Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cadre juridique pour les médias sociaux

Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011

Résumé

Les médias ou réseaux sociaux sont des plateformes plus ou moins ouvertes, interactives et participatives, permettant de communiquer, d'établir des relations et de les entretenir. De manière simple et à peu de frais, les utilisateurs peuvent, individuellement ou collectivement, produire des contenus et les partager avec d'autres. Par conséquent, la limite entre auteur, producteur, exploitant et utilisateur, de même que celle entre communication privée et communication publique, devient de plus en plus floue. Le financement des médias sociaux est en majeure partie assuré par la vente des données fournies par les utilisateurs à des entreprises qui les utilisent ensuite à des fins publicitaires.

En réponse à la question soumise par la conseillère nationale Viola Amherd à propos du cadre juridique régissant les médias sociaux, le présent rapport expose les normes et recommandations internationales, à la lumière desquelles il examine les dispositions suisses existantes. Il arrive à la conclusion que dans le domaine de la radio et de la télévision, par exemple, il n'est actuellement pas nécessaire de créer de loi spéciale sur les médias sociaux. Les nouveaux canaux de communication s'accompagnent certes d'une vaste palette d'avantages et de risques, mais l'expérience montre que le droit suisse ne présente pas de grosses lacunes. Appliquées à bon escient, les dispositions générales contenues dans les lois en vigueur (p. ex. LPD, CP, CC, LCD) apportent une réponse adéquate à la plupart des problèmes que posent ou que pourraient poser les plateformes sociales aux particuliers et à la collectivité.

Toutefois, il n'est pas certain que les dispositions existantes se révèlent efficaces dans la pratique. Ce doute concerne notamment l'application du droit en cas de conflit, ce qui ne va pas sans soulever de difficultés compte tenu de l'orientation internationale des plateformes, de la communication anonyme et du problème posé par l'identification de la responsabilité des divers participants (utilisateurs, exploitants de plateformes, fournisseurs de services, etc.). Le caractère transfrontalier de la chose implique que le législateur suisse n'a souvent que peu de possibilités d'exercer son influence. Dans certains domaines toutefois, il n'est pas exclu que des modifications de la loi puissent quelque peu améliorer la situation, par exemple en matière de protection des données, de protection de la jeunesse et d'identification de la responsabilité des fournisseurs de services qui permettent l'accès à un réseau (exploitants de plateforme et fournisseurs de services).

Plusieurs de ces thèmes font actuellement l'objet d'analyses. Les travaux de révision de la loi sur la protection des données clarifieront s'il est nécessaire que le législateur intervienne. S'agissant de la protection de la jeunesse, l'efficacité des mesures engagées fait l'objet d'une évaluation dans le cadre du programme national "Jeunes et médias".

En outre, il devient de plus en plus urgent d'examiner en détail la nécessité d'instaurer des dispositions spéciales définissant la responsabilité civile des exploitants de plateformes et des fournisseurs de services. Si l'analyse révèle qu'une modification de la loi s'impose, un projet de consultation sera présenté.

S'agissant des aspects relevant du droit des télécommunications, ils seront abordés dans le projet de révision de la loi sur les télécommunications soumis à consultation. Selon la planification du Conseil fédéral, ce projet sera élaboré durant la législature en cours.

Les diverses activités et investigations ne portent pas uniquement sur les médias sociaux; elles sont à considérer dans l'ensemble de l'ordre juridique. Il n'en reste pas moins que les différents éléments du droit doivent composer un tout cohérent, aussi en ce qui concerne les médias sociaux. La circulation des informations entre les services compétents impliqués doit être assurée. De plus, il semble souhaitable de dresser un nouvel état des lieux relatif au cadre juridique des médias sociaux dès que les travaux d’analyse seront terminés et que leur orientation sera mieux définie.

Table des matières

1 Introduction: Postulat Amherd 11.3912

Dans son postulat du 29 septembre 2011[1], la conseillère nationale Viola Amherd signale que les médias sociaux apportent une nouvelle dimension dans la communication et l'utilisation des médias qui menace de remettre en cause l'application de lois nationales et de valeurs clés. Cela concerne notamment des règles au sujet de la protection des données, de la lutte contre le racisme ou, plus généralement, de la protection de la sphère privée. Toujours selon elle, il est possible qu'il faille réguler les médias sociaux au moyen d'une législation propre.

Dans le postulat, la conseillère nationale demandait au Conseil fédéral, par la transmission du postulat, d'établir un rapport sur l'état actuel de la législation sur les médias sociaux, dans lequel il répondrait particulièrement aux questions suivantes:

- Quelle est la législation actuelle, en Suisse et à l'étranger, au sujet des médias sociaux?
- Quelles sont les lacunes du droit? Comment peut-on les combler?
- Que penserait le Conseil fédéral de l'élaboration d'une loi sur les médias sociaux qui prenne en considération les particularités de ces nouvelles plates-formes de communication?

Dans son avis du 23 novembre 2011, le Conseil fédéral a écrit que l'on peut se demander si le droit en vigueur (notamment la LPD, le CC, le CP et la LDA) traite cette évolution de manière adéquate et s'il définit suffisamment les responsabilités des personnes impliquées. Les domaines problématiques sont, par exemple la protection des consommateurs, dépassés par l'utilisation non souhaitée de leurs données et l'impossibilité fréquente de transférer leurs données d'une plateforme sociale à une autre. Il est en outre particulièrement difficile d'appliquer le droit en vigueur aux médias sociaux car les exploitants de ce type de plateformes sont souvent actifs à l'échelle internationale, et que les législations nationales atteignent leurs limites. Le Conseil fédéral a proposé d'accepter le postulat.

Le présent rapport a été rédigé sous la direction de l'Office fédéral de la communication. Les travaux se sont réalisés en coordination avec l'Office fédéral de la justice, le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI), l'Office fédéral des assurances sociales et l'Office fédéral de la santé, ainsi qu'avec le groupe d'experts chargé de réviser la loi sur la protection des données. Trois expertises externes (sur les questions de terminologie dans le domaine des médias sociaux, sur l'application du droit dans le contexte international et par les privés lésés) ont également été prises en compte.

[1] http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113912

2 Médias sociaux (réseaux sociaux)

2.1 Terme

Grâce à la large bande, les médias ou réseaux sociaux[2] se sont fortement répandus dans le monde entier. En Suisse, ils sont beaucoup utilisés: 47% de la population font partie de communautés ou de réseaux sociaux privés en ligne, 22% utilisent des réseaux professionnels en ligne et 11% le service de microblogging Twitter[3]. Deux tiers des entreprises, autorités et organisations disposent d'une page sur les réseaux sociaux[4]. Il s'agit de plateformes plus ou moins ouvertes, interactives et participatives, permettant de communiquer, d'établir des relations et de les entretenir. De manière simple et à peu de frais, les utilisateurs peuvent, individuellement ou collectivement, produire des contenus et les partager avec d'autres. En Suisse, plus d'un million de personnes produisent et diffusent leurs propres contenus sur l'internet, principalement en publiant des photos et des images mobiles[5].

Les formes de médias sociaux ne cessent de se multiplier et de se diversifier. Selon l'architecture du média conçue par l'exploitant et selon les possibilités de mise en réseau, elles offrent différentes possibilités d'utilisation, d'interaction et de participation à la conception même de la plateforme.

Les médias sociaux permettent souvent des coopérations non planifiées. Des utilisateurs trouvent des contenus d'autres utilisateurs pertinents pour eux-mêmes, les reprennent, les améliorent, les retravaillent et les placent dans un nouveau contexte. Peuvent en résulter des œuvres collectives de grande ampleur, réalisées sans planification préalable[6].

Pour la plupart des utilisateurs, les médias sociaux servent essentiellement à échanger des messages privés à l'intérieur d'un cercle restreint de personnes qui en général se connaissent. Or, ces canaux sont également exploités pour diffuser des messages publicitaires professionnels visant à influencer le comportement des consommateurs en matière d'achat ou la formation de l'opinion publique.

Parmi les principales caractéristiques des réseaux sociaux, on parle de plus en plus de la suppression de certaines limites dans les canaux de communication et les médias traditionnels, à savoir:

2.1.1 Suppression de la limite entre auteur, producteur, diffuseur et utilisateur

Alors qu'avec les médias traditionnels, les fournisseurs de prestations (p. ex. rédacteurs professionnels, réalisateurs de films, entreprises de médias) se distinguent clairement des bénéficiaires des prestations (le public), les participants à un réseau social combinent facilement le rôle de producteur et celui de consommateur. Des amateurs peuvent, individuellement ou collectivement, créer leurs propres contenus ou modifier les contenus de tiers et décider de les diffuser auprès d'autres utilisateurs.

2.1.2 Suppression de la limite entre communication privée et communication publique

Traditionnellement, il existe deux canaux distincts pour la communication privée et pour la communication publique. Dans la communication privée, en général, l'expéditeur connaît le ou les destinataires (p. ex. conversation personnelle, courrier ou communication téléphonique); dans la communication publique, ce n'est pas le cas.

---

[2] Dans le présent rapport, les deux termes sont synonymes.

[3] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich, p. 16, 19

[4] Bernet ZHAW Studie Social Media Schweiz 2012, p. 3 ss; publié sous: http://www.bernet.ch/socialmediastudie (en allemand uniquement)

[5] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich, p. 17

[6] Aguiton C./Cardon D., p. 52

De nombreuses offres de médias sociaux permettent de passer aisément de la communication privée à la communication publique sur la même plateforme. En outre, le fait que les médias traditionnels sont également présents sur les réseaux sociaux et peuvent contribuer à médiatiser les contenus et les activités des utilisateurs.

2.1.3 Suppression de la limite entre traitement local des données et traitement à distance

Grâce aux médias sociaux, les utilisateurs ne doivent plus déposer leurs données et contenus dans un lieu physique. Ils y ont accès partout où ils ont accès à leurs réseaux. Or, si la sauvegarde de contenus sur les serveurs de tiers offre une grande flexibilité et une grande efficacité, elle entraîne souvent une certaine perte de contrôle sur les données et les contenus, notamment ceux liés à des personnes.

2.2 Catégorisation des réseaux sociaux

Etant donné la diversité des plateformes, de leurs fonctions et de leurs niveaux de complexité, et compte tenu du fait qu'elles évoluent et se transforment en permanence, il n'est guère possible de catégoriser clairement les médias sociaux. De surcroît, ceux-ci ne constituent ni un simple développement des médias traditionnels, ni un moyen de communication réservé à la communication individuelle[7]. Toutefois, dans le domaine de la recherche, les médias sociaux sont souvent classés selon les critères suivants:

2.2.1 Fonctions

Les médias sociaux offrent généralement plusieurs fonctions. La recherche propose diverses catégorisations, qui distinguent les fonctions orientées sur le contenu et les fonctions orientées sur les relations.

2.2.1.1 Fonctions orientées sur le contenu

- Gestion de l'information et du savoir
  Production, recherche, réception, gestion et échange d'opinions, de connaissances et d'informations, p. ex. Wikis, bookmarking social, balisage, RSS, blogosphères ou plateformes d'intérêts spécifiques[8]

- Divertissement ou découverte de mondes virtuels
  Echange de contenus à des fins de divertissement ou d'expérimentation/découverte de mondes virtuels (éventuellement ludiques), p. ex. YouTube, certains jeux interactifs en ligne, etc.

2.2.1.2 Fonctions orientées sur les relations

- Gestion des relations
  Entretien des relations existantes et établissement de nouvelles relations (p. ex. sur des plateformes de contact), échange, mise en lien de personnes partageant les mêmes intérêts, p. ex. les plateformes d'intérêts spécifiques, comme myspace pour les musiciens.

- Gestion de l'identité et de la réputation
  Présentation (sélective) de certains aspects de sa propre personne, p. ex. dans des blogs personnels, des podcasts, etc.

---

[7] Neuberger, Christoph, "Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick". In. Neuberger, Christoph; Gehrau, Volker (Hrsg): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, p. 34

[8] Schmidt, Jan, "Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen". in: Zerfass, notamment (Hrsg): Kommunikation, Partizipation und Wirkungen im Social Web. Bd – 1 – Köln 2008, p. 71

2.2.2 Possibilités de participer

Les possibilités techniques de participer sont elles aussi multiples. La classification des médias sociaux repose sur le taux de participation à l'élaboration des contenus, qui peut aller de la simple évaluation jusqu'à la conception ou la modification des contenus. Elle se réfère également au caractère public de la communication, laquelle va de la communication individuelle à la communication publique de masse en réseau.

2.2.3 Modèles de financement

Tout ce qui est rare est cher, paraît-il, mais avec les réseaux sociaux, on observe exactement le contraire: la valeur d'un produit ou d'un service augmente avec le nombre d'utilisateurs. Ce phénomène est appelé effets de réseau[9]. Dans les offres de médias sociaux, ces effets agissent sur plusieurs acteurs. Si le nombre de membres augmente, tous les utilisateurs voient la probabilité de rencontrer des pairs augmenter; pour les programmateurs, il devient alors plus intéressant de mettre à disposition des applications sur ces plateformes, et les annonceurs ont d'avantage de chances de s'adresser à des groupes très ciblés. Par conséquent, les réseaux sociaux commencent souvent par suivre une stratégie qui leur permet d'acquérir rapidement de nouveaux membres même si, dans un premier temps, elle ne génère pas de véritables revenus. Ils cherchent à fidéliser les utilisateurs, afin d'empêcher que ceux-ci ne se tournent vers d'autres réseaux.

Les économies d'échelle que présentent les réseaux et forums sociaux incitent fortement à l'acquisition ou à la fusion de médias dans le but de réaliser les plus grands bénéfices possibles. Cette dynamique peut créer un contexte dans lequel quelques plateformes occupent une position dominante, du moins pendant un certain temps.

Les médias sociaux suivent des modèles commerciaux ou non commerciaux. Depuis les débuts de l'internet, l'utilisation des contenus est traditionnellement gratuite. Il existe encore actuellement de nombreux réseaux sociaux qui ne poursuivent pas de but commercial, mais s'engagent pour la communauté. Etant donné que leurs utilisateurs les considèrent souvent comme des œuvres collectives auxquelles ils témoignent une certaine loyauté, ils sont facilement prêts à financer l'entretien de la plateforme. Il arrive aussi que les pouvoirs publics financent des réseaux sociaux lorsque la création d'offres destinées à des groupes cibles particuliers, comme les enfants et les jeunes, présente un intérêt public.

Les réseaux sociaux fondés sur des modèles commerciaux sont principalement soutenus par des taxes d'utilisation et par la publicité. Dans ce dernier cas, il s'agit principalement d'annonces publicitaires adaptées aux contenus diffusés sur l'écran et conçues pour attirer l'attention. Plus rarement, ce sont des publicités statiques. Comme les membres de réseaux sociaux créent leur profil en fournissant des informations les concernant, ils mettent à disposition une quantité relativement importante de données personnelles. Celles-ci sont revendues à des entreprises qui les utilisent ensuite à des fins publicitaires. Les profils permettent de cibler parfaitement les destinataires. La rémunération est calculée sur la base de 1000 diffusions de publicité ou d'un tarif par clic selon lequel l'annonceur paie uniquement lorsque les destinataires cliquent sur son annonce. Ainsi, les groupes cibles des plateformes spécialisées[10] présentent une grande valeur financière. Les utilisateurs "paient" avec leurs données personnelles la gratuité des services mis à leur disposition par les médias sociaux.

---

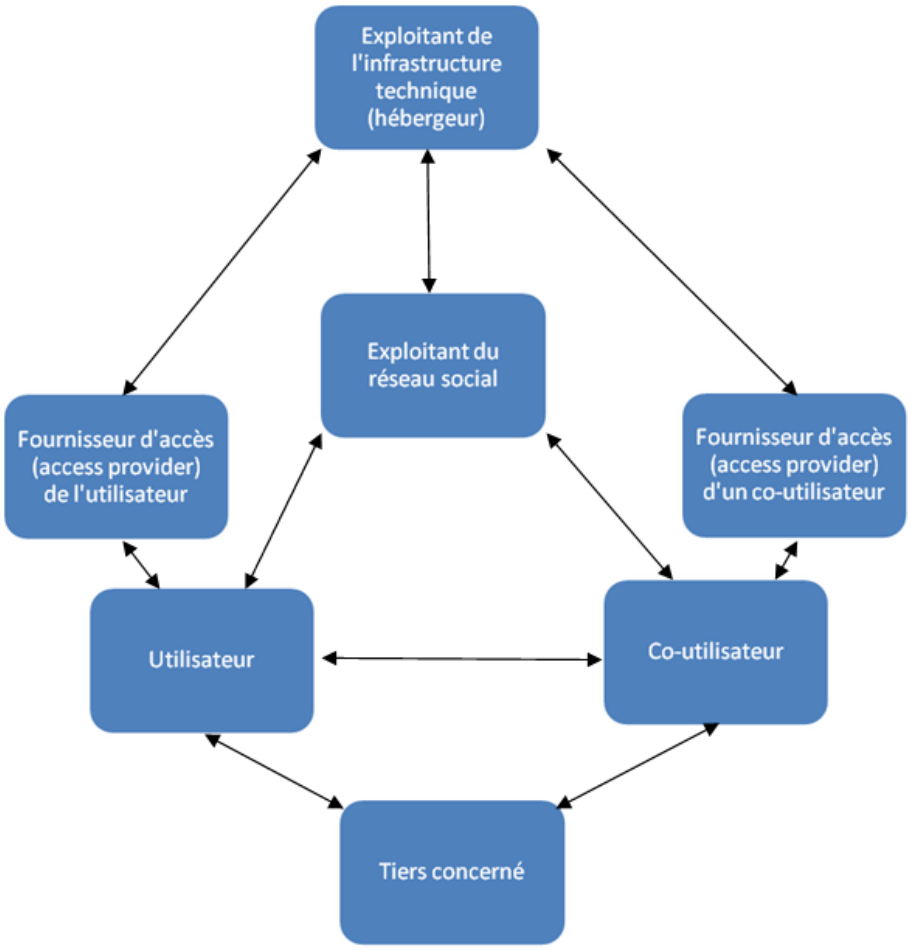
[9] Von Rimscha M. Björn, "Geschäftsmodelle für Social Media" in: Grimm, Petra; Zöllner, Oliver (Hrsg): Schöne neue Kommunikationswelt oder Ende der Privatheit? Stuttgart 2012, p. 303 s.

[10] P. ex. sur les plateformes destinées au monde professionnel, comme Xing ou LinkedIn

2.3 Rôles en lien avec l'utilisation des réseaux sociaux

Les réseaux sociaux regroupent plusieurs acteurs jouant des rôles spécifiques. Ces différents rôles ne se distinguent pas toujours clairement les uns des autres et le passage de l'un à l'autre est souvent très facile[11]. Ainsi, les exploitants de plateformes peuvent intervenir également en tant qu'hébergeurs.

L'organigramme simplifié ci-après donne un premier aperçu de la situation:



2.3.1 Exploitants de plateformes

Les exploitants de plateformes mettent à disposition des utilisateurs un cadre destiné à l'échange de contenus créés ou repris par ces derniers. Les plateformes les plus utilisées en Suisse ont leur siège à l'étranger. C'est le cas, par exemple de Facebook, YouTube et Twitter. Toutefois, il existe aussi des exploitants de plateformes suisses, comme les fournisseurs de blogs, dont certains sont parfois poursuivis en justice devant les tribunaux suisses en raison de contrats litigieux (p. ex. la SSR[12] ou certains éditeurs de journaux[13]).

---

[11] Cf. les explications sur les différents acteurs de la communication internet fournies dans le rapport de la Commission d'experts "Cybercriminalité"", DFJP 2003, p. 29ss

[12] Voir par exemple le litige à propos d'un commentaire diffamatoire publié sur le blog de l'émission de télévision Alpenfestung (ATF 136 IV 145)

[13] Voir par exemple le litige à propos d'un article portant atteinte à la personnalité d'un acteur politique publié sur une plateforme de blog exploitée par la Tribune de Genève (TF 5A_792/2011 du 14.1.2013)

A travers l'architecture et le design de la plateforme, les exploitants choisissent les possibilités d'interaction et de diffusion des contenus. Ils déterminent également dans quelle mesure les utilisateurs peuvent créer des espaces de communication privés, partiellement ou totalement publics, et s'ils ont la possibilité d'échanger des contenus entre ces espaces. Ils peuvent attirer l'attention des utilisateurs sur des contenus spécifiques grâce à des classements et des liens. En outre, ils définissent quelles données ils collectent auprès des utilisateurs, quels droits ils acquièrent sur les données et contenus échangés et comment ils les exploitent économiquement.

Le plupart des exploitants de plateformes établissent des règles de comportement vis-à-vis des utilisateurs ou de tiers non impliqués ainsi que pour la création, l'utilisation ou la diffusion de contenus. Dans les conditions d'utilisation, ils peuvent indiquer quels contenus ou quels comportements ne son pas souhaités ou pas autorisés. Cependant, ils n'opèrent qu'un contrôle rédactionnel léger en comparaison des médias traditionnels. Alors que ceux-ci chargent généralement un comité de rédaction de sélectionner les contenus avant la publication (*ex-ante*), sur les réseaux sociaux, le contrôle s'effectue après la publication (*ex-post*) et les contenus non-conformes aux conditions d'utilisation ou critiqués par d'autres utilisateurs ne sont retirés qu'après coup. Certaines plateformes laissent aux utilisateurs le soin de définir eux-mêmes ces règles et les renvoient à leur responsabilité ainsi qu'à leur capacité d'organisation.

