dans ces deux affaires aurait été bien plus restreinte.
> 342. Il en va de même pour les données de communication associées. Comme indiqué dans le rapport établi à l'issue du contrôle des activités de surveillance, pour chaque individu, le volume de données de communication actuellement disponible est normalement supérieur au volume de données de contenu, car chaque contenu s'accompagne de multiples données de communication [...]. Si le contenu d'une communication, crypté ou non, peut ne rien révéler d'utile sur son expéditeur ou son destinataire, les données de communication associées, en revanche, peuvent révéler un grand nombre d'informations personnelles telles que l'identité et la localisation de l'expéditeur et du destinataire, ou encore l'équipement par lequel la communication a été acheminée. De plus, toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent désormais faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts [...].
> 343. Un autre élément est plus important encore : dans la décision *Weber et Saravia* et dans l'arrêt *Liberty et autres* [...], la Cour n'a pas expressément tenu compte du fait qu'il s'agissait d'une surveillance dont la nature et l'échelle étaient différentes de celles examinées dans les affaires précédentes. Or les inter-

204 *Ibid.*, § 341.

ceptions ciblées et l'interception en masse présentent un certain nombre de différences importantes »[205].

La Cour rappelle également la distinction à apporter dans la protection à octroyer à la surveillance ciblée et la surveillance de masse comme suit :

> « Le présent grief porte sur l'interception en masse par les services de renseignement de communications transfrontières. Même si ce n'est pas la première fois que la Cour examine ce type de surveillance (*Weber et Saravia*, décision précitée, et *Liberty et autres*, arrêt précité), il est apparu au cours de la procédure que l'appréciation d'un tel régime soulève des difficultés spécifiques. À l'époque actuelle, où le numérique est de plus en plus présent, la grande majorité des communications se fait sous forme numérique et est acheminée à travers les réseaux mondiaux de télécommunication de manière à emprunter la combinaison de chemins la plus rapide et la moins chère sans aucun rapport significatif avec les frontières nationales. La surveillance qui ne vise pas directement les individus est par conséquent susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère. »[206]

Ce préalable posé, elle procède à une description ou définition des étapes inhérentes à la surveillance massive comme suit :

> « La Cour juge que l'interception en masse est 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. Sous réserve de ce qui précède, la Cour considère néanmoins que les étapes du processus d'interception en masse qu'il convient d'examiner peuvent être décrites 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 »[207].

Ensuite, et dans un souci de dépassement de sa jurisprudence classique dont elle a préalablement montré les limites, la Cour établit les critères spécifiquement applicables à l'examen de conformité des mesures de surveillance de masse. Elle rappelle par ailleurs que ces mesures de surveillance ne sont pas interdites, en soi, par l'article 8 de la C.E.D.H., notamment s'agissant d'assurer

205 *Ibid.*, §§ 341-343.
206 *Ibid.*, § 322.
207 *Ibid.*, § 325.

« la sécurité nationale » ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves[208].

Cependant, la Cour considère qu'afin de réduire autant que possible le risque d'abus, le processus doit être encadré par des « garanties de bout en bout »[209], de sorte que la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, ci-dessus définies, par une autorité indépendante du pouvoir exécutif, et ce, dès la définition de l'objet et de l'étendue de l'opération jusqu'au contrôle opéré *a posteriori*. Ces facteurs sont, de l'avis de la Cour, « des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 »[210].

Il découle de ce principe de protection procédural « de bout en bout » que pour déterminer si l'État a agi dans les limites de sa marge d'appréciation, la Cour analysera conjointement les critères selon lesquels la mesure doit être « prévue par la loi » et sa nécessité. Elle recherchera 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 »[211].

En conclusion, au gré de la jurisprudence de la Cour en matière de surveillance de masse, le principe de légalité, étendu une première fois à l'examen de la nécessité, à savoir l'évaluation la proportionnalité du régime de surveillance,

208 *Ibid.*, § 347. La Cour y rappelle que les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet. Cependant, la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place.
209 *Ibid.*, § 350.
210 *Ibid.* La Cour renvoie à cet égard au rapport de la Commission de Venise, selon lequel deux des garanties les plus importantes dans un régime d'interception en masse sont l'autorisation et le contrôle du processus (§ 197).
211 *Ibid.*, § 361.

au regard des buts légitimes poursuivis, puis de la « stricte nécessité », connaît une nouvelle extension. La légalité matérielle portera en outre sur les éléments procéduraux garantissant « de bout en bout » les risques d'abus.

