Berne, le 5 avril 2018

Réponse de la Suisse au questionnaire du HCDH sur le droit à la vie privée à l'ère digitale, selon la résolution du Conseil des droits de l'homme 34/7

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

a) **«** Recent development in national and regional legislation » en lien avec la révision de la loi fédérale sur la protection des données (LPD).

i) Au plan fédéral[1]

La législation fédérale en matière de protection des données fait actuellement l'objet d'une révision d'envergure. Le 15 septembre 2017, le Conseil fédéral a adopté un projet de loi, ainsi qu'un rapport explicatif. Le projet de révision poursuit plusieurs objectifs, qui se complètent.

Il vise tout d'abord à adapter la législation suisse aux évolutions technologiques. Il introduit dans ce but différentes mesures visant notamment à renforcer les droits des personnes concernées, les obligations des responsables du traitement, et les pouvoirs du Préposé fédéral à la protection des données et à la transparence (PFPDT). Il vise également à maintenir et renforcer la compétitivité de la Suisse en créant un environnement propre à faciliter les flux transfrontières de données et à améliorer son attractivité pour de nouvelles activités en lien avec la société numérique.

Le projet doit ensuite permettre à la Suisse de rendre sa législation compatible avec le projet de modernisation de la convention du Conseil de l'Europe STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (P-STE 108), afin de pouvoir ratifier la convention modernisée le plus vite possible.

Le projet a enfin pour objectif d'intégrer dans la législation suisse certains développements du droit de l'Union européenne. Il s'agit tout d'abord de transposer la directive (UE) 2016/680, qui est un développement de l'acquis de Schengen que la Suisse s'est engagée à reprendre. Il s'agit ensuite de rapprocher la législation suisse du règlement (UE) 2016/679, afin de pouvoir continuer à bénéficier de la décision de la Commission européenne reconnaissant qu'elle offre un niveau de protection des données adéquat.

Le projet du Conseil fédéral contient une révision totale de la loi fédérale du 19 juin 1992 sur la protection des données[2] ([LPD] qui implique la révision d'environ 60 lois spéciales) ainsi que la révision partielle des lois spéciales applicables au domaine de la coopération policière et judiciaire instaurée par Schengen.

La révision est actuellement en phase de procédure parlementaire. En janvier dernier, la commission compétente[3] a décidé de scinder le projet du Conseil fédéral. Il s'agit de traiter en premier lieu

[1] Voir le message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017; FF 2017 6565, 6592s (https://www.admin.ch/opc/fr/federal-gazette/2017/6565.pdf).
[2] RS 235.1
[3] La commission des institutions politiques du Conseil national.

uniquement les modifications législatives nécessaires à la transposition de la directive 2016/680. Les autres modifications seront examinées dans un second temps. Le premier paquet de la révision devrait être traité au plénum du Conseil national cet été.

ii) Au plan cantonal

En Suisse, chaque canton a sa propre législation en matière de protection des données, qui régit le traitement de données par des organes cantonaux. La plupart ont des lois additionnelles spécifiques au traitement de données par les autorités de police. L'accord d'association de la Suisse à Schengen lie également les cantons. Les dispositions de la directive (UE) 2016/680 devront donc être transposées également par les cantons, si besoin est, conformément à la répartition constitutionnelle des compétences entre la Confédération et les cantons. Il en va de même du P-STE 108.

b) « Recent development in national and regional case law »