2.3.2 Fournisseurs de services techniques (hébergeurs et fournisseurs d'accès)

La communication *via* les réseaux sociaux repose sur une infrastructure technique. Certains exploitants de plateformes sauvegardent les données sur leurs propres serveurs, alors que de nombreux autres préfèrent recourir aux services de tiers (souvent des hébergeurs), qui leur mettent à disposition contre rémunération l'infrastructure technique (espace mémoire, capacité de calcul, capacité de transmission) pour le trafic automatisé de données. Comme la plupart des exploitants de plateforme occupant une place importante sur le marché suisse, la majorité des hébergeurs ont leur siège à l'étranger. Leur responsabilité n'est en général pas engagée sur les aspects rédactionnels, mais selon la constellation[14], ils sont techniquement en mesure de supprimer de leurs ordinateurs des contenus non souhaités.

La liaison entre les ordinateurs des utilisateurs de médias sociaux et les serveurs contenant le matériel de données des plateformes est assurée par les fournisseurs d'accès. Utilisateurs et fournisseurs d'accès sont liés par contrat. En Suisse, les utilisateurs optent en général pour les services d'un fournisseur établi en Suisse, notamment Swisscom. Les fournisseurs d'accès ne sont souvent pas en mesure de supprimer des contenus non souhaités (car ceux-ci ne sont pas sauvegardés sur leurs serveurs). Ils peuvent toutefois bloquer de manière ciblée l'accès à certains contenus.

2.3.3 Utilisateurs et co-utilisateurs

Les contenus sont en général établis par les utilisateurs (*user generated content*), tout comme les renvois vers les contenus de tiers. Pour ce faire, les utilisateurs ont besoin aussi bien du soutien technique des fournisseurs d'accès que de l'accès aux médias sociaux concernés. En règle générale, ils peuvent choisir à qui ils destinent leur communication, à savoir s'ils entendent partager leurs contenus avec un large public ou uniquement avec un cercle choisi de personnes. Ils opèrent dans le cadre des possibilités offertes par les exploitants des plateformes et dans celui des dispositions relatives au contenu.

Du point de vue de l'exploitant, les utilisateurs ont une (co)responsabilité dans la manière dont ils se comportent les uns vis-à-vis des autres, ainsi que pour les contenus qu'ils diffusent à grande échelle sur les réseaux sociaux. Souvent, la responsabilité des utilisateurs pour des activités contraires aux bases légales ou aux droits de tiers n'est pas clairement définie. Il arrive aussi fréquemment que les

[14] L'hébergeur ne peut pas supprimer des contenus sur un serveur qu'il loue. Il ne peut que couper le courant ou démonter physiquement le disque dur, ce qui serait souvent disproportionné.

utilisateurs ne la connaissent pas. Cette situation peut engendrer des risques pour les utilisateurs qui mènent ces activités ou pour ceux s'en trouvent lésés.

2.3.4 Tiers concernés

Les activités réalisées sur les réseaux sociaux peuvent aussi toucher des tiers qui ne sont pas actifs sur les réseaux correspondants. C'est par exemple le cas lorsque des contenus qui concernent des tiers sont repris par les médias de masse ou que des membres utilisent ces données sur des réseaux sociaux sans en avoir l'autorisation.

2.3.5 Médias traditionnels et autres services de médias

Les médias traditionnels aident les médias sociaux à attirer l'attention, à acquérir de nouveaux membres et à augmenter les recettes publicitaires. De leur côté, les médias sociaux sont de plus en plus utiles aux médias traditionnels en leur fournissant des contenus et des nouveautés.

Du fait de ces interactions, la limite entre communication privée et communication publique est souvent floue pour les utilisateurs. De nombreux médias traditionnels sont présents sur les médias sociaux ou reliés à de grands réseaux, comme Facebook.

Les moteurs de recherche constituent d'autres relais puisqu'ils renvoient les utilisateurs vers des contenus publiés non seulement dans les médias traditionnels mais aussi sur les réseaux sociaux. Il existe également des collaborations économiques, notamment pour l'échange et l'exploitation des données relatives aux utilisateurs à des fins commerciales ou autres.

2.4 Observations préliminaires sur l'implication juridique des participants aux médias sociaux

2.4.1 Droits et obligations découlant de la Constitution

En Suisse (et apparemment aussi à l'étranger), il n'existe pas de dispositions légales spécifiques relative à la communication sur les réseaux sociaux. Toutefois, l'utilisation de ceux-ci ne se déroule pas dans une zone de non-droit.

Au plus haut niveau normatif, la législation garantit aux participants à la communication (non seulement aux utilisateurs, mais aussi aux exploitants de plateformes et aux fournisseurs d'accès) une protection contre l'ingérence de l'Etat. La Constitution suisse et la Convention européenne des droits de l'homme garantissent la libre communication (art. 16, 17, 21, 22, 23, 34 Cst. ainsi qu'art. 10 et 11 CEDH) et la liberté économique (art. 27 Cst.). Toutefois, ces libertés ne sont pas absolues; elles peuvent être restreintes par l'Etat. Les autorités doivent remplir des exigences strictes. En vertu de l'art. 36 Cst., toute restriction d'une liberté fondamentale doit être fondée sur une base légale, justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui et proportionnée au but visé. Il est absolument interdit d'intervenir sur l'essence des droits fondamentaux, notamment par une censure étatique systématique des contenus de la communication (art. 17, al. 2, Cst.).

S'agissant de la communication effectuée par des particuliers *via* les médias sociaux, l'Etat est soumis à deux obligations. Il doit lui-même respecter les droits fondamentaux et veiller à ce que des particuliers ne restreignent pas illégalement les droits d'autres particuliers.

L'utilisation des réseaux sociaux offre des avantages, mais comportent également divers risques pour les personnes ainsi que pour le bien commun. A des fins de protection des droits fondamentaux d'autrui et de l'intérêt public (comme la sécurité ou la santé publique[15]), l'Etat et tenu de prendre certaines mesures juridiques. Il doit par exemple prévoir des instruments de protection de la vie privée

[15] Notamment des mesures contre la publicité pour l'alcool et le tabac ou contre l'abus de stupéfiants.

et de la vie familiale (art. 13 Cst., art. 8 CEDH) des individus, notamment des dispositions légales de protection contre les publications déshonorantes ou diffamatoires.

Les enfants et les jeunes doivent bénéficier d'une protection particulière. La Convention de l'ONU relative aux droits de l'enfant exige la protection de l'enfant contre toute forme d'exploitation préjudiciable à son bien-être (art. 36) et garantit sa protection contre toute atteinte illégale à son honneur et à sa réputation (art. 16)[16]. La Cour européenne des droits de l'homme (CEDH) exige de l'Etat qu'il prenne des mesures efficaces lorsque des publications immorales diffusées sur l'internet portent atteinte à la vie privée d'un jeune (publication d'une petite annonce indécente)[17].

L'Etat a également des obligations en matière de liberté des médias. Il doit prendre des mesures appropriées pour empêcher que des acteurs privés puissants, notamment économiquement, abusent de leur influence sur l'opinion publique.

2.4.2 Droits et obligations prévus dans la législation actuelle

2.4.2.1 Respect des prescriptions légales générales

Les dispositions constitutionnelles sont précisées dans les lois. La législation suisse contient plusieurs prescriptions qui définissent en détails les droits des intéressés ou les limitent. Ces prescriptions ne s'appliquent pas uniquement à la communication sur les réseaux sociaux, mais par exemple aussi aux déclarations faites *via* les canaux traditionnels comme les journaux, la radio, les lettres ou les communications téléphoniques. Il s'agit notamment de règles inscrites dans le droit pénal, le droit civil (protection de la personnalité) et le droit de la protection des données. Les prescriptions correspondantes et leur portée pour les médias sociaux sont présentées plus en détail au chapitre 4 du présent rapport.

2.4.2.2 Une réglementation spéciale pour les exploitants de plateformes dans le droit des télécommunications?

Le droit suisse contient une réglementation spéciale pour certains fournisseurs ou transporteurs d'informations, qui s'applique par exemple aux diffuseurs de programmes de radio et de télévision traditionnels soumis aux dispositions de la loi sur la radio et la télévision (LRTV).

Des dispositions spéciales sur la fourniture de services de télécommunication, à savoir le transport par des moyens de télécommunication (transmission) d'informations pour le compte de tiers (y compris de programmes de radio et de télévision) sont inscrites dans la loi sur les télécommunications (LTC). Quiconque fournit un service de télécommunication doit l'annoncer à l'Office fédéral de la communication (art. 4 LTC), remplir des exigences en matière d'organisation (art. 6 LTC), observer le secret des télécommunications (art. 43 LTC), participer aux procédures de conciliation (art. 12c LTC), appliquer des prix transparents (art. 12a LTC), lutter contre la publicité de masse déloyale (art. 45a LTC) et remplir de nombreuses autres obligations. La LTC date d'une époque où la fourniture de services de télécommunication dépendait encore de la possession d'un réseau spécialement prévu à cet effet ou du moins de l'accès autorisé à un tel réseau. Avec l'évolution technologique, ce lien étroit entre réseau et services a disparu. Aujourd'hui, les conditions techniques sont tout autres (p. ex. internet, Smartphones). Des services peuvent être offerts de différentes manières et sans la participation active des exploitants de réseau, ce qui a donné naissance à des modèles commerciaux totalement nouveaux (p. ex. le financement par la publicité).

Selon le droit en vigueur, celui qui transporte des informations entre au moins deux autres parties au moyen de techniques de télécommunication fournit un service de télécommunication (art. 3, let. b,

[16] Convention relative aux droits de l'enfant conclue à New York le 20 novembre 1989, entrée en vigueur pour la Suisse le 26 mars 1997 (Convention de l'ONU relative aux droits de l'Enfant), RS 0.107

[17] Jugement de la CEDH "K.U. v. Finnland" (référence de la plainte: 2872/02) du 2.12.2008: Refus injustifié de la justice finlandaise d'obliger le fournisseur d'accès à livrer les données litigieuses

LTC). Ce n'est en général pas le cas des exploitants de plateformes sociales, qui constituent plutôt l'une des parties entre lesquelles des informations sont transportées. Toutefois, il existe des exceptions, où les exploitants de plateformes sont au moins coresponsables du transport d'informations entre des tiers, ce qui fait d'eux des fournisseurs de services de télécommunication selon la définition en vigueur. Un exemple de ce cas de figure est celui des messages envoyés par un membre de Facebook à un autre au moyen de Facebook-Messenger. Indépendamment du fait qu'il est difficile, avec les instruments actuels, de faire appliquer le droit national des télécommunications contre des exploitants de plateformes sans siège en Suisse et actifs au niveau mondial, de nombreuses dispositions du droit des télécommunications en vigueur ne sont de toute manière pas adaptées aux activités de ces derniers.

3 Potentiel et risques des médias sociaux

3.1 Généralités

De plus en plus présents dans le quotidien de nombreuses personnes, les médias sociaux intéressent aussi bien les particuliers que les Etats et les organisations internationales. Le Conseil de l'Europe et l'Union européenne, par exemple, se sont penchés à plusieurs reprises sur leur potentiel et leurs risques.

3.2 Potentiel des médias sociaux

Avec les médias sociaux, les particuliers peuvent créer des contenus et les diffuser rapidement, facilement et à peu de frais. Ils les utilisent pour se divertir, avoir des échanges culturels, débattre ou s'assurer un revenu. En outre, les médias sociaux favorisent l'action et la mobilisation politiques de la population. De plus en plus de personnes disposent par ce biais de nouvelles possibilités de participer au débat public[18].

La *Cour européenne des droits de l'homme* a relevé qu'aujourd'hui l'internet comptait parmi les moyens d'expression et de création d'information les plus importants sur les questions politiques ou d'intérêt général[19].

Le *Conseil de l'Europe* a élaboré une série de recommandations destinées à ses 47 membres afin d'aider les gens à utiliser l'internet et les nouveaux service de communication (y compris les réseaux sociaux) pour mieux faire valoir leurs droits fondamentaux[20]. A cette fin, il convient par exemple d'encourager l'éducation aux médias dans la population[21]. Pour sensibiliser les acteurs à leur responsabilité vis-à-vis des citoyens et les inciter à coopérer davantage, le Conseil de l'Europe collabore de plus en plus avec les milieux économiques et la société civile dans le domaine de l'internet et des nouveaux médias[22].

La recommandation du Conseil de l'Europe sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux[23] souligne que les médias sociaux jouent un rôle important dans la promotion de la liberté de l'information, de la liberté d'opinion et de la liberté de rassemblement et renforcent la participation des personnes à la vie politique, sociale et culturelle. Dans une recommandation sur la diversité de la presse, le Conseil de l'Europe invite expressément les Etats membres à soutenir le développement des réseaux sociaux afin de favoriser le pluralisme des médias et les espaces de dialogue[24].

Pour garantir le bon fonctionnement d'un système de médias indépendant et pluraliste dans la société de l'information, le Conseil de l'Europe a élaboré un concept définissant une nouvelle conception des

---

[18] Des données quantitatives sont publiées, par exemple, dans Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, p. 130 s.

[19] Jugement de la CEDH en l'affaire "Ahmet Yildirim c. Turquie" (N°3111/2010) du 18.12.2012 sur le blocage de la plateforme Google Sites en violation des dispositions de la CEDH

[20] http://www.coe.int/t/dghl/standardsetting/media/doc/cm_FR.asp?

[21] L'éducation aux médias désigne l'aptitude de choisir et d'utiliser les médias, de comprendre les contenus et de les juger de manière critique, de comprendre l'économie des médias et de reconnaître leur influence, de communiquer dans différents contextes et d'effectuer des transactions.

[22] Voir p. ex. les lignes directrices en matière de droits de l'homme élaborées en collaboration avec les fournisseurs de services internet et les fabricants de jeux en ligne: http://hub.coe.int/de/human-rights-guidelines-for-internet-service-providers-and-online-games-providers/ .

[23] Recommandation CM/Rec(2012)4 du Comité des Ministres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux du 04.04.2012 (Recommandation du Conseil de l'Europe relative aux réseaux sociaux).

[24] Recommandation CM/Rec(2007)2 sur le pluralisme des médias et la diversité du contenu des médias. La Cour européenne des droits de l'homme a par exemple cité cette recommandation dans son arrêt "Centro Europa 7 S.R.L. & Di Stefano c. Italie" (N° 38433/09) du 7.6.2012 (ch. 72, 134), qui avait pour objet le manque de pluralisme des médias italiens.

médias, qui devrait permettre d'appliquer de manière graduelle et différenciée les principes de base qui sous-tendent la réglementation des médias traditionnels également à de nouveaux médias, tels que les réseaux sociaux[25].

Les *organes de l'UE* aussi s'intéressent au potentiel multiple des réseaux sociaux. Ils mettent en évidence par exemple la grande utilité des plateformes sociales pour le respect des droits de l'homme, la participation politique[26] et l'indépendance des médias en matière d'information[27]. Ils soulignent également le contenu novateur et créatif des réseaux sociaux ainsi que leur importance pour l'économie [28] et demandent que l'utilisation créative de ces médias soit encouragée[29].

3.3 Risques des réseaux sociaux

La position dominante d'un petit nombre de plateformes mondiales peut toutefois aussi comporter des risques, par exemple en réduisant la diversité de l'information et des opinions ou en utilisant cette entreprise à des fins politiques ou économiques. En outre, les contenus diffusés via les réseaux sociaux présentent plusieurs dangers pour les intérêts individuels et les intérêts généraux (la question est examinée en détail au chapitre 4 du présent rapport).

La *recommandation du Conseil de l'Europe* sur les réseaux sociaux souligne les risques de ceux-ci avant tout dans des domaines comme la gestion potentiellement discriminatoire des plateformes sociales, les dangers pour les enfants et les jeunes et le manque de protection de la sphère privée et des données.

Le *Comité économique et social européen (CESE)* considère également le manque de protection de la sphère privée ainsi que des enfants et des jeunes comme l'un des principaux problèmes posés par les réseaux sociaux[30]. Il recommande l'introduction d'une autoréglementation ou d'une coréglementation par les institutions de l'UE qui devrait devenir contraignante si elle n'est pas appliquée. En raison de l'évolution dynamique des réseaux, le CESE demande non seulement la formulation de prescriptions générales technologiquement neutres pour la réglementation des plateformes, mais aussi le suivi d'une politique favorisant les compétences numériques de la population et un développement des connaissances des instances de plainte en ligne (hotlines internet) pour la surveillance des comportements abusifs sur les réseaux sociaux.

---

[25] Recommandation CM/Rec(2011)7 sur une nouvelle conception des médias.

[26] Communication conjointe "Les droits de l'homme et la démocratie au cœur de l'action extérieure de l'UE – Vers une approche plus efficace" KOM(2011) 886 définitive, p. 14, 20s. ou avis du Comité des régions sur "le service universel dans les communications électroniques" et "les réseaux et l'internet du futur ", JO C vom 28.5.2009, p. 41 et recommandation du Parlement européen sur le renforcement de la sécurité et des libertés fondamentales sur Internet, (2008/2160(INI), JO C 117 E du 6.5.2010, p. 206.

[27] Résolution du Parlement européen du 07. 09.2010 sur le journalisme et les nouveaux médias – Créer une sphère publique en Europe JO 308 E du 25.10.2011, p. 55

[28] Voir l'avis sur "L'Internet des objets" JO C 77 du 31.3.2009, p.28, ou la communication "Rapport sur la compétitivité numérique de l'Europe – Principaux résultats de la stratégie i2010 2005-2009", KOM(2009) 390 définitif, p. 10

[29] Conclusions "Renforcer le potentiel de création et d'innovation des jeunes, 2012/C 169/01, p. 2; Rapport sur la compétitivité numérique de l'Europe – Principaux résultats de la stratégie der i2010-Strategie 2005-2009", KOM(2009) 390 définitif, p. 12; Avis "Une stratégie numérique pour l'Europe", 2011/C 15/07, p. 38

[30] Avis "L'utilisation responsable des réseaux sociaux et la prévention de troubles associés", JO C 351 vom 15.11.2012, p. 31

4 Etat de la législation en matière de réseaux sociaux

4.1 Remarque préliminaire

Comme nous l'avons vu plus haut, les réseaux sociaux peuvent être d'une grande utilité dans notre société de communication moderne. Mais ils recèlent également des risques, dont certains sont d'ordre juridique. Nous allons analyser ci-dessous divers problèmes que peuvent poser les réseaux sociaux aux utilisateurs, à d'autres acteurs indirects ou à la collectivité. Les solutions apportées à ces problèmes à l'étranger ou dans le cadre du droit international seront ensuite passées en revue, et la situation juridique actuelle en Suisse sera examinée.

4.2 Gestion discriminatoire des réseaux sociaux

4.2.1 Conditions d'accès au service problématiques et refus d'accès

4.2.1.1 Contexte

Pour utiliser les réseaux sociaux, il est souvent nécessaire de communiquer des informations personnelles (telles que son nom ou son adresse e-mail), la portée et la nature de ces informations pouvant varier d'un média à un autre. Du fait du modèle commercial le plus répandu dans le secteur (commercialisation de données clients) et afin de pouvoir contrôler les contenus qui s'échangent au sein de leur réseau, les exploitants de plateformes ont généralement tout intérêt à disposer de données fiables quant à l'identité de leurs membres. Si les règles édictées par les exploitants sont parfois contournées, la majorité des utilisateurs de médias sociaux semble toutefois communiquer des informations véridiques au sujet de leur identité, au risque de le regretter par la suite, notamment si la transparence quant au traitement réservé à ces informations laisse à désirer.

Les renseignements saisis par le futur utilisateur lors de l'inscription peuvent également contenir des informations révélatrices de certains aspects de son identité et susceptibles d'amener l'exploitant à lui refuser l'accès au service. Cela peut notamment poser problème lorsqu'une telle exclusion se fonde sur l'appartenance de l'utilisateur à un groupe donné (défini par des caractéristiques comme la race, la nationalité, les opinions politiques, la religion, l'orientation sexuelle, le sexe etc.).

On peut aussi imaginer que des individus ou des entreprises soient jugés indésirables pour d'autres motifs, de nature économique, par exemple. Les modèles commerciaux des réseaux sociaux visant généralement à regrouper la plus grande communauté possible, le refus d'admettre de nouveaux membres constitue toutefois une exception.

4.2.1.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe met en garde contre les pratiques discriminatoires de certains exploitants, telle l'exclusion d'utilisateurs.

4.2.1.3 La législation en Suisse

En vertu du principe de la liberté contractuelle, les individus et les entreprises privées ont le droit de déterminer librement s'ils souhaitent conclure un contrat, avec qui et pour quel contenu[31]. Selon le droit suisse, les exploitants de plateformes sont donc en principe libres de choisir avec qui ils souhaitent conclure un contrat. La liberté contractuelle connaît toutefois des limites. Dans certains cas, un prestataire peut ainsi être tenu de conclure des contrats avec des intéressés (obligation de contracter).

L'obligation de contracter est régie de manière explicite par l'art. 261bis CP, lequel stipule que celui qui aura refusé à une personne ou à un groupe de personnes, en raison de leur appartenance raciale, ethnique ou religieuse, une prestation destinée à l'usage public encourt une sanction pénale (ce serait

[31] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, p. 171 s.

par exemple le cas si un exploitant de plateforme excluait une communauté d'intérêts en raison de son appartenance ethnique). De manière similaire, l'art. 6 de la loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (LHand, RS 151.3) interdit aux entités privées qui fournissent des prestations au public de traiter les personnes handicapées de façon discriminatoire du fait de leur handicap. Toute personne qui subit une telle discrimination peut demander au tribunal le versement d'une indemnité (art. 8, al. 3, LHand). La loi reconnaît en outre aux organisations nationales d'aide aux handicapés le droit d'agir devant les instances civiles afin de faire constater une discrimination (art. 9, al. 3, let. a, LHand).

