Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Centre suisse de compétence pour les droits humains (CSDH)
Centro svizzero di competenza per i diritti umani (CSDU)
Swiss Centre of Expertise in Human Rights (SCHR)

Newsletter CSDH No 24 du 23 avril 2014
Domaine thématique Droits humains et économie

Le droit à la sphère privée à l'ère numérique

Internet et les réseaux sociaux: un défi pour le respect de la vie privée et la protection des données

de Christine Kaufmann et Giulia Reimann

(Traduction de l'allemand)

Pertinence pratique

- Ces dix à vingt dernières années, l'environnement numérique s'est développé de manière fulgurante, conservant régulièrement un temps d'avance sur la protection des données.
- Le traitement des données personnelles constitue toujours une atteinte à la sphère privée. Afin d'assurer la protection de la sphère privée, il convient de créer des réglementations suffisantes qui justifient ces atteintes. Les droits en vigueur hors ligne sont aussi protégés en ligne.
- Les craintes croissantes d'attentats terroristes poussent les États à renforcer la surveillance numérique des données personnelles.
- Des efforts sont menés aussi bien au niveau national qu'au niveau international afin de trouver un équilibre entre la protection de la sphère privée et la protection de la sécurité publique.
- Bien que l'obligation de protection incombe en premier lieu à l'État, les entreprises peuvent elles aussi fournir une contribution importante à la protection de la sphère privée.

L'environnement internet

Les droits humains s'appliquent dans le monde virtuel et numérique aussi bien que dans la vie réelle. Le droit à la sphère privée (art. 13 Cst., art. 8 CEDH, art. 17 Pacte II de l'ONU, art. 12 DUDH) ou la liberté d'opinion et d'information (art. 16 Cst, art. 10 CEDH, art. 19 Pacte II de l'ONU, art. 19 DUDH) sont d'ailleurs particulièrement concernés par les technologies numériques. Grâce aux récents développements informatiques, il nous est aujourd'hui possible de communiquer plus facilement, plus rapidement et plus fréquemment qu'auparavant. Les possibi-

lités d'acquisition et d'échange d'informations sur les sujets les plus variés sont quasi sans limites, ce qui peut avoir un impact positif sur la participation au processus démocratique.

Toutefois, les progrès technologiques peuvent également représenter une menace pour le droit à la sphère privée et le droit à l'autodétermination informationnelle. Facebook, qui enregistre des données personnelles, en est un parfait exemple. Le réseau social utilise en effet les données qu'il stocke afin de placer de la publicité ciblée sur le compte de ses utilisateurs. La diffusion par Google Street View d'images de personnes non totalement anonymisées ou les révélations du lanceur d'alerte Edward Snowden sont d'autres exemples des dérives des progrès technologiques.

Big Data

Grâce aux plus récentes technologies, il est aujourd'hui possible de collecter d'immenses quantités de données, de les enregistrer et de les rendre accessibles. On entend par big data (données massives ou datamasse) la collecte massive et l'analyse systématique de données. Le préposé fédéral à la protection des données et à la transparence (PFPDT) définit les données massives au travers de quatre caractéristiques principales: de grosses quantités de données (volume) traitées à grande vitesse (velocity), la diversité des données (variety) et la plus-value (value) que l'analyse des données est censée produire. Le terme «data mining» est parfois utilisé pour désigner la simple recherche d'informations et donc la première étape des big data. Les big data offrent de toutes nouvelles possibilités à différents niveaux. Ils sont ainsi utiles aux sciences sociales et aux instituts de recherche de marché, qui peuvent observer et analyser le comportement des utilisateurs d'internet. En outre, les entreprises en ligne utilisent les big data afin d'optimiser leurs services. Dans le domaine de la sécurité publique, la lutte contre le terrorisme se fonde aujourd'hui essentiellement sur les données personnelles collectées sur internet. Selon le PFPDT, il existe cependant des tensions entre l'exploitation des big data et les principes de base de la protection des données.

