“Mieux protéger les personnes dans un contexte de flux international de données :

La nécessité d’une supervision démocratique et effective des services de renseignement”

Déclaration conjointe
par
Alessandra Pierucci, Présidente du Comité de la Convention 108
et
Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l’Europe

Strasbourg, 7 septembre 2020

Des années après que les révélations de Snowden ont mis en lumière l'ampleur de la surveillance de masse exercée par les autorités publiques, la numérisation de nos sociétés s'est poursuivie à un rythme rapide, accélérée notamment par la crise sanitaire actuelle qui a obligé nombre d'entre nous à travailler, à apprendre et à se socialiser à distance.

Des données personnelles sont générées par chacune de nos frappes sur un clavier, chaque mouvement effectué sous le regard des caméras et des smartphones, tout message envoyé ou toute photo prise. Comme nos vies deviennent de plus en plus numériques et que les services en ligne s'entremêlent à l'échelle internationale, nos données personnelles traversent les frontières, nationales ou régionales, et notre protection efficace devient difficile à assurer.

La vie privée et la protection des données sont des droits fondamentaux. Ils sont essentiels au bon fonctionnement des sociétés démocratiques et le sont devenus encore plus à l'ère numérique.

Le droit à la vie privée est universellement reconnu par l'article 12 de la Déclaration universelle des droits de l'homme et par l'article 17 du Pacte international relatif aux droits civils et politiques. Au niveau régional, le Conseil de l'Europe a récemment célébré le 70ème anniversaire de la Convention européenne des droits de l'homme, avec ses garanties à l'article 8 sur le droit au respect de la vie privée. Plus récemment, l'Union européenne (UE) a inclus le respect de la vie privée et la protection des données dans sa Charte des droits fondamentaux.

Ces droits ne peuvent être compromis : ils ne peuvent être légalement limités que dans des conditions spécifiques et strictes, comme cela peut être le cas par exemple, lorsqu'il existe des menaces à la sécurité nationale ou, comme plus récemment, pour notre santé.

Ces restrictions de nos droits fondamentaux à la vie privée et à la protection des données sont étroitement circonscrites et un nombre de garanties doivent être observées pour que de telles interférences soient autorisées et que l'essence des droits et libertés fondamentales soit respecté.

La Cour de justice de l'Union européenne a récemment rappelé l'importance cruciale, au niveau international, de garanties appropriées, de droits opposables et de voies de recours effectives lorsque des données à caractère personnel sont traitées à des fins de sécurité publique, de défense et de sûreté de l'État.

Dans son arrêt "Schrems II[1]" du 16 juillet 2020, la Cour a réaffirmé que les données à caractère personnel transférées en dehors de l'UE doivent bénéficier d'un niveau de protection essentiellement équivalent à celui garanti au sein de l'UE par le Règlement général sur la protection des données (RGPD), lu à la lumière de la Charte des droits fondamentaux.

La Cour a conclu que tel n'était pas le cas dans le cadre de l'accord du "*Privacy Shield*" conclu entre l'UE et le gouvernement des États-Unis d'Amérique[2], car les limitations de la protection des données à caractère personnel transférées à partir de l'UE - découlant de la législation interne des États-Unis sur l'accès et l'utilisation de ces données par les autorités publiques et les services chargés de l'application de la loi américains - n'étaient pas « encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire »[3].

Les implications de cette décision vont au-delà des transferts de données entre l'UE et les États-Unis ; elle soulève des questions plus larges sur les transferts internationaux, offrant ainsi une nouvelle occasion de renforcer le cadre universel de la protection des données et de répondre à la nécessité d'un instrument juridique mondial sur les services de renseignement.

[1] *Commissaire à la protection des données c. Facebook Irlande et Maximilian Schrems* (Cas C-311/18, « Schrems II »)
[2] Décision 2016/1250 sur l'adéquation de la protection offerte par le « Privacy Shield » UE/USA, invalidé le 16 juillet 2020.
[3] Communiqué de presse de la CJUE 91/20 du 16 juillet 2020.

Un enjeu mondial

Au lendemain de la décision Schrems II, certaines voix influentes ont appelé à la conclusion d'un accord international juridiquement contraignant pour la protection de la vie privée et des données personnelles.

Cet instrument existe déjà : il s'agit de la Convention 108+.