En droit privé, l'obligation générale de contracter découle de la protection de la personnalité telle que prévue par le droit civil (art. 28, 28*a*, al. 1, ch. 2, CC) ainsi que de l'interdiction de faits contraires aux mœurs (art. 41, al. 2, CO)[32]. La condition est que la partie qui offre propose de manière générale et publique des biens ou des services répondant aux besoins courants[33], que la partie demandeuse n'ait pas, du fait de la position dominante de l'autre partie, d'alternative acceptable et que le prestataire ne puisse invoquer aucune raison objective justifiant son refus de contracter[34].

Le droit des cartels[35] limite lui aussi la liberté contractuelle, mais uniquement celle des entreprises en position dominante sur le marché. Les entreprises recourent de plus en plus aux offres des réseaux sociaux, notamment à des fins publicitaires et pour entretenir les liens avec leurs clients. Si un réseau social occupant une position dominante, par exemple sur le marché de la publicité, venait à refuser l'accès à ses services à des entreprises intéressées, il pourrait se mettre en infraction avec le droit des cartels pour cause de refus d'entretenir des relations commerciales (art. 7, al. 2, let. a, LCart).

L'analyse montre qu'en matière de souscription de contrats, le droit suisse confère une grande liberté (en termes de parties contractantes, de contenu, etc.) aux individus et aux entreprises privées. Cette liberté est toutefois limitée par la loi dès lors qu'un partenaire se trouve en position dominante sur le marché ou que la conclusion du contrat est refusée en raison de caractéristiques propres au cocontractant. Dans ces cas, la conclusion du contrat peut être exigée par voie légale.

4.2.2 Censure de contenus par les exploitants de réseaux sociaux

4.2.2.1 Contexte

Dans leurs conditions d'utilisation, de nombreux exploitants de réseaux sociaux prévoient des codes de conduite applicables aux échanges sur leurs plateformes ainsi qu'une liste de contenus généralement interdits. Sont ainsi souvent prohibés les contenus à caractère pornographique, raciste, discriminatoire, offensant ou exagérément violent. Les réseaux sociaux d'envergure mondiale conçoivent généralement leurs procédures de contrôle des contenus de manière à ce qu'elles respectent les lois de la plupart des pays pour ce qui est des contenus illicites. Il en résulte que des contenus peuvent être supprimés même dans des pays où ils ne poseraient aucun problème légal.

Les contrôles se font selon différentes méthodes. Les utilisateurs peuvent ainsi signaler les contenus suspects à l'exploitant, lequel se charge ensuite de les analyser et, si nécessaire, de les éliminer. A côté de cela, les exploitants mettent souvent en œuvre des logiciels de filtrage censurant automatiquement certains contenus. Certaines infractions peuvent également conduire à la suppression définitive de comptes d'utilisateur. Toutes ces méthodes peuvent *in fine* entraîner la suppression de contenus parfaitement inoffensifs, par exemple la photo d'une mère en train d'allaiter. Cela pose notamment problème lorsque les contenus publiés et partagés ne sont ni illicites ni socialement dommageables ou lorsqu'ils ne sont partagés qu'au sein de groupes restreints d'utilisateurs.

---

[32] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, p. 179

[33] Bien et services aujourd'hui pratiquement accessibles à tous et faisant partie du quotidien. Voir ATF 129 III 35 cons. 6.3.

[34] ATF 129 III 35 cons. 6.3.

[35] Loi fédérale du 6 octobre 1995 sur les cartels et autres restrictions à la concurrence (LCart), RS 251

4.2.2.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe demande que les utilisateurs soient clairement informés sur la politique éditoriale du fournisseur de service de réseau social en ce qui concerne ses modalités de traitement de contenus apparemment illicites et ce qu'il considère comme un contenu ou un comportement inapproprié sur le réseau et que les mécanismes de contrôle mis en place n'entraînent pas une limitation abusive de la liberté d'expression et de l'accès à l'information. Dans sa Déclaration sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés, le Conseil de l'Europe met en outre en garde contre le danger de voir des pressions politiques sur les prestataires de services Internet conduire à des ingérences dans l'exercice de la liberté d'expression des clients et alerte les Etats membres sur la gravité des violations des droits fondamentaux susceptibles d'en résulter. Par ailleurs, le Conseil de l'Europe demande que les utilisateurs soient informés qu'un filtre est activé et, s'il y a lieu, qu'ils puissent reconnaître et contrôler le niveau de filtrage auquel est soumis le contenu qu'ils consultent. Ils devraient en outre avoir la possibilité de contester le filtrage du contenu et de demander des explications[36].

4.2.2.3 La législation en Suisse

Celui qui transmet des contenus à des tiers est libre, dans les limites fixées par la loi, de décider quels contenus il souhaite transmettre ou non. Des limites spécifiques sont certes définies par la loi sur la radio et la télévision et par la loi sur les télécommunications, qui prévoient certaines obligations de diffusion. Toutefois, les exploitants de plateformes n'y sont normalement pas soumis. De plus, des questions relevant du droit de la concurrence peuvent se poser: le refus, par des entités privées se trouvant en position dominante, de véhiculer certains contenus peut entraver de manière illégale l'accès de tiers à la concurrence ou son exercice (art. 7 loi sur les cartels; LCart) si l'entreprise en position dominante ne peut justifier son refus par des raisons objectives (illicéité ou caractère contraire aux mœurs des contenus à diffuser, manque de place, etc.). Si un réseau social vient à acquérir une position dominante sur le marché et s'il se trouve en mesure de décider de manière largement arbitraire de la diffusion ou non de contenus, la question se pose de savoir si des obligations en matière de diffusion des contenus – par analogie avec les obligations incombant aux diffuseurs de programmes radio ou télé (contenus) ou aux fournisseurs de services de télécommunications (transmission) – peuvent se justifier à son encontre. Astreindre les exploitants de plateformes à une obligation légale de diffuser certains contenus revient néanmoins à restreindre leurs droits fondamentaux (par exemple leur liberté économique), restriction qui doit donc être fondée sur les bases légales usuelles (art. 36 Cst.).

Dans certains cas, la suppression de contenus peut en outre porter atteinte aux droits d'auteur (c'est-à-dire au droit moral d'auteur) ou à la protection de la personnalité telle que prévue par le code civil (art. 28 CC).

L'Etat peut également restreindre directement les droits fondamentaux en matière de communication en empêchant les intervenants privés de les exercer. Il est ainsi imaginable qu'un strict contrôle des contenus exercé par un exploitant de plateforme soit en fait indirectement imputable à l'Etat. Lorsque la situation juridique est ambigüe du fait du manque de précision des prescriptions légales, il peut notamment arriver que des intervenants privés ne sachent pas avec certitude si des propos tenus sur leurs réseaux sont légaux ou non[37]. Des dispositions imprécises en matière de responsabilité des fournisseurs de services et des exploitants de plateformes pour ce qui est des contenus illicites diffusés par des tiers peuvent donc amener les entreprises à supprimer, dans le doute, des contenus ne posant pourtant aucun problème légal afin d'éviter toute poursuite dont elles pourraient faire l'objet.

---

[36] Recommandation CM/Rec(2008)6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet

[37] Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, p. 376

4.3 Atteinte à d'autres intérêts individuels par les exploitants de plateformes

4.3.1 Problème de fond: manque de contrôle des utilisateurs sur leurs propres données

4.3.1.1 Contexte

Du point de vue des dispositions régissant la protection des données, le manque de contrôle exercé par les utilisateurs sur leurs propres données est un réel problème[38]. Les formes prises par ce manque de contrôle sont des plus diverses.

L'autonomie des utilisateurs pour ce qui est de l'utilisation de leurs données ne dépend pas seulement de leur décision de s'inscrire ou non à un réseau social et des informations personnelles qu'ils y révèlent[39], mais aussi et surtout des logiciels proposés par les exploitants des plateformes dans la mesure où ils limitent souvent le contrôle exercé par les utilisateurs sur leurs données en raison d'un paramétrage insuffisant en matière de protection de la sphère privée. La possibilité, pour des tiers ayant accès à d'autres profils utilisateurs, d'insérer sur ces profils des textes et des photos sans avoir à recueillir l'accord préalable du titulaire du profil ou de télécharger, sans y être invités, des contenus en provenance de ces profils se révèle également problématique.

Les utilisateurs voient de plus en plus le contrôle de leurs données personnelles leur échapper du fait des exigences qui leur sont imposées en matière de consentement au traitement de leurs données. Par ailleurs, le flux régulier de nouvelles applications et de nouveaux services ainsi que la modification fréquente des conditions d'utilisation et des déclarations de protection des données obligent les utilisateurs à rechercher sans cesse les informations leur permettant de savoir quelles méthodes de traitement des données ont cours à l'instant T. Les informations relatives à l'utilisation des données de profil et de mouvement sont en outre souvent difficiles à trouver, et il est rare que des explications transparentes soient fournies aux utilisateurs à propos de l'objectif du traitement desdites données, de l'éventuelle transmission de ces données à des tiers ou simplement des mécanismes permettant de faire valoir certaines exigences en matière d'origine et d'habilitation.

La protection des données relatives aux personnes n'utilisant pas les réseaux sociaux est également souvent défaillante. Certains exploitants de réseaux (Facebook en particulier) proposent par exemple aux utilisateurs d'importer dans leur profil leurs contacts téléphoniques, e-mail ou de messagerie instantanée (fonction "retrouver des amis"), ce qui permet à l'exploitant de voir lesquels des contacts ainsi transférés ne sont pas encore membres du réseau. La plateforme a alors coutume d'utiliser, avec le consentement du membre, les adresses indiquées afin d'envoyer des invitations et publicités (non sollicitées par le destinataire) aux non-membres.

L'octroi de prérogatives étendues aux exploitants de plateformes dans les conditions générales de vente (CGV), que les utilisateurs sont tenus d'accepter sous peine de ne pas pouvoir utiliser le service, limite encore un peu plus le contrôle exercé par les utilisateurs sur leurs données personnelles. Si les réseaux sociaux disponibles sont peu nombreux ou si les plateformes alternatives manquent d'attrait du fait des communautés réduites qu'elles possèdent, les conditions d'utilisation restrictives imposées par les exploitants des plateformes peuvent poser problème. Nombre de réseaux s'octroient ainsi *des droits d'utilisation étendus sur les données d'utilisateur*. La suppression de contenus par les utilisateurs ne change généralement rien à cet état de fait, et ceux-ci auraient tort

---

[38] Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données (FF 2012 255, 268). L'association allemande de consommateurs Stiftung Warentest a mené auprès de dix réseaux sociaux très populaires une étude portant sur des critères tels que "Organisation et transparence", "Traitement des données utilisateurs", "Sécurité des données", "Droits des utilisateurs, "Protection de la jeunesse" et "Irrégularités dans les CGV". Cette étude a mis en lumière diverses carences dans les domaines concernés. Les plateformes américaines Facebook, LinkedIn et Myspace mais aussi les réseaux allemands que sont Xing ou Stayfriends sont particulièrement mal notés. Pour plus de détails, voir Stiftung Warentest, "Datenschutz bei Onlinenetzwerken", 2010, à l'adresse: http://www.test.de/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-0/.

[39] Quelque 38% des internautes en Suisse indiquent renoncer à publier des données personnelles sur les réseaux sociaux. Voir à ce sujet l'étude de l'Office fédéral de la statistique "Internet dans les ménages suisses. Résultats de l'enquête Omnibus TIC 2010", p. 44, 84.

de croire que ce faisant, ils effacent définitivement leurs contenus (y compris les données se trouvant sur le serveur de l'exploitant du réseau).

L'exemple suivant, tiré de la pratique du PFPDT, illustre les inconvénients que peut entraîner un manque de contrôle à l'égard des données: l'organisateur d'une grande manifestation avait choisi un réseau social pour principal canal de communication, mais l'exploitant de la plateforme a supprimé les pages correspondantes peu de temps avant la manifestation. L'organisateur n'ayant aucun autre moyen que le réseau pour contacter les participants, il s'est trouvé dans l'impossibilité de leur faire parvenir les dernières informations quant au déroulement de la manifestation. Par ailleurs, bien qu'ayant payé pour être présent sur le réseau, l'organisateur n'avait aucun interlocuteur direct chez l'exploitant de la plateforme et s'est donc vu dans l'obligation de faire valoir sa requête via le formulaire général de contact, ce qui n'a pas permis de donner des indications en temps utile aux participants.

4.3.1.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe exhorte les exploitants de plateformes à renforcer la transparence quant au traitement des données, à obtenir un consentement éclairé de la part des personnes concernées par le traitement des données et à indiquer clairement aux utilisateurs le caractère public ou privé des informations les concernant. Il demande par ailleurs que les exploitants de plateformes aident les utilisateurs à comprendre les paramètres par défaut de leur profil. Les utilisateurs devraient pouvoir décider en toute connaissance de cause du degré d'accessibilité de leur données à des tiers ("opt in", "multi-layered access"). Le Conseil de l'Europe ajoute que les exploitants de réseaux sociaux doivent s'abstenir de collecter et de traiter des données relatives à des personnes qui n'utilisent pas leurs services (notamment les adresses e-mail ou les données biométriques) et mettre en place une configuration par défaut et des logiciels de réseau qui respectent la vie privée. Par ailleurs, les utilisateurs ne doivent être autorisés à publier des contenus concernant des tiers qu'avec l'accord de ces derniers.

La proposition du comité consultatif en vue de la révision de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1) relève entre autres que les réseaux sociaux et les blogs requièrent une attention particulière[40]. Elle prévoit ainsi d'élargir les droits des utilisateurs et d'imposer que les services, produits et processus de traitement des données prennent en compte dès leur conception les implications de la protection des données. Elle préconise également de renforcer les pouvoirs des autorités nationales chargées de la protection des données et d'imposer aux Etats membres du Conseil de l'Europe de fournir à celles-ci une assistance en termes de ressources humaines, techniques et financières leur permettant d'exercer leurs pouvoirs de manière indépendante et efficace[41].

Dans le cadre de la réforme de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[42] (qui doit se traduire par un règlement directement applicable dans les Etats membres de l'UE), différentes mesures sont prévues afin d'améliorer le contrôle exercé par les utilisateurs sur leurs données à caractère personnel. Les dispositions proposées comportent des exigences strictes en termes de consentement quant au traitement des données pour une ou plusieurs finalités spécifiques, ainsi que des obligations étendues en termes d'information et de renseignement, notamment pour ce qui a trait à la situation spécifique des enfants. La proposition de règlement prévoit des mesures techniques qui répondent aux principes de la protection des données dès la conception et de la

---

[40] Moderniser la convention 108, T-PD-BUR(2012)01Rev2_fr, p. 3

[41] Rapport abrégé du Comité consultatif de la Convention 108, T-PD (2012) RAP 29 Abr_fr, p. 23 (art. 5), 24 ss (art. 7, 7bis, 8, 8bis), 27 (art. 12bis)

[42] Proposition de Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, p. 31

protection des données par défaut, une minimisation des données ainsi qu'une conservation des données limitée dans le temps[43].

4.3.1.3 Protection conférée par le droit suisse sur la protection des données contre les atteintes à la personnalité découlant du traitement des données

Les contenus mis en ligne par les utilisateurs de réseaux sociaux sont d'une manière générale à considérer comme des données personnelles[44] au sens de la loi fédérale sur la protection des données (LPD, RS 235.1). Souvent, il s'agit même de données personnelles sensibles[45] ou de profils de la personnalité, qui requièrent une protection plus importante que celle accordée aux données personnelles classiques. La loi sur la protection des données protège les personnes physiques et morales notamment contre les atteintes à la personnalité résultant du traitement de données personnelles par des entités privées (art. 12 LPD), ce qui place en principe les exploitants de réseaux sociaux dans le champ d'application de la loi. Ceux-ci étant pour la plupart basés à l'étranger, les prétentions civiles quant à la juridiction compétente sont examinées à la lumière de conventions internationales[46] ou de l'art. 129 ss de la loi fédérale sur le droit international privé[47]. A noter par ailleurs que, selon la jurisprudence du Tribunal fédéral[48], le PFPDT n'est habilité à se pencher sur un cas d'erreurs systémiques que si le traitement des données présente des points d'ancrage prépondérants en Suisse.

Dans le cas précis des réseaux sociaux, on peut imaginer différentes violations des principes généraux en matière de traitement des données énoncés à l'art. 12 LPD. Quelques exemples:

- Si, lors de la collecte de données personnelles, l'exploitant d'un réseau social n'avertit pas qu'il va ensuite les vendre à des tiers afin que ceux-ci puissent les utiliser à des fins de marketing, ou s'il n'indique pas clairement qu'il entend lui-même évaluer et utiliser ces données à des fins publicitaires, il enfreint les principes énoncés à l'art. 4, al. 3 et 4 LPD, selon lesquels le traitement des données doit répondre à une finalité à indiquer à la personne concernée et être reconnaissable pour celle-ci. Si l'exploitant du réseau social transmet les données à des tiers, celles-ci demeurent, pour ce qui est de leur traitement, attachées à la finalité qui a été indiquée lors de leur collecte initiale[49]; en outre, la communication à des tiers de données personnelles sensibles ou de profils de la personnalité est illégale en l'absence de motif justificatif (art. 12, al. 2, let. c LPD).

- La collecte, le traitement et la conservation par des exploitants de réseaux sociaux de données plus nombreuses que nécessaire pour les buts de traitement indiqués par eux peuvent constituer une infraction aux principes de la proportionnalité et de la finalité du traitement des données (art. 4, al. 2 et 3 LPD). Par ailleurs, le principe de la proportionnalité du traitement des données semble important lorsque des données personnelles sensibles (ayant par exemple trait à

---

[43] Art. 6, al. 1, let. a, art. 7, 11, 14, 15, 23 de la proposition de Règlement général de l'UE sur la protection des données, COM(2012) 11 final; voir à ce sujet Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, p. 60 s.

[44] Selon l'art. 3, let a LPD, sont considérées comme données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable. D'après l'ATF 138 II 346 cons. 6.1, une personne est réputée identifiable dès lors que, même si les seules données ne permettent pas de l'identifier de manière univoque, il est possible de déduire son identité des circonstances, du contexte d'une information ou d'informations complémentaires (par exemple s'il est possible de trouver un propriétaire grâce à la localisation de son bien-fonds).

[45] Selon l'art. 3, let. c LPD, on entend par données sensibles les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, sur la santé, la sphère intime ou l'appartenance à une race, sur des mesures d'aide sociale ou sur des poursuites ou sanctions pénales et administratives.

[46] Notamment la Convention du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Convention de Lugano, CL), RS 0.275.12

[47] RS 291; LDIP

[48] Cf. ATF 138 II 346 cons. 3

[49] BSK-DSG, Maurer-Lambrou Urs/Steiner Andrea, 2. Aufl., Basel 2006, art. 4, N. 16, p. 83

l'appartenance à une race, à la sphère intime ou à des opinions religieuses et politiques, art. 3, let. c, LPD) sont utilisées à des fins de marketing.

- Si les données d'un réseau social font l'objet d'un vol ou d'une fuite dus au fait que l'exploitant n'a pas pris les précautions appropriées du point de vue organisationnel et technique, cela est normalement constitutif d'une violation du principe de la sécurité des données (art. 7, al. 1, LPD). Selon les circonstances, on peut par ailleurs déduire du principe de la sécurité des données et du principe de la bonne foi (art. 4, al. 2, LPD) une obligation pour l'exploitant de la plateforme de signaler la fuite ou le vol de données[50].

- Les principes relatifs au traitement des données s'appliquent également aux utilisateurs. Ainsi, si ces derniers chargent sur une plateforme des contacts provenant de leurs répertoires téléphoniques et d'adresses e-mail ou de services de messagerie instantanée, les exploitants de plateformes et ceux qui publient ces données sont tenus, pour respecter le principe de la finalité et faire en sorte que le traitement soit reconnaissable (art. 4, al. 3 et 4, LPD), d'informer les personnes concernées de la collecte des données et de l'utilisation qui va en être faite si cela n'est pas évident au regard des circonstances.

- La LPD ne prévoit certes pas de protection particulière pour les enfants, mais le respect de certains principes de traitement (traitement reconnaissable, bonne foi) exigera, dans le cas de données personnelles relatives à des enfants, une plus grande prudence que celle normalement attendue lorsqu'il est question du traitement de données personnelles relatives à des adultes.

4.3.1.4 Motifs justificatifs – notamment consentement en matière de traitement des données

Un traitement des données portant atteinte à la personnalité peut être justifié par un intérêt public ou privé prépondérant, par la loi ou par le consentement de la victime (art. 13, al. 1, LPD). D'après le Tribunal fédéral, l'invocation d'un motif pour justifier un traitement de données personnelles qui soit contraire aux principes généraux de traitement des données n'est pas à exclure d'emblée, mais les motifs avancés ne doivent être acceptés qu'avec la plus grande circonspection en tenant compte du cas d'espèce[51].

S'agissant du traitement des données par les exploitants de plateformes, le principal motif justificatif est le consentement accordé par les personnes intéressées. Pour pouvoir utiliser les services proposés par les réseaux sociaux, les utilisateurs doivent en général accepter, dans les conditions générales (CG), des clauses relatives au traitement des données. Ce faisant, ils autorisent le traitement des données décrit dans les CG de l'exploitant de la plateforme. Des questions peuvent toutefois se poser quant à la validité et à la portée de ces consentements.