Surveillance de masse et protection des données

En Suisse, c'est la loi fédérale sur la protection des données (LPD) qui régit toute opération relative aux données personnelles ; elle vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (art. 1 LPD). Selon l'art. 3 al. a LPD, il faut entendre par données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable. Il en va ainsi, selon le Tribunal fédéral, des adresses IP, à la condition que leurs détenteurs soient concrètement identifiables (ATF 136 II 508). Par ailleurs, certaines données personnelles sont considérées comme sensibles, telles que les opinions ou activités religieuses ou politiques, les données sur la santé ou la sphère intime ou les sanctions pénales. Certaines nouvelles applications ou certains nouveaux appareils qui enregistrent les données de santé personnelles directement sur le smartphone ou dans un cloud font actuellement l'objet de vifs débats quant à leur compatibilité avec la protection des données.

Il existe des tensions entre les big data et les principes de base de la loi fédérale sur la protection des données, notamment au niveau de l'assignation d'un but précis et de la retenue quant à la quantité de données collectées. La collecte de big data ne correspond pas à un traitement de don-

nées ciblé, mais à une surveillance massive automatisée au moyen d'algorithmes mathématiques. Selon le PFPDT, une telle collecte de masse ne garantit pas un anonymat suffisant, la combinaison de différentes données (anonymisées) rendant possible la génération de renseignements personnels. La plupart des utilisateurs d'internet ne sont pas conscients que leurs données peuvent être enregistrées et exploitées et ignorent également le but de la collecte de données. Or, cela pose problème en ce sens que la collecte de données personnelles demande en règle générale l'autorisation des individus concernés. Les conditions générales (CG) sont souvent extrêmement volumineuses et peu accessibles pour l'utilisateur. L'imprévisibilité des progrès technologiques représente par ailleurs une autre difficulté. Les données anonymes d'aujourd'hui seront peut-être facilement attribuables à une personne demain.

Outre le droit à la protection de la sphère privée, l'application d'autres droits humains est menacée par la collecte de données personnelles, notamment la liberté d'opinion et d'information. La crainte que ses données personnelles soient surveillées peut pousser un individu à renoncer à utiliser certains services. Si ce renoncement devient la seule option, faute de services alternatifs sûrs, cela peut entraîner une limitation de la liberté d'opinion et d'information. Les standards minimaux internationaux en matière de protection des données visent ainsi tout particulièrement à empêcher de telles limitations ou du moins à les réduire.

Efforts internationaux

Au mois de décembre 2013, l'Assemblée générale de l'ONU est arrivée à la conclusion que, en raison du caractère mondial et ouvert d'internet, des progrès rapides dans le domaine des technologies de l'information et des communications, la sphère privée ainsi que la liberté d'expression de tout un chacun étaient de plus en plus menacées (A/RES/68/167). Depuis, l'Assemblée générale soutient la position selon laquelle les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne. Elle a ainsi prié le Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) de rédiger un rapport sur la protection et la promotion du droit à la vie privée à l'ère numérique, qui lui a été présenté le 30 juin 2014 (A/HRC/27/37). Dans son rapport, le HCDH arrive à la conclusion que les instruments internationaux des droits humains forment un cadre clair permettant de garantir le droit à la vie privée. Il cite ainsi l'art. 12 de la Déclaration universelle des droits de l'homme et l'art. 17 du Pacte international relatif aux droits civils et politiques, en vertu desquels nul ne peut être l'objet d'immixtions arbitraires ou illégales dans sa vie privée. Ce même droit est d'ailleurs ancré à l'art. 8 de la Convention européenne des droits de l'homme et à l'art. 13 de la Constitution fédérale suisse. Selon le HCDH, une protection appropriée de la vie privée à l'ère du numérique et son ancrage dans la législation représentent un défi de taille pour la communauté internationale et l'ensemble des États. C'est pourquoi le Conseil des droits de l'homme de l'ONU a décidé fin mars 2015 de nommer un Rapporteur sur le droit à la vie privée (voir communiqué du 26.03.2015).

