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)

Droit à la sphère privée à l'ère numérique – Devoirs de protection de l'État face aux activités des entreprises

Mise à jour de l'étude du CSDH publiée le 22 septembre 2016[1]

12 février 2020

Les questions entourant la protection de la vie privée sur Internet ne cessent de gagner en actualité. Dans cette mise à jour, le CSDH présente l'évolution de la législation et de la jurisprudence observée depuis la publication de l'étude en 2016, en prêtant une attention particulière au règlement relatif à la protection des données personnelles de l'Union européenne et à la jurisprudence qui en découle.

Le droit au respect de la vie privée s'applique aussi à Internet

Le droit confère aux États un double mandat : garantir les droits humains, mais aussi protéger les individus contre tout abus commis par des tiers. Ce devoir de protection s'applique également dans le domaine des techniques numériques de l'information et de la communication, notamment pour préserver la vie privée. En l'occurrence, les États ont devant eux un chantier imposant : sur Internet, les opérations de traitement de données ont très souvent lieu à l'étranger sur les serveurs de fournisseurs de services d'envergure mondiale, de sorte qu'il n'est pratiquement plus possible de faire de distinction entre communications nationales et communications internationales. Cette évolution pose de nouvelles questions en matière de protection de la vie privée : quelle est la responsabilité des fournisseurs de services ? Quelle est celle des États ? Quels facteurs de rattachement permettent de déterminer la compétence ?

Sources internationales du droit

Le droit au respect de la vie privée est inscrit à l'article 12 de la Déclaration universelle des droits de l'homme et est garanti de façon contraignante en particulier par l'article 17 du Pacte international relatif aux droits civils et politiques (Pacte II de l'ONU). En Europe, c'est l'article 8 de la Convention européenne des droits de l'homme (CEDH) qui s'applique. Ces dernières années, les organes internationaux suivants se sont penchés sur le droit à la sphère privée à l'ère numérique, contribuant ainsi à concrétiser ce sujet : le Comité des droits de l'homme des Nations Unies, le Haut-

---

[1] Centre suisse de compétence pour les droits humains (CSDH), *Droit à la sphère privée à l'ère numérique – Devoirs de protection de l'État face aux activités des entreprises*, par Kaufmann Christine, Ghielmini Sabrina, Medici Gabriela et Pulver Fanny, Berne, 22 septembre 2016 (en allemand, avec un résumé en français), disponible à l'adresse https://www.skmr.ch/frz/domaines/economie/publications/etude-sphere-privee.html (consulté le 12 février 2020).

Commissariat des droits de l'homme des Nations Unies, divers rapporteurs-euses spéciaux des Nations Unies (promotion et protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, liberté d'opinion et d'expression, droit à la vie privée), le Conseil de l'Europe, la Cour européenne des droits de l'homme (CourEDH), l'OCDE, l'OSCE et l'Union européenne (UE).

L'obligation de protéger les droits humains vaut tant pour le numérique que pour l'analogique

Comme le montre l'étude du CSDH de 2016, l'obligation de protection valable à l'ère analogique reste inchangée à l'ère numérique, du moins dans la pratique des organes chargés de surveiller l'application des conventions internationales. Cette obligation porte sur le stockage, le traitement et la transmission des données par les États eux-mêmes, mais aussi par des entreprises privées. En conséquence, les États doivent adopter les mesures qui s'imposent (d'ordre légal, administratif, organisationnel, technique ou autre) pour garantir une protection suffisante de la sphère privée. Toute atteinte à cette sphère doit remplir les conditions usuelles en la matière, les États devant par ailleurs prévoir des garanties procédurales et des mécanismes d'application.

Les activités des plateformes en ligne dans le domaine de la (cyber)criminalité transfrontière, de la sécurité d'Internet et de la teneur d'informations publiées et diffusées (comme les fausses nouvelles et les discours de haine) posent des problèmes particuliers aux États.

Il existe deux facteurs de rattachement qui fondent les obligations de protection de l'État : le lieu où les données sont traitées et le domicile de la personne dont les données sont traitées. Du fait de la prohibition de la discrimination, les distinctions opérées en raison de la nationalité de ces personnes sont problématiques. Pour cette raison, les données personnelles traitées en Suisse qui appartiennent à des personnes séjournant à l'étranger doivent elles aussi être protégées. Les États ont également le devoir de protéger les individus lors de la transmission de données transfrontière.

