Protection des données personnelles et cyber(in)sécurité

Marilia Maciel-Hibbard

Dans **Politique étrangère 2018/2 Été** , pages 55 à 66
Éditions **Institut français des relations internationales**

ISSN 0032-342X
ISBN 9782365678155
DOI 10.3917/pe.182.0055
Date de mise en ligne : 08/06/2018

Protection des données personnelles et cyber(in)sécurité

Par **Marilia Maciel-Hibbard**

Marilia Maciel-Hibbard est chercheur en chef en politique numérique à DiploFoundation, et doctorante en sciences de l'information et de la communication à l'université de Bordeaux-Montaigne.

À mesure que s'interconnectent humains et objets, la protection de la vie privée recule. Les entreprises du Net vivent de l'exploitation des données individuelles de masse. Les États s'affranchissent des règles usuelles pour collecter les données afin de lutter contre le terrorisme et la délinquance. Les dispositifs légaux ne garantissent pas l'équilibre entre sécurité et protection des individus. La justice sera appelée dans l'avenir à jouer un rôle accru au service de cette dernière.

politique étrangère

Certains des enjeux éthiques et politiques les plus graves auxquels nous avons aujourd'hui à faire face sont directement liés à l'essor des nouvelles technologies. La généralisation de l'usage de l'ordinateur a lancé le processus vertigineux de la numérisation. De plus, internet a connecté infrastructures critiques, appareils personnels, appareils portables ainsi qu'un nombre toujours croissant d'objets quotidiens, permettant ainsi l'échange entre eux d'informations stockées numériquement.

Cette connectivité généralisée conduit vers une ère de l'omniprésence de l'informatique, où les technologies les plus significatives sont celles qui se font oublier et pénètrent notre quotidien jusqu'à s'y confondre[1]. Même si les utilisateurs sont de moins en moins conscients de la présence de ces technologies, la production d'une empreinte numérique détaillée découle indirectement des activités en ligne. Cette traîne de données personnelles commence pratiquement avant notre conception et demeure après la mort[2].

Les données sont devenues de plus en plus essentielles. Elles forment la base de technologies émergentes, comme l'intelligence artificielle.

1. M. Weiser, « The Computer for the 21st Century », *Scientific American*, septembre 1991, p. 94-104.
2. G. Fletcher *et al*., « A Day in the Digital Life: A Preliminary Sousveillance Study », 7 septembre 2011, disponible sur : <https://papers.ssrn.com>.

Les entreprises du Net font également un usage poussé des données pour améliorer leur lien avec les utilisateurs grâce à des services personnalisés, et pour permettre à d'autres entreprises de toucher avec leurs produits des publics particuliers[3]. Les données sont essentielles à l'essor d'entreprises comme Google ou Facebook, leurs revenus dépendant fortement de la publicité basée sur celles-ci. Le nouveau modèle commercial d'internet ne fait pas payer ses services aux utilisateurs, mais produit ses recettes par la vente d'informations les concernant à des publicitaires.

Ces données sont également de plus en plus volatiles. Elles peuvent être violées, transférées, copiées ou corrompues de manière furtive, ce qui pose problème quant aux piliers de la sécurité informationnelle que sont la confidentialité, l'intégrité et la disponibilité. Problème lié : comment contrôler la sécurité des données personnelles, les protéger contre une destruction accidentelle ou non autorisée, contre la perte, l'accès non autorisé, la modification ou la dissémination ? Dans le contexte numérique, les objectifs de sécurité de l'information coïncident avec ceux de la sécurité des données personnelles. Ce constat a conduit ces deux domaines à interagir, et à produire ensemble des outils comme les méthodologies d'évaluation des risques, ou des mesures de sécurité qui devraient être adoptées par ceux qui traitent et contrôlent les données.