Des problèmes peuvent ainsi survenir lorsque le discernement (art. 16 CC) d'une personne semble pouvoir être remis en question pour ce qui est du contenu du contrat, notamment lorsque des *enfants* autorisent la publication de données personnelles les concernant. Les enfants non capables de discernement sont représentés par leurs parents dans le cadre de l'autorité parentale. On peut présumer que les parents sont en mesure de donner pour le compte de leurs enfants leur consentement à certaines formes de traitement de données (par exemple la publication de la photo d'un jeune enfant sur un réseau social[52]).

Les enfants capables de discernement peuvent agir de manière autonome dès lors qu'il en va de droits qui leur sont strictement personnels, comme c'est le cas des droits en lien étroit avec la personnalité (art. 19*c*, al. 2, CC) en jeu lors du traitement de leurs données personnelles. Ils peuvent

---

[50] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 106, N. 16

[51] Voir ATF 138 II 346 cons. 7.2 avec renvoi à l'ATF 136 II 508 cons. 5.2.4.

[52] S'agissant de la problématique liée aux droits de l'homme dans le cas de telles prises de vue, voir l'arrêt de la CEDH n° 1234/05 "Reklos et Davourlis contre la Grèce" du 15 janvier 2009.

donc en principe révéler des informations les concernant sans avoir à obtenir l'assentiment de leurs parents (pour plus de détails, voir point 4.6.1.3). Mais, pour que le consentement d'un enfant capable de discernement à un traitement des données qui porte atteinte au droit de la personnalité soit valable, celui qui procède au traitement des données doit formuler et présenter les informations requises de manière à ce que l'enfant puisse les comprendre et en apprécier la portée. Par ailleurs, étant donné que l'utilisation faite des données des utilisateurs varie fréquemment, que les déclarations relatives à la protection des données sont parfois opaques et que les conséquences de certains types de traitement de données sont difficilement mesurables, ces consentements peuvent connaître des limitations en termes de contenu.

Devant la longueur et le style rébarbatif qui caractérisent généralement les CG, les utilisateurs renoncent bien souvent à les lire lorsqu'ils concluent un contrat. Si des dispositions relatives au traitement des données sont intégrées aux CG et si les utilisateurs ne les lisent pas lors de la conclusion du contrat (acceptation globale), leur consentement ne couvre pas les clauses inhabituelles et sans lien avec l'objet à moins qu'une mention expresse y fasse référence[53]. En cas de doute, les clauses ambiguës des CG sont interprétées au détriment de celui qui s'en prévaut. Si aucun résultat clair ne ressort de l'interprétation d'une condition d'utilisation, cette dernière doit être interprétée dans le sens le plus favorable à l'utilisateur.

L'utilisateur est réputé avoir consenti à un traitement de données portant atteinte à la personnalité dès lors que son consentement est valable et n'a pas été révoqué[54]. Pour être valable, le consentement doit avoir été accordé librement (c'est-à-dire en dehors de toute tromperie, menace ou contrainte) avant le traitement des données et sur la base d'informations appropriées[55]; il doit en outre être explicite si le traitement porte sur des données sensibles ou sur des profils de la personnalité (art. 4, al. 5 LPD). En ce qui concerne les réseaux sociaux, la forme et le contenu des informations fournies aux utilisateurs jouent à cet égard un rôle important. Celles-ci doivent en effet être claires, concrètes, correctes, faciles d'accès, reconnaissables et non trompeuses[56].

Si les données personnelles à traiter sont de nature classique, le consentement peut être tacite, c'est-à-dire découler du comportement de la personne concernée, par exemple si celle-ci publie elle-même les données la concernant sur des réseaux sociaux[57]. Toutefois, plus les données à traiter sont sensibles, plus le consentement doit être clair[58]. Sur Internet, un clic de souris confirmant l'acceptation d'une clause relative au traitement des données telle que demandée pour l'utilisation de la plupart des réseaux sociaux semble satisfaire aux exigences formelles nécessaires à l'expression d'un consentement explicite[59].

Dès lors que les utilisateurs acceptent les conditions d'utilisation des réseaux sociaux, ils acceptent – à condition qu'ils en aient été dûment informés – le fonctionnement concret du service et donc, par exemple, le fait que des tiers puissent publier sans leur accord préalable des contenus à leur sujet et sur leur profil. Pour autant que l'activité de ces tiers ne soit pas contraire à la législation en vigueur (diffamation, violation du droit à l'image ou du secret professionnel, etc.), les utilisateurs n'ont aucun moyen de s'y opposer. Il est possible de réagir en renonçant à appartenir aux réseaux sociaux pratiquant ce type de communication ouverte ou en supprimant les contenus gênants de son propre

---

[53] BSK-DSG, Rampini Corrado, 2. Aufl., Basel 2006, Art. 13, p. 194 N. 13 ainsi que Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 112 N. 90

[54] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 386, N. 3

[55] Avis très critiques quant à la politique de confidentialité de Facebook: Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010, p. 56, 59 et Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, p. 63 s.

[56] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 106, N. 75

[57] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 108, N. 79

[58] FF 2003 1939 ss

[59] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 108, N. 78

profil. Toutefois, ces suppressions ne sont que d'une utilité limitée si les contenus en cause ont suscité un vif intérêt de la communauté et ont donné lieu à de nombreuses copies ou à la création de nombreux liens.

4.3.1.5 Données personnelles accessibles au public

Sont réputées accessibles au public les données personnelles pouvant être consultées par un nombre élevé de personnes sans obstacle majeur. Si les utilisateurs de réseaux sociaux mettent en ligne des données les concernant, il n'y a en règle générale pas d'atteinte à la personnalité lorsque ceux-ci ont rendu lesdites données accessibles à tout un chacun et ne se sont pas formellement opposés à leur traitement (art. 12, al. 3, LPD). Il en va de même en cas de communication transfrontière des données personnelles dans des pays ne disposant pas d'une législation assurant un niveau de protection adéquat des données (art. 6, al. 2, let. f, LPD).

En principe, les utilisateurs peuvent décider de l'accessibilité de leurs informations en jouant sur les paramètres proposés. Sur la plupart des réseaux sociaux, différentes formes de communications dotées de protections plus ou moins avancées de la sphère privée sont en effet proposées par les exploitants afin de couvrir un spectre allant des communications privées aux communications de masse. Si les utilisateurs sont dûment informés des possibilités qui s'offrent à eux en termes de formes de communication et de protection de la sphère privée, il est possible de déduire de la forme de communication pour laquelle ils ont opté s'ils entendaient procéder à une communication privée ou s'ils souhaitaient que les informations soient accessibles au public.

Le traitement de données personnelles rendues accessibles au public peut toutefois constituer une atteinte à la personnalité si les données sont utilisées à des fins et dans des circonstances pour lesquelles une appréciation objective permet de dire que l'accès au public ne s'applique pas[60]. Ce point est important pour les données rendues accessibles au public sur Internet notamment du fait de la facilité avec laquelle elles peuvent être consultées[61]. Lorsque quelqu'un rend ses photos accessibles au public sur un réseau social, celles-ci peuvent en principe être consultées par tout un chacun. Pour autant, leur utilisation sans l'accord préalable de l'auteur, par exemple dans le cadre d'une campagne publicitaire, n'est pas autorisée. L'utilisation d'images de ce type dans le cadre d'articles ou de comptes rendus classiques dans les médias peut également poser problème.[62]

Dans ce contexte, il s'agit dès lors de déterminer au cas par cas si le téléchargement et l'enregistrement – sans demande préalable d'autorisation – de contenus en provenance de profils tiers correspondent encore au but dans lequel les informations ont été publiées. Le principe veut que les autres membres du réseau social aient dans tous les cas à se conformer aux mêmes principes de protection des données que l'exploitant de la plateforme.

4.3.1.6 Problématique du transfert de droits exhaustifs d'utilisation aux exploitants de plateformes

Il y a lieu de s'interroger sur la validité d'un contrat conclu entre les utilisateurs et les exploitants de plateformes et prévoyant expressément la conservation et l'utilisation non limitées dans le temps de tous les contenus publiés par les utilisateurs sur les réseaux sociaux. Il n'est en effet pas exclu qu'un tel contrat puisse dans certains cas être qualifié de transaction juridique contraire au droit de la personnalité (art. 19, al. 2, et art. 20, al. 1, CO, art. 27, al. 2, CC), d'autant plus que les données publiées sur des réseaux sociaux et faisant ensuite l'objet de liens constituent souvent des données

---

[60] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, p. 381, N. 76.

[61] BSK-DSG, Rampini Corrado, 2. Aufl., Basel 2006, Art. 12, N. 18, p. 187 s.

[62] En sa qualité d'organe d'autocontrôle institutionnalisé en matière de journalisme, le Conseil suisse de la presse a à plusieurs reprises mis en demeure les représentants de la presse de faire preuve de retenue lors de l'utilisation d'informations publiées par des particuliers sur Internet. Une personne qui publie des photos sur un blog ou sur une autre plateforme accessible à tout un chacun n'approuve pas du même coup leur réutilisation par un autre média. Les journalistes doivent mettre soigneusement en balance la protection de la sphère privée et le droit à l'information du grand public; voir à ce sujet l'avis du Conseil suisse de la presse n° 43/2010 du 1er septembre 2010: Internet und Privatsphäre; www.presserat.ch/28340.htm.

sensibles ou des profils de la personnalité et que la proportionnalité entre la prestation et sa contrepartie peut être mise en doute (offre d'une infrastructure de communications de la part de l'exploitant de la plateforme contre transfert très complet de droits d'utilisation des données personnelles de la part des utilisateurs)[63]. Dans ce contexte, l'influence déterminante exercée par les utilisateurs lorsqu'il s'agit de décider des données à publier sur les réseaux sociaux joue toutefois un rôle important.

4.3.1.7 Autres instruments de protection offerts par le droit suisse

Les instruments de protection offerts par le droit suisse contre les méthodes opaques de collecte, de traitement et de publication de données par les exploitants de réseaux sociaux ne se limitent néanmoins pas à la loi sur la protection des données. Ils incluent notamment les possibilités offertes par le droit privé en matière de **contestation de contrat** en cas d'erreur importante (art. 23 ss CO) ou de dol (art. 28 CO)[64].

En outre, le recours à des conditions générales (CG) abusives peut constituer une pratique déloyale au sens de l'art. 8 de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD; RS 241). Depuis sa dernière révision (1er juillet 2012), la LCD stipule ainsi qu'agit de façon déloyale celui qui, notamment, utilise des conditions générales qui, en contradiction avec les règles de la bonne foi prévoient, au détriment du consommateur, une disproportion notable et injustifiée entre les droits et les obligations découlant du contrat[65]. Aux termes du nouvel art. 8 LCD, il n'est donc plus nécessaire que les CG soient de nature à provoquer une erreur pour pouvoir être qualifiées d'abusives, ce qui rend possible un contrôle ouvert du contenu par le consommateur[66]. S'agissant spécifiquement des CG des exploitants de réseaux sociaux, la question est de savoir si les clauses autorisant une adaptation unilatérale des conditions d'utilisation par les exploitants de plateformes sans préavis et sans communication personnelle sont conformes au nouvel art. 8 LCD.

La violation répétée et non justifiée des principes de traitement prévus par la loi sur la protection des données pourrait en outre se révéler déloyale au sens de la clause générale de l'art. 2 LCD si celui qui traite les données parvient à se ménager un avantage sur la concurrence au travers de la violation de la LPD[67]. Pensons notamment au traitement et à l'utilisation à des fins publicitaires de données personnelles obtenues sur des réseaux sociaux de manière contraire à la loi sur la protection des données.

4.3.1.8 Appréciation

Force est de constater que, d'une manière générale, le droit suisse en vigueur offre, grâce à la formulation ouverte de ses prescriptions, une protection relativement importante contre le traitement souvent problématique des données sur les réseaux sociaux. Un certain nombre d'obstacles, également valables pour les réseaux sociaux, empêchent toutefois d'assurer une protection réellement efficace des données. Ils résident par exemple dans la difficulté qu'il y a bien souvent à identifier les traitements de données problématiques, dans la progression exponentielle des traitements de données ayant une portée internationale (ce qui complique sérieusement les enquêtes et l'application de la législation, voir à ce sujet le chapitre 5 ci-après) et dans la probabilité

---

[63] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6. Aufl., Bern 2012, p. 171 ss

[64] Au sujet de ces voies de recours, voir Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 p. 108, 111-114.

[65] RO 2011 4910

[66] En supprimant le critère de la volonté d'induire en erreur, le législateur a voulu ouvrir la voie à un contrôle ouvert du contenu (FF 2009 5566).

[67] Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, p. 65 s.

relativement faible de sanctions. A cela s'ajoute le fait que les utilisateurs font rarement valoir leurs droits et que le PFPDT touche à ses limites tant les cas portés à sa connaissance sont nombreux[68].

Un potentiel d'amélioration existerait par ailleurs à travers la mise en place de paramètres plus propices à la protection des données (dès la conception, ou *privacy by design*, et par défaut, ou *privacy by default*) et une formulation plus compréhensible des conditions relatives à la protection des données. Dans son rapport d'évaluation de la LPD, le Conseil fédéral envisage un approfondissement de la notion de *privacy by design*, la promotion de technologies plus favorables à la protection des données et la mise en place de mesures visant à améliorer le contrôle et la maîtrise des données.[69]

4.3.2 Création et exploitation de profils d'utilisateur étendus (data mining)

4.3.2.1 Contexte

Lors de leur inscription, mais aussi du fait de leurs activités sur les réseaux sociaux et des métadonnées générées par l'utilisation d'Internet (durée de connexion, origine géographique approximative de l'adresse IP, durée de présence et mouvements sur le site Web etc.), les utilisateurs révèlent une foule d'informations les concernant. Le placement du bouton "J'aime" sur des sites tiers permet ainsi à Facebook d'obtenir des données relatives aux visiteurs de ces sites.

Mais il est rare que les gestionnaires de plateformes indiquent clairement l'usage fait des informations ainsi collectées. Le recoupement de toutes les informations laissées par l'utilisation de réseaux sociaux peut permettre la création de profils très parlants quoique non exempts d'erreurs. En cas de revente de paquets de données par les exploitants de plateformes, des tiers peuvent être en mesure d'exploiter ces profils dans le but de proposer des biens et des services, ce qui est doublement problématique compte tenu de l'instrumentalisation économique de ces données et du potentiel de discrimination pouvant en découler.

4.3.2.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

La Recommandation du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage [70] traite de la surveillance, de la collecte et de la mise en relation de données à caractère personnel sur Internet et demande que les utilisateurs bénéficient d'une protection étendue dans la mesure où les réseaux sociaux sont une source importante pour ce type de traitement de données. A ce titre, le Conseil de l'Europe dénonce le manque de transparence du profilage, son potentiel de discrimination à l'égard des personnes concernées et la protection insuffisante des enfants contre la collecte de données de ce type. La Recommandation demande par ailleurs que l'accès aux biens et aux services (et aux informations les concernant) soit possible sans que des données à caractère personnel n'aient à être communiquées au fournisseur du bien ou au prestataire du service. Il est en outre demandé que les prestataires de services dans le domaine de la société de l'information garantissent un accès non profilé aux informations relatives à leurs services.

L'article 20 de la Proposition de règlement général de l'UE sur la protection des données[71] a pour ambition de protéger les personnes physiques (sous réserve de certaines exceptions) contre un traitement automatisé de leurs données visant à analyser ou à prévoir certaines caractéristiques liées à leur personne ou à leur situation. Pour bénéficier de cette protection, les personnes concernées doivent être affectées de manière significative par ledit traitement ou se voir imposer des effets

---

[68] Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données (FF 2012 259-265, 267).

[69] Rapport du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données, point 5.2.2 (FF 2012 268)

[70] Recommandation CM/Rec(2010)13

[71] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final

juridiques par celui-ci. Selon l'art. 19, par. 2 de la Proposition, lorsque les données à caractère personnel sont traitées à des fins de marketing direct, les personnes concernées ont le droit de s'y opposer gratuitement.

Pour leur part, les autorités américaines veillant sur la concurrence et la protection des consommateurs (Federal Trade Commission, FTC) ont exigé des prestataires Internet la mise en place d'une option "Do-Not-Track" laissant aux consommateurs le soin de décider quelles informations relatives à leurs activités en ligne peuvent être partagées, avec qui et dans quel but (notamment pour ce qui est des mesures de marketing direct) [72].

Le Trans Atlantic Consumer Dialogue (TACD)[73] a publié une résolution relative aux réseaux sociaux[74]. Il milite pour l'adoption de lois prévoyant, entre autres, que les réseaux sociaux ne subordonnent pas l'accès à leurs services à l'acceptation par les utilisateurs d'un traitement de leurs données qui soit destiné à des fins de marketing. Il demande en outre que l'accord explicite de utilisateurs soit indispensable pour que puisse avoir lieu un traitement des données destiné à des fins de marketing et que les enfants de moins de 16 ans ainsi que les sites Web essentiellement visités par des enfants de cette tranche d'âge soient par principe exclus de toute mesure publicitaire.

4.3.2.3 La législation en Suisse

La collecte et l'assemblage des données générées par l'activité des utilisateurs conduisent bien souvent à la création de profils de la personnalité au sens de l'art. 3, let. d LPD. La loi sur la protection des données formule des exigences spécifiques pour ce qui est du traitement des profils de la personnalité (art. 4, al. 5, art. 11*a*, al. 3, let. a, art. 12, al. 2, let. c, art. 14 LPD).

Si les exploitants de plateformes créent des profils de la personnalité en assemblant des données, cet assemblage est susceptible de violer le principe de la bonne foi (art. 4, al. 2, LPD). En outre, le maître de fichier a l'obligation d'informer les personnes concernées de toute collecte de profils de la personnalité (art. 14 LPD). D'autre part, le transfert de données d'utilisateurs à Facebook via le placement du bouton "J'aime" sur des sites Web tiers peut également contrevenir au principe du traitement reconnaissable (art. 4, al. 4, LPD) en raison d'un manque d'information des internautes à propos du transfert desdites données. Par ailleurs, l'indication d'objectifs de traitement très généraux au moment de la collecte des données, par exemple la création et le traitement de profils utilisateurs "à des fins de marketing", est susceptible de ne pas satisfaire au principe de finalité (art. 4, al. 3, LPD) dans la mesure où, au moment de la collecte, les utilisateurs n'ont pas suffisamment conscience de l'utilisation qui sera faite ultérieurement des données qu'ils ont réunies dans leur profil.

La collecte d'une grande variété de données personnelles et leur recoupement afin de créer des profils de la personnalité peuvent également contrevenir au principe de la proportionnalité du traitement des données (art. 4, al. 2, LPD). Au-delà de cela, la création de profils de la personnalité peut également faire entorse au principe de l'exactitude des données (art. 5 LPD) puisque la collecte,

---

[72] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, FTC Report March 2012, disponible sous: http://www.ftc.gov/opa/2012/03/privacyframework.shtm. Portant sur la protection de la sphère privée des consommateurs sur Internet, le rapport formule des recommandations à l'intention des prestataires Internet. Il demande, entre autres, que les entreprises développent leurs services en ligne de manière à ce qu'une protection élevée de la sphère privée soit mise en place par défaut (privacy by design) et que les consommateurs soient dûment informés du but, de la portée et du type d'utilisation dont leurs données font l'objet.

[73] Le TACD est un forum regroupant des associations de consommateurs américaines et européennes qui élabore des recommandations en matière de protection des consommateurs à l'intention du gouvernement américain et de l'Union européenne; voir sous: http://www.tacd.org/.

[74] Resolution on Social Networking of May 2010, Doc No. Infosoc 43-09; disponible sous (en anglais): http://tacd.org/index.php?option=com_docman&task=cat_view&gid=83&Itemid=40 .

l'assemblage et l'évaluation automatisés de données se traduisent par la perte du contexte d'origine dans lequel les données ont été obtenues, ce qui peut entraîner des résultats erronés[75].

Le consentement des personnes à l'élaboration de profils de la personnalité doit être exprimé de manière explicite (art 4, al. 5 LPD), ce qui accroît les exigences quant aux informations à fournir sur la création, l'utilisation et la transmission de profils de la personnalité, notamment lorsque celles-ci sont contenues dans les CGV. Le caractère explicite d'un consentement peut ainsi être mis en doute si des objectifs inhabituels de traitement des données ou de transfert à des tiers ne sont pas expressément mis en avant. Le consentement doit être explicite si un traitement des profils de la personnalité contraire aux principes de traitement ou si une communication de profils de la personnalité à des tiers doit être justifié(e) par le consentement des personnes concernées (art. 13, al. 1, en lien avec art. 4, al. 5, LPD). Ce point revêt une importance particulière dans le cas des réseaux sociaux étant donné que leurs modèles commerciaux sont généralement basés sur la vente de profils d'utilisateurs, ce qui doit être qualifié de communication de données à des tiers.

La LPD ne prévoit pas de protection particulière des enfants contre la création et le traitement de profils de la personnalité. En la matière s'appliquent toutefois à nouveau les spécificités inhérentes au consentement au traitement des données personnelles d'un enfant (voir point. 4.3.1.3 plus haut). Il n'existe par ailleurs pas d'interdiction de principe en ce qui concerne les activités publicitaires ciblant les enfants de moins de 16 ans ou les sites Internet s'adressant à eux.

Le **secret des télécommunications** prévu par l'art. 43 LTC et par l'art. 321ter CP protège la confidentialité des télécommunications. Il n'offre toutefois pas un rempart inviolable contre la création de profils de la personnalité. Ce n'est en effet que dans de rares exceptions, à savoir lorsque les exploitants de plateformes transportent des informations entre plusieurs utilisateurs, que le secret des télécommunications pourrait protéger les utilisateurs contre le transfert à des tiers des données faisant l'objet desdites télécommunications et contre leur utilisation en vue de la création de profils de la personnalité.