Enfin, la Cour en cette affaire étend son examen au transfert des données interceptées vers une partie tierce, tel que cela est visé au cinquième critère de l'arrêt *Weber*, en relevant que :

> « [Elle] n'a, à ce jour, fourni aucune indication spécifique concernant les précautions à prendre pour la communication d'éléments interceptés à d'autres parties. Or il est clair aujourd'hui que certains États partagent régulièrement des informations avec leurs partenaires du renseignement et, parfois même, leur donnent un accès direct à leur propre système. Dès lors, la Cour considère que la transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales devrait être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle devrait être soumise à certaines garanties supplémentaires relatives au transfert lui-même »[212].

Elle fixe ainsi des conditions de licéité des transferts des données collectées au moyen d'interception massive entre les États :

- Première condition : les circonstances dans lesquelles un tel transfert peut avoir lieu doivent être clairement énoncées dans le droit interne.
- Deuxième condition : l'État expéditeur doit s'assurer que « l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées »[213].
- Troisième condition : les garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière.

Enfin, la Cour considère que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant, assurant ainsi le principe de garanties procédurales « de bout en bout ».

La Cour opère ainsi un nouveau tournant dans sa jurisprudence en matière de surveillance massive en rappelant le développement d'obligations procédurales positives, notamment visant à garantir la transparence des traitements de données et l'accès à un recours effectif à charge des États, sous l'impulsion et en application des mesures et obligations découlant du droit à la protection des données.

Cette évolution jurisprudentielle qui, et cela ne peut être critiqué, témoigne d'un développement autonome du droit fondamental à la protection des données personnelles tend vers une logique plus managériale visant essentiellement à encadrer de manière optimale l'usage d'informations personnelles[214].

212 *Ibid.*, § 362.

213 *Ibid.*

214 J.-Ph. Foegle, « Chronique du droit "post-Snowden" : la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme*, 30 mars 2016, § 33, disponible sur le site https://journals.openedition.org/revdh/2074, consulté en dernier lieu le 4 décembre 2021.

Cette approche du risque d'abus pourrait être effectuée au détriment de l'article 8 de la C.E.D.H. et du droit à la vie privée et familiale, en ce qu'il présente un risque non négligeable de perte de sens du droit à la vie privée au profit d'une approche managériale. À titre exemplatif, au nom de la « lutte contre le terrorisme », des atteintes de plus en plus larges à la vie privée des personnes au motif de l'existence de garanties procédurales adéquates pourraient être admises, voire se normaliser. La question principale est de savoir si l'article 8 peut se satisfaire d'une telle approche binaire alors que les droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel se doivent d'exister au-delà de simples procédures au risque de vider l'article 8 de toute effectivité.

B. Enseignements de la Cour de justice de l'Union européenne

La question de la conformité des mesures de surveillance massive, et particulièrement de la récolte et de l'utilisation des données personnelles, est au centre de l'attention de la Cour de justice qui a rendu plusieurs arrêts majeurs en la matière[215].

Deux arrêts rendus en 2014, l'un concernant la Hongrie et l'autre l'Irlande, ont clairement prohibé la surveillance de masse en se basant sur une violation des dispositions de la Charte à laquelle il est ainsi reconnu toute sa puissance et sa portée. Le plus connu des deux, l'arrêt *Digital Rights Ireland*[216], prohibe radicalement toute surveillance de masse en invalidant intégralement la directive 2006/24[217] sur la conservation des données à caractère personnel, bâtie sous impulsion anglaise dans le contexte émotionnel des attentats de Londres de juillet 2005[218]. Cette jurisprudence est affinée par celle invalidant tour à tour le *Safe Harbor*[219], puis le *Privacy*

215 C.J.C.E., 30 mai 2006, *Parlement c. Conseil*, aff. jointes C-317/04 et C-318/04, EU:C:2006:346 ; C.J.U.E., 10 février 2009, *Irlande c. Parlement et Conseil*, aff. C-301/06, EU:C:2009:68 ; C.J.U.E., 13 juin 2013, *Schwarz*, aff. C-291/12, EU:C:2013:670 ; C.J.U.E., 8 avril 2014, *Commission c. Hongrie*, aff. C-288/12, EU:C:2014:237 ; C.J.U.E., *Digital Rights Ireland*, précité ; C.J.U.E., 16 avril 2015, *Willems e.a.*, aff. jointes C-446/12 à C-449/12, EU:C:2015:238 ; C.J.U.E., 6 octobre 2015, *Schrems*, aff. C-362/14, EU:C:2015:650 (ci-après *Schrems I*) ; C.J.U.E., 26 juillet 2017, avis 1/15 ; C.J.U.E., 21 décembre 2019, *Tele2 Sverige*, aff. jointes C-203/15 et C-698/15, EU:C:2016:970 ; C.J.U.E., 16 juillet 2020, *Facebook Ireland et Schrems*, aff. C-311/18, EU:C:2020:559 (ci-après *Schrems II*).