Dans certains domaines, l'antagonisme entre sécurité et vie privée est de plus en plus clair : en matière de prévention de la cybercriminalité, de sécurité nationale et pour la collecte de renseignements. Le coût grandissant de la cybercriminalité pour l'économie, les exemples d'infiltration potentiellement invalidante d'infrastructures critiques par des hackers, les cyberattaques d'ampleur mondiale, et l'usage supposé d'internet pour préparer des attentats : tous ces risques plaident pour la collecte et l'analyse de données afin de prévenir ou de punir les comportements nuisibles. Les données nécessaires incluant notamment les données personnelles, les conditions d'un conflit entre garanties de sécurité et protection de la vie privée sont aujourd'hui établies.

La quantité de données sur les individus dont disposent aujourd'hui entreprises privées et gouvernements est sans précédent. Dans ce contexte, il n'est pas rare d'entendre dire que « la vie privée est chose du passé[4] »,

3. C. Liem *et al*., « The Economic Value of Personal Data for Online Platforms, Firms and Consumers », Bruegel, 14 janvier 2016, disponible sur : <http://bruegel.org>.
4. P. Cashmore, *Privacy Is Dead, and Social Media Hold the Smoking Gun*, CNN, 28 octobre 2009, disponible sur : <http://edition.cnn.com>.

ou que « la surveillance est le modèle commercial d'internet[5] ». La limite entre "vie en ligne" et "vie hors ligne" tend à s'estomper, et dans ce jeu des données figurent désormais également des données biométriques et génétiques.

Les entreprises collectent les données en échange de services et de produits, et les gouvernements les collectent pour les besoins de l'administration publique et au prétexte d'accroître la sécurité. On voit émerger des visions des plus critiques du pouvoir écrasant que la collecte de données donne aux géants d'internet, et des problèmes qu'il génère en termes de vie privée et de concurrence. Trop peu d'efforts ont été encore faits pour empêcher une collecte excessive de données de la part des autorités publiques, en particulier lorsqu'elle est justifiée en termes sécuritaires.

Les tendances en matière de sécurité, et leur impact sur la vie privée

Les années 1980 et 1990 ont connu quelques tentatives de rénover les cadres juridiques de la protection de la vie privée et des données en liaison avec la société de l'information naissante. Le Congrès américain a, par exemple, mis à jour sa loi sur la surveillance électronique en 1986, dans l'ordonnance *Electronic Communications Privacy Act* (ECPA), qui visait à assurer la protection des e-mails, fichiers conservés sur ordinateur et enregistrements de communications. En 1995, l'Union européenne (UE) a adopté la Directive sur la protection des données 95/46/CE[6], avec pour objectif de protéger les données personnelles tout en garantissant le flux des données entre les États membres.

Les cadres juridiques en matière de protection des données se sont étoffés au fil des ans, mais parallèlement s'est développée une législation considérable facilitant les enquêtes et la collecte de renseignements – cette dernière concernant particulièrement les communications sur internet –, renforçant le pouvoir exercé jusque-là de fait par les organismes gouvernementaux. L'équilibre sécurité/vie privée s'est donc dégradé en faveur de la première. Cette évolution a été grandement influencée par la mondialisation du terrorisme et l'entrée du cyberespace dans les problématiques de sécurité.

Les attentats du 11 septembre 2001 ont représenté un tournant, et leur impact sur l'opinion a été décisif. En 2002, les Américains se divisaient

5. F. Rashid, « Surveillance Is the Business Model of the Internet: Bruce Schneier », *Blog Schneier on Security*, 9 avril 2014, disponible sur : <www.schneier.com>.
6. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995. Journal officiel, n° L 281/31 du 23 novembre 1995.

sur la surveillance par le gouvernement de leurs activités en ligne : 45 % des sondés y étaient favorables, 47 % défavorables. Al-Qaïda a exécuté ses plans en grande partie grâce à une préparation méticuleuse en matière de collecte de renseignements et de contre-espionnage, notamment par l'usage des communications électroniques[7], d'où l'adoption du *Patriot Act* de 2001, qui a largement étendu les pouvoirs d'enquête et de surveillance des autorités. Certaines voix influentes ont alors affirmé : « Les événements du 11 septembre 2001 ont révélé que le danger terroriste qui plane sur les États-Unis est plus important que la plupart des gens ne le pensaient jusque-là […]. Il est raisonnable qu'une telle révélation conduise à la limitation de nos libertés civiles[8]. »