La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (plus connue sous le nom de "Convention 108")[4] est le seul instrument multilatéral juridiquement contraignant sur la protection de la vie privée et des données à caractère personnel ouvert à tous les pays du monde.

La Convention 108 a été ouverte à la signature en 1981 et a depuis lors influencé diverses lois internationales, régionales (comme par exemple l'UE) et nationales sur la protection de la vie privée. Elle compte actuellement 55 États parties[5] et son comité compte plus de 25 observateurs, formant un forum mondial de plus de 70 pays des six continents qui travaillent ensemble sur la protection des données.

La Convention 108 a récemment été modernisée afin que cet instrument historique soit adapté aux nouvelles réalités d'un monde de plus en plus connecté et de renforcer sa mise en œuvre effective. Le protocole[6] modifiant la Convention 108 a été ouvert à la signature le 10 octobre 2018 à Strasbourg et a depuis été signé et ratifié par de nombreux pays[7].

Une fois entré en vigueur, le protocole d'amendement permettra d'atteindre deux objectifs essentiels : faciliter les flux de données et respecter les droits de l'homme et les libertés fondamentales, y compris la dignité et l'intégrité humaines à l'ère numérique.

[4] Texte de l'instrument de 1981 disponible à : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108
[5] Liste complète des parties disponible à : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=64GsTZPR
[6] Protocole d'amendement, STCE No. 223, disponible à : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223
[7] A ce jour : 36 signatures et 6 ratifications, Liste complète disponible à : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223/signatures.

La Convention 108+ (Convention 108 modifiée par le protocole) est appelée à devenir la norme internationale en matière de protection de la vie privée et des données à l'ère numérique ; c'est un outil durable pour faciliter les transferts internationaux de données tout en garantissant un niveau approprié de protection des personnes à l'échelle mondiale.

C'est aux décideurs politiques et aux gouvernements du monde entier qu'il revient aujourd'hui de décider de saisir le potentiel de cette convention.

Le rapporteur spécial des Nations Unies sur le droit à la vie privée, le professeur Joseph A. Cannataci, a déjà recommandé à deux reprises "à tous les États membres des Nations unies d'adhérer à la Convention 108+[8]".

Outre son caractère mondial, deux autres caractéristiques importantes de la Convention 108+ sont particulièrement pertinentes dans les réflexions qui ont suivi la décision Schrems II et ses implications au niveau international.

Premièrement, dans le contexte des transferts de données à partir de l'UE et de la nécessité d'assurer effectivement un niveau de protection adéquat essentiellement équivalent à celui qui est assuré au sein de l'Union, il importe de rappeler que le considérant 105 du RGPD fait explicitement référence à la Convention dans le cadre du régime d'adéquation. Pour décider du niveau de protection des données d'un pays souhaitant obtenir une décision d'adéquation, il convient de tenir compte de son éventuelle adhésion à la Convention. La pertinence de la Convention dans le contexte d'une évaluation du caractère adéquat est donc expressément reconnue par le RGPD. Le fait d'être Partie à la Convention pourrait également faciliter à l'avenir l'évaluation au cas par cas que les entreprises sont tenues de faire dans le cadre de clauses contractuelles types[9] du niveau de protection essentiellement équivalent à garantir.

Deuxièmement, en ce qui concerne la question spécifique du traitement des données personnelles à des fins de sécurité et de défense nationales, la Convention 108+ contient, dans son article 11, un solide système de vérifications et de contrepoids qui complète son champ d'application entièrement horizontal défini par son article (article 3 de la Convention)[10].

[8] Rapport annuel 2018 sur le Droit à la vie privée à l'Assemblée générale des Nations Unies (Rapport A/73/45712) et Rapport annuel du 1 mars 2019 au Conseil des Droits de l'Homme des Nations Unies (Rapport A/HRC/40/63).
[9] Voir le paragraphe 134 de la décision Schrems II.
[10] La Convention s'applique à tous les traitements de données personnelles dans les secteurs public et privé, y compris aux services de sécurité et de renseignement.

Les droits prévus par la Convention ne peuvent être limités que lorsque cela est prescrit par la loi et que la restriction constitue une mesure nécessaire et proportionnée dans une société démocratique sur la base de motifs précis et limités, y compris la sécurité et la défense nationales.