Il convient également de mentionner au niveau international les Principes directeurs de l'OCDE à l'intention des entreprises multinationales. Ceux-ci abordent la protection de la vie privée dans le chapitre portant sur les intérêts des consommateurs. Les entreprises sont ainsi priées de «respecter la vie privée des consommateurs et de prendre des mesures raisonnables pour assurer la sécurité des données à caractère personnel qu'elles collectent, conservent, traitent ou diffusent». En cas de violation de cette disposition par une entreprise, les personnes lésées peuvent

s'adresser au Point de contact national. Chaque État membre de l'OCDE ou chaque État ayant accepté ces principes directeurs est en effet tenu de mettre sur pied un tel Point de contact. Celui-ci peut alors proposer des procédures de médiation et de conciliation et émettre des recommandations en fonction de la situation (voir article du CSDH du 01.02.2012).

Développements en Europe

Dans l'UE, des standards minimaux en matière de droit à la protection des données ainsi qu'un droit à l'effacement des données ont été instaurés lors de l'introduction en 1995 de la directive relative à la protection des données à caractère personnel (95/46/CE). Une révision complète de la réglementation en matière de protection des données au sein de l'UE fait actuellement l'objet de discussions sur la base de deux récentes propositions: un nouveau règlement relatif à la protection des données (COM(2012) 11 final) et une nouvelle directive relative à la protection des données dans le cadre de poursuites pénales (COM(2102) 10 final). Cette révision doit notamment assurer aux citoyennes et citoyens le contrôle de leurs données, tout particulièrement sur internet. Afin de prendre en compte les derniers développements technologiques, la directive relative à la protection de la vie privée (2002/58/CE) a été complétée, en 2009 déjà, par la directive sur les cookies (2009/136/CE). Les cookies enregistrent par exemple les noms d'utilisateurs, les mots de passe et certaines préférences, ce qui peut s'avérer utile pour l'utilisateur. Toutefois, les cookies permettent aussi d'analyser le comportement de navigation des internautes et ainsi de définir des profils d'utilisateurs. La directive sur les cookies a permis d'introduire le principe du consentement préalable de l'internaute. La personne doit ainsi donner son accord à l'enregistrement de données par les cookies et en être dûment informée au préalable.

Dans le cadre d'un renvoi préjudiciel, la Cour de justice de l'Union européenne (CJUE) a invalidé la directive 2006/24/CE sur la conservation des données. La directive donnait aux autorités étatiques le droit, sous certaines conditions, de stocker en vue d'une possible utilisation ultérieure des données générées et traitées lors de la mise à disposition de services de communication électroniques accessibles publiquement ou de réseaux de communication publics. La Cour de justice a ainsi estimé que la directive était formulée de manière trop imprécise compte tenu de l'importance de la violation de la vie privée. En outre, elle a souligné que le niveau de protection garanti par les opérateurs et exploitants privés n'était pas suffisant, la directive leur permettant de tenir compte des aspects économiques et notamment du coût de l'application de mesures de sécurité. Enfin, elle a rappelé que la suppression définitive des données au terme du délai d'enregistrement n'était pas garanti (Arrêt C-293/12 du 8 avril 2014).