On a en conséquence assisté à un renversement de la vision idéaliste et majoritairement positive qui sous-tendait la Déclaration d'indépendance du cyberespace de 1996[9], qui mettait en question l'étendue des souverainetés et l'application de leurs règles dans le cyberespace. Moins d'une décennie plus tard, internet n'était plus vu comme un espace de liberté sans précédent, mais comme le lieu de menaces jusqu'alors inconnues. Combinées à la prolifération des activités criminelles en ligne, certaines opérations de grande ampleur sur internet ont dès lors fait la une dans le monde entier : attaques contre des sites internet publics et privés en Estonie en 2007 ; cyberattaques pendant le conflit Géorgie-Russie en 2008 ; introduction en 2009 du virus informatique Stuxnet dans les centrifugeuses iraniennes destinées à l'enrichissement de l'uranium. Ces événements ont eu pour effet de redéfinir la sémantique cybersécuritaire : de nouvelles expressions sont apparues, comme « cyberarme » ou « cybersiège » ; d'autre part, les stratégies de défense nationale ont introduit le cyberespace comme cinquième champ d'affrontement, le considérant comme un « nouveau théâtre d'opérations[10] » se nourissant des discours des acteurs clés, gouvernementaux et non-gouvernementaux.

Un processus de « sécuritisation[11] » du cyberespace s'est ainsi ouvert, se nourrissant des discours des acteurs concernés, gouvernementaux, avec ses conséquences sur les choix politiques. Des thèmes traditionnels du champ politique classique ont rejoint celui de la sécurité, redéfinis au

7. J. I. Gaetano, « The 9/11 Attacks – A Study of Al Qaeda's Use of Intelligence and Counterintelligence », *Studies in Conflict & Terrorism*, vol. 32, n° 3, 2009, p. 171-187, disponible sur : <www.tandfonline.com>.
8. R. A. Posner et D. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven, Yale University Press, 2011.
9. J. P. Barlow, « A Declaration on the Independence of Cyberspace », Electronic Frontier Foundation, 1996, disponible sur : <www.eff.org>.
10. *The National Defense Strategy of the United States of America,* département de la Défense, 2005, disponible sur : <www.au.af.mil>.
11. B. Buzan *et al.*, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner Publishers, 1998.

nom d'une menace existentielle. Cela amène des conséquences profondes : si l'on redéfinit un enjeu comme sécuritaire, des mesures extraordinaires peuvent être envisagées pour réduire la menace. On aboutit de fait à un « état d'exception » où les règles normales sont librement interprétées, ou ignorées. Plus un événement social relève de la « sécurité », plus les réactions gouvernementales pour le contrôler peuvent être extrêmes, exceptionnelles.

La perception selon laquelle les sociétés contemporaines font l'expérience d'un État de crise permanent alimente l'obsession sécuritaire, bouleversant l'équilibre entre vie privée et sécurité. La prolifération des attentats terroristes contribue à renforcer cette vision des choses : en 2016, deux pays sur trois ont subi un attentat terroriste ; en 2017, 77 pays (pour la plupart en développement) ont subi des attentats mortels – contre 65 l'année précédente[12]. En temps de crise, la balance entre sécurité et vie privée penche traditionnellement vers la première ; par temps calme, elle se redresse en faveur de la liberté. Mais des niveaux d'alerte constamment élevés – comme l'état d'urgence français, qui a perduré pendant près de deux ans après les attentats de 2015 à Paris, restreignent ce va-et-vient.