Il y a plusieurs arrêts de la Cour européenne des droits de l'homme (CourEDH) contre la Suisse qui concernent la protection des données personnelles.[4] Ces arrêts ne concernent pourtant pas l'ère du numérique. L'arrêt le plus récent est *Vukota-Bojic c. Suisse* du 18 octobre 2016 (req. n° 61838/10) qui concerne la surveillance en secret de la requérante par des détectives privés, engagés par un assureur, dans le cadre d'une procédure visant l'octroi des prestations au titre de l'assurance-accident obligatoire. La Cour a conclu que la surveillance n'avait pas été prévue par la loi et qu'il a eu violation de l'article 8 CEDH[5] (Droit au respect de la vie privée). Suite à l'arrêt de la CourEDH, la Caisse nationale suisse d'assurance en cas d'accidents (CNA ou Suva) a publié un communiqué de presse le 20 octobre 2016 dont il ressort qu'il renoncerait pour l'instant à l'engagement de détectives dans le cadre de la lutte contre la fraude à l'assurance.[6] De plus, le Tribunal fédéral a rendu deux arrêts de principe en été 2017 dont il ressort que la pertinence de l'arrêt rendu par la Cour ne se limite pas au domaine d'assurance-accident, mais vaut dans tous les domaines du droit (ATF 143 I 377 et 143 IV 387).[7] En date du 16 mars 2018, les deux chambres de l'Assemblée fédérale ont adopté une modification de la *loi fédérale sur la partie générale du droit des assurances sociales [LPGA] (Base légale pour la surveillance des assurés)*, dont l'article 43a (Observation) prévoit une base légale pour la surveillance des assurés.[8] La nouvelle loi est sujette au référendum.

Enfin, il convient de noter qu'en date du 2 mars 2018, le Tribunal fédéral a rendu un arrêt (1C_598/2016) concernant l'admissibilité de l'enregistrement et de la conservation de données secondaires de télécommunications[9]. Dans cet arrêt, le Tribunal fédéral a examiné la conservation de données à la lumière de l'article 8 CEDH et de la jurisprudence de la CourEDH.

L'article 13 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst., Rs. 101)

---

4 Voir pour des exemples plus anciens *Khelili c. Suisse* du 18 octobre 2011, req. n° 16188/07 (classement comme « prostituée » dans la base des données de police de Genève) ; *Amann c. Suisse* du 16 février 2000, Grande Chambre, req. n° 27798/95, Recueil des arrêts et décisions 2000-II (interception d'un appel téléphonique ; établissement et conservation d'une fiche) ; *Kopp c. Suisse* du 25 mars 1998, req. n° 23224/94 (mise sur écoute de lignes téléphoniques d'un cabinet d'avocats).

5 Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH ; RS 0.101)

6 https://www.suva.ch/fr-ch/la-suva/news-et-medias/medias#uxlibrary-open=/fr-CH?atomid=8478c1f1630b49f19f3fed6d06408735%26showContainer=1

7 ATF 143 I 377 et ATF 143 IV 387

8 Objet 16.0479

9 1C_598/2016

garantit expressément la protection de la sphère privée.

La loi fédérale sur la protection des données du 19 juin 1992 (LPD, RS 235.1) régit le traitement de données concernant des personnes physiques et morales effectué par des personnes privées et des organes fédéraux (Art. 2, al.1). Cette loi de première génération est actuellement en cours de révision car elle est dépassée par les évolutions technologiques et sociétales. Le Conseil fédéral a présenté un projet de loi le 15 septembre 2017 qui vise à renforcer la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs données. Il vise en outre à assurer le maintien de l'équivalence du niveau de protection entre la Suisse et l'UE. Le 11 janvier 2018, la Commission des institutions politiques du Conseil national (CIP-N) est entrée en matière sur la révision totale de la LPD et a décidé de scinder la révision en deux étapes.

La nouvelle loi fédérale sur le renseignement (LRens, RS 121[10]) est entrée en vigueur le 1er septembre 2017 de même que les trois ordonnances qui y sont liées.

2. Surveillance and communications interception:

a) Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

Le 1er septembre 2017 a marqué l'entrée en vigueur de la nouvelle loi fédérale sur le renseignement (LRens) qui prévoit des conditions très claires, limitatives et respectueuses des droits humains en ce qui concerne la surveillance technique de personnes aux fins de renseignement (cf. articles 26 et suivants LRens). Une telle surveillance des moyens de communications de personnes privées ou d'organisations ne peut intervenir qu'en cas de menace concrète et sérieuse pour la sécurité du fait du terrorisme, de l'espionnage prohibé, de la prolifération ou d'attaques contre les infrastructures critiques, et que lorsque les autres moyens moins intrusifs ne permettent pas de parvenir aux résultats nécessaires pour la défense de la sécurité du pays. Le système d'autorisation par une autorité judiciaire et une autorité politique contribue également à garantir la protection du droit à la sphère privée.