216 C.J.U.E., *Digital Rights Ireland*, précité.

217 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de service de communications électroniques accessibles au public ou de réseaux publics de communication et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105/54, 13 avril 2006, invalidée.

218 M.-L. Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », *La Revue des droits de l'homme*, 14 mai 2014, pp. 1-4 ; Fl. Benoit-Rohmer, « Protection des données personnelles », note sous C.J.U.E., *Digital Rights Ireland*, *Rev. trim. dr. eur.*, 2015, p. 168.

219 C.J.U.E., *Schrems I*, invalidant la décision 200/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection

Shield[220] sur la question des transferts de données vers les États tiers dans un contexte de méfiance grandissante à la suite des révélations d'Edward Snowden en 2013, arrêts sur lesquels la Cour E.D.H. semble s'appuyer dans son arrêt *Big Brother Watch*.

Ces affaires emblématiques, sélectionnées pour les besoins de la présente contribution, actent le combat de la Cour pour une meilleure protection du droit fondamental au respect de la vie privée, et particulièrement de la protection des données à caractère personnel.

1. L'arrêt *Digital Rights Ireland*

Saisie sur question préjudicielle posée par la High Court irlandaise à la suite du recours introduit par la société Digital Rights Ireland, la Cour de justice[221] se prononce sur la question de la violation de la Charte par les mesures législatives et administratives nationales transposant la directive 2006/24 relative à la conservation de données relatives aux communications électroniques[222].

La question soulevée consistait à déterminer si l'obligation faite aux opérateurs de télécommunications de conserver les données de communications électroniques pendant une durée minimale de six mois, afin d'en permettre la disponibilité en cas d'enquête sur des infractions graves, était compatible avec les droits fondamentaux des individus, et en particulier les articles 7 et 8 de la Charte. La Cour de justice de l'Union européenne dispose en l'occurrence que :

> « L'ingérence que comporte la Directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère [...] d'une vaste ampleur et [...] doit être considérée comme particulièrement grave. [...] [L]a circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante »[223].

L'arrêt présente plusieurs intérêts majeurs. Premièrement, marquant une rupture nette avec sa jurisprudence précédente, et notamment son arrêt du 10 février 2009[224], la Cour de justice pose pour la première fois tout son raisonnement sur une grille d'analyse fournie uniquement par la Charte afin d'évaluer la justification de l'ingérence, causée par la directive 2006/24. Elle

assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des *États*-Unis d'Amérique, *J.O.C.E.*, L 215, 25 août 2000, pp. 7-47.

220 C.J.U.E., *Schrems* II.

221 C.J.U.E., *Digital Rights Ireland*, précité.

222 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, p. 870.

223 C.J.U.E., *Digital Rights Ireland*, § 37.

224 C.J.U.E., *Irlande c. Parlement et Conseil*.

marque un nouveau pas dans son émancipation de la Cour E.D.H., déjà amorcé avec l'arrêt *Volker und Markus Schecke et Eifert*, du 9 novembre 2010[225].

Il s'ensuit que la Cour de justice évalue la justification de l'ingérence, causée par la directive aux droits garantis par les articles 7 et 8 de la Charte, sur pied des dispositions de l'article 52, § 1er, de la Charte, qui énonce ce qui suit :

> « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

Force est de constater que la grille de lecture est peu ou prou la même que celle mise en œuvre par l'article 8, § 2, de la C.E.D.H., même si la formulation n'est pas identique. La Cour de justice examinera donc tour à tour les questions de savoir si :

- la limitation de l'exercice du droit garanti est « prévue par la loi » ;
- la limitation respecte le principe de proportionnalité ;
- la limitation est nécessaire ; et enfin
- la limitation répond à des objectifs d'intérêt général reconnus par l'Union ou à un besoin de protection des droits et libertés d'autrui.

Deuxièmement, la Cour procède à une réflexion sur les métadonnées qui, « prises dans leur ensemble, 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 [et] les relations sociales de ces personnes »[226].