En France : état d'urgence et loi antiterroriste

Un moment exceptionnel de remise en question de la pertinence des mesures sécuritaires au regard de la vie privée est intervenu après la révélation d'Edward Snowden en 2013. Cet ancien employé de la National Security Agency (NSA) a révélé que cette agence pratiquait une surveillance de masse des communications numériques. L'étendue et l'intensité de cette surveillance ont provoqué de très larges réactions dans le monde[13]. Le *Patriot Act* de 2001 fut remplacé par le *Freedom Act* de 2015 ; les Nations unies adoptèrent des résolutions sur le droit à « la vie privée à l'ère numérique[14] » ; et des commissions spéciales commencèrent à enquêter sur ces allégations de surveillance de masse. La balance devait néanmoins de nouveau pencher vers la sécurité après chaque nouvelle attaque terroriste, les Parlements nationaux adoptant une succession de mesures en faveur d'un renforcement de la sécurité.

12. Institute for Economics & Peace, *Global Terrorism Index,* 2017, disponible sur : <http://globalterrorismindex.org>.
13. M. Maciel *et al*., *NoC Internet Governance Case Studies Series: The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial)*, 2015, disponible sur : <https://ssrn.com>.
14. Voir surtout Assemblée générale des Nations unies, « The Right to Privacy in the Digital Age », A/RES/68/167, 2013, et Assemblée générale des Nations unies, « The Right to Privacy in the Digital Age », A/C.3/71/L.39/Rev.1, 2016.

Les plus grands États européens, Allemagne, France, Royaume-Uni, ont adopté des lois renforçant leurs capacités de surveillance et de renseignement. La loi britannique *Investigatory Powers Act* votée en 2016 en est un exemple. Elle donne, entre autres, de nouveaux pouvoirs aux services de renseignement et aux organes de maintien de l'ordre en matière de mandats pour l'interception de masse, l'acquisition de masse et l'interférence de masse avec divers équipements. Pris ensemble, ces trois types de mandats autorisent les services de renseignement britanniques à collecter en masse des métadonnées étrangères, à intercepter les communications en masse, et à pirater en masse les réseaux et systèmes informatiques du monde entier. Ces lois sont examinées par la Cour européenne des droits de l'homme.

En Allemagne, la loi *Communications Intelligence Gathering Act* de 2016 a renforcé les pouvoirs du Service fédéral de renseignement (BND). Ce dernier a désormais le droit de rassembler et d'analyser toutes les informations, y compris toutes les données personnelles, qui lui sont nécessaires pour identifier des « mots-clés pertinents » ou des « réseaux de télécommunications pertinents » à surveiller. Certains des plus grands *Internet eXchange Points* (IXP) se trouvent en Allemagne, *hub* central pour une grande partie du trafic internet mondial. Une fois identifiés les mots-clés et réseaux de télécommunications pertinents, le BND peut donc collecter le contenu des communications qui transitent par eux.

Deux semaines après les attentats de novembre 2015 à Paris, la France a adopté sa loi sur les communications électroniques internationales. Elle donne le pouvoir à la Direction générale de la sécurité extérieure (DGSE) d'intercepter, collecter et surveiller les communications envoyées à l'étranger ou reçues de l'étranger, sans se plier à des principes clés visant à prévenir l'interférence abusive dans la vie privée, comme la proportionnalité ou la nécessité. En 2016, le Conseil constitutionnel français a censuré certaines parties de cette loi, ce manque de supervision étant susceptible de conduire à une violation de la vie privée[15].

En 2017, le président Emmanuel Macron a décidé la levée de l'état d'urgence en échange de l'adoption d'une loi antiterroriste[16] qui a transformé certaines dispositions du contrôle d'exception en loi ordinaire. Cette loi permet en particulier aux services de renseignement de surveiller les communications par téléphone et par e-mail ; elle prolonge également

15. Décision n° 2016-590 QPC du 21 octobre 2016.
16. Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, JORF n° 0255 du 31 octobre 2017.

jusqu'en 2020 leur droit à surveiller les communications sans fil entre téléphones portables et antennes-relais. Les personnes suspectes seront contraintes de fournir leurs identifiants et mots de passe internet. Dans la pratique, cette nouvelle loi pérennise l'état d'urgence : Gérard Collomb, ministre de l'Intérieur, n'a-t-il pas déclaré devant le Parlement : « Nous sommes toujours en état de guerre[17] » ?