Dans le domaine du renseignement, des lois et ordonnances réglementent précisément la recherche, le traitement et la communication des données. Le respect des dispositions de ces lois est entre autre contrôlée par le Préposé fédéral à la protection des données et à la transparence (PFPDT).

b) Role of business enterprises in contributing to, or facilitating government surveillance activities, including:

i) Sale of surveillance technology by business enterprises and ensuing responsibilities;

L'exportation de la technologie de surveillance par une personne physique ou morale dont le domicile ou le siège se trouve sur le territoire douanier suisse est soumise à la législation fédérale sur le contrôle des biens. Plus spécifiquement, l'exportation et le courtage de tels biens (marchandises, technologies et logiciels), ainsi que le transfert de biens immatériels (p.ex. savoir-faire, droits) y afférents sont réglementés par l'Ordonnance sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles en combinaison avec la Loi fédérale et l'Ordonnance sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques.

Des entreprises ou individus qui souhaitent exporter de la technologie de surveillance sont par conséquent tenus par la loi de respecter les obligations suivantes et, le cas échéant, d'assumer la

[10] RS 121

responsabilité pénale (peine privative de liberté ou peine pécuniaire) pour des infractions:

- **Obligation d'obtenir un permis d'exportation** du Secrétariat d'Etat à l'économie (SECO).
- **Obligation de renseigner** le SECO et de lui fournier tous les documents nécessaires à l'appréciation globale d'un cas ou à un contrôle, notamment un descriptif d'entreprise, la confirmation de commande, le contrat de vente, la facture, et surtout une déclaration de destination finale.
- **Obligation d'assurer un contrôle interne** fiable du respect des prescriptions en matière de contrôle à l'exportation. Le contrôle interne inclut, entre autres, la classification des biens soumis au contrôle à l'exportation ainsi que la vérification de l'identité du client et de la destination finale. Dans le sens d'un devoir de diligence, les entreprises sont amenées à signaler d'éventuels doutes (p.ex. identité du client pas claire, réponses évasives, mode de paiement/expédition inhabituels, demande d'une discrétion exagérée etc.) au SECO.

Rôle des entreprises dans la contribution ou la facilitation d'activités de surveillance gouvernementale et responsabilités

La technologie fournie par les entreprises peut contribuer et faciliter la surveillance de la part des gouvernements, y compris celle utilisée en masse par les consommateurs. Par exemple, les utilisateurs de téléphones portables acceptent plus ou moins volontairement que leur localisation physique puisse être tracée. Cette information permet un profilage sur les habitudes des consommateurs, leurs relations, leurs modes de consommation, qui peut être vendu à d'autres entreprises et peut facilement être racheté par des gouvernements.

Les entreprises ont une responsabilité, sous les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, pour les impacts en matières de droits de l'homme des actions de tiers en lien avec leurs opérations, produits ou services, même si elles n'ont pas contribué directement à ces impacts.

Les entreprises doivent exercer un minimum de diligence raisonnable par rapport à la commercialisation de ces données, tout comme par rapport à la vente de technologie et à l'utilisation qui peut en être faite par des régimes répressifs. Ceci est surtout valable en ce qui concerne l'accès à des données personnels ou la vente de logiciels de surveillance utilisés par des gouvernements pour réprimer les activités légitimes de défenseurs des droits de l'homme. Le risque d'abus de la part de gouvernements est réel dans des Etats répressifs mais aussi dans ceux où toutes les sauvegardes propres à un état de droit ne sont pas assurées. Les entreprises qui fournissent ces données et/ou technologies sont tenues de prévenir l'utilisation abusive de celles-ci. Si elles exercent la diligence raisonnable appropriée elles devraient être en mesure de rompre la relation d'affaires ou la prestation des services en question par la mise en œuvre de clauses contractuelles pertinentes.