Troisièmement, la Cour de justice procède à un examen de la portée des technologies sur la mesure de surveillance concernée, et notamment son caractère non ciblé, observant que :

> « [L]a directive 2006/24 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. [...] [L]a directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception,

225 C.J.U.E., 9 novembre 2010, *Volker und Markus Schecke et Eifert*, aff. jointes C-92/09 et 93/09, EU:C:2010:662.

226 C.J.U.E., *Digital Rights Ireland*, § 27.

de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »[227].

Quatrièmement, s'agissant de l'examen des mesures de surveillance non ciblée ou massive, la Cour de justice introduit un contrôle strict de la proportionnalité. En effet, le caractère non ciblé de la mesure de conservation des données de communication constitue dès lors un élément capital, impactant directement l'évaluation de la proportionnalité de la mesure :

> – « [T]out en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves »[228].
> – « En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict. [...] S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire »[229].

L'on relève du récent avis de l'avocat général Campos Sánchez-Bordona en les affaires conjointes *Space Net, Telekom Deutschland* du 18 novembre 2021 la confirmation de cette jurisprudence en ce que :

> « [L]'obligation de stockage généralisée et indifférenciée [la législation allemande] impose couvre un très large éventail de données relatives au trafic et de données de localisation. La limite temporelle imposée à ce stockage ne remédie pas à ce défaut, puisque, en dehors du cas de figure justifié par la défense de la sécurité nationale, le stockage des données relatives aux communications électroniques doit être sélectif en raison du risque sérieux que comporterait leur conservation généralisée. L'avocat général rappelle en outre que, en tout état de cause, l'accès à ces données constitue une ingérence grave dans les droits fondamentaux à la vie privée et familiale et à la protection des données à caractère personnel [Articles 7 et 8 de la Charte], indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité »[230].

227 *Ibid.*, §§ 56-57.
228 *Ibid.*, § 59.
229 *Ibid.*, §§ 48 et 52.
230 C.J.U.E., « Conclusions de l'avocat général dans les affaires jointes C-793/19 SpaceNet et C-794/19 Telekom Deutschland, dans l'affaire C-140/20 Commissioner of the Garda Síochána e.a. et dans les affaires jointes C-339/20 VD et C-397/20 SR », communiqué de presse n° 206/21, 18 novembre 2021.

Il précise également que « la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation n'est justifiée que par la protection de la sécurité nationale, ce qui n'inclut pas la poursuite des infractions, même graves »[231] et que l'accès aux données conservées doit être « soumis au contrôle préalable d'une juridiction ou d'une autorité indépendante, comme l'exige la jurisprudence de la Cour »[232].

Ainsi, s'agissant de l'objectif d'intérêt général laissé à l'appréciation des États, contrairement à la jurisprudence classique de Cour E.D.H., la Cour de justice n'autorise qu'un pouvoir d'appréciation réduit[233] impliquant la nécessité d'un contrôle strict[234] de l'ingérence dans les droits fondamentaux, qui doit s'opérer « dans les limites du strict nécessaire »[235].

La Cour de justice finira par convaincre la Cour E.D.H., de sorte que l'arrêt de la Cour E.D.H., s'inspirant directement du présent arrêt, marque l'avènement d'une analyse équivalente des juges européens sur la question de la surveillance de masse.

2. L'arrêt *Tele2 Sverige* du 21 décembre 2016

En l'occurrence, la Cour de justice est sollicitée par voie de questions préjudicielles posées par la Suède[236] et l'Angleterre en vue de clarifier l'interprétation de la directive 2002/58 sur la vie privée et les communications électroniques[237], lue à la lumière de la Charte et notamment ses articles 7 et 8. Ce fut l'occasion pour la Cour de justice de réaffirmer une nouvelle fois sa détermination à garantir les droits fondamentaux des citoyens face aux législations prévoyant une obligation générale pour les fournisseurs de services de communications électroniques, de conservation « systématique, continue, généralisée et indifférenciée de données relatives au trafic et des données de localisation, sans aucune exception »[238]. La Cour a réitéré une analyse analogue à celle de l'arrêt *Digital*