Les programmes gouvernementaux de collecte d'informations sont problématiques même lorsque celles-ci ne sont pas transférées à une tierce partie. Ils ne respectent généralement pas les procédures habituelles et sont mis en place à l'insu des personnes concernées. Qui plus est, en rassemblant des données éparses d'apparence anodine, le gouvernement peut obtenir des profils et avoir accès à des informations que les personnes souhaitent garder secrètes : état de santé, opinions politiques ou orientation sexuelle… Un tel profilage pourrait renforcer les préjugés ou les discriminations à l'encontre de certains citoyens. En Chine, le gouvernement crée des bases de données sur les individus avec le soutien du secteur privé. Il pourrait les utiliser à l'avenir pour déterminer le degré de fiabilité de chacun, et peser fortement sur divers aspects de la vie sociale, comme l'accès au crédit[18].

Le rôle des décisions de justice

Les cours de justice ont grandement contribué à établir que la relation vie privée/sécurité ne devait pas déboucher sur une opposition entre droit collectif de la société et droit des individus. La vie privée doit être perçue comme une valeur sociale. La société accorde une place à l'individu parce que cette place bénéficie à la société, y compris en termes de démocratie et d'exercice de la liberté d'expression.

Cette opposition injustifiée entre vie privée et sécurité est renforcée par l'usage généralisé du mot « équilibre ». Tenter d'équilibrer deux éléments ne signifie pas nécessairement trouver un équilibre, mais signifie en tous cas qu'ils sont pris dans un mouvement de balance où l'un se trouve en haut tandis que l'autre se trouve en bas. Toutes les mesures sécuritaires ne font pas intrusion dans la vie privée. Il est donc important aujourd'hui de convaincre les pouvoirs publics d'examiner attentivement l'ensemble des mesures potentielles qui pourraient être employées pour collecter les informations dont ils ont besoin, en privilégiant celles qui n'entrent pas en conflit avec le droit à la vie privée.

17. France Inter, le 2 octobre 2017.
18. « Big Data Meets Big Brother as China Moves to Rate its Citizens », *Wired*, 21 octobre 2017, disponible sur : <www.wired.co.uk>.

L'exigence de la protection de la vie privée aboutit rarement à l'annulation des mesures sécuritaires. Ces dernières sont presque toujours maintenues, même si elles font l'objet d'une supervision, parfois de limitations. La question n'est pas de savoir si la surveillance des communications en ligne peut être effectuée par des autorités compétentes, mais de déterminer comment on pourrait la mettre en œuvre conformément aux principes de nécessité, de proportionnalité et de respect des procédures.

Certains tribunaux ont largement participé à l'émergence de doctrines permettant de faire coïncider lois et politiques avec la protection des droits fondamentaux – et en particulier la Cour de justice de l'Union européenne (CJUE).

Le rôle de la CJUE

En 2014, une Directive de l'UE sur la conservation des données[19], adoptée après les attentats de Madrid (2004) et de Londres (2005) a été suspendue par la CJUE. Elle visait à harmoniser les dispositifs législatifs des États membres, et exigeait la conservation des données collectées lors d'échanges sur téléphones fixes ou portables, ainsi que sur internet et par e-mail, et ce pour une période de six mois à deux ans. La Cour européenne a considéré que cette Directive était contraire au principe de proportionnalité, et ne s'accompagnait pas d'assez de garde-fous pour assurer la protection des données conservées contre un risque d'usage abusif ou d'accès et d'usage illégaux[20].

La CJUE a également eu à évaluer des lois nationales. Lors de son examen de la loi britannique *Investigatory Powers Act*, elle a affirmé son incompatibilité avec le droit européen, la loi ne prévoyant pas une autorisation indépendante pour les demandes d'accession aux données conservées. La conservation des données était elle-même jugée excessive, l'accès aux données et leur rétention ne se limitant pas aux cas de crimes graves[21].

En 2015, la CJUE a invalidé l'accord « Sphère de sécurité » sur le transfert de données, passé entre l'UE et les États-Unis. Ce jugement était

19. Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105/54, 2006.