Davantage d'obligations pour les entreprises privées

La protection de la sphère privée reste pour l'essentiel une tâche de l'État, tant en vertu des conventions internationales que d'après des évaluations faites dans le cadre d'initiatives multipartites antérieures dans le secteur des technologies de l'information et de la communication (TIC). Il n'en reste pas moins que des entreprises privées sont de plus en plus souvent dans le viseur des organes internationaux, car elles traitent des volumes de données toujours plus grands, qu'elles stockent pour leur propre usage commercial ou qu'elles transmettent à des États ou à d'autres entreprises. D'autres entreprises conçoivent par ailleurs des techniques qui permettent aux États de surveiller les activités en ligne.

Dans ce contexte, les instances internationales exhortent toujours plus les entreprises à prendre leurs responsabilités en la matière, en respectant ce faisant les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme. On observe par ailleurs une tendance toujours plus forte à saluer et à exiger l'instauration de la transparence en matière de traitement

de données, la possibilité pour l'utilisateur de garder la maîtrise de ses propres données et le recours à des mesures techniques, comme des configurations standard et des techniques favorables à la protection des données.

Le cas concret de l'Union européenne

Le nouveau règlement relatif à la protection des données personnelles de l'Union européenne

En mettant en vigueur en mai 2018 son nouveau règlement relatif à la protection des données personnelles (RGPD), l'UE a accompli un grand progrès vers l'harmonisation du niveau de la protection des droits et des libertés fondamentales en lien avec le traitement de données personnelles. Une avancée due en particulier à l'application extraterritoriale du règlement : celui-ci s'applique en effet aux entreprises établies dans le territoire de l'Union, mais aussi à celles dont le siège est situé en dehors et pour lesquelles le marché européen est un débouché. En conséquence, le RGPD s'applique dès le moment où les données d'une personne séjournant dans un pays membre de l'Union sont traitées, indépendamment de l'emplacement de l'entreprise qui les traite. Cette disposition s'aligne sur la jurisprudence antérieure de la Cour de justice de l'Union européenne (CJUE) (voir l'arrêt *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos* [C-131/12] du 13 mai 2014).

Le droit au déréférencement : suppression de la liste des résultats des moteurs de recherche

Le nouveau règlement incorpore un droit déjà reconnu par la jurisprudence : le droit au déréférencement. Ce droit signifie que les données personnelles de la personne qui en fait la demande doivent, à certaines conditions, être effacées. Il s'agit, dans chaque cas d'espèce, de trouver le juste équilibre entre, d'une part, ce droit et par conséquent le droit au respect de la vie privée et, d'autre part, la liberté d'expression et d'information du fournisseur de services et du public. Dans un arrêt qu'elle vient de rendre concernant Google (*Google LLC c. Commission nationale de l'informatique et des libertés [CNIL]* [C-507/17)] du 24 september 2019), la CJUE a dû interpréter pour la première fois ce droit au déréférencement. L'objet du litige était la question de savoir si le déréférencement exigé devait se réaliser dans toutes les extensions nationales du moteur de recherche de Google ou seulement dans les États membres de l'Union européenne. Dans son arrêt, la CJUE a conclu, en interprétant le RGPD à la lettre, que le droit européen n'oblige pas l'exploitant d'un moteur de recherche de déréférencer les liens sur l'ensemble des versions de son moteur de recherche. La Cour précise que les exploitants peuvent se limiter à prendre des mesures efficaces pour empêcher l'accès aux données verrouillées par le biais de versions correspondant aux États non membres de l'Union européenne. Elle indique aussi expressément que l'autorité de contrôle ou l'autorité judiciaire d'un État membre demeure compétente pour effectuer une pesée des intérêts en présence et enjoindre, le cas échéant, à l'exploitant du moteur de recherche de procéder à un déréférencement sur l'ensemble des versions de ce moteur.

En rendant cet arrêt, la CJUE a restreint de façon surprenante l'extraterritorialité du RGPD (du moins pour ce qui est du droit au déréférencement). Elle a toutefois laissé (de façon intentionnelle, sans doute) une porte ouverte aux États qui voudront appliquer ce principe, mais il faudra que la personne concernée saisisse la justice et fasse valoir un intérêt prépondérant.