231 *Ibid.*
232 *Ibid.*
233 C.J.U.E., *Digital Rights Ireland*, § 48.
234 *Ibid.*
235 *Ibid.*, § 52.
236 En l'occurrence, à la suite de l'invalidation de la directive 2006/24 par la C.J.U.E., une société, la Tele2 Sverige, fournisseur de services de communications électroniques, a notifié l'autorité suédoise de surveillance des télécommunications qu'elle cesserait, à compter du 14 avril 2014, de conserver les données relatives aux communications électroniques visées par la loi sur les communications électroniques suédoises, et procéderait à la suppression des données conservées jusqu'alors. Néanmoins, la direction générale de la police nationale suédoise, qui fait appel régulièrement au service de la Tele2 Sverige, porte plainte en raison du fait que cette dernière avait cessé de lui communiquer les données utiles à ses enquêtes. Dans le cadre du recours de la société, la Suède adresse à la C.J.U.E. une question préjudicielle.
237 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, *J.O.C.E.*, L 201/37, 31 juillet 2002.
238 C.J.U.E., *Tele2 Sverige*, §§ 46, 50, 62, 97, 103, 105, 112 et 134.

Rights Ireland, en affirmant être en présence d'une « ingérence particulièrement grave »[239].

La Cour y pose sa jurisprudence relative à l'accès aux données et métadonnées par les États membres encadrant anticipativement la transposition de la directive 2016/680 du 27 avril 2016 sur la collecte des métadonnées à des fins de politique pénale (recherche, détection et prévention des infractions pénales).

La Cour de justice y rappelle que l'ensemble des métadonnées sont, en termes de risques pour la vie privée, aussi sensibles que le contenu des correspondances, en ce qu'elle énonce 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, 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 [...]. En particulier, 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 »[240].

Ensuite, elle confirme l'importance de prévoir un contrôle préalable d'une juridiction ou autorité administrative indépendante[241], notamment quand la surveillance entraîne une ingérence particulièrement grave aux droits et libertés des individus, par un traitement massif systématique, continu, généralisé et indifférencié des données sans aucune exception.

Cette notion de conservation « généralisée et indifférenciée des données » fait directement écho à l'accès « massif » souligné par la Cour de justice dans son premier arrêt *Schrems* invalidant l'accord *Safe Harbor*[242]. C'est donc assez logiquement que la Cour y a également condamné le fait que ces législations nationales n'exigeaient pas que les données en cause soient « conservées sur le territoire de l'Union »[243] ni qu'elles soient « irrémédiablement détruites au terme de leur durée de conservation »[244].

La Cour a conclu que ces régimes dérogatoires au droit fondamental au respect de la vie privée et de protection des données à caractère personnel ne s'opéraient pas dans les limites strictement nécessaires[245] dans une société démocratique.

239 *Ibid.*, §§ 100, 125 et 134 ; C.J.U.E., *Digital Rights Ireland*, § 37.

240 C.J.U.E., *Tele2 Sverige*, § 99.

241 C.J.U.E., « Arrêt dans les affaires jointes C-203/15 Tele2 Sverige AB/ Post-och telestyrelsen et C-698/15 Secretary of State for the Home Department/Tom Watson e.a. », Communiqué de presse n° 145/16, 21 décembre 2016.

242 Voy *infra*, point 3 « Les arrêts *Schrems I* et *Schrems II*: Safe Harbor et Privacy Shield ».

243 C.J.U.E., *Tele2 Sverige*, §§ 114, 122 et 125.

244 *Ibid.*, § 122.

245 *Ibid.*, §§ 103, 107-110, 118 et 119. Voy. le considérant n° 30 de la directive 2002/58 : « les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires ».

En somme, la Cour n'autorise la conservation de données à titre préventif que pour autant que celle-ci soit ciblée et non massive, qu'elle vise uniquement à lutter contre la criminalité grave, que les catégories de données conservées soient limitées au strict nécessaire et que l'accès des autorités nationales soit soumis à un contrôle préalable et à des garanties procédurales, notamment s'agissant des transferts hors de l'Union[246].

3. Les arrêts *Schrems I* et *Schrems II* : Safe Harbor et Privacy Shield

Les présentes affaires s'inscrivent dans le combat mené par Maximillian Schrems, doctorant et chercheur autrichien, afin d'assurer une protection effective des données à caractère personnel, notamment face aux GAFAM[247]. Respectivement un an et demi et cinq ans et demi après l'arrêt *Digital Rights Ireland*, de manière cohérente, la Cour de justice confirme sa position[248] et son engagement à garantir les droits issus de la Charte, et notamment la protection des données à caractère personnel dans les deux affaires *Schrems c. Data Protection Commissioner*[249].