20. Affaires jointes C-293 et C-594/12, Digital Rights Ireland Ltd. contre le ministère des Communications, de l'Action pour le climat et de l'Environnement, le ministère de la Justice et de l'Égalité, le Commissaire de la Garda Siiochana, Irlande, le Procureur général, et Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl *et al*., jugement du 8 avril 2014, ECR I-238, 2014.

21. Affaires jointes C-203/15 Tele2 Sverige AB contre l'administration suédoise des Postes et télécommunications et C-698/15 le secrétaire d'État à l'Intérieur contre Tom Watson *et al*.

l'aboutissement d'une bataille juridique lancée en 2013 par Maximillian Schrems, citoyen autrichien qui avait porté plainte contre l'autorité de protection des données irlandaise, après que celle-ci ait rejeté sa plainte contre le stockage des données utilisateurs effectué par Facebook aux États-Unis[22]. Selon le plaignant, et en dépit de l'existence de l'accord « Sphère de sécurité », les données n'étaient pas suffisamment protégées, comme cela a d'ailleurs été démontré par les révélations récentes sur les agissements de la NSA.

Après cette affaire, l'UE est apparue clairement tiraillée entre son intérêt à garantir le libre échange de données à des fins de développement économique, et l'impératif d'éviter une érosion des droits à la vie privée des citoyens européens lors du passage des données dans plusieurs espaces juridiques au-delà des frontières européennes. La réforme des règlements européens en matière de protection des données tente de résoudre ce dilemme.

Le RGPD et sa cousine méconnue la Directive européenne pour la protection des données dans les secteurs police et justice

La réforme des règles européennes en matière de protection des données, publiée en mai 2016, est entrée en application en mai 2018. Elle comprend le Règlement européen sur la protection des données (RGPD) et la Directive pour la protection des données dans les secteurs police et justice. Le RGPD vient remplacer la Directive européenne sur la protection des données de 1995. La réforme est destinée à moderniser et à harmoniser la protection des données à travers l'UE, élément essentiel de la stratégie pour un marché unique numérique.

Le RGPD est applicable à toute entité de contrôle et de traitement de l'information établie dans l'UE, ou offrant des biens ou services aux citoyens de l'UE, ce qui signifie qu'elle pourrait être appliquée en dehors de l'Union. Plusieurs entreprises basées aux États-Unis ont, par exemple, tenté d'aligner leurs pratiques commerciales sur le RGPD avant son entrée en application, au regard de la gamme de moyens à disposition des Européens pour faire respecter ces nouvelles règles – parmi lesquels sanctions et amendes.

Le nouveau règlement européen a aussi ouvert la discussion sur les règles concernant la vie privée en vigueur aux États-Unis. D'aucuns

22. C-362/14, Maximillian Schrems contre le Commissaire à la protection des données, jugement du 6 octobre 2015, ECLI: EU:C:2015:650.

soutiennent que les États-Unis devraient s'inspirer du RGPD, et pointent du doigt les défauts d'un système de lois disparates, et de leur foi en l'autorégulation, qui permet aux géants d'internet de poursuivre leurs intérêts financiers sans prendre suffisamment en considération les questions relatives à la vie privée. Cette opinion a été confortée par les révélations sur la société Cambridge Analytica, qui utilise des données politiques à des fins de communication, et a obtenu les données de 87 millions d'utilisateurs de Facebook, établi 30 millions de profils de personnalité, et vendu ces données à des personnalités politiques cherchant à influencer les électeurs aux États-Unis, le tout sans consentement des usagers.

L'affaire Cambridge Analytica

Cet épisode Cambridge Analytica est le plus récent d'une série qui a contribué à faire évoluer les mentalités vis-à-vis des plates-formes internet. Autrefois perçues comme permettant le développement de la liberté d'expression et des mouvements pro-démocratie, elles apparaissent désormais comme des brasseurs de désinformation et de *fake news*, des géants monopolistiques étouffant les compétiteurs naissants, des maîtres de l'évasion fiscale, et des entreprises respectant fort peu le droit à la vie privée de leurs clients.