4.3.3 Pas de droit à l'oubli

4.3.3.1 Contexte

Le manque de contrôle exercé par les utilisateurs sur les données les concernant sur les réseaux sociaux se manifeste également par la difficulté qu'il y a à supprimer définitivement les comptes utilisateurs. Dans la plupart des cas, la suppression d'un compte n'entraîne que la désactivation d'un profil, les données restant quant à elles stockées sur le serveur de l'exploitant de la plateforme. La suppression définitive de tous les contenus est certes souvent possible, mais pas toujours. Et la procédure se révèle tellement compliquée – voire incompréhensible – qu'elle produit un effet dissuasif sur les utilisateurs. En outre, les utilisateurs actifs sont susceptibles de laisser un grand nombre d'informations et de contenus sur d'autres pages et profils du réseau, informations et contenus qu'il est en pratique quasiment impossible d'effacer dans leur intégralité.

D'autre part, l'éventuelle suppression d'un profil d'origine voit ses effets limités par la possibilité, sur certaines plateformes, de télécharger et d'enregistrer des données en provenance de profils d'autres utilisateurs, ce qui peut se traduire par une multiplication des fichiers privés. Ainsi, même lorsqu'un utilisateur supprime son profil d'origine, rien ne dit que ses données ne restent pas stockées ailleurs. Les tiers ont du reste d'autres moyens pour archiver des données (captures d'écran, par exemple) et, partant, les republier ultérieurement.

[75] Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 p. 108, 109.

4.3.3.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

La Recommandation sur les services de réseaux sociaux du Conseil de l'Europe et la Proposition de règlement général de l'UE sur la protection des données[76] prévoient dans certaines circonstances un droit à l'oubli numérique, la suppression des données à caractère personnel et l'interdiction de toute publication ultérieure de données [77]. Il est ainsi notamment prévu un droit des enfants à l'oubli et à l'effacement des données[78].

Le projet de révision de la loi allemande sur les télécommunications prévoit lui aussi un droit à l'effacement des comptes d'utilisateurs et de tous les contenus générés par les utilisateurs sur les réseaux sociaux[79].

4.3.3.3 La législation en Suisse

Le droit à l'oubli sur les réseaux sociaux concerne en premier lieu la possibilité de supprimer les contenus préalablement publiés par les utilisateurs de réseaux sociaux. Il s'agit là d'un droit à la suppression qui peut être déduit de la loi sur la protection des données et de la protection de la personnalité offerte par le code civil.

La **loi sur la protection des données** interdit tout traitement de données à caractère personnel allant à l'encontre de la volonté expresse d'une personne (art. 12, al. 2, let. b, LPD). Etant donné que la conservation et l'archivage de données personnelles peuvent faire l'objet d'une interdiction expresse de traitement, il est normalement possible, sur la base du droit d'opposition, d'exiger une suppression totale ou partielle de données personnelles[80]. Il est également possible de retirer le consentement au sens de l'art 13, al. 1 LPD, qui constitue un motif justifiant un traitement des données portant atteinte à la personnalité. Ce retrait ne porte toutefois que sur les traitements de données à venir et non sur ceux qui ont déjà été effectués[81]. De même, si le consentement a été donné à une conservation de données non limitée dans le temps, il est par principe possible de le retirer pour les stockages de données à venir.

Si des tiers contreviennent, sans motif justificatif, aux principes de traitement posés par la loi sur la protection des données, il peut en résulter, en vertu de l'art. 15, al 1, LPD, un droit à la suppression des données concernées. Est par exemple concerné le cas où d'autres utilisateurs publieraient des données personnelles de la personne concernée sur des réseaux sociaux sans que cela ne soit reconnaissable par elle (art. 4, al. 2 et 4 LPD). Il est également possible que des utilisateurs communiquent à d'autres membres du réseau ou à des entreprises tierces des données personnelles sensibles ou des profils de la personnalité sans motif justificatif (art. 12, al. 2, let. c, LPD), qu'ils traitent des données personnelles d'autrui dans un but autre que celui pouvant être déduit lors de leur collecte (par exemple lorsque des avis émis sur un forum ou à l'occasion d'une discussion sur un réseau social sont repris et réutilisés dans un contexte étranger à la finalité initiale)[82] ou qu'ils traitent des données personnelles contre la volonté expresse de la personne concernée (art. 12, al. 2, let. b, LPD).

La **protection de la personnalité telle que prévue par le code civil** (art. 28 CC) donne également des arguments plaidant en faveur d'un droit à la suppression mais qui dépendent de l'évaluation faite des intérêts en jeu et de l'existence ou non de motifs justificatifs écartant l'illicéité d'une atteinte à la

---

[76] Art. 17 de la Proposition de règlement général de l'UE sur la protection des données, COM(2012) 11 final

[77] Voir à ce sujet Treyer Tobias, Das "Recht auf Vergessen" im digitalen Zeitalter, in: medialex 2013, p. 61 s.

[78] Art. 17, al. 1 de la Proposition de règlement général sur la protection des données, COM(2012) 11 final. Voir également la Déclaration du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur Internet.

[79] Gesetzesentwurf Änderung Telemediengesetz, 17/6765

[80] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 32, p. 362

[81] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 104 s., p. 118 s.

[82] Cela pourrait se révéler contraire aux principes de la finalité et de l'exactitude des données (art. 4, al. 3 et 5 LPD).

personnalité. L'art. 28 CC comporte différents éléments. Il est ainsi possible de faire valoir un droit à l'oubli en invoquant la protection de l'intégrité psychique, de la sphère privée, de l'honneur ou du droit à l'image, au nom ou à la parole. L'art. 28 CC interdit à des tiers de se procurer ou de publier des contenus relevant de la sphère secrète ou privée ou des photographies de personnes sans leur consentement (ou sans autre motif justificatif valable). De son côté, l'art. 28*a*, al. 1, ch. 2 CC donne aux personnes concernées le droit de faire cesser une atteinte en cours, par exemple via la suppression de contenus portant atteinte à la personnalité sur Internet. Si des utilisateurs publient des contenus les concernant sur des réseaux sociaux et si ces contenus sont ensuite traités par des tiers, il convient alors de savoir que les consentements donnés pour un but donné ne s'appliquent pas à d'autres buts d'utilisation[83]. Du point du vue du code civil, posent ainsi problème l'utilisation, à titre de pseudo-citation, d'un avis émis par une personne[84], l'utilisation de photographies publiées par une personne sans son consentement préalable et dans un contexte ou dans un but autres que ceux d'origine[85], ou encore l'utilisation du nom d'une personne d'une manière portant atteinte à sa personnalité[86]. On peut également imaginer qu'un consentement octroyé à un moment donné est susceptible d'être retiré, sachant toutefois que l'existence d'un droit à la suppression dépend de l'évaluation concrète qui est faite des intérêts en jeu[87].

S'agissant de l'existence ou non d'un droit à la suppression, il importe également de savoir sous quelle forme la personne concernée a publié ses contenus (communication privée ou publique?), quelle est la nature desdits contenus (relèvent-ils de la sphère secrète, privée ou publique?) et qui est la personne concernée. Si les contenus ont été rendus accessibles à tout un chacun par la personne concernée elle-même (au sens de l'art. 12, al. 3, LPD), cette circonstance sera à l'avantage de l'exploitant de la plateforme lors de l'évaluation des intérêts en jeu faite afin de déterminer l'existence ou non d'un droit à la suppression (art 13, al. 1, LPD; art. 28, al. 2, CC). Toutefois, plus les données auront un caractère relatif à la personnalité, plus l'intérêt de la personne concernée sera mis en avant lorsqu'il s'agira de déterminer l'existence ou non d'un droit à la suppression, et ce, même si c'est la personne concernée qui les a elle-même publiées à un autre moment. Si les personnes concernées sont des personnages appartenant de manière absolue ou relative à l'histoire contemporaine[88] ou des agents publics, la nécessité de préserver le droit à l'information du grand public peut s'opposer à la suppression des contenus. Mais, même dans leur cas, le passage du temps peut faire renaître un droit à l'oubli[89]. Si des données personnelles ayant été publiées alors que la personne concernée était encore un enfant doivent être supprimées, l'atteinte à sa personnalité est, au regard de la nécessité particulière de protection dévolue aux enfants et du discernement parfois limité qui est le leur, plus rapidement constituée que dans le cas de données relatives à des adultes.

Il existe un autre problème relevant du droit à l'oubli, à savoir celui de la "succession numérique", autrement dit du traitement des données laissées sur Internet par des personnes décédées. Le droit

---

[83] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 48, p. 269

[84] Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: medialex 2011 p. 197, 199

[85] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 20, p. 260 en précisant que les retouches d'images, photomontages et manipulations photographiques devenus courants dans le monde numérique, mais aussi l'utilisation d'images d'archives dans un contexte tout autre que celui du moment auquel la photographie a été faite, conduisent immanquablement à des problèmes.

[86] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 1, p. 320

[87] BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 48, p. 259

[88] Les sportifs, responsables politiques, artistes, leaders économiques et autres personnalités influentes sont des personnages appartenant de manière absolue à l'histoire contemporaine; les personnages appartenant de manière relative à l'histoire contemporaine sont ceux suscitant l'intérêt du grand public à l'occasion d'un évènement ponctuel. Voir BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 52, p. 271

[89] Voir par exemple l'ATF 109 II 353 cons. 3 ainsi que BSK-ZGB I, Meili Andreas, 4. Aufl., Basel 2010, Art. 28, N. 52, p. 271

des successions, le droit des personnes et la loi sur la protection des données n'offrent en la matière qu'une réponse incomplète[90].

L'analyse montre que la législation en vigueur garantit dans une certaine mesure un droit à l'oubli, lequel peut toutefois, selon les intérêts en jeu (par exemple la nécessité d'informer le grand public ou encore la proportionnalité des mesures imposées aux exploitants de plateformes), être significativement limité[91].

Bien que des moyens juridiques existent pour faire disparaître certains contenus, il peut toutefois se révéler extrêmement compliqué de parvenir à leur suppression totale des réseaux sociaux. Et le téléchargement ou la réutilisation des contenus par des tiers ne fait qu'exacerber le problème.

Dans son rapport d'évaluation de la LPD, le Conseil fédéral a envisagé de préciser le droit relatif à l'oubli.[92]

4.3.4 Accès aux données des profils d'utilisateurs via les moteurs de recherche

4.3.4.1 Contexte

Il est possible, par des métadonnées intégrées aux sites Web, d'ordonner aux robots de recherche de ne pas reprendre certains contenus ou certaines pages dans leur index ou dans leur mémoire cache. Les exploitants de réseaux sociaux peuvent donc configurer en conséquence l'accès aux données des utilisateurs par les moteurs de recherche. Le problème vient alors des réseaux sociaux qui ne permettent pas à leurs utilisateurs de décider si les données qu'ils ont publiées sur des réseaux sociaux peuvent ou non être trouvées par des moteurs de recherche, qu'ils soient internes ou externes.

4.3.4.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

La Recommandation du Conseil de l'Europe sur la protection des droits de l'homme dans le contexte des moteurs de recherche[93] demande que les utilisateurs aient le droit d'exiger des fournisseurs de moteurs de recherche la suppression immédiate de leurs données personnelles si celles-ci restent stockées par les moteurs de recherche dans des copies de sites Web originaux déjà supprimés. Par ailleurs, les utilisateurs devraient pouvoir exiger des fournisseurs de moteurs de recherche qu'ils suppriment ou qu'ils corrigent les données traitées les concernant. Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe demande en outre que les utilisateurs aient la possibilité de prendre une décision éclairée quant à l'indexation de leurs données et qu'ils aient le droit de demander la suppression des données les concernant dans les mémoires cache des moteurs de recherche.

Le projet de révision de la loi allemande sur les médias électroniques demande lui aussi que les comptes d'utilisateurs et les contenus générés par les utilisateurs ne puissent être trouvés dans des moteurs de recherche externes qu'après leur consentement[94].

---

[90] A ce sujet, voir Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012.

[91] Selon la jurisprudence de la Cour européenne des droits de l'homme, la CEDH ne confère aux personnes concernées aucun droit à la suppression de publications illicites stockées dans des archives en ligne. Il n'appartient pas à la justice d'éliminer toutes les traces de publications illicites: arrêt de la CEDH "Wegrzynowski & Smolczewski c. Pologne" (requête n° 33846/07) du 16 juillet 2013, point 65.

[92] Rapport du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données, point 5.2.2 (FF 2012 268)

[93] Recommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche

[94] Gesetzesentwurf Änderung Telemediengesetz, 17/6765

4.3.4.3 La législation en Suisse

En autorisant les moteurs de recherche à accéder aux données personnelles de leurs membres, les réseaux sociaux effectuent une communication de données au sens de la loi sur la protection des données (art. 3, let. e et f, LPD), communication qui est soumise aux principes relatifs au traitement des données. Le principe selon lequel la collecte des données doit être reconnaissable (art. 4, al. 4, LPD) garantit aux personnes concernées le droit d'être informées de l'accessibilité aux moteurs de recherche des données personnelles qu'elles ont publiées sur les réseaux sociaux à condition que ladite accessibilité ne soit pas déjà évidente au vu des circonstances.

Compte tenu de la profusion de données publiées sur les réseaux sociaux et de leur caractère souvent très personnel, la probabilité est grande qu'elles constituent des données sensibles ou des profils de la personnalité. Dans la majorité des cas, du fait de l'absence d'autres motifs justificatifs (art. 13, al. 1, LPD), l'obtention d'un consentement explicite (art. 4, al. 5, LPD) à l'accessibilité des données personnelles aux moteurs de recherche est nécessaire. Le principe de la finalité implique que les tiers, dans le cas présent les fournisseurs de moteurs de recherche, soient eux aussi tenus par l'objectif de traitement indiqué à la collecte des données[95].

Si les fournisseurs de moteurs de recherche contournent les limitations imposées par les exploitants de réseaux sociaux aux robots de recherche pour ce qui est de l'accès aux données des utilisateurs et s'ils collectent malgré tout ces données pour les rendre ensuite librement accessibles, cette pratique doit être qualifiée, en raison de son caractère secret[96], de collecte de données illicite (art. 4, al. 1, LPD).

4.3.5 Problèmes liés à la reconnaissance d'images

4.3.5.1 Contexte

Les photographies téléchargées sur les réseaux sociaux et comportant des personnes identifiables ainsi que des indications relatives à leur profil d'utilisateur peuvent contribuer au développement et à l'amélioration des logiciels de reconnaissance faciale. Ceux-ci sont alors susceptibles d'exploiter ces données afin de les comparer avec des personnes se trouvant sur des photographies publiées ultérieurement et d'affecter ces images à un profil d'utilisateur. Si des tiers téléchargent sur une plateforme des images montrant d'autres membres du réseau, les logiciels de cette nature sont en mesure de suggérer un lien entre les personnes ainsi représentées et des profils existants ("tag suggest")[97]. En outre, les logiciels de reconnaissance faciale sont capables d'identifier les personnes souhaitant pourtant conserver leur anonymat (par exemple sur un site Web de rencontres) ou, grâce à la photo se trouvant sur le réseau social et au nom qui y est attaché, d'établir un lien avec leur curriculum vitae publié sur le site Internet de l'entreprise pour laquelle elles travaillent.

La reconnaissance automatique d'autres informations contenues sur des images sur la foi des contours, des couleurs ou de la structure des objets représentés (*content based image retrieval*) va dans une direction similaire. La fonction peut identifier des bâtiments ou des éléments précis et éventuellement conduire à la localisation géographique d'un cliché, à la publication d'adresses, à du harcèlement ou à d'autres agissements dommageables ou illégaux.

---

[95] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 47, p. 95

[96] La collecte secrète de données va à l'encontre des principes de la bonne foi et du traitement reconnaissable des données (art. 4, al. 2 et 4 LPD).

[97] Par exemple, la personne A vérifie avec un logiciel de reconnaissance faciale les images réalisées par la personne B et reconnaît alors la personne C, puis la nomme sur la photo.

4.3.5.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Sur injonction du préposé irlandais à la protection des données, Facebook a désactivé son logiciel de reconnaissance faciale au sein de l'Union européenne[98]. Un compromis qui fait suite à une vérification générale de la compatibilité des services de la société avec le droit irlandais et européen sur la protection des données. Et le PFPDT estime que cet accord s'applique également à la Suisse.

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe exige que les technologies ayant une influence déterminante sur la sphère privée des utilisateurs (car reposant par exemple sur le traitement de données sensibles ou biométriques, à l'instar des logiciels de reconnaissance faciale) garantissent un niveau élevé de protection desdites données et qu'ils ne puissent pas être mis en œuvre sans le consentement des utilisateurs.

Dans le cadre d'un avis relatif à la reconnaissance faciale appliquée aux services en ligne et mobiles[99], le groupe de travail "Article 29", un organe consultatif indépendant de la Commission européenne, s'est penché sur les risques inhérents à ces technologies en termes de protection des données et a formulé à l'intention des services traitant des données des recommandations soulignant la nécessité d'obtenir un consentement valable de la part des utilisateurs, de crypter les données transmises et de les conserver de manière sûre.

4.3.5.3 La législation en Suisse

Pour que les logiciels de reconnaissance faciale puissent être utilisés sur les réseaux sociaux, il faut en premier lieu que des photographies soient publiées sur des plateformes de ce type. Du fait du droit à l'image qui découle de l'art. 28, al. 1, CC, tout individu est protégé contre une utilisation illicite de sa propre image[100]. Il est par principe interdit de publier une photo de quelqu'un, déjà existante ou non, sans son consentement préalable ou a posteriori; en outre, le consentement obtenu à la prise d'une photo ne couvre pas tous les types de publication ultérieure envisageables, mais uniquement celui qui pouvait être déduit par la personne concernée au moment de la prise de vue[101].

Le droit sur la protection des données, dont les dispositions de droit privé viennent compléter et concrétiser la protection générale de la personnalité[102], protège contre toute publication de photographies d'une personne[103] à l'insu de celle-ci. Le principe selon lequel la collecte de données doit être reconnaissable (art. 4, al. 4, LPD) impose que les personnes figurant sur des images doivent au moins pouvoir déduire des circonstances que des photos d'elles sont publiées sur des réseaux sociaux. De plus, en vertu du principe de la finalité, les données personnelles ne peuvent être traitées que dans le but qui a été arrêté au moment de leur collecte. En l'absence de motifs justificatifs (art. 13, al. 1, LPD), la publication de photographies d'une personne sur des réseaux sociaux n'est de ce fait autorisée que si, lors de la prise des photographies, il était reconnaissable que celles-ci étaient destinées à être publiées sur des réseaux sociaux.

Si des photographies de personnes sont publiées sur des réseaux sociaux, leur analyse et leur mise en relation avec des profils d'utilisateur au moyen de logiciels de reconnaissance faciale ne sont

---

[98] Report of Re-Audit Facebook Ireland Ltd of the Data Protection Commissioner du 21 septembre 2012; disponible à l'adresse: http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f; Driessen Benedikt / Dürmuth Markus, Anonymität und Gesichtserkennung, in: digma 2013, p. 54

[99] Avis 00727/12/FR WP 192 du groupe de travail "Article 49"

[100] Bächli Marc, Das Recht am eigenen Bild, Basel 2002, p. 69

[101] A moins qu'il existe un motif justificatif valable au sens de l'art. 28, al. 2 CC. Le droit à l'image est limité par des intérêts de publication justifiés (liberté d'expression selon l'art. 10 CEDH); concernant la jurisprudence de Strasbourg dans ce domaine, voir Zeller Franz, Das eigene Bild und sein begrenzter Schutz, in: digma 2013/2, p. 50 s.

[102] Schweizer Michael, Recht am Wort, Bern 2012, p. 209

[103] Sont également considérées comme des données personnelles au regard de la loi sur la protection des données des images de personnes s'il est possible de les relier à une personne; les photographies sont par conséquent elles aussi concernées.

autorisées que si les personnes concernées ont été informées de ce type d'utilisation[104], ce qui n'est jamais le cas pour les photographies publiées par des tiers sans le consentement des personnes concernées. Les photographies constituent souvent des données sensibles (art. 3, let. c, LPD), ce qui se traduit par un renforcement des exigences en matière de protection des données[105]. En principe, l'utilisation d'un logiciel de reconnaissance faciale liée à la fonction "tag suggest" contrevient également au principe de la proportionnalité du traitement des données (art. 4, al. 2, LPD).

Mais comment trancher dans le cas d'une personne qui publie volontairement ses propres photographies sur un réseau social et rend son profil accessible à tout un chacun (art. 12, al. 3, LPD) via les paramètres de confidentialité? Si des données personnelles accessibles à tout un chacun font l'objet d'un traitement dans un but pour lequel elles n'ont, au regard des circonstances, objectivement pas été rendues accessibles, cela est malgré tout susceptible de constituer une atteinte à la personnalité[106]. Etant donné l'apparition relativement récente des logiciels de reconnaissance faciale, des doutes subsistent néanmoins quant au fait de savoir si une personne rendant ses photographies accessibles à tout un chacun les a également publiées pour qu'elles fassent l'objet d'un traitement de cette nature. Il convient dans ce cas également de vérifier l'existence d'un consentement à un traitement concret[107].

Dans le cas de la reconnaissance automatique de caractéristiques et d'objets sur des photographies par des logiciels, ces informations doivent être considérées comme des données techniques. Les données techniques demeurent des données personnelles au sens de la loi sur la protection des données lorsqu'elles peuvent être mises en relation avec une personne précise. Entrent par exemple dans cette catégorie les biens-fonds ou les véhicules à moteur[108]. A ce titre, ces éléments bénéficient donc de la protection offerte par le droit sur la protection des données.