Elle s'attaque en l'occurrence et de manière plus spécifique à la question de la légalité des transferts de données vers les États-Unis[250] dans le cadre des traitements du réseau social Facebook. Dans son premier arrêt, la Cour de justice répond à la question de la légalité du transfert vers les États-Unis et la validité de la décision d'adéquation 2000/520/CE de la Commission européenne, plus connue sous le nom de *Safe Harbor*. Cette décision considérait le niveau de protection assurée par les États-Unis adéquat en termes de protection des données à caractère personnel. Dans le second arrêt[251], la Cour vérifie la légalité de la décision d'adéquation 2016/1250 de la Commission, appelée *Privacy Shield*

246 A.-L. Villedieu, « Données personnelles : la défense du droit à la vie privée face à la volonté des États membres d'imposer une surveillance généralisée », *LEXplicite*, 31 mai 2017, disponible sur le site www.lexplicite.fr/donnees-personnelles-defense-droit-vie-privee-surveillance-generalisee/, consulté en dernier lieu le 4 décembre 2021.

247 GAFAM est l'acronyme des géants du Web, à savoir Google (Alphabet), Appel, Facebook (devenu Meta), Amazon et Microsoft. Il s'agit des cinq grandes firmes américaines qui dominent le marché du numérique, parfois également nommées les *Big Five*, ou encore *The Five*. Cet acronyme correspond au sigle GAFA initial, auquel est ajouté le M de Microsoft. Certains utilisent également l'acronyme GAFAMI pour ajouter I.B.M. à l'ensemble.

248 C.J.U.E., *Digital Rights Ireland*, § 52 : « S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire ». Voy. aussi le § 48 de cet arrêt.

249 C.J.U.E., *Schrems I*.

250 L'article 25, § 1er, de la directive 95/46/CE pose le principe suivant : le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ne peut avoir lieu que si ce pays assure un niveau de protection « adéquat » à de telles données, pouvant être constaté par une décision de la Commission. Inversement, le considérant 57 de la même directive prévoit l'interdiction d'un transfert de ces données vers un pays tiers lorsque celui-ci n'offre pas ledit niveau de protection., cité par J.-Ph. Foegle, « Chronique du droit "Post-Snowden" », *op. cit.*, p. 1.

251 C.J.U.E., *Schrems I*, en particulier les §§ 78 et 92.

et succédant au *Safe Harbor*, ainsi que l'application des Clauses Standard de la Commission aux transferts vers les États-Unis[252].

Dans sa première décision, rendue le 6 octobre 2015, la Cour a, dans son évaluation de la légalité de la décision de la Commission, pris en considération la masse de personnes visées et la portée des traitements. Elle précise, à cet effet, que la nécessité d'offrir des garanties suffisantes contre les abus était d'autant plus cruciale que ces données sont soumises à un traitement automatique[253] et une conservation « généralisée [...] de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées »[254].

Il s'ensuit qu'une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée[255]. Le traitement massif d'informations concernant un nombre élevé de personnes apparaît dès lors, en l'absence de règles précises et de garanties suffisantes, constituer une violation du droit à la vie privée, même dans l'objectif de la protection de la sécurité nationale[256].

Dans son analyse, la Cour de justice a ainsi conclu au manque de « garanties suffisantes contre les abus »[257], « même dans l'objectif de la protection de la sécurité nationale »[258], invalidant la décision *Safe Harbor* de la Commission, elle-même prise sur le fondement de la directive 95/46 en ce qui concerne la violation de la protection des données et de la vie privée respectivement inscrites aux articles 7 et 8 de la Charte.

Dans son second arrêt, appelé *Schrems II*, la Cour de justice va plus loin dans l'expression de sa méfiance à l'égard des États-Unis, estimant que la législation actuellement en vigueur aux États-Unis ne permet pas d'assurer un niveau de protection adéquat pour les citoyens européens dont les données transiteraient par ou vers les États-Unis, en mobilisant le R.G.P.D.

Elle invalide, à nouveau, la décision d'adéquation de la Commission dont l'objet était précisément de pallier les insuffisances du *Safe Harbor*, en tirant les enseignements de la jurisprudence de la Cour E.D.H. Selon la Cour de justice, le niveau de protection accordé aux États-Unis en matière de données à caractère personnel n'est pas adéquat au sens du R.G.P.D., en ce que « le droit de ce

252 Décision 2010/87/EU du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement et du Conseil.

253 C.J.U.E., *Schrems I*, § 91.

254 *Ibid.*, § 93.

255 *Ibid.*, § 94.