Un mois plus tard, la CJUE a établi dans l'affaire Google un «droit à l'oubli» sur la base de la réglementation en matière de protection des données de l'UE. Le droit à l'oubli veut qu'une personne ait dans certaines circonstances le droit d'obtenir l'effacement d'informations personnelles des résultats de recherche d'un moteur de recherche. Ces circonstances sont réunies quand la liste des résultats ne répond plus aux finalités visées du traitement des données par l'exploitant du moteur de recherche, quand elle est excessive par rapport à ces finalités ou qu'elle n'est plus nécessaire. Dans le cas concret, le plaignant voulait empêcher qu'une recherche Google de son nom fasse apparaître dans la liste des résultats des articles de journaux portant sur une vente aux enchères immobilière vieille de seize ans et liée à une saisie pratiquée en recouvrement de dettes de sécurité sociale. La Cour de justice a estimé que, dans ce cas, l'intérêt du plaignant au respect

de sa sphère privée était supérieur aux intérêts économiques de Google et qu'il n'existait pas un intérêt prépondérant du public à avoir accès à l'information en question. Contrairement à ce qui est souvent – à tord – relaté, l'exploitant du moteur de recherche ne doit pas dans ce genre de cas supprimer les données personnelles quand cela est demandé par la personne concernée, mais simplement supprimer les liens correspondants de la liste de résultats (Arrêt C-131/12 du 13 mai 2014). A la suite de cet arrêt, le groupe de travail sur la protection des données de l'UE – organe responsable de la surveillance du droit de l'UE en matière de protection des données – a adopté des critères à l'intention des délégué-e-s nationaux/nationales à la protection des données, qui définissent de manière concrète les conditions d'application du «droit à l'oubli» (14 EN/WP 225 du 26 novembre 2014).

L'instrument central de la protection des données du Conseil de l'Europe est, outre la protection de la sphère privée garantie par la CEDH, la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1985 (Convention de protection des données). La Convention a pour l'heure été ratifiée par 45 États membres sur 47. En Suisse, elle est entrée en vigueur en 1998. La Convention n'étant pas adaptée aux derniers développements technologiques en matière de traitement des données, elle fera prochainement l'objet d'une révision. Ainsi, le droit à la protection des données au sens d'un droit fondamental irrévocable et les mécanismes de mise en œuvre et d'application de la Convention seront renforcés.

Obligations légales des États en matière de protection des données

Les États sont non seulement tenus de respecter les droits humains et d'assurer leur mise en œuvre, mais ils ont aussi l'obligation de protéger les individus contre toute éventuelle violation des droits humains causée par des tiers. Dans le domaine de la protection des données, cette obligation de protection incombe aux États quand des entreprises privées collectent des données personnelles à des fins personnelles et, par là même, violent la sphère privée des utilisateurs. Les États doivent donc adopter des mesures ciblées afin d'empêcher et de sanctionner ce type de violations. Il peut ainsi s'agir de l'adoption de nouvelles législations (lois sur la protection des données), de la mise à disposition de mécanismes de plainte, de poursuites pénales, etc. Cette obligation de protection étatique contre les violations des droits humains commises par des entreprises privées est définie concrètement par les Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme. Les États ne sont certes pas directement responsables des violations commises par des tiers. Toutefois, en l'absence de mesures ciblées pour empêcher ces violations, d'enquêtes et d'investigation sur ces violations ou de voies de recours pour les victimes, ils ne respectent pas leur obligation de protéger les droits humains.

La Cour européenne des droits de l'homme (CrEDH) reconnaît certaines obligations étatiques en matière de protection des droits humains, par exemple dans le cadre de l'art. 8 CEDH, qui établit le droit au respect de la vie privée et familiale (p. ex. arrêt Aksu contre la Turquie du 15 mars 2012, § 59). L'art. 8 contient également l'intégrité et la confidentialité de la correspondance personnelle, ce qui signifie par exemple que la surveillance de la communication numérique représente une violation de la sphère privée et qu'elle doit être suffisamment justifiée. Dans l'affaire Copland contre le Royaume-Uni du 3 avril 2007, la CrEDH a reconnu la violation de l'art. 8 CEDH, un établissement public de formation ayant fait surveiller les communications téléphoniques, les courriers électroniques ainsi que la connexion à internet d'une employée afin de dé-