4.3.6 Problèmes liés à la géolocalisation (technologies de localisation)

4.3.6.1 Contexte

Certains réseaux sociaux proposent des services localisant les utilisateurs (dont les données sont généralement transmises via des smartphones) grâce des technologies telles que le GPS ou le WLAN et leur fournissant différentes informations relatives à l'endroit où ils se trouvent. Certains réseaux sociaux se sont même totalement spécialisés dans la fourniture de services de géolocalisation de cette nature[109]. Selon le mode de communication adopté par les utilisateurs, les exploitants de plateformes peuvent se trouver en mesure de relier un grand nombre de données aux géodonnées récoltées. Dans certaines circonstances, ils peuvent ainsi savoir non seulement où se trouvent approximativement les utilisateurs, mais aussi dans quel type de bâtiment (cinéma, restaurant etc.), avec qui, ce qu'ils y font et si cela leur plaît.

La synchronisation de services de localisation de cette nature avec des réseaux sociaux peut amener les utilisateurs à révéler, consciemment ou non, des informations (à propos des lieux qu'ils fréquentent et des activités qu'ils y pratiquent) que des tiers sont susceptibles d'utiliser pour des buts non visés par les utilisateurs. Ces technologies sont dès lors à même de faciliter des comportements préjudiciables tels que l'usurpation d'identité, la cyberintimidation, le harcèlement ou la manipulation

---

[104] Ceci découle des exigences en termes de consentement issues de l'art. 28, al. 2, CC et de l'art. 13, al. 1 LPD ainsi que des principes de la bonne foi et de la finalité du traitement des données selon l'art. 4, al. 2 et 3, LPD.

[105] Voir art. 4, al. 5, art. 11*a*, al. 3, let. a, art. 12, al. 2, let. C, et art. 14 LPD.

[106] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 76, p. 381

[107] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 84, p. 383

[108] BSK-DSG, Belser Urs, 2. Aufl., Basel 2006, Art. 3, N. 5, p. 64. Dans ce sens, également ATF 138 II 346 cons. 6.2.

[109] Voir à ce sujet Foursquare (https://foursquare.com/) ou Friendticker (http://en.friendticker.com/).

psychologique par Internet. En outre, les géodonnées peuvent permettre à des tiers de savoir où se trouvent les personnes concernées, où elles vivent et ainsi favoriser les cambriolages[110].

4.3.6.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans un avis datant de mai 2011, le groupe de travail "Article 29"[111] s'est penché sur les risques que font planer les services de géolocalisation sur la protection des données[112]. En la matière, l'élément clé est le consentement des utilisateurs, qui, d'après l'avis, n'est pas valable lorsqu'il repose sur une acceptation forcée des CG ou s'il consiste seulement en une possibilité de non-participation. Les services de géolocalisation devraient être désactivés par défaut et les utilisateurs se voir proposer la possibilité de les activer. Il convient que les utilisateurs soient explicitement informés des finalités du traitement lorsque celles-ci sortent de l'ordinaire, par exemple lorsqu'elles concernent la création de profils ou la mise en place d'un ciblage comportemental. Si les utilisateurs ont été informés d'un transfert des données ou de changements au niveau des finalités du traitement, leur silence ne doit pas avoir valeur de consentement. Une icône d'alerte s'affichant sur les dispositifs finaux doit indiquer aux utilisateurs l'activation du service de géolocalisation, et les prestataires de services doivent, même si leurs services restent inchangés, solliciter régulièrement le consentement des utilisateurs. Pour finir, les délais de conservation ne doivent pas excéder ce qui est nécessaire, et les utilisateurs doivent avoir un droit à recevoir des informations dans un format lisible ainsi qu'à modifier et à supprimer leur données.

4.3.6.3 La législation en Suisse

Au sens de la législation sur la protection des données, les géodonnées constituent des données personnelles lorsqu'un lien avec une personne physique ou morale existe ou lorsqu'il est possible d'en établir un au prix d'efforts raisonnables[113]. La localisation de terminaux mobiles attribués à des individus et la combinaison de données techniques et personnelles permettent en outre de créer des profils de la personnalité ou des données sensibles[114], dont le traitement est soumis à des exigences strictes par la loi sur la protection des données. Les risques posés par les services de géolocalisation des réseaux sociaux en termes de droit sur la protection des données sont par essence couverts par les principes de traitement inclus dans la loi sur la protection des données.

Le principe de la *proportionnalité* (art. 4, al. 2, LPD) s'applique ainsi lorsque les données collectées et mises en relation dépassent ce qui est nécessaire pour la finalité du traitement; le cas échéant, le principe de la proportionnalité peut même obliger à l'anonymisation des données géocodées[115].

Le principe de la *finalité* (art. 4, al. 3, LPD) porte sur les modifications intervenant dans la finalité du traitement lorsque les exploitants de plateformes utilisent a posteriori les données personnelles collectées pour d'autres buts. La génération de données personnelles habituelles, de profils de la personnalité ou de données sensibles grâce à la synchronisation de géodonnées avec d'autres données publiées sur des réseaux sociaux doit être reconnaissable par les personnes concernées[116], et les exploitants de réseaux sociaux doivent éviter, lors de la synchronisation des données, de créer des données inexactes (art. 5, al. 2, LPD).

---

[110] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, p. 162 s.

[111] http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/Cooperation/Art29

[112] Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents du 16.05.2011, 881/11/FR WP 185

[113] FF 2006 7442 s.

[114] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, p. 48 s., 55 s.

[115] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, p. 47

[116] S'appliquent ici les principes de la bonne foi et du traitement reconnaissable des données ainsi que l'obligation d'informer imposée au maître d'un fichier lors de la collecte de profils de la personnalité ou de données personnelles sensibles (art. 4, al. 2, et 4 et art. 14 LPD).

Se pose encore une fois, comme pour nombre de services proposés par les réseaux sociaux, le problème du manque d'information des utilisateurs à propos de la portée, de la transmission, du type et de la finalité du traitement des données relatives à leur localisation, ce qui peut soulever des doutes quant à la validité de leur *consentement*[117].

L'art. 45*b* de la loi sur les télécommunications (LTC) encadre le recours à la géolocalisation pour les clients de prestataires de services de télécommunications. La géolocalisation est autorisée dans trois cas: 1) lorsque cela est nécessaire pour la fourniture desdits services de télécommunication ou pour leur facturation; 2) lorsque le client a donné son consentement; 3) lorsque les données ont été anonymisées. Pour autant, les prestataires de services de réseaux sociaux n'étant pas, dans leur grande majorité, également prestataires de services de télécommunications (voir point 2.4.2.2* plus haut), l'art. 45*b* est rarement applicable.

4.3.7 Dépendance excessive des utilisateurs à l'égard d'un réseau social

4.3.7.1 Contexte

La communauté économique parle d'effet de "lock-in" (verrouillage) pour désigner le fait qu'une entreprise, par suite d'investissements importants destinés à favoriser la collaboration avec un partenaire, ait ensuite beaucoup de mal à renoncer à cette collaboration. Le partenaire se trouve alors en mesure d'exploiter cette situation en imposant des conditions particulièrement désavantageuses.

Les utilisateurs de réseaux sociaux peuvent se trouver dans une situation similaire lorsqu'ils ont investi tellement de temps et d'argent pour configurer leur compte sur un réseau social qu'un changement leur apparaît impensable. La plateforme peut alors dégrader les conditions d'utilisation sans que les utilisateurs ne puissent y réagir en se repliant vers une plateforme concurrente.

Tel peut notamment être le cas lorsque des images, des films, de la musique, des textes ou d'autres données chères à l'utilisateur sont stockés sur la plateforme. Par ailleurs, certains utilisateurs sont, via la plateforme, en contact avec tellement de personnes (blog ou canal YouTube personnel, par exemple) qu'ils ne peuvent songer à passer à une autre plateforme qu'à la condition expresse de pouvoir emporter ces contacts avec eux.

Un changement de plateforme peut également se révéler impossible lorsque la plateforme constitue l'unique moyen pour des utilisateurs d'échanger des nouvelles et que, sans elle, ils seraient coupés de leurs contacts. Dans ce cas d'espèce, le mode de communication anonyme via la plateforme peut aussi répondre à une demande des autres utilisateurs, qui préfèrent que la plateforme ne divulgue pas leur adresse e-mail. Un transfert des coordonnées dans le cas d'un changement de plateforme irait donc à l'encontre de leurs souhaits. Une solution existe toutefois à ce conflit d'intérêts lorsque les utilisateurs quittant une plateforme n'emportent avec eux que la possibilité de contacter ultérieurement ceux qui le souhaitent.

Quelques plateformes offrent aux utilisateurs la possibilité d'emporter avec eux les données qu'ils avaient stockées chez elles. Un portage de cette nature entre les plateformes devrait cependant être la règle dans la mesure où lui seul permettrait aux utilisateurs de pouvoir changer plus facilement de prestataire.

4.3.7.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe exige que les données soient transférables vers un autre prestataire dans un format électronique exploitable.

[117] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012, p. 65

La Proposition de règlement général de l'UE sur la protection des données prévoit elle aussi un droit à la portabilité des données[118]. Si des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, les personnes concernées doivent avoir le droit d'obtenir une copie des données ainsi traitées dans un format structuré, couramment utilisé et permettant la réutilisation des données. Si les personnes concernées ont fourni les données à caractère personnel, elles ne doivent pas moins pouvoir les transférer à un autre système dans un format électronique couramment utilisé sans que celui qui a traité lesdites données n'y fasse obstacle.

4.3.7.3 La législation en Suisse

En droit suisse, aucune norme n'oblige les réseaux sociaux à mettre à la disposition des utilisateurs quittant leur plateforme les données qu'ils y ont eux-mêmes publiées ou stockées. Une telle norme permettrait pourtant de lutter contre une dépendance excessive des utilisateurs à l'égard de certaines plateformes.

On peut à cet égard établir un parallèle avec la portabilité des numéros de téléphone existant dans le domaine des télécommunications, qui poursuit un but similaire en permettant aux clients de conserver leur numéro de téléphone lorsqu'ils changent d'opérateur ou lorsqu'ils déménagent. Comme les clients peuvent, en cas de changement d'opérateur, transférer leur numéro au nouveau prestataire et ainsi s'épargner le désagrément de communiquer un nouveau numéro à tous leurs contacts, ils sont plus facilement enclins à faire jouer la concurrence.

Il convient toutefois de noter que le marché des réseaux sociaux est en plein mouvement. La dépendance des utilisateurs à l'égard d'une plateforme donnée n'est de ce fait pas aussi importante qu'elle pourrait l'être sur un marché mature, où la conservation de la clientèle existante devient cruciale pour les entreprises. Reste maintenant à savoir si les exploitants, forts du souhait de conserver leurs clients existants, vont les empêcher de transférer leurs données. Dans la pratique, nombre des données clients présentes sur les réseaux sociaux sont aujourd'hui déjà portables. Au vu de cette mise à disposition librement consentie, il ne semble pas encore nécessaire d'imposer une obligation spécifique de portabilité des données. D'autant plus que l'imposition d'une telle obligation soulèverait plusieurs questions: quelles données les utilisateurs auraient-ils le droit d'emporter? Les données combinées par l'exploitant avec d'autres données afin de générer une utilité supplémentaire (par exemple la désignation des utilisateurs sur des photographies publiées par des tiers) seraient-elles concernées? Quid des données créées grâce à des programmes appartenant à l'exploitant de la plateforme? Sous quel format les données seraient-elles transférables?

Nul ne sait encore comment la situation va évoluer sur ce front. Il convient donc d'attendre pour voir comment les choses vont tourner et, si nécessaire, de prendre ensuite des mesures légales en la matière (voir à ce sujet le point 7.2.4.4).

4.4 Atteinte aux intérêts individuels par des tiers

4.4.1 Atteinte à l'honneur et atteinte illicite à la personnalité

4.4.1.1 Contexte

Les réseaux sociaux ne sont pas à l'abri des jugements de valeur diffamatoires ou des fausses allégations[119]. Les tribunaux suisses ont déjà eu à se prononcer dans des affaires de ce type[120]. Or, les atteintes à la réputation via les réseaux sociaux sont difficilement comparables avec les diffamations par voie de presse, par exemple. A l'étranger, il a été reconnu que la communication en

[118] Art. 18 de la Proposition de règlement général de l'UE sur la protection des données, COM(2012) 11 final

[119] Dans son rapport annuel 2011, le SCOCI (service de coordination de la lutte contre la criminalité sur Internet) note ainsi une recrudescence des atteintes à l'honneur dans les signalements qui lui ont été communiqués et constate que les criminels se servent de plus en plus d'Internet pour réaliser leurs méfaits. Voir Rapport annuel 2011 du SCOCI, p. 6.

[120] Voir notamment l'arrêt du 9 mai 2011 du tribunal de district de Saint-Gall (insultes sur Facebook); http://wifimaku.com/pages/viewpage.action?pageId=5669650.

ligne empruntant des canaux tels que les blogs ou Twitter mettait à rude épreuve l'efficacité de l'arsenal juridique existant en matière de protection de la réputation[121].

Les personnes concernées sont donc confrontées à des risques nouveaux et difficilement appréciables. Etant donné qu'il est souvent possible de poster des contenus sur des profils tiers sans l'accord préalable de leur titulaire, avoir la maîtrise de son propre profil se révèle très compliqué. Compte tenu de la rapidité et de la simplicité avec lesquelles des contenus non vérifiés peuvent se répandre sur les réseaux sociaux et de l'impact social qu'ils peuvent avoir sur les contacts des utilisateurs, des jugements de valeur diffamatoires ou de fausses allégations peuvent causer des torts considérables.

Les invitations de groupe sur Facebook représentent un autre phénomène susceptible de tenir la réputation des utilisateurs. Lorsqu'une personne est invitée à rejoindre un groupe par un ami sur Facebook, elle en devient automatiquement membre, qu'elle ait ou non donné son consentement. Elle est certes immédiatement informée de cette invitation et peut instantanément sortir du groupe, mais, selon la nature du groupe et l'identité des personnes invitées, il est alors déjà trop tard pour éviter que sa réputation ne soit entachée.

4.4.1.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Pour se protéger contre de fausses allégations proférées en public, l'une des mesures possibles réside dans le droit de réponse. La recommandation du Conseil de l'Europe sur le droit de réponse dans le nouvel environnement des médias[122] demande qu'il s'applique à tous les outils de communication destinés à la diffusion périodique auprès du public d'informations éditées, en ligne ou hors ligne. Si des contenus contestés restent à la disposition du public dans des archives électroniques et qu'un droit de réponse a été accordé, un lien devrait être créé entre les deux afin d'attirer l'attention des utilisateurs sur le fait que l'information originelle a fait l'objet d'une réponse.

Le Parlement européen et le Conseil de l'UE ont par ailleurs appelé les Etats membres à prendre des mesures visant à garantir le droit de réponse dans les médias en ligne[123]. En 2011, dans son rapport sur l'application de cette recommandation, la Commission européenne a constaté l'absence de cohérence dans l'instauration d'un droit de réponse couvrant les médias en ligne dans les Etats membres[124] et a exhorté ces derniers à accroître l'efficacité des systèmes existants.

4.4.1.3 La législation en Suisse

Les dispositions du code pénal (art. 173-178 CP) et du code civil (art. 28 s. CC) visant à protéger l'honneur s'appliquent en principe aux activités sur les réseaux sociaux. La protection économique de l'honneur garantie par l'art. 28 CC est complétée par l'art. 3, al. 1, let. a, LCD.

A titre d'instrument de défense, le CC prévoit notamment le droit de réponse à l'égard de faits présentés dans les médias à caractère périodique qui sont destinés ou accessibles au grand public (art. 28*g* à 28*l* CC). Le législateur a volontairement formulé la notion de médias de manière ouverte, si bien que le droit de réponse peut tout aussi bien s'appliquer aux nouvelles formes de médias et qu'il

---

[121] Voir la littérature étrangère récente, notamment Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, p. 710 ss ; Richardson Megan, Honour in a Time of Twitter, Journal of Media Law 2013, p. 45 ss.

[122] Recommandation Rec(2004)16 sur le droit de réponse dans le nouvel environnement des médias

[123] Recommandation du Parlement européen et du Conseil sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne, Journal officiel L378 du 27 décembre 2006, p. 74

[124] Rapport de la Commission sur l'application de la recommandation du Conseil du 24 septembre 1998 concernant la protection des mineurs et de la dignité humaine, et de la recommandation du Parlement européen et du Conseil du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne – Protéger les enfants dans le monde numérique, COM(2011) 556 final, p. 10

ne dépend pas du canal de diffusion[125]. Les profils d'utilisateur sur les réseaux sociaux peuvent-ils être qualifiés de médias à caractère périodique? Tout dépend de l'utilisation que le titulaire du profil fait de la plateforme et de la fréquence de ses publications. Si les blogs de journalistes alimentés régulièrement, par exemple, peuvent être considérés comme des médias à caractère périodique au sens du CC, c'est plus discutable dans le cas des forums de discussion[126].

Les obstacles pratiques aux actions menées contre des propos calomnieux ou portant atteinte à la personnalité sur les réseaux sociaux semblent résider principalement dans *l'application du droit*, si l'auteur d'une atteinte à l'honneur n'est pas identifiable et si les enquêtes dépendent de la propension à coopérer des exploitants de plateforme et des fournisseurs de services. Il est notamment très compliqué d'agir rapidement contre des publications sur des plateformes étrangères[127]. (Si les personnes impliquées sont suisses, l'application du droit est en revanche facilitée par le fait que les requêtes en élimination et en constatation peuvent être déposées à l'encontre de tous ceux ayant pris part à l'atteinte à la personnalité.[128])

A noter en outre que plus les contenus blessants ou diffamatoires se diffusent vite et à grande échelle, plus les instruments juridiques perdent de leur efficacité: même si la victime a fait valoir avec succès ses droits à la personnalité devant un tribunal, elle ne peut pas exclure que les contenus illicites refassent surface ailleurs.[129]

4.4.2 Intimidation et harcèlement en ligne (cyberbullying et cyberstalking)

4.4.2.1 Contexte

L'atteinte à la personnalité peut prendre la forme d'actes d'intimidation en ligne (cyberbullying ou cybermobbing)[130], ce qui consiste à diffuser des textes, des images ou des films diffamatoires par les moyens de communication modernes (téléphone portable, chats, réseaux sociaux, portails vidéo, forums ou blogs) dans le but de dénigrer, de ridiculiser ou de blesser quelqu'un[131], des attaques qui sont en général répétées ou qui se déroulent sur une période prolongée[132].

Le harcèlement en ligne (cyberstalking) consiste lui à utiliser des outils de communication électroniques comme les réseaux sociaux pour persécuter des tiers. La notion de harcèlement englobe le fait d'épier la personne, d'enquêter sur elle ou de prendre contact avec elle. Très souvent, le harcèlement a lieu entre des personnes qui se connaissent déjà ou qui se côtoient. Les informations publiées par les utilisateurs eux-mêmes sur les réseaux sociaux peuvent être mises à profit pour des sollicitations en ligne, mais aussi pour découvrir l'adresse de victimes potentielles, examiner leurs habitudes et les harceler ensuite physiquement.

---

[125] ATF 113 II 369 cons. 3, p. 371

[126] Voir entre autres Barrelet Denis/Werly Stéphane, Droit de la communication, Berne 2011, N 1683.

[127] Voir à ce sujet Schneider-Marfels Karl-Jascha, Facebook, Twitter & Co: "Imperium in imperio", Jusletter du 20 février 2012.

[128] Voir arrêt du Tribunal fédéral au sujet de blogs de lecteurs hébergés par la Tribune de Genève (TF 5A_792/2011 du 14 janvier 2013).

[129] Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, p. 713

[130] Les deux termes sont utilisés comme des synonymes dans le présent rapport.

[131] Une étude menée de novembre 2010 à juin 2012 auprès de 960 écoliers (dont 49% de filles, pour une moyenne d'âge de 13,5 ans) dans les cantons du Valais, de Thurgovie et du Tessin a révélé que le nombre de victimes et d'auteurs de ces actes était certes très faible, mais que les cas avaient augmenté entre 2010 et 2012. Voir: chiffres non publiés de l'étude netTEEN (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Universität Zürich). Il semble par ailleurs que la cyberintimidation soit étroitement liée à d'autres formes traditionnelles d'intimidation chez les jeunes dans la mesure où, la plupart du temps, les auteurs sont également en confrontation avec leurs victimes dans la vie réelle. Voir: Perren Sonja, Professionswissen für Lehrerinnen und Lehrer – Grundlagen für die Aus- und Weiterbildung von Lehrerinnen und Lehrern, Hrsg.: H.U. Grunder, K. Kansteiner-Schänzlin, H.Moser, p. 15.

[132] Rapport du Conseil fédéral "Protection contre la cyberintimidation" du 26 mai 2010, consultable à l'adresse: http://www.ejpd.admin.ch/content/ejpd/fr/home/dokumentation/info/2010/ref_2010-06-02.html.

Les phénomènes du harcèlement et de l'intimidation en ligne ne s'observent pas seulement sur les réseaux sociaux, mais ils y prennent de l'ampleur car ils y ont trouvé un terrain favorable[133]. La possibilité d'utiliser les réseaux sociaux sous un pseudonyme permet aux agresseurs d'agir dans l'ombre, ce qui facilite le harcèlement ou le dénigrement d'autrui. Sur les réseaux sociaux, les actes calomnieux peuvent en outre être commis de manière à ce qu'ils soient visibles pour d'autres personnes, ce qui ne fait qu'accabler davantage les victimes.

4.4.2.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe plaide pour un partage des meilleures pratiques destinées à la prévention du harcèlement et de la sollicitation en ligne et demande à ce que les exploitants de plateformes mettent en place des mécanismes de plainte efficaces et réagissent avec diligence aux plaintes.