Les entreprises devraient analyser et mettre en place des procédures permettant d'identifier comment éviter que les données ou les technologies puissent être abusées pour violer les droits de l'homme.

Cette diligence raisonnable peut être exercée en adoptant les précautions suivantes dans une perspective de prévention :

- s'assurer que le client n'ait pas d'antécédents de violations des droits de l'homme ou d'exploitation abusive des données
- identifier quelle est l'utilisation que le client entend faire des données ou de la technologie qu'il prévoit d'acquérir
- inclure des clauses de protection des droits dans les contrats avec la possibilité de les rompre en cas d'abus.
- développer des moyens technologiques permettant d'interrompre un service en cas d'abus par le client.

ii) Business enterprises' internal safeguards and remedial mechanisms.

Voies de recours et sauvegardes

Les entreprises devraient aussi s'assurer qu'il y existe des mécanismes d'accès à des voies de recours – judiciaires et non-judiciaires - en cas de violations des droits de l'homme. Le type de plainte possible concerne la manière dont les données personnelles ont été acquises, si elles sont stockées de manière sûre, si la manière de les traiter ne viole pas la liberté d'expression et le droit à la sphère privée. Si ce n'est pas le cas, les entreprises devraient mettre en place elles-mêmes des mécanismes accessibles de traitement des plaintes à caractère non judiciaire.

Les grandes entreprises du secteur de l'informatique et du web devraient développer des politiques encore plus restrictives en ce qui concerne les demandes d'information de la part de gouvernements répressifs afin de protéger les données personnelles des utilisateurs. Elles devraient adopter une politique de transparence par rapport à toute demande. Toute demande de surveillance et d'interception de la part d'une autorité étatique doit avoir une base légale et être dûment justifiée, mais cela ne suffit souvent pas lorsqu'il y a des raisons de croire que les moyens technologiques employés à cet effet contribueront à violer les droits de l'homme.

3. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

Le projet de révision de la LPD prévoit expressément les principes de *privacy by design* et *privacy by default*.

4. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particulars business enterprises, related human rights protection gaps and ways to bridge those gaps.

Le projet de révision de la LPD met en œuvre différents outils dont l'analyse d'impact relative à la protection des données pour les projets, du secteur privé ou des autorités, qui présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. Il étend également l'obligation d'informer les personnes concernées sur leurs droits d'accès. Il encourage l'autoréglementation, par le biais de codes de conduite qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Par ailleurs, les principes de la protection des données dès la conception et par défaut *(privacy by design* et *privacy by default)* sont expressément mentionnés dans la loi. L'indépendance et le rôle du PFPDT sont en outre renforcés.

5. Growing reliance on data-driven technology and biometric data:

a) How can new technologies help promote and protect the right to privacy

b) What are the main challenges regarding the impact on the right to privacy and other human rights?

c) What are the avenues for adequate protection of the right to privacy against threats created by those technologies? How can the international community, including the UN, address human rights challenges arising in the context of new and emerging digital technology?

Une résolution sur la protection des données et l'action humanitaire internationale a été adoptée lors de

la dernière Conférence internationale des commissaires à la protection des données et à la vie privée à Amsterdam qui a abouti à la création d'un groupe de travail pour analyser les exigences en matière de protection des données dans l'action humanitaire internationale et coopérer avec les acteurs concernés dans ce domaine. Le groupe de travail, piloté par une représentant du PFPDT, a notamment travaillé avec les acteurs humanitaires internationaux, principalement dans le cadre du projet « Protection des données dans l'action humanitaire » du Brussels Privacy Hub (BPH) et du Comité international de la Croix Rouge (CICR) qui a abouti à la publication d'un manuel sur la protection des données dans l'action humanitaire . Ce manuel a pour objectif de sensibiliser les organisations humanitaires à la protection des données personnelles et les aider à respecter les normes en la matière. Il répond aussi au besoin de lignes directrices précises pour l'interprétation des principes de protection des données applicables à l'action humanitaire, en particulier lorsque de nouvelles technologies sont en jeu.

6. Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalised groups, and approaches to protect those individuals.

Voir réponse Q5.

7. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organisations.

Selon un arrêt du Tribunal fédéral (ATF 109 Ia 273[11]), qui concerne la surveillance de la correspondance postale, téléphonique et télégraphique, une exclusion générale de tout avis ultérieur aux personnes touchées viole le principe de la proportionnalité ainsi que l'article 13 CEDH (Droit à un recours effectif) ; on peut renoncer exceptionnellement à un tel avis lorsqu'il est de nature à compromettre le but de la surveillance.

Dans l'arrêt ATF 138 I 6[12], le Tribunal fédéral s'est exprimé de nouveau sur le droit à un recours effectif au sens de l'art. 13 CEDH (consid. 6.1) et la licéité de la surveillance secrète et de la conservation secrète de données personnelles, conditions à l'ajournement des renseignements (consid. 6.2). Il a jugé que les modalités du droit indirect d'être renseigné, le fait de limiter la conservation des données ainsi que la surveillance parlementaire constituent des mécanismes de protection des droits fondamentaux (consid. 7.1-7.3). Il a en outre estimé que les recommandations adressées aux autorités compétentes dans le cadre de la surveillance secrète ont un caractère impératif (consid. 7.4), et s'est prononcé sur les conditions à la délivrance de renseignements après la disparition de l'intérêt au maintien du secret (consid. 7.5). Il a conclu que, dans l'ensemble, la réglementation de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 21 mars 1997 (LMSI ; RS 120[13]) respecte l'article 13 CEDH (consid. 7.7). L'article 18 LMSI en question a été abrogé par le chiffre II 1 de l'annexe à la Loi fédéral du 25 septembre 2015 sur le renseignement (LRens ; RS 121), avec effet au 1er septembre 2017.[14]

Dans un arrêt encore plus récent concernant la surveillance des forums de discussions (ATF 140 I

[11] ATF 109 Ia 273
[12] ATF 138 I 6
[13] RS 120
[14] RO 2017 4095; FF 2014 2029.

353[15]), le Tribunal fédéral a constaté que § 32f al. 2 de la Loi sur la police du canton de Zurich (LPol/ZH) permet la surveillance des communications sur les plateformes de discussions virtuelles qui ne sont accessibles qu'à un nombre limité d'utilisateurs (*closed User Groups*). Une telle récolte d'informations peut porter atteinte à la sphère privée et au secret des télécommunications (consid. 8.4). Elle s'étend en principe à l'ensemble des utilisateurs de ce moyen de communication. Il s'agit d'une méthode de surveillance très large qui permet la récolte et l'exploitation de données sur la sphère privée de nombreuses personnes contre lesquelles il n'existe aucun soupçon de comportement illicite (consid. 8.7.2.1). La disposition n'est pas compatible avec le principe de proportionnalité, car elle ne soumet la surveillance à aucune autorisation judiciaire préalable et n'accorde ni information ultérieure, ni protection juridique aux personnes concernées (consid. 8.7.2.4). § 32f LPol/ZH a été abrogé par cet arrêt du Tribunal fédéral.[16]

La nouvelle loi fédérale sur le renseignement (LRens) est entrée en vigueur le 1er septembre 2017 de même que les trois ordonnances qui y sont liées. Le Service fédéral de renseignement est soumis à la surveillance du PFPDT, du Parlement, du Conseil fédéral, de l'administration fédérale et du Département fédéral de la défense, de la protection de la population et des sports. Le PFPDT est en contact étroit avec la délégation parlementaire de contrôle et peut collaborer avec les autorités étrangères de protection des données en cas de besoin.

[15] ATF 140 I 353

[16] OS 69, 476, unter: www.zhlex.zh.ch > offizielle Sammlung > Band 69 > Seite 476 ou https://www.zh.ch/internet/de/rechtliche_grundlagen/gesetze/erlass.html?Open&Ordnr=550.1%2C69%2C476.