256 Sur ces deux arrêts, voy. notamment J.-Ph. Foegle, « Chronique du droit "Post-Snowden" », *op. cit.*

257 C.J.U.E., *Schrems I*, § 93.

258 Fr. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, p. 872 ; C.J.U.E., *Schrems I*, § 93.

pays tiers ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa règlementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences »[259].

En cause de cette insécurité, on retrouve plusieurs programmes de surveillance américains fondés sur l'article 702 du *Foreign Intelligence Surveillance Act* (FISA) de 1978[260] et sur l'*Executive Order* 12333 de 1981[261], permettant aux agences de renseignement de collecter et traiter massivement des données. Ces programmes donnent lieu à des ingérences qui ne sont pas clairement encadrées[262] et contre lesquelles les personnes concernées ne bénéficient pas d'un droit de recours effectif[263]. Un autre élément ayant affaibli le *Privacy Shield* est la modification apportée par Donald Trump à l'*US Judicial Redress Act* via un *Executive Order* du 25 janvier 2017. En effet, la clause 14 prescrit que « les agences doivent, dans la mesure où cela est compatible avec la loi applicable, s'assurer que leurs politiques de confidentialité excluent les personnes qui ne sont pas des citoyens américains ou des résidents permanents légaux des protections de la loi sur la protection de la vie privée concernant les informations personnellement identifiables »[264].

La décision d'adéquation 2016/1250 ainsi annulée par la Cour de justice emporte dans son sillage l'inadéquation des clauses contractuelles types adoptées par la Commission européenne, par sa décision 2010/87/EU, pour encadrer des transferts de données vers les États-Unis, même si ces dernières restent valides en leur principe. La Cour de justice précise que le choix des clauses contractuelles types pour encadrer un transfert implique une responsabilisation de l'exportateur des données personnelles, qui doit vérifier « au cas par cas [...] si le droit du pays tiers de destination assure une protection appropriée [...] en fournissant, au besoin, des garanties supplémentaires à celles offertes par ces clauses »[265].

L'exportateur des données personnelles a donc l'obligation de procéder à une analyse effective de la législation et des pratiques en vigueur dans le pays tiers,

259 C.J.U.E., *Schrems* II, § 168.

260 FISA, pub. L. 95-511, 92 Stat. 1783, 50 U.S.C. ch 36 ; il s'agit d'une loi fédérale américaine qui établit des procédures pour la surveillance physique et électronique et la collecte de renseignements étrangers entre puissances étrangères et agents de puissances étrangères soupçonnés d'espionnage ou de terrorisme.

261 L'*Executive Order* 12333, du 4 décembre 1981, signé par le président Ronald Reagan ; il s'agit d'un décret intitulé *United States Intelligence Activities* visant à étendre les pouvoirs et les responsabilités des agences de renseignement américaines et à ordonner aux dirigeants des agences fédérales américaines de coopérer pleinement aux demandes d'information de la C.I.A.

262 *Ibid.*, §§ 180-185.

263 *Ibid.*, §§ 191 et 192.

264 *Executive Order 13768 of January 25, 2017 Enhancing Public Safety in the Interior of the United States*, disponible sur le site www.govinfo.gov/content/pkg/FR-2017-01-30/pdf/2017-02102.pdf, consulté en dernier lieu le 4 décembre 2021. Traduction libre de : « Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information ».

265 C.J.U.E., *Schrems* II, § 134.

et l'importateur des données doit l'assister au besoin. À défaut de pouvoir mettre en place des mesures supplémentaires suffisantes, l'exportateur des données personnelles doit suspendre le transfert.

En guise de conclusion, la Cour de justice a très vite donné le ton et montré la voie à suivre à sa grande sœur la Cour E.D.H. en distinguant la grille d'analyse à appliquer à la surveillance de masse de celle applicable à la surveillance ciblée. En outre, s'agissant plus spécifiquement de la surveillance de masse, les deux cours procèdent à un basculement progressif mais certain vers une protection autonome des données à caractère personnel au détriment du droit à la vie privée. Il s'ensuit une grille d'analyse, distincte, s'agissant notamment de l'examen de la proportionnalité et de stricte nécessité ou l'attention toujours plus soutenue de l'examen des garanties procédurales offert dans le cadre de la surveillance de masse.