La campagne de sensibilisation aux dangers de la Toile "klicksafe", financée par la Commission européenne, diffuse des informations, notamment sur le phénomène de la cyberintimidation, fait le point sur les dispositions légales en vigueur et donne des conseils aux personnes concernées[134].

La Corée du Sud a tenté de faire face à de retentissants cas de cyberintimidation et de problèmes d'équité en lien avec des élections[135] en instaurant une obligation de révéler son identité sur les réseaux sociaux[136]. La décision de la Cour constitutionnelle sud-coréenne, qui a jugé anticonstitutionnelle l'obligation de révéler son identité[137], la multiplication des attaques ayant ciblé les serveurs des sites Web concernés et le vol des données personnelles de millions de Sud-Coréens ont conduit la Commission coréenne des communications à supprimer le système de vérification de l'identité jusqu'en 2014[138]. Une licence obligatoire a été introduite en juin 2013 à Singapour pour les portails d'information comptant plus de 50 000 utilisateurs.[139]

4.4.2.3 La législation en Suisse

Le droit suisse ne contient pas de dispositions spécifiques sur la cyberintimidation ou le harcèlement en ligne. Le code civil et le code pénal traitent cependant de nombreux actes pouvant relever de ces deux domaines s'ils sont commis à l'aide de moyens de communication électroniques. Dans son rapport relatif à la cyberintimidation, le Conseil fédéral considère du reste qu'en l'état actuel des

---

[133] Dans son rapport annuel 2011, le SCOCI (service de coordination de la lutte contre la criminalité sur Internet) constate que les signalements pour menaces et contraintes sont en forte hausse et que les réseaux sociaux sont souvent utilisés pour commettre ce type de délits. Il note également que 30 des cas signalés sous les catégories délits contre l'honneur, menaces et contraintes relèvent de l'intimidation en ligne, sans indiquer toutefois si ces actes avaient été commis via les réseaux sociaux ou par e-mail. (Voir Rapport annuel 2011 du SCOCI, p. 6.) Selon un document interne du SCOCI relatif au rapport annuel 2011, les réseaux sociaux ont servi de vecteur à neuf des cas de délit contre l'honneur signalés et à trois des cas annoncés dans les catégories menaces, contraintes et extorsions. Cette hausse marquée ne s'est néanmoins pas confirmée en 2012 et ne constitue donc pas une tendance en tant que telle selon le SCOCI (rapport annuel 2012 du SCOCI, p. 9).

[134] Voir http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/.

[135] Introduction d'un système d'identification obligatoire des personnes qui s'expriment pour ou contre des candidats à des élections sur des sites Web ou des forums Internet, via le Public Officials Election Act (POEA) en 2005

[136] Voir le rapport du 21 mars 2011 sur la Corée du Sud du rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/17/27/Add.2 et le rapport sur la Corée du Sud d'OpenNet Initiative; à consulter à l'adresse suivante: http://www.access-controlled.net/profiles/.

[137] La Cour constitutionnelle sud-coréenne a considéré que l'obligation de révéler son identité était anticonstitutionnelle: "South Korea's real-name net law is rejected by court", 23.08.2012; consultable à l'adresse: http://www.bbc.co.uk/news/technology-19357160.

[138] Voir à ce sujet Kate Jee-Hyung Kim, Lessons Learned from South Korea's Real-Name Policy, 17.01.2012, à l'adresse: http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system et "Real-name Internet law on way out", Korea Joonang Daily, 30.12.2011; à l'adresse: http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2946369.

[139] Voir à ce sujet NZZ n° 123 du 31 mai 2013, p. 5: "Lizenzpflicht für Onlinemedien – Singapur verschärft die Aufsicht über Nachrichtenportale im Internet".

choses, rien ne semble indiquer que l'arsenal pénal existant serait insuffisant pour couvrir efficacement ce phénomène[140].

Les actes relevant du harcèlement en ligne ou de la cyberintimidation entrent ainsi dans le champ d'application de la protection de l'honneur prévue par le code pénal (art. 173-178 CP) et par le code civil (art. 28 ss CC). Outre les prétentions résultant de l'art. 28*a* CC, les personnes souhaitant se protéger contre des atteintes à la personnalité prenant la forme de violence, de menace ou de harcèlement peuvent requérir un juge d'interdire à un tiers de prendre contact avec elles (art. 28*b*, al, 1, ch. 3 CC), ce qui inclut explicitement les contacts par voie électronique.

Cette protection est complétée par celle découlant des articles 135 (représentation de la violence), 143bis (accès indu à un système informatique), 144bis (détérioration de données), 156 (extorsion et chantage), 179^{novies} (soustraction de données personnelles), 180 (menaces), 181 (contrainte), 197 (pornographie) et 198 (contraventions contre l'intégrité sexuelle) du code pénal.

Là aussi, la principale difficulté réside dans l'application du droit, même si le fait que l'auteur des actes en question évolue généralement dans l'entourage de la victime (école, travail etc.) tend à faciliter son identification. En 2012, le SCOCI a noté un recul des signalements d'infractions contre l'honneur, recul qui pourrait s'expliquer par une plus grande retenue en matière d'usage de réseaux sociaux dans le sillage de la médiatisation croissante de la cyberintimidation[141].

4.4.3 Usurpation d'identité et autres manipulations malveillantes

4.4.3.1 Contexte

Sur de nombreux réseaux sociaux, *l'usurpation d'identité* est un jeu d'enfant. En matière de cybercriminalité, l'usurpation d'identité et autres abus similaires sur les réseaux sociaux sont en augmentation et servent souvent à commettre des délits de nature patrimoniale[142]. L'usurpation d'identité peut en outre être utilisée pour compromettre la réputation d'une personne ou porter atteinte à sa personnalité ou à son honneur. Les malfaiteurs créent un profil au nom d'une personne connue et profitent de sa notoriété ou mettent à mal sa réputation par des actes malveillants. Il peut également arriver qu'ils créent un profil au nom d'une personne de leur entourage afin de lui nuire en la ridiculisant ou en diffusant en son nom des contenus illicites ou préjudiciables.

Apparaître sous un pseudonyme sur les réseaux sociaux peut également se révéler avantageux pour les fauteurs de trouble, qui peuvent ainsi s'infiltrer dans des cercles auxquels ils n'auraient pas accès sous leur vrai nom ou devenir amis en ligne avec des personnes qui n'auraient jamais accepté leur demande si elles avaient eu connaissance de leur véritable identité.

Les identités volées ou inventées peuvent être mises à profit à des fins malveillantes de toutes sortes, notamment pour accumuler des informations en vue d'actes illicites tels que la manipulation psychologique ("grooming"), le harcèlement en ligne, la cyberintimidation, le phishing, le spamming ou la propagation de virus informatiques.

---

[140] Rapport du Conseil fédéral "Protection contre la cyberintimidation" du 26 mai 2010. Le Conseil fédéral a par ailleurs rejeté la demande, soumise dans la motion Freysinger 10.4054, d'introduire dans le code pénal une norme réprimant spécifiquement le harcèlement psychologique sur le lieu de travail, estimant que les agissements en question étaient déjà largement réglementés et qu'une norme supplémentaire n'apporterait aucun bénéfice dans la mesure où elle ne règle en rien les problèmes posés par la difficulté de prouver les faits et par les rapports de pouvoir. Voir http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20104054. Le Conseil national a lui aussi rejeté à *130 voix contre 33 et 11 abstentions* l'introduction d'une norme pénale réprimant le harcèlement psychologique.

[141] Rapport annuel du SCOCI, p. 9

[142] ENISA Threat Landscape Report du 28 septembre 2012, p. 21 ss; consultable à l'adresse: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.

4.4.3.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Dans sa Recommandation sur les services de réseaux sociaux, le Conseil de l'Europe appelle à la mise en place de mécanismes appropriés afin de traiter les réclamations contre les comportements abusifs sur les réseaux sociaux, notamment en ce qui concerne l'usurpation d'identité. Les Etats membres doivent imposer aux exploitants de plateformes de prendre les mesures de sécurité les plus adaptées pour protéger les données personnelles contre tout accès illicite par des tiers. Cela devrait comprendre des mesures de cryptage des communications entre l'utilisateur et les sites de réseaux sociaux. Les exploitants de plateformes sont également exhortés à signaler aux utilisateurs toute violation de sécurité afin qu'ils puissent prendre des mesures préventives (en changeant leur mot de passe, par exemple).

La Commission européenne propose par ailleurs la création d'un centre européen de lutte contre la cybercriminalité[143] qui aurait entre autres pour mission de protéger les profils d'utilisateur sur les réseaux sociaux contre le piratage afin de prévenir les usurpations d'identité sur Internet[144].

4.4.3.3 La législation en Suisse

La création par un tiers d'un profil de réseau social sous un nom protégé par la loi ou sans l'accord de l'ayant-droit constitue une infraction à la protection du nom prévue par l'art. 29, al. 2, CC. Cette disposition protège les personnes lésées par une usurpation de leur nom, ce qui recouvre le nom civil ou officiel d'une personne physique, mais aussi tout pseudonyme, surnom, sigle, acronyme et nom abrégé, pour autant que ceux-ci soient communément perçus comme le nom d'un individu[145].

Il peut y avoir atteinte au droit à l'image conformément à l'art. 28 CC si un individu utilise des images non autorisées d'une autre personne afin de se créer un profil sous l'identité de celle-ci.

Sur les réseaux sociaux offrant des fonctions de communication privée (à l'instar de Facebook), l'intrusion de tiers dans des profils ne leur appartenant pas dans le but de prendre connaissance de communications privées auxquelles les intéressés ne leur ont pas donné accès constitue aussi une violation de la sphère secrète ou privée (art. 28 CC). Il est par ailleurs interdit d'utiliser des profils tiers ou créés sous un faux nom pour inciter d'autres personnes à révéler des informations privées les concernant.

Du point de vue de la loi sur la protection des données, le fait de soustraire des données personnelles en se présentant sous une fausse identité peut constituer une infraction aux principes de la bonne foi et de la collecte reconnaissable des données (art. 4, al. 2 et 4, LPD)[146]. Si des tiers publient des informations sensibles concernant autrui par le biais d'un profil créé sous un faux nom, ils contreviennent à l'art. 12, al. 2, let. c, LPD.

Si des tiers piratent un profil, y prennent connaissance d'informations qui ne sont pas librement accessibles, y modifient des contenus ou changent le mot de passe de l'ayant-droit, ils peuvent tomber sous le coup de l'art. 143bis CP (accès indu à un système informatique), de l'art. 144bis CP (détérioration de données) et de l'art. 179^{novies} CP (soustraction de données personnelles).

Les profils créés sous une fausse identité ou sous un nom inventé peuvent servir à accomplir divers forfaits. Figurent en tête de liste les délits patrimoniaux et contre l'honneur tels que la contrainte ou la menace (art. 173-177, 146, 147, 156, 180, 181 CP) mais aussi les atteintes à la personnalité et le

---

[143] Communication "Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité", COM(2012) 140 final

[144] Communiqué de presse de la Commission européenne du 28 mars 2012 "Un Centre européen de lutte contre la cybercriminalité pour combattre la criminalité sur l'internet et protéger les consommateurs en ligne", IP/12/317

[145] BSK-ZGB I, Bühler Roland, 4. Aufl., Basel 2010, Art. 29, N. 4 et 7, p. 321 s. et N.16, p. 325

[146] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 14, p. 81 et N. 56, p. 99

harcèlement (art. 28 et 28*b*, al. 1 ch. 3, CC). L'art. 3, al. 1, let. o, LCD offre une protection contre le spamming, tandis que l'art. 144bis CP (détérioration de données) porte entre autres sur l'utilisation et la propagation de virus informatiques par le biais des réseaux sociaux.

En se fondant sur l'art. 14*f*^{bis} de l'ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications (ORAT)[147], des mesures efficaces peuvent être prises contre le phishing et la diffusion de logiciels malveillants sur les domaines .ch, mais aussi, dans certains cas, contre l'utilisation de fausses identités.

Il ressort de l'analyse que le droit existant couvre largement les délits liés à une usurpation d'identité en ligne. Dans les faits, il peut toutefois se révéler compliqué d'identifier les auteurs de ces actes, en particulier lorsqu'il s'agit de pirates professionnels, afin de les traduire en justice.

4.4.4 Surveillance des propos tenus sur les réseaux sociaux (social media monitoring)

4.4.4.1 Contexte

Les entreprises, les autorités, les organisations et certains particuliers ont un intérêt à savoir ce qui se dit à leur sujet sur les réseaux sociaux. Cela peut les inciter à mettre en place une veille systématique et permanente leur permettant de reprendre le contrôle de leur image. Des outils automatisés sont alors utilisés afin d'absorber ce flux d'informations non structurées.

L'un des problèmes posés par la surveillance des réseaux sociaux tient au fait qu'elle ne couvre pas seulement les contenus publiés sur les réseaux mais qu'elle porte aussi sur des données relatives à leurs auteurs. Les personnes ou organismes procédant à cette surveillance obtiennent ainsi des informations sur le vrai nom – ou au moins le pseudonyme – des auteurs, et parfois même sur leur âge, leur sexe, leur profession, leur employeur, leur origine et sur toute autre donnée publiée. Dans ce contexte, le fait qu'ils puissent se renseigner ainsi sur les convictions et sur les opinions politiques d'utilisateurs est particulièrement gênant.

4.4.4.2 La législation en Suisse

Le principe de la finalité ne couvre pas automatiquement tout type de traitement de données techniquement possible sur les réseaux. Même publiées, les données ne peuvent donc pas, en vertu de la loi sur la protection des données, être utilisées pour d'autres buts sans autre forme de procès. Les données personnelles sur les plateformes de réseaux sociaux sont souvent destinées aux seuls amis ou sont publiées dans un cercle ou dans un contexte donnés. Sans informations transparentes sur une surveillance de réseaux sociaux, la personne concernée ne dispose pas des connaissances requises sur l'utilisation qui est faite de ses données personnelles dans le cadre de la surveillance. Les membres de réseaux sociaux doivent au moins pouvoir déduire d'après les circonstances que des outils de surveillance sont mis en œuvre. Si des données personnelles sont publiées au sujet de tiers, ces tiers ne sont ni informés, ni consultés quant à cette surveillance. C'est pourquoi, dans bien des cas, il ne peut pas être présumé que les personnes concernées auraient rendu leurs données personnelles sur les réseaux sociaux accessibles à tout un chacun au sens de l'art. 12, al. 3, LPD.

Sur son site Internet, le PFPDT a formulé des recommandations pour un monitoring des médias sociaux conforme aux règles de la protection des données[148]. Le traitement des données personnelles doit ainsi se limiter au minimum nécessaire à l'exploitation des données et être effacé aussi vite que possible ou rendu anonyme. Les données non publiques (notamment les données concernant un groupe fermé d'utilisateurs ou un cercle d'amis) ne doivent pas être utilisées. Le monitoring doit se limiter à l'analyse d'opinions et de commentaires émis publiquement.

---

[147] RS 784.104

[148] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html?lang=fr

4.5 Atteinte à des intérêts communs

4.5.1 Propos racistes et discriminatoires (discours haineux)

4.5.1.1 Contexte

Comme le reste de la Toile, les réseaux sociaux peuvent être utilisés afin de diffuser des contenus racistes prenant la forme d'images, de textes et de vidéos[149]. Ils peuvent en outre être investis par des groupements racistes qui s'en servent pour s'organiser et pour recruter de nouveaux membres.

Certains détournent également les réseaux sociaux de leur usage d'origine afin de discriminer des personnes sur la base de caractéristiques autres que la race, notamment leur orientation sexuelle, leur origine, leur religion, leur handicap, leur mode de vie, leur langue, leur position sociale, leurs convictions politiques et leurs opinions, leur sexe ou leur âge.

Le contrôle et la suppression des contenus racistes et discriminatoires sont compliqués par le fait que, sur les réseaux sociaux, la diffusion de ces contenus et l'interconnexion des utilisateurs se font beaucoup plus facilement et rapidement que sur des sites Internet classiques.

La lutte contre ce phénomène se heurte par ailleurs au problème posé par les différences entre les législations nationales pour ce qui est des contenus racistes et discriminatoires. Certains contenus punissables en Suisse peuvent ainsi être parfaitement légaux dans d'autres pays[150]. Cela ne va pas sans poser des difficultés aux médias accessibles à l'échelle internationale, et les exploitants de réseaux sociaux ont dès lors tendance à bloquer sur demande certains contenus et certaines pages dans les pays où ils sont litigieux. C'est ainsi que Twitter a bloqué le compte d'un groupe d'extrême-droite interdit en Allemagne pour les utilisateurs de Twitter ayant indiqué lors du paramétrage de leur compte qu'ils vivaient en Allemagne[151].

4.5.1.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Le protocole additionnel du 28 janvier 2003 à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, porte expressément sur la diffusion de contenus racistes et xénophobes par Internet. La Convention du 23 novembre 2001[152] sur la cybercriminalité est entrée en vigueur en Suisse le 1er janvier 2012. Le protocole additionnel a été ratifié par le Conseil fédéral, mais n'est pas encore entré en vigueur en Suisse.

L'organisation "jugendschutz.net"[153] a été créée en application du § 18 du Traité d'Etat entre les Länder allemands concernant la protection de la jeunesse dans les médias[154]. En Allemagne, jugendschutz.net lutte activement contre les contenus racistes et discriminatoires publiés sur Internet et sur les réseaux sociaux. Elle accomplit par ailleurs un travail de sensibilisation à destination du grand public au travers de journées de prévention, de cycles de formation ou de publications telles que la brochure "Klickt's? Geh Nazis nicht ins Netz!"[155]. Elle combat entre autres l'utilisation des

---

[149] Selon un document interne du SCOCI relatif au rapport annuel 2011, les réseaux sociaux ont servi de vecteur ou de cadre à neuf des cas de discrimination raciale signalés en 2011 (qui étaient au nombre de 30 environ).

[150] La tolérance à l'égard des discours haineux est ainsi nettement plus grande aux Etats-Unis que dans la plupart des pays d'Europe occidentale. Voir à ce sujet la décision rendue le 22 mai 2000 par le Tribunal de Grande Instance de Paris dans l'affaire *LICRA contre Yahoo!*, en vertu de laquelle la vente d'objets nazis sur le site de vente aux enchères de Yahoo – légale selon le droit américain, mais interdite par le Code pénal français – a été déclarée illégale.

[151] "Erste landesspezifische Sperre auf Twitter: Account von verbotener rechtsextremistischer Vereinigung in Deutschland gesperrt"; consultable sous: https://netzpolitik.org/2012/erste-landesspezifische-sperre-auf-twitter-account-von-verbotener-rechtsextremistischer-vereinigung-in-deutschland-gesperrt/

[152] RS 0.311.43

[153] http://www.jugendschutz.net/

[154] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien vom 10. bis 27.09.2002, Bay.GVBI Nr. 5/2003, p. 147 s.

[155] http://www.jugendschutz.net/materialien/klickts.html

réseaux sociaux par les groupes d'extrême-droite. Netz-Gegen-Nazis.de[156] est une autre plateforme allemande poursuivant des objectifs similaires.

L'initiative INACH (International Network Against Cyberhate)[157] lancée par jugendschutz.net a quant à elle pour cheval de bataille l'incitation à la haine sur Internet, et notamment le harcèlement psychologique via les médias sociaux. Le réseau qu'elle constitue se compose de bureaux de communication de plusieurs pays, qui échangent leurs stratégies en matière de meilleures pratiques et œuvrent à la suppression des contenus et des sites discriminatoires et punissables sur Internet.

4.5.1.3 La législation en Suisse

L'art. 261bis CP interdit différentes formes de discrimination envers les personnes en raison de leur appartenance raciale, ethnique ou religieuse. Cette disposition s'applique en principe à tous les types de communication imaginables via les réseaux sociaux, qu'il s'agisse de photos, de vidéos, d'images ou de textes, à condition toutefois que la communication soit *publique*[158]. Selon la doctrine[159], les propos exprimés sur les réseaux sont considérés comme publics si le cercle de destinataires ne se limite pas à des personnes unies par une relation de confiance (via un paramétrage restrictif de la sphère privée sur Facebook, par exemple).

Les tribunaux suisses ont déjà jugé plusieurs affaires relatives à des propos racistes tenus sur les réseaux sociaux[160]. L'art. 261*bis* CP ne porte cependant que sur les discriminations en raison de l'appartenance raciale, ethnique ou religieuse, et donc pas sur toutes les discriminations interdites par la Constitution (art. 8, al. 2, Cst.), qui incluent également celles reposant, entre autres, sur le sexe, l'âge, le handicap ou l'orientation sexuelle. Seul le droit de la personnalité (art. 28 ss CC) offre une certaine protection aux personnes faisant l'objet sur les réseaux sociaux d'une discrimination du fait d'autres caractéristiques liées à leur personnalité.

Au niveau suisse, la Commission fédérale contre le racisme (CFR)[161] et le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)[162] sont les fers de lance de la traque contre le racisme sur Internet. Lorsque la CFR découvre des propos racistes sur les réseaux sociaux, elle les signale au SCOCI, qui, après un premier examen et une sauvegarde des données, transmet les annonces[163] aux autorités pénales compétentes en Suisse et à l'étranger. Le SCOCI œuvre par ailleurs de son côté en cherchant des contenus punissables sur Internet et en analysant la cybercriminalité. Etant donné que les exploitants de réseaux sociaux sont souvent basés à l'étranger, la répression des infractions est difficile, surtout lorsqu'il s'agit d'identifier un auteur. D'après les renseignements fournis par le SCOCI, la suppression des contenus potentiellement punissables ne pose en revanche aucun problème dans la pratique. La diffusion de contenus racistes ou discriminatoires est interdite par les conditions d'utilisation de la plupart des réseaux sociaux et, si leur attention est attirée sur des contenus litigieux, les exploitants procèdent normalement aux suppressions qui s'imposent.