terminer si elle faisait un usage excessif des ressources de l'établissement durant les heures de travail à des fins personnelles. La CrEDH n'avait jusqu'alors jamais été confrontée à une affaire dans laquelle il était reproché à un État de ne pas avoir assumé son obligation de prendre des mesures préventives contre un traitement illégal de données personnelles numériques par des tiers privés. En effet, les deux plaintes pendantes auprès de la CrEDH concernant les affaires de la NSA contre le Royaume-Uni et portant notamment sur une violation de l'art. 8 CEDH (N° 58170/13 Big Brother Watch et al. c. Royaume-Uni et N° 62322/14 Bureau of Investigative Journalism et Alice Ross c. Royaume-Uni) concernent des atteintes à la vie privée commises par l'État et non par des personnes particulières.

Les États ont certes l'obligation de veiller à l'application des droits humains et tout particulièrement à la protection des données. Toutefois, cette obligation peut entrer en conflit avec les propres intérêts de l'État en matière de traitement des données personnelles. Dans l'affaire NSA, 200'000 personnes à travers le monde ont fait l'objet d'une surveillance permanente entre 2007 et 2013, ce qui constitue une violation grave de leur sphère privée. Pour justifier ces violations, le Royaume-Uni et les États-Unis ont déclaré qu'elles étaient indispensables à la lutte contre le terrorisme et à la sécurité publique générale et qu'elles n'étaient donc pas disproportionnées. La CrEDH doit encore se prononcer sur cet argument.

La CrEDH n'est pas la seule instance à devoir traiter de l'obligation des États à protéger les individus contre les violations de la sphère privée par des entreprises privées. La CJUE se penche en effet actuellement sur une plainte déposée par un ressortissant autrichien contre les autorités irlandaises de protection des données, à qui il reproche de ne pas avoir empêché la transmission de données massives par Facebook aux autorités américaines, ce qui constituerait une violation des droits fondamentaux en matière de protection de la sphère privée et de la réglementation de l'UE en matière de protection des données. Selon le droit de l'UE, la transmission de données à des autorités étrangères est autorisée à condition qu'il existe des standards comparables à la réglementation de l'UE en matière de protection des données. La Commission européenne avait rendu en 1999 un arrêt sur les Principes de la sphère de sécurité concernant les États-Unis (2000/520/CE). Celui-ci établissait qu'il suffisait à une organisation ou à une entreprise établie aux États-Unis d'émettre une déclaration selon laquelle elle acceptait les dispositions de protection en vigueur dans l'UE pour remplir les conditions en matière de niveau de protection. La Cour de justice doit donc à présent décider si l'arrêt de la Commission présente un caractère contraignant pour la Cour irlandaise, en charge de la plainte déposée par le ressortissant autrichien contre le délégué à la protection des données, ou si la Cour irlandaise peut elle-même se prononcer sur le cas (C-362/14 Schrems c. Data Protection Commissioner).

L'obligation de protection des États pose la question des possibilités concrètes dont jouissent les États pour contrôler les entreprises privées d'internet. D'une part, le secteur privé jouit de la liberté de contracter ; d'autre part, les États doivent tout d'abord avoir connaissance d'éventuelles violations contre le règlement en matière de protection des données avant de pouvoir prendre des mesures correspondantes. En raison des évolutions constantes dans le domaine des technologies, assurer ce contrôle s'avère en outre de plus en plus difficile. Par ailleurs, la plupart des grandes entreprises d'internet, telles que Facebook, Google, Twitter, Dropbox, sont établies aux États-Unis et sont donc soumises aux dispositions américaines en matière de protection des données. Or, celles-ci offrent une protection plutôt faible par rapport aux réglementations des États euro-

péens. La législation américaine ne connaît par exemple pas de limitation dans le temps pour le stockage de données. Elle ne connaît pas non plus le droit à la rectification des données erronées ou le droit d'être informé-e des données personnelles enregistrées.