Conclusion

Si la surveillance n'est pas un phénomène nouveau, son caractère « massif » apparaît plus soutenu par le développement récent des technologies de l'information et de la communication, et particulièrement d'Internet. Les risques pour les libertés fondamentales apportés par la surveillance de masse sont d'autant plus importants que la qualité des outils s'améliore de manière permanente et que les flux informationnels augmentent de manière exponentielle. À titre d'exemple, un article dans la presse spécialisée paru en février 2021 annonçait que « plus de 1,5 milliard de smartphones devraient s'écouler cette année si l'on en croit les analyses et prédictions du cabinet d'études et d'analyses des marchés Gartner. Cela représenterait une hausse de 11,4 % par rapport à 2020 et le plus gros des ventes se réaliserait en Asie, en Europe de l'Ouest et en Amérique Latine »[266]. Or, 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.

C'est, en somme, ce raisonnement qui, partant du droit à la vie privée et eu égard aux risques nouveaux créés par l'évolution technologique et notamment ceux induits par la surveillance massive, a œuvré à la reconnaissance du droit à la protection des données comme une liberté fondamentale *in se*. Ainsi, la Charte a élevé en liberté la protection des données à caractère personnel via son article 8. Cela entraîne, par ailleurs, la création ou la confirmation de droits subjectifs tels que le droit à l'information, le droit d'accès et le droit à ne pas être soumis à une décision automatisée.

266 A. Siméon, « Marché du smartphone : une hausse de 12 % des ventes en 2021 et un bond de 250 % des appareils 5G », *01net*, 4 février 2021, disponible sur le site www.01net.com/actualites/marche-du-smartphone-une-hausse-de-12percent-des-ventes-en-2021-et-un-bond-de-250percent-des-appareils-5g-2033082.html, consulté en dernier lieu le 4 décembre 2021.

La protection des données à caractère personnel et sa consécration distincte du droit au respect de la vie privée et familiale s'inscrivent dans la considération que « l'informatique est l'un des domaines les plus importants de l'évolution scientifique et technique du XX^e siècle affectant ainsi la liste des droits fondamentaux »[267]. Définitivement rangé au titre de droits-créance et consacré par l'article 8 de la Charte, le droit à la protection des données finit par faire de l'ombre à sa grande sœur, la protection de la vie privée, en imposant de nouvelles obligations et offrant de nouveaux droits subjectifs aux individus.

Il faut néanmoins rester prudent et ne pas succomber à la tentation de l'efflorescence de nouveaux droits de l'homme liés à l'évolution des technologies de l'information et de la communication, particulièrement s'agissant de la protection de la vie privée, au risque d'un affaiblissement du caractère fondamental de ce droit[268], car lorsque « tout devient fondamental, rien ne l'est plus vraiment »[269].

Si la surveillance de masse peut s'avérer intéressante pour rencontrer certaines situations mettant en péril la sécurité nationale ou la santé publique, il ne faut cependant pas oublier que ces mesures doivent, de manière incontournable, répondre à certaines conditions telles que la nécessité tant au niveau de l'ingérence elle-même qu'à celui des données qui sont effectivement traitées. L'ingérence ne peut pas non plus se satisfaire de lois adoptées sans respecter le débat parlementaire nécessaire à mette en balance les intérêts en présence.

Les cours de justice européennes, que ce soit de l'Union européenne ou du Conseil de l'Europe, établissent des garde-fous mais encore faut-il que les États les acceptent, ce qui n'est pas encore garanti au regard de certains États membres qui préfèrent le populisme aux libertés fondamentales.

267 O. Dord, « Droits fondamentaux », *in Dictionnaire des droits de l'homme*, Paris, P.U.F., 2008, p. 265.

268 À l'instar de la formulation utilisée par Sandrine Turgis, nous parlerons de « droits-gigognes », puisqu'« il est possible de relever que se dessine en la matière un phénomène qui pourrait être qualifié de "droits-gigognes" puisque sur le fondement d'un droit fondamental sont identifiées plusieurs composantes qui peuvent elles-mêmes englober d'autres éléments. La déclinaison pourrait sembler infinie. De plus, dans l'hypothèse dans laquelle l'une de ces composantes serait elle-même qualifiée de droit de l'homme, elle pourrait prendre son autonomie et donner naissance à une nouvelle lignée de droits-gigognes » (S. Turgis, « Chapitre 3 – Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ? », *in* C. de Terwangne et Q. Van Enis (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1re éd., Bruxelles, Bruylant, 2019, p. 116).

269 Y. Poullet, « Quelques réflexions d'avant-propos » *in* C. de Terwangne et Q. Van Enis (dir.), *ibid.*, p. 11.