Suppression d'informations illégales

La CJUE a été amenée à se prononcer sur l'application extraterritoriale de la directive sur le commerce électronique (*Eva Glawischnig-Piesczek c. Facebook Ireland Limited* [C-18/18] du 3 octobre 2019). Cette directive précise expressément qu'un prestataire de services d'hébergement comme Facebook n'est pas tenu de rechercher activement et de supprimer de sa propre initiative des contenus potentiellement illicites. La Cour a dû examiner la légitimité de la décision d'un État qui, allant à l'encontre de la directive pourtant très claire sur le sujet, a obligé un hébergeur à supprimer dans le monde entier des informations déclarées illicites ainsi qu'à supprimer des informations de contenu équivalent et à en interdire l'accès. En l'espèce, il s'agissait de la suppression de propos diffamatoires tenus sur Facebook concernant une femme politique qu'un tribunal autrichien avait déjà déclarés illicites. Dans sa pesée des intérêts en présence, la CJUE a en particulier tenu compte du fait que les contenus en question avaient déjà été jugés illicites par un tribunal national. Par ailleurs, la diffusion d'informations illicites sur Internet place les tribunaux face à une tâche colossale, car tout ce qui figure sur les plateformes en ligne peut être modifié à tout moment et lu dans le monde entier. Faisant valoir la rapidité à laquelle des dommages supplémentaires pouvaient être occasionnés ainsi que l'ampleur de la diffusion possible, la CJUE a confirmé tant l'application extraterritoriale de la directive que l'obligation faite au prestataire, Facebook en l'occurrence, d'éliminer les contenus équivalents.

La Cour a précisé que l'obligation de supprimer et de bloquer les informations jugées illicites et celles de contenu équivalent est licite dans la mesure où les différences dans la formulation de ce contenu ne contraignent pas le prestataire à procéder de manière autonome à une appréciation. En d'autres termes, il n'y a pas lieu de tenir compte des différences de formulation dès lors que les informations ont manifestement la même teneur. En conséquence, si des internautes diffusent des commentaires illicites sur des plateformes, les juridictions nationales peuvent contraindre les hébergeurs à supprimer non seulement le contenu en question, mais aussi à chercher les commentaires de même teneur et à les effacer.

La CJUE a par ailleurs reconnu l'effet extraterritorial des injonctions faites par les juridictions nationales, estimant qu'il est du devoir des États membres d'étendre au niveau mondial les effets des mesures qu'ils prennent. Elle n'a toutefois pas tranché la question de savoir sur quelle base légale et dans l'application de quel droit un État membre pourrait honorer cette obligation.

Les deux arrêts illustrent, chacun à leur manière, à quel point les transmissions de données transfrontières posent des problèmes d'interprétation juridique. Ils dénotent aussi une nouvelle tendance d'imposer aux prestataires des obligations directes afin de préserver la vie privée de leurs utilisateurs-trices et la volonté d'étendre au niveau mondial le champ d'application de la protection des données.

Évolution observée depuis 2016

En 2016, nous avions montré la façon dont diverses instances internationales avaient alors concrétisé le droit à la sphère privée à l'ère numérique. Le droit et la jurisprudence ayant évolué depuis lors, nous exposons ci-dessous les principales avancées qui se sont produites ces dernières années.

Nations Unies

- Actuellement, les activités du Rapporteur spécial des Nations Unies sur le droit à la vie privée sont axées principalement sur les mégadonnées et les données en libre accès, sur la sécurité et la surveillance, sur les données médicales, sur le traitement des données par les entreprises et sur la notion de vie privée. Le Rapporteur spécial a émis ses premières recommandations en matière de mégadonnées et de données en libre accès[2].
- Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression du 6 avril 2018 (A/HRC/38/35) : ces dernières années, le Rapporteur spécial a accordé davantage d'attention aux contenus en ligne générés par les utilisateurs-trices, comme les contenus transmis par les réseaux sociaux. Dans ce rapport, il propose un cadre réglementaire dans lequel la modération des contenus se fonde sur les droits humains. Ce cadre aborde tant les obligations des États que la responsabilité des entreprises qui gèrent les plateformes en ligne.
- Rapport du 3 août 2018 de la Haut-Commissaire de l'ONU aux droits de l'homme sur le droit à la vie privée à l'ère du numérique (A/HRC/39/29) : ce rapport identifie les principaux chantiers concernant le droit à la vie privée à l'ère numérique et aborde tant les obligations des États que la responsabilité incombant aux entreprises à cet égard.
- Résolution du 26 septembre 2019 de l'Assemblée générale des Nations Unies (A/HRC/Res/42/15) : cette résolution demande aux États d'adopter les mesures nécessaires pour garantir le droit à la vie privée à l'ère numérique.

Conseil de l'Europe

- Recommandation CM/Rec(2018)2 du 7 mars 2018 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'Internet, tels que fournisseurs d'accès, exploitants de moteurs de recherche ou plateformes diverses. Cette recommandation aborde notamment les mécanismes de plainte utiles en cas de violations de droits humains dans le domaine numérique, telles que les atteintes à la vie privée ou les propos discriminatoires, et souligne l'importance de la transparence, par exemple en ce qui concerne le traitement des données personnelles et la modération des contenus.
- Protocole d'amendement (STCE n° 223) à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) du Conseil de l'Europe : adoption le 18 mai 2018.