Responsabilité des entreprises

Les entreprises privées sont liées aux dispositions nationales en matière de protection des données du pays dans lequel elles sont établies ou dans lequel elles exercent leurs activités commerciales. Dans un contexte commercial mondialisé, il est souvent difficile de définir quelles dispositions doivent être appliquées. Le HCDH consacre d'ailleurs un chapitre entier de son rapport du 30 juin 2014 sur la vie privée à l'ère numérique au rôle des entreprises privées. Sont traitées dans ce chapitre les entreprises qui collectent et traitent des données personnelles ou les entreprises qui mettent à disposition des logiciels correspondants, par exemples les entreprises de télécommunication, les fournisseurs d'accès à internet ou les plateformes sociales.

Le rapport souligne que la protection de la sphère privée doit être assurée même en cas de délégation de responsabilités publiques, telle qu'observée dans le domaine de la sécurité publique avec la transmission de compétences judiciaires à des entreprises privées (§ 42). Les entreprises sont tenues de respecter la sphère privée et ce, indépendamment du fait que l'État s'acquitte ou non de ses propres obligations en matière de droits de l'homme (§ 43).

En outre, le HCDH se réfère explicitement aux Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme (voir les articles CSDH de la newsletter du 06.05.2011 et du 31.10.2012), qui établissent que les entreprises sont tenues de respecter les droits humains, de ne pas contribuer aux atteintes des droits humains et de veiller à les empêcher (Chapitre II A, 11). Le document accorde une place prépondérante à la diligence raisonnable des entreprises en matière de droits humains dans le domaine numérique (Chapitre II B, 17 ss. des principes). Toute atteinte potentielle contre le droit à la sphère privée et contre les autres droits humains commise dans le cadre des activités économiques d'une entreprise sur internet devrait être identifiée à l'avance et autant que faire se peut évitée ou du moins réduite.

Le HCDH souligne par ailleurs que, en cas de demandes d'accès aux données émanant d'autorités publiques, il est attendu des entreprises qu'elles s'efforcent d'honorer dans la plus grande mesure possible le droit à la sphère privée ainsi que les autres droits humains éventuellement concernés (§ 45). Il faudra pour cela interpréter les demandes de l'État aussi étroitement que possible et informer les personnes concernées, afin d'assurer une transparence suffisante et de permettre aux internautes de s'opposer à ces demandes si elles ou ils le souhaitent. Le rapport recommande aux entreprises d'instituer des mécanismes de réclamation pour les internautes (§ 46), qui leur permettent d'exiger la suppression de certaines données.

Ces recommandations adressées aux entreprises privées ne changent en rien le fait que l'obligation en matière de protection de la sphère privée et d'autres droits humains concernés par les développements numériques incombe en premier lieu aux États.

Situation en Suisse

La Suisse a élaboré différentes dispositions légales qui servent de base pour le traitement des données personnelles et prévoient des mesures correspondantes en cas de violation de la sphère privée. La loi fédérale sur la protection des données en fait partie. Selon l'art. 12 LPD, les personnes privées ont le droit de traiter des données personnelles, à condition de ne pas porter atteinte à la personnalité des personnes concernées. En cas de violation de la personnalité, la personne a la possibilité d'entamer une procédure civile analogue à celle garantie à l'art. 28 CC (protection de la personnalité). Le droit en vigueur permet donc d'intenter une action en justice contre les entreprises violant illégalement la sphère privée (voir ATF 138 II 346 Google Street view: le Tribunal fédéral a établi qu'il incombait à Google d'assurer sans frais l'anonymisation ultérieure des personnes reconnaissables sur Google Street View). Toutefois, en cas de violations de la personnalité ou de toute autre atteinte à la sphère privée commise par des entreprises privées établies à l'étranger, c'est-à-dire dans un pays qui dispose d'autres réglementations en matière de protection des données, apparaissent diverses difficultés.