Le paragraphe 3 de l'article 11 traite spécifiquement des activités de traitement à des fins de sécurité et de défense nationales, et stipule clairement que ces activités de traitement doivent faire l'objet d'un examen et d'un contrôle indépendants et efficaces.

Si la Convention 108+ fournit un cadre juridique international solide pour la protection des données à caractère personnel, elle ne répond pas pleinement ni explicitement à certains des défis posés par les capacités de surveillance sans précédent dans notre ère numérique. Depuis des années, les appels[11] en faveur d'un instrument juridique international exhaustif en matière de droits de l'homme pour encadrer les opérations des services de renseignement se sont intensifiés, et la nécessité de garanties solides au niveau international qui complètent et précisent celles offertes par la Convention 108+ ne peut plus être ignorée.

Une base solide pour les réflexions futures

Depuis plus de 60 ans, la Cour européenne des droits de l'homme a, par son abondante jurisprudence, développé d'importantes garanties pour la protection du droit à la vie privée consacré par l'article 8 de la Convention européenne des droits de l'homme, y compris dans un certain nombre d'affaires clés concernant la surveillance à grande échelle des communications[12] par les services de renseignement. L'article 13 sur le droit à un recours effectif est une autre protection clé pour l'individu.

[11] Voir notamment :
- la Déclaration de 2013 du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux : https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016805c801b
- la Résolution 2045 (2015) sur les opérations de surveillance massive de l'Assemblée parlementaire du Conseil de l'Europe (APCE) appelant à un « code du renseignement» multilatéral : http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=21692&lang=en
- le Rapport 2016 au Conseil des Droits de l'Homme des Nations Unies du Rapporteur spécial des Nations Unies sur la vie privée, Joseph A. Cannataci : https://undocs.org/en/A/HRC/31/64
- le Rapport 2014 à l'Assemblée Générale des Nations Unies du Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Ben Emmerson : https://daccess-ods.un.org/TMP/5945256.35242462.html

[12] Voir Fiche thématique sur la surveillance de masse : https://www.echr.coe.int/Documents/FS_Mass_surveillance_FRA.pdf et le rapport de recherche sur la jurisprudence en matière de sécurité nationale : https://rm.coe.int/16806ae199

Afin de déterminer si des ingérences dans le droit à la vie privée ou à la correspondance sont nécessaires dans une société démocratique, et si un juste équilibre est trouvé entre les différents intérêts en jeu, la Cour examine si l'ingérence est conforme à la loi, poursuit un but légitime, est nécessaire et proportionnée au but poursuivi. Elle a ainsi élaboré des garanties et des conditions précises que les services de renseignement doivent respecter.

L'augmentation exponentielle des échanges commerciaux et d'informations que l'on observe à l'ère numérique exige que des garanties plus solides soient assurées pour les données personnelles, où qu'elles circulent et où qu'elles aboutissent. Il est aujourd'hui plus que jamais nécessaire d'aborder la question complexe et sensible du contrôle démocratique et efficace des services de renseignement au niveau international.

La décision Schrems II touche à deux exigences spécifiques : la nécessité de voies de recours (c'est-à-dire des droits de recours individuels effectifs et opposables, devant un tribunal indépendant et impartial[13]) et, en ce qui concerne l'ampleur de certains programmes de surveillance, l'absence de limitations à l'accès aux données personnelles par des autorités de l'État, ce qui viole le principe de stricte nécessité et de proportionnalité des restrictions au droit au respect de la vie privée[14].

La Cour de justice de l'UE a conclu que « le droit de ce pays tiers ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa réglementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences.[15]» comme elle l'avait déjà fait dans sa première décision "Schrems I[16]" invalidant le précédent accord UE-USA "safe harbour".

Au niveau des Nations Unies, les États membres ont rappelé dans la Résolution 68/167 sur le droit à la vie privée à l'ère numérique[17] que « la surveillance illicite ou arbitraire ou l'interception des communications, ainsi que la collecte illicite ou arbitraire de données personnelles, qui sont des actes extrêmement envahissants, portent atteinte aux droits à la vie privée et à la liberté d'expression et pourraient aller à l'encontre des principes de toute société démocratique », et ont appelé tous les pays à « créer des conditions qui permettent de les prévenir, notamment en veillant à ce que

[13] Voir paragraphe 191 et suiv. de la décision Schrems II
[14] Voir paragraphes 179, 180, 183 à 185 de la décision Schrems II
[15] Voir paragraphe 168 de la décision Schrems II
[16] *Maximillian Schrems c. Data Protection Commissioner* (Cas C-362/14, "Schrems I").
[17] Résolution disponible à : https://undocs.org/fr/A/RES/68/167

la législation nationale applicable soit conforme aux obligations que leur impose le droit international des droits de l'homme ».