[2] Pour une vue d'ensemble des activités et des recommandations des Nations Unies dans ce domaine, voir les rapports annuels adressés par le Rapporteur spécial sur le droit au respect de la vie privée à l'Assemblée générale des Nations Unies (A/71/368, A/72/43103 et A/73/45712) et au Conseil des droits de l'homme (A/HRC/31/64, A/HRC/34/60; A/HRC/37/62 et A/HRC/40/63), disponibles à l'adresse https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx (consulté le 22 octobre 2019).

- Lignes directrices du Conseil de l'Europe sur l'intelligence artificielle et la protection des données du Comité consultatif de la convention pour la protection des données (STE n° 108), publiées le 25 janvier 2019.
- Recommandation de la Commissaire aux droits de l'homme de mai 2019 : recommandation adressée aux États membres concernant l'intelligence artificielle et ses effets sur les droits humains.
- Arrêts rendus depuis septembre 2016 par la CourEDH sur le droit au respect de la vie privée à l'ère numérique (sélection) :
  - *Pihl c. Suède* (n° 74742/14) du 7 février 2017 : commentaire anonyme diffamatoire sur un blog ;
  - *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* (n° 931/13) du 27 juin 2017 : diffusion de données déjà rendues publiques (examiné sous l'angle de l'art. 10 CEDH) ;
  - *Bărbulescu c. Roumanie* (n° 61496/08) du 5 septembre 2017 : mesures de surveillance de l'utilisation d'Internet au travail ;
  - *Centrum för rättvisa c. Suède* (n° 35252/08) du 19 juin 2018 : surveillance de masse exercée par les services de renseignement (renvoyé devant la Grande Chambre le 19 février 2019, cet arrêt n'a pas encore force obligatoire) ;
  - *M.L. et W.W. c. Allemagne* (n° 60798/10 et 65599/10) du 28 juin 2018 : archives en ligne d'un journal ;
  - *Big Brother Watch et autres c. Royaume-Uni* (n° 58170/13, 62322/14 et 24960/15) du 13 septembre 2018 : surveillance de masse et échange de données avec les États-Unis ;
  - *Catt c. Royaume-Uni* (n° 43514/15) du 24 janvier 2019 : radiation de données figurant dans une base de données de la police.

OCDE

- Le Groupe de travail de l'OCDE sur la sécurité de l'information et la protection de la vie privée dans l'économie numérique élabore, pour le compte du Conseil de l'OCDE, des recommandations et des rapports à l'intention des gouvernements et d'autres parties prenantes afin de veiller à ce que la sécurité numérique et la protection de la vie privée favorisent l'essor de l'économie numérique ;
- Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, version revue, 2013 ;
- Gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et document d'accompagnement, 2015 ;
- Recommandation du Conseil de l'OCDE sur la gouvernance des données de santé, 2017 ;
- Recommandation du Conseil de l'OCDE sur l'intelligence artificielle, 2019.

OSCE

Depuis 2015, la thématique des droits humains à l'ère numérique est régulièrement à l'ordre du jour des réunions sur la mise en œuvre des engagements concernant la dimension humaine de l'OSCE (HDIM).[3]

Union européenne

- Le nouveau règlement général relatif à la protection des données personnelles (RGPD) de l'UE est entré en vigueur le 25 mai 2018[4].
- Arrêts de la Cour de justice de l'Union européenne :
  - *Tele2 Sverige AB c. Post-och telestyrelsen* (C-203/15) et *Secretary of State for the Home Department c. Tom Watson et autres* (C-698/15) du 21 décembre 2016 : surveillance de masse des communications électroniques aux fins de la lutte contre la criminalité ;
  - *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) du 5 juin 2018 : injonction visant à désactiver un site de fans sur Facebook ;
  - *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) du 24 septembre 2019 : droit au déréférencement, la suppression demandée ne devant pas être effectuée sur toutes les versions d'un moteur de recherche mais seulement sur les versions des États membres ;
  - *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (C-18/18) du 3 octobre 2019 : interprétation du droit au déréférencement selon le RGPD et obligations des hébergeurs de supprimer des informations illicites ou d'en bloquer l'accès sur ordre d'un tribunal.

[3] Voir par exemple OSCE, Réunion sur la mise en œuvre des engagements concernant la dimension humaine, du 11 au 22 septembre 2017, ordre du jour commenté, 31 août 2017, disponible à l'adresse https://www.osce.org/odihr/337506?download=true (consulté le 22 octobre 2019).

[4] Pour de plus amples considérations sur les conséquences du RGPD de l'UE pour la Suisse, voir Préposé fédéral à la protection des données et à la transparence, *Le RGPD et ses conséquences sur la Suisse*, novembre 2018, disponible à l'adresse https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR.pdf.download.pdf/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR.pdf (consulté le 22 octobre 2019).