En raison des rapides développements technologiques et sociaux à travers le monde, une révision rapide de la LPD s'impose. Le 1er avril 2015, le Conseil fédéral a chargé le Département fédéral de justice et police - DFJP d'élaborer un avant-projet d'adaptation de la réglementation suisse en matière de protection des données en tenant compte des réformes actuelles au sein de l'UE et du Conseil de l'Europe dans le domaine de la protection des données. L'objectif de la révision est multiple: une intervention plus en amont – et donc un renforcement – de la protection des données, une sensibilisation accrue des personnes concernées, l'amélioration de la transparence, le renforcement de la surveillance des données et de leur maîtrise et la protection des mineur-e-s (voir le rapport en allemand sur le groupe de travail révision LPD Bericht der Begleitgruppe Revision DSG). L'avant-projet devrait être présenté d'ici à la fin du mois d'août 2016.

C'est le Préposé fédéral à la protection des données et à la transparence (PFPDT) qui est responsable en Suisse de veiller au respect de la loi fédérale sur la protection des données. Il peut notamment établir les faits d'office ou à la demande de tiers et émettre des recommandations sur la base de ses constatations. Dans le secteur privé, le préposé agit avant tout en tant que conseil. En cas de conflits entre individus ou entre des personnes privées et l'État, il joue avant tout un rôle de médiateur.

Surveillance des télécommunications et service de renseignement

La loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) fait actuellement l'objet d'une révision totale et n'entrera pas en vigueur avant 2017. En lien avec la révision de la LSCPT, le Conseil national a donné son accord le 11 mars 2015 au développement et à l'exploitation du système de traitement de données relatif à la surveillance des télécommunications ainsi que des systèmes d'information de police de la Confédération (Bulletin officiel du Conseil national, session de printemps, neuvième séance). Cette révision doit permettre d'adapter la surveillance des télécommunications aux dernières évolutions technologiques et de faciliter le travail du service de Surveillance de la correspondance par poste et télécommunication (SCPT). En Suisse, le service SCPT est responsable de la surveillance de la correspondance par poste et télécommunication, dont fait partie internet. Le SCPT prend des mesures de

surveillance des télécommunications uniquement à la demande des autorités de poursuite pénale dans le cadre d'une procédure pénale. En dehors des procédures pénales, les télécommunications ne peuvent être surveillées qu'en cas de recherches de personnes disparues. C'est auprès des fournisseurs de services de télécommunication (FST), et donc essentiellement auprès d'entreprises privées, que le SCPT collecte les données nécessaires. En Suisse, toute personne souhaitant proposer un service de télécommunication doit en informer l'Office fédéral de la communication (OFCOM). La liste de l'OFCOM comprend environ 560 FST.

La révision totale de la LSCPT n'a pas pour objectif une augmentation quantitative de la surveillance des télécommunications, mais une amélioration qualitative. Le Conseil fédéral attend du Service SCPT qu'il porte une grande attention à la question de la protection des données, la surveillance touchant directement des données personnelles (voir le Message du Conseil fédéral). Du point de vue du Conseil fédéral, la révision de la LSCPT offre une base légale suffisante pour justifier les atteintes aux données personnelles.

L'extension de la conservation des données à titre préventif représente un point critique de la nouvelle LSCPT. Les fournisseurs de services de télécommunication sont désormais tenus de conserver durant douze mois (et non plus six) les données nécessaires à l'identification des internautes ainsi que les données de télécommunication et de facturation. Pour justifier cette mesure, le Conseil fédéral soutient que «l'ingérence dans les droits fondamentaux que constitue la conservation de données [personnelles] même en l'absence de soupçon est contrebalancée par des règles très strictes concernant aussi bien l'accès à ces données que l'utilisation qui peut en être faite, ainsi que par des voies de droit ouvertes aux personnes concernées». Le Conseil fédéral considère l'arrêt de la CJUE du 8 avril 2014 comme non pertinent concernant la Suisse.

La loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) et la loi fédérale sur le renseignement civil (LFRC) représentent d'autres bases légales pour le traitement de données personnelles. Elles permettent, à certaines conditions, au Service de renseignement de la Confédération (SRC) et à d'autres organes de sécurité de traiter des données personnelles. Il s'agit toutefois de traitements de données ciblés, toute information incorrecte ou non indispensable devant être effacée.

En lien avec la révision de la LSCPT et avec d'autres réformes d'ordre organisationnel au sein des services d'information et de sécurité, une loi unique sur le renseignement devrait à présent être promulguée (LRens), afin de remplacer la LMSI et la LFRC. La proposition de loi fait l'objet de vifs débats. La nouvelle loi accorderait en effet l'autorisation par exemple d'écouter les conversations téléphoniques, de surveiller les chatrooms ou d'infiltrer les systèmes informatiques. Toutefois, ces mesures ne peuvent être adoptées qu'à certaines finalités définies par la loi, à savoir la lutte contre le terrorisme, contre le commerce d'armes de destruction massive et contre l'espionnage. En outre, elles doivent au préalable être autorisées par le Tribunal administratif, par la Délégation pour la sécurité du Conseil fédéral et par le Chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Le Conseil national a adopté la loi sur le renseignement le 17 mars 2015 par 119 voix contre 65 et 5 abstentions. Le Conseil des États doit à présent se prononcer sur la loi. S'il ne procède à aucune modification, la loi sera probablement soumise à un référendum.

Conclusion pour la Suisse

En Suisse comme ailleurs, les développements technologiques ont entraîné une augmentation des risques pour la sphère privée et pour la protection des données. Les entreprises d'internet privées, qui traitent des données, sont certes tenues de respecter la réglementation nationale en matière de protection des données. Toutefois, à l'image des dispositions légales de la plupart des pays européens, la réglementation suisse reste à la traîne par rapport aux rapides évolutions de l'informatique et se voit de plus en plus confrontée à des défis juridiques.

La protection des données ne fait pas partie des thèmes abordés par les rapports nationaux de la Suisse adressés aux organes conventionnels de l'ONU ni des thèmes traités dans le cadre de l'examen périodique universel (EPU). Cela pourrait changer à l'avenir. En effet, si des efforts sont menés pour adapter le droit suisse – notamment la réglementation en matière de protection des données et de surveillance des télécommunications – aux évolutions de la technologie numérique, on ne connaît cependant pas encore leurs effets. Les révisions prévues de la LRens et de la LSCPT soulèvent de houleux débats juridiques et politiques. Certains craignent que ne soit créée une «mini-NSA» qui, invoquant les intérêts liés au maintien du secret, finisse par échapper à tout contrôle (voir notamment Votum Glättli, Bulletin officiel du Conseil national, session de printemps 2015, douzième séance).

Enfin, il convient de se demander comment la Suisse compte protéger les citoyennes et citoyens contre les violations de leur sphère privée commises par des entreprises d'internet étrangères, celles-ci étant soumises à d'autres dispositions en matière de protection des données. Seuls des standards internationaux pourront apporter une solution à ce problème. L'engagement de la Suisse dans les commissions de l'ONU et du Conseil de l'Europe qui s'occupent de cette thématique n'en est que plus essentiel.

Documentation

- Rapport de l'OHCHR „The right to privacy in the digital age"
- PFPDT: à propos de la Protection des données
- Fiche thématique de la CrEDH "Nouvelles technologies"
- Fiche thématique du OHCHR "Droits de l'homme, terrorisme et lutte antiterroriste"

Contact

- christine.kaufmann@menschenrechte.uzh.ch

Comment citer cet article

Christine Kaufmann, Giulia Reimann: Le droit à la sphère privée à l'ère numérique.
Newsletter CSDH No 24 du 23 avril 2015
http://www.skmr.ch/cms/upload/pdf/150423_Eco_privee_fr.pdf