Créer de telles conditions implique aujourd'hui que les pays s'entendent au niveau international sur la mesure dans laquelle la surveillance effectuée par les services de renseignement peut être autorisée, dans quelles conditions et avec quelles garanties, ainsi que sur un contrôle indépendant et effectif[18].

La jurisprudence de la Cour européenne des droits de l'homme a établi que pour être autorisée, l'ingérence dans les droits des personnes doit remplir un certain nombre de conditions ; elle doit notamment être fondée sur le droit (ce qui signifie que les circonstances et les conditions doivent être définies par des dispositions légales et que les implications doivent être prévisibles pour les personnes) et doit être proportionnée et nécessaire dans une société démocratique. Les personnes concernées doivent avoir accès à des recours effectifs :

> *« que compte tenu du risque qu'un système de surveillance secrète destiné à protéger la sécurité nationale sape, voire détruise, la démocratie sous couvert de la défendre, elle doit vérifier qu'existent des garanties adéquates et suffisantes contre les abus (Klass et autres, 1978, §§ 49-50), et que cette appréciation dépend de toutes les circonstances de la cause, par exemple de la nature, de l'étendue et de la durée des mesures possibles, des raisons requises pour les ordonner, des autorités compétentes pour les permettre, les exécuter et les contrôler, et du type de recours fourni par le droit interne »[19].*

Le temps est venu d'utiliser les nombreux critères élaborés par les tribunaux, y compris la Cour suprême des États-Unis, pour définir ce qui constitue les garanties adéquates et efficaces, une responsabilité effective et un contrôle indépendant des services de renseignement[20], et trouver un consensus au niveau mondial sur cette question cruciale.

[18] Voir le Document thématique "La surveillance démocratique et effective des services de sécurité nationale » publié par le Commissaire aux droits de l'Homme du Conseil de l'Europe : https://rm.coe.int/ref/CommDH/IssuePaper(2015)2

[19] *Big Brother Watch et autres c. Royaume Uni*, 13/09/2018, §18.

[20] Voir aussi les recherches publiées par l'Agence pour les droits fondamentaux de l'Union européenne (FRA) sur 'Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne – Volumes I et II "

Un forum idéalement placé

Le Statut du Conseil de l'Europe offre le champ d'action matériel et territorial nécessaire à cet important travail.

Il lui permet de travailler sur des questions mondiales et avec la participation de toutes les régions du monde (comme c'est déjà le cas avec la Convention 108+ ou encore la Convention de Budapest sur la lutte contre la cybercriminalité qui compte 65 États Parties[21]). Le Conseil de l'Europe peut aussi traiter des questions de sécurité et de défense nationales qui sont en dehors de la juridiction de l'Union européenne[22].

Un travail important a déjà été effectué en matière de lutte contre le terrorisme. Il ne sera pas difficile de réunir sous un même toit des experts en sécurité nationale et des experts en protection des données, comme cela a déjà été fait avec les experts en protection des données et ceux chargés de l'application de la loi, dans le cadre des travaux du comité sur la cybercriminalité.

Le moment est crucial pour les pays du monde entier. Ils doivent définir la voie à suivre pour les 70 prochaines années de protection des droits de l'homme. Reconnaissant l'importance essentielle de la protection des données et l'importance des transferts transfrontaliers de données dans l'environnement numérique actuel, ils devraient adhérer à la Convention 108+ et saisir le potentiel unique qu'offre le Conseil de l'Europe et la chance qui leur est donnée de traiter de la question du fonctionnement des services de renseignement sous l'égide d'une organisation des droits de l'homme universellement respectée.

Alessandra Pierucci et Jean-Philippe Walter

[21] Liste complète disponible à https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=g9DW3Zr4

[22] Article 4.2 du Traité de l'Union européenne