Il est donc compréhensible que l'on s'intéresse à la manière dont les grandes entreprises d'internet vont s'adapter au RGPD. Mais cette focalisation sur les omissions et agissements répréhensibles des plates-formes internet a détourné l'attention des enjeux liés à la protection même de la vie privée, cet oubli profitant aux services de renseignement et autres organismes de maintien de l'ordre, friands de données. Le RGPD exclut et exempte certaines activités de son périmètre d'action : par exemple les activités des autorités nationales ayant pour but la prévention, l'investigation, la détection ou la poursuite d'infractions pénales, ou l'accomplissement des fonctions judiciaires (art.2(2)).

Le RGPD ne concerne donc pas le traitement des données par les forces de police ni les tribunaux, qui devront se conformer à une autre Directive européenne pour la protection des données dans les secteurs de la police et de la justice[23]. Celle-ci prend en compte les besoins et caractéristiques spécifiques du traitement des données personnelles par la police et la justice

23. Directive (UE) 2016/680 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.

pénale, et permet une certaine flexibilité dans le traitement des données lié à la sécurité. Le principe de limitation des finalités, par exemple, ne sera pas ici toujours strictement appliqué, les informations collectées sur une affaire particulière pouvant avoir un intérêt inattendu pour la résolution d'autres affaires.

La Directive promeut l'harmonisation de pratiques de traitement des données – particulièrement diverses et contradictoires dans l'UE, car liées à l'histoire et à la culture de chaque État membre. Toutes les autorités ayant partie liée à la sécurité dans l'UE devront introduire les mesures prévues par la Directive dans leur traitement habituel des données personnelles. À noter : cette directive ne s'applique pas au traitement de données personnelles « dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union » (et tout particulièrement la sécurité nationale), ni au traitement « par les institutions, organes et organismes de l'Union ». Cette dernière exemption signifie que la Directive ne concerne aucun des organismes, institutions et bases de données européens travaillant sur les questions de sécurité, comme Europol, Eurojust, ou les systèmes d'information Schengen et des douanes, qui continueront vraisemblablement à appliquer leur politique *ad hoc* habituelle de protection des données.

***

À mesure que se propage l'informatique, immergeant les humains dans un écosystème d'interconnexion entre personnes et objets, les enjeux concernant la vie privée se multiplient. Le volume de données sur les individus dont disposent les entreprises privées et les gouvernements est sans précédent. Alors que l'opinion publique et les autorités gouvernementales commencent à avoir une vision critique de la puissance écrasante que la collecte de données donne aux entreprises numériques, les efforts pour restreindre la collecte excessive de données par les autorités gouvernementales demeurent insuffisants, surtout quand la sécurité leur sert de prétexte.

La « sécuritisation » du cyberespace permet l'application de mesures exceptionnelles, visant à réduire des menaces comme le terrorisme. Des niveaux d'alerte toujours plus soutenus conduisent à l'adoption par les Parlements nationaux d'une succession de réglementations visant à accroître la sécurité. L'Allemagne, la France et le Royaume-Uni, entre autres, ont adopté des lois renforçant leurs capacités de surveillance et de collecte de renseignement. En dépit de certaines avancées, le nouveau Règlement européen sur la protection des données ne s'attaque pas au

problème de la collecte de données à des fins de sécurité, et consolide par là l'approche compartimentée qui oppose sécurité et protection des données et de la vie privée.

Les cours de justice ont un rôle important à jouer pour redéfinir la relation entre vie privée et sécurité. La CJUE a déjà prononcé des jugements historiques sur ces questions. On peut prédire que, dans leur recherche de protection, organisations et usagers d'internet auront demain de plus en plus souvent tendance à faire appel à la justice. Les décisions judiciaires auront donc dans les années à venir une influence grandissante sur l'interaction entre sécurité et vie privée.

PE

Mots clés
Internet
Cyberespace
Vie privée
Union européenne