---

[156] http://www.netz-gegen-nazis.de/

[157] http://www.inach.net/index.php

[158] S'agissant de l'interprétation large du terme "public" par le Tribunal fédéral, voir notamment ATF 130 IV 111.

[159] Voir Fiolka Gerhard, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, vor Art. 258 N. 25

[160] Voir notamment celle concernant un commentaire sur Facebook dirigé contre une camarade d'école de couleur (décision n° 2010-32 dans le Recueil de cas juridiques de la Commission fédérale contre le racisme; http://www.ekr.admin.ch/dienstleistungen/00169/)

[161] http://www.ekr.admin.ch/aktuell/index.html?lang=fr

[162] http://www.cybercrime.admin.ch/content/kobik/fr/home.html

[163] La part de la discrimination raciale ne s'est établie qu'à 0,78% dans toutes les annonces reçues en 2012; Rapport annuel 2012 du SCOCI, p. 4.

4.5.2 Pornographie

4.5.2.1 Contexte

Des problèmes liés à la diffusion de contenus pornographiques peuvent se poser sur les réseaux sociaux au même titre que sur le reste de la Toile lorsque les contenus en question relèvent de la pornographie dure (par exemple des représentations d'actes sexuels avec des enfants ou des animaux, cf. l'art. 197, ch. 3, CP) mais aussi – s'ils sont accessibles à des personnes de moins de 16 ans – de la pornographie "soft". Aux fins du présent rapport, c'est le problème de la pédopornographie qui se trouve à l'avant-plan.

Les contenus pédopornographiques étant en principe bannis partout dans le monde, les cercles qui se livrent à ces activités optent généralement pour des canaux de diffusion et de communication en ligne plus anonymes que les réseaux sociaux classiques. Les représentations d'abus sexuels sur des enfants sont dès lors vendues via des sites Web marchands ou échangées au sein de groupes fermés ou de réseaux peer-to-peer[164], qui sont propices à un échange en toute discrétion de matériel de pornographie enfantine[165]. La publication ou la diffusion de contenus pédopornographiques par le biais de plateformes perméables est par conséquent plutôt rare.

4.5.2.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

La Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2011 (RS 0.311.43), qui a également un caractère contraignant pour la Suisse, a pour objectif une harmonisation de la réglementation au niveau international et un renforcement de la coopération entre les Etats signataires, ce qui est important compte tenu du fait que les délits liés à Internet sont souvent transfrontaliers. L'art. 9 de la Convention contient des dispositions relativement détaillées sur les infractions se rapportant à la pédopornographie.

Plusieurs organisations, établies dans divers pays, se consacrent à la traque et à la suppression des contenus préjudiciables et illicites sur Internet. En Angleterre, on peut ainsi citer l'Internet Watch Foundation, qui s'occupe notamment des contenus pédopornographiques sur Internet[166].

Par suite de l'adhésion de la Suisse à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels du 25 octobre 2007, il est à prévoir qu'à l'avenir, la consommation intentionnelle de pornographie dure – ce qui inclut le simple fait d'en regarder sur les réseaux sociaux sans télécharger de contenus – sera également punissable[167].

4.5.2.3 La législation en Suisse

L'art. 197 CP protège les moins de 16 ans et les adultes non consentants contre toute exposition à de la pornographie. Il interdit par ailleurs la pornographie dure. L'art. 197 CP recense la plupart des actes et des objets pouvant conduire à ce que de la pornographie "soft" parvienne aux mauvais destinataires par le biais des réseaux sociaux ou à ce que de la pornographie dure soit diffusée ou consultée via les réseaux sociaux. Si des contenus pornographiques sont publiés – par exemple sous la forme d'une vidéo YouTube – sans restrictions d'accès efficaces, ils sont rendus accessibles à des moins de 16 ans. Dès lors, il ne suffit pas de placer un avertissement qui disparaît lorsqu'on clique

---

[164] Informations sur le thème de la pornographie enfantine sur le site du Service de coordination de la lutte contre la criminalité sur Internet, http://www.cybercrime.admin.ch/content/kobik/fr/home/themen/kinderpornografie.html

[165] Voir les communiqués de presse du 3 avril 2012 de l'Office fédéral de la police "La pornographie enfantine reste la catégorie la plus signalée au SCOCI en dépit d'un recul du nombre de communications de soupçons", http://www.fedpol.admin.ch/content/fedpol/fr/home/dokumentation/medieninformationen/2012/2012-04-03.html.

[166] http://www.iwf.org.uk/

[167] FF 2012 7096 et FF 2012 7133.

dessus[168], ni de restreindre l'utilisation d'une page à l'aide d'un mot de passe si le contrôle de l'âge est défaillant[169].

Les contenus pornographiques – y compris "soft" – font partie des contenus que la plupart des exploitants de plateformes interdisent d'ordinaire dans leurs conditions d'utilisation et qu'ils sont en mesure d'effacer de manière simple et rapide grâce à des fonctionnalités de notification et de retrait et à des programmes de filtrage.

Le contexte international dans lequel s'inscrit souvent la diffusion de pornographie illicite constitue un obstacle de taille pour les autorités pénales du fait de l'hétérogénéité des prescriptions et des mesures prévues par les différentes juridictions. Le SCOCI reçoit un nombre élevé de signalements relevant de la pornographie illicite (impliquant des enfants, notamment)[170]. Il mène des enquêtes en la matière au niveau fédéral et exerce aussi une surveillance indépendante des soupçons qui lui sont transmis.

4.5.3 Rassemblements de masse constituant une menace pour l'ordre public

4.5.3.1 Contexte

Les réseaux sociaux ont le potentiel, appréciable dans une société démocratique, de contribuer à la formation et à l'expression de l'opinion, en particulier pour les minorités. Ils permettent parfois de mobiliser dans un laps de temps très minime une grande quantité de personnes[171], ce qui peut toutefois, dans les cas extrêmes, avoir des conséquences négatives et menacer considérablement l'ordre public.

En marge d'une manifestation baptisée "Tanz dich frei", qui a eu lieu en mai 20013 à la suite d'une invitation lancée sur Facebook, une minorité de perturbateurs a ainsi causé d'importants dégâts dans le centre de Berne. En tant que partie plaignante dans le cadre de la procédure pénale, la ville a notamment demandé que Facebook soit mis en demeure de révéler les données d'identification relatives au compte en cause[172].

4.5.3.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Les graves débordements qui se sont produits le 21 septembre 2012 à Haren, aux Pays-Bas, illustrent bien les problèmes posés par les rassemblements de masse organisés via les réseaux sociaux. Le déclencheur a été une annonce d'événement postée sur Facebook par une adolescente qui fêtait son 16e anniversaire mais qui avait oublié de rendre l'invitation privée. L'information s'est répandue comme une traînée de poudre sur Twitter et Facebook sous le nom "Projet X Haren" et plusieurs milliers de jeunes se sont présentés sur place. L'ambiance, d'abord bon enfant, a dégénéré sous l'effet notamment de l'alcool, et les forces de l'ordre ont eu beaucoup de peine à contenir le déferlement de violence qui en a résulté.

Dans un rapport publié en mars 2013, une commission d'enquête a entre autres recommandé que les autorités se familiarisent avec le fonctionnement des réseaux sociaux. Un suivi ciblé des plateformes – sans surveillance systématique d'individus – devrait leur permettre à l'avenir d'anticiper les menaces de cette nature pour l'ordre public et de prévenir les dérapages. Les exploitants de réseaux sociaux doivent par ailleurs être incités à supprimer immédiatement tout appel à des activités litigieuses. Il

---

[168] ATF 131 IV 64 cons. 10.3.

[169] Arrêt du Tribunal fédéral 6S.26/2005, cons. 3.2

[170] La pornographie illicite impliquant des enfants a représenté près d'un tiers de toutes les annonces reçues en 2012; Rapport annuel 2012 du SCOCI, p. 4.

[171] Pour plus de détails sur les opportunités qu'ouvrent les réseaux sociaux en termes de diversité de communication, voir le point 3.2 ci-avant.

[172] Communiqué de la ville de Berne daté du 12 juin 2013: http://www.bern.ch/mediencenter/aktuell_ptk_sta/2013/06/strafanzeige/view?searchterm=tanz dich frei

convient en outre qu'ils rendent leurs membres, en particulier les plus jeunes, plus attentifs aux risques qu'implique le mélange, typique des réseaux sociaux, entre communication privée et publique.[173]

4.5.3.3 La législation en Suisse

Quiconque amène volontairement une personne à commettre un délit (à l'instar d'un dommage à la propriété) encourt, si l'infraction a été commise, la peine applicable à l'auteur de cette infraction (art. 24 CP). D'autre part, l'incitation publique à un délit impliquant de la violence contre autrui ou contre des biens est punie par le code pénal d'une peine privative de liberté de trois ans au plus ou d'une amende (art. 259 CP). Cette incitation n'a pas à porter sur des actes clairement définis ni à s'adresser à des personnes désignées, mais elle doit, selon la jurisprudence, dénoter une certaine insistance. Le fait de reprendre à son compte des messages émanant de tiers ("retweet") peut dès lors constituer une incitation explicite [174].

Un simple appel à participer à une manifestation non autorisée ne tombe en revanche pas sous le coup de cet article, mais il peut contrevenir à des prescriptions cantonales ou communales[175]. Comme cela a été dit plus haut pour d'autres dispositions pénales (notamment en matière de discrimination raciale; cf. point 4.5.1.3), la frontière entre propos publics et privés est toutefois souvent floue sur les réseaux sociaux.

Tout comme les atteintes à l'honneur, les incitations au sens de l'art. 259 CP entrent également dans le champ d'application de la disposition régissant la punissabilité des médias (art. 28 CP)[176]. En vertu de cette disposition, seul l'auteur de l'incitation publique peut être tenu pour pénalement responsable (ou, à défaut, si l'auteur ne peut être découvert ou ne peut être traduit devant un tribunal suisse, le rédacteur responsable ou la personne responsable de la publication en cause).

Les poursuites contre les auteurs de mises en ligne illicites sur les plateformes font l'objet du point 5.2, et les mesures de blocage et de suppression celui du point 5.4 ci-après.

4.5.4 Menace pour la santé publique

4.5.4.1 Contexte

Les réseaux sociaux offrent un espace d'échange et de rencontre à des intérêts très divers. Selon les thèmes abordés et les motivations de chacun, cela peut avoir des répercussions sociales ou sanitaires sur les utilisateurs. Les forums sur lesquels des individus dialoguent au sujet du suicide, de l'anorexie ou de l'automutilation sont ainsi susceptibles de glorifier ces phénomènes, voire de les encourager. Cela peut conduire à une minimisation du problème, au renforcement de tendances autodestructrices et, dans le pire des scénarios, à un passage à l'acte. Mais, s'il comporte des risques, Internet dispense également aux personnes concernées des informations qui peuvent les aider à surmonter des problèmes de ce type[177].

Autre problème, l'abondance de forums spécialisés dans l'échange d'informations sur les maladies, les médicaments et les traitements, dont la qualité n'est pas toujours vérifiable. En Suisse, 44% de la population utilise Internet pour se renseigner sur des thèmes liés à la santé, même si Internet est le plus souvent considéré comme une source information destinée à compléter des discussions avec

---

[173] Rapport de la commission "Project X – Haren" du 8 mars 2013, p. 31 ss; téléchargeable en néerlandais à l'adresse http://de.scribd.com/doc/129273298/Hoofdrapport-rellen-Haren

[174] Fiolka Gerhard, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, Art. 259 N. 12

[175] Voir à ce sujet l'art. 8 du règlement de la Ville de Berne sur les manifestations sur la voie publique (Reglement der Stadt Bern über Kundgebungen auf öffentlichem Grund) http://www.bern.ch/leben_in_bern/stadt/recht/dateien/143.1/.

[176] Voir Zeller Franz, Basler Kommentar Strafrecht II, 3. Aufl. Basel 2013, Art. 28, N. 65.

[177] Voir notamment, dans le domaine des troubles alimentaires, le site de l'Arbeitsgemeinschaft Ess-Störungen (AES); à l'adresse: www.aes.ch.

des professionnels ou des amateurs éclairés. Notons à cet égard que la demande d'informations en ligne sur la santé et d'applications participatives est appelée à augmenter. Parmi les personnes qui se servent d'Internet pour s'informer sur des questions de santé, deux sur trois ne se fient pas aux informations ainsi trouvées[178]. Cette population verrait comme un gage de confiance la mise en place de contrôles ou de certifications dans le domaine de la santé en ligne. Le risque demeure néanmoins que les internautes moins méfiants aillent puiser des informations partiales ou fausses sur les portails dédiés à la santé, ce qui pourrait, dans le pire des cas, avoir des répercussions néfastes sur leur santé.

4.5.4.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

En Allemagne, l'organisme "jugendschutz.net" s'emploie à sensibiliser la population sur les dangers liés aux portails s'adressant aux jeunes et glorifiant ou encourageant le suicide, l'anorexie ou l'automutilation[179]. "Jugendschutz.net" informe les jeunes et les parents, évalue l'offre Internet dans ce domaine et s'efforce d'éradiquer les contenus problématiques. L'organise dialogue également avec les exploitants de plateformes et propose aux prestataires qui souhaitent supprimer ce genre de contenus de renvoyer les internautes vers un site sur les troubles alimentaires qui recense les initiatives de sensibilisation et les organismes de conseil[180].

En vertu du § 18, al. 1 de la loi allemande sur la protection de la jeunesse[181], l'office fédéral compétent[182] est habilité à inscrire les médias papier et les télémédias susceptibles de mettre en danger le développement des enfants ou des adolescents sur une liste des médias dangereux pour la jeunesse. Cet office a notamment dans son collimateur les forums qui glorifient l'anorexie ou le suicide[183].

4.5.4.3 La législation en Suisse

Les échanges entre personnes partageant les mêmes affinités sur des thèmes comme les idées suicidaires, l'anorexie ou l'automutilation relèvent en principe de la liberté d'opinion et bénéficient donc de la protection qui va de pair. Aucune base légale ne permet concrètement d'entamer des poursuites si ce phénomène se révèle préjudiciable pour la société. La Confédération peut agir à titre informatif pour préserver la santé de la population. L'Office fédéral de la santé publique (OFSP) s'investit ainsi dans de nombreux domaines présentant des interfaces avec les thèmes du suicide, de l'anorexie et de l'automutilation. Jusqu'ici, il ne s'est néanmoins pas penché spécifiquement sur la question des pratiques dangereuses pour la santé susceptibles d'être encouragées par les réseaux sociaux.

Par ailleurs, il n'existe à ce jour aucune base légale restreignant les échanges entre particuliers à propos de médicaments ou de modes de traitement, tant que ces échanges ne visent pas à influer sur la concurrence[184]. L'OFSP appelle de ses vœux une plus grande transparence sur les informations de santé diffusées via Internet et sur les forums consacrés à ces questions. Il existe

---

[178] A ce sujet, voir: eHealth Suisse, rapport Portail de santé publique, adopté par le comité de pilotage le 26 janvier 2012, p. 6, 7, 12.

[179] http://www.jugendschutz.net/selbstgefaehrdung/index.html

[180] http://www.anaundmia.de/

[181] Jugendschutzgesetz du 23 juillet 2002, BGBl. I, p. 2730

[182] http://www.bundespruefstelle.de/

[183] Voir à ce sujet la décision de l'office fédéral de contrôle relative à l'inscription sur cette liste d'un blog dédié à l'anorexie: BPjM-Entscheid Nr. 5601 du 4 décembre 2008 – "Pro Ana"; consultable à l'adresse: http://www.doerre.com/jugendschutz/20081204_bpjm_index.pdf.

[184] Cf. art. 31 ss loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (LETh; RS 812.21), et art. 4, let. c ordonnance du 17 octobre 2001 sur la publicité pour les médicaments (OPMéd; RS 812.212.5), selon lequel la publicité diffusée par des moyens audiovisuels et autres supports d'images, de sons ou de données ainsi que par tout système de transmission de données, par exemple l'internet, fait partie des types de publicité destinée aux professionnels.

certes des labels de qualité attestant du sérieux des informations publiées dans ce domaine sur Internet[185], mais à ce jour, ils portent plus sur des sites Web donnés que sur les réseaux sociaux.

4.5.5 Manipulation de la formation d'opinion à des fins commerciales

4.5.5.1 Contexte

Certaines entreprises utilisent les réseaux sociaux pour diffuser, par l'intermédiaire d'acteurs rémunérés par elles et se présentant comme des consommateurs indépendants, des informations positives ou trompeuses sur leurs produits ou leurs services. Par ce procédé, une poignée d'individus est à même d'induire en erreur d'importants groupes de personnes. Le même résultat peut être obtenu au travers de faux blogs (en anglais *flogs*, pour *fake blogs*) ou de faux-nez (ou sockpuppets, c'est-à-dire de fausses identités en ligne) qui peuvent sembler indépendants mais qui ont été créés à des fins purement publicitaires. Ces méthodes sont également utilisées pour dénigrer des entreprises concurrentes.

D'autres problèmes peuvent découler du format de communication propre aux réseaux sociaux. Pensons par exemple à l'utilisation de Twitter à des fins publicitaires: les tweets étant limités à 140 caractères, la transparence quant à l'auteur, au contexte, à l'origine et à la motivation de certains messages peut se heurter à un problème de place.

4.5.5.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

L'UE ne reste pas les bras croisés face au phénomène des méthodes publicitaires opaques sur les réseaux sociaux[186]. La directive de l'UE relative aux droits des consommateurs[187], qui régit la conclusion de contrats entre des entreprises et des consommateurs, traite notamment du respect des obligations d'information des entreprises en ce qui concerne les contraintes techniques liées à certains médias, telles que les limitations du nombre de caractères sur certains écrans de téléphones portables. Cette directive formule des exigences minimales en matière d'information et impose que les consommateurs soient renvoyés vers d'autres sources d'information, par exemple un numéro de téléphone gratuit ou un lien hypertexte vers le site Web de l'entreprise. Elle est intéressante dans le contexte des réseaux sociaux dans la mesure où certains d'entre eux, Twitter par exemple, se caractérisent par un nombre limité de caractères. De plus, les utilisateurs sont toujours plus nombreux à se connecter aux réseaux sociaux via des appareils mobiles (smartphones, en particulier), ce qui soulève des problèmes d'information et de place.

Les autorités américaines en charge de la concurrence et des droits des consommateurs (Federal Trade Commission, FTC) ont émis des directives visant à protéger les consommateurs contre la publicité déloyale ou mensongère[188]et à aider les annonceurs à respecter le droit en vigueur[189]. Ces directives exigent que les liens financiers et matériels (versements ou cadeaux) unissant des annonceurs et des tiers faisant de la publicité pour leur compte (notamment des blogueurs, des

---

[185] Citons par exemple les labels attribués par la fondation Health on the Net (HON), www.hon.ch.

[186] Dans sa résolution sur l'effet de la publicité sur le comportement des consommateurs (2010/2052(INI)), le Parlement européen dénonce, au point 17, le développement d'une publicité cachée sur Internet non couverte par la directive relative aux pratiques commerciales déloyales via la diffusion de commentaires sur des réseaux sociaux, forums ou blogs, se distinguant difficilement dans leur contenu d'une simple opinion. Le Parlement suggère donc aux Etats membres d'encourager l'émergence d'observateurs/de modérateurs de forums formés aux risques posés par la publicité cachée.

[187] Directive 2011/83/UE relative aux droits de consommateurs, modifiant le directive 93/13/CEE et la directive 1999/44/CE et abrogeant la directive 85/577/CEE et la directive 97/7/CE

[188] Guides Concerning the Use of Endorsements and Testimonials in Advertising, FTC 16 CFR Part 255; à l'adresse: http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf

[189] En particulier la Section 5 Federal Trade Commission Act (15 U.S.C. 45) to the use of endorsements and testimonials in advertising; consultable à l'adresse: http://www.ftc.gov/ogc/ftcact.shtm . La FTC veille au respect des directives; en cas d'infraction, elle est habilitée à mener une enquête afin de déterminer si la pratique en cause est conforme au droit en vigueur; voir à ce sujet: http://www.ftc.gov/opa/2009/10/endortest.shtm.

célébrités etc.) soient indiqués en cas d'activité publicitaire sur les réseaux sociaux (y compris sur ceux, comme Twitter, où le nombre de caractères est limité)[190].

4.5.5.3 La législation en Suisse

Les dispositions de la loi fédérale sur la concurrence déloyale[191], qui régissent l'activité publicitaire indépendamment des produits, des secteurs ou des médias, s'appliquent également à Internet et, partant, aux activités publicitaires sur les réseaux sociaux[192].

Conformément à la clause générale de l'art. 2 LCD, la publicité dissimulée et la tromperie quant au caractère publicitaire de pratiques influant sur les rapports de concurrence constituent un comportement déloyal[193]. Dès lors que des individus reçoivent d'une entreprise des produits gratuits ou de l'argent en contrepartie d'avis positifs exprimés au sujet de cette entreprise et de son offre sur leurs blogs ou sur leurs profils et que ce lien n'est pas indiqué de manière transparente, ce comportement peut être déloyal au sens de la clause générale de l'art. 2 LCD[194] s'il est objectivement susceptible d'influencer le fonctionnement du marché concerné. La publicité trompeuse peut en outre entrer dans le champ d'application de l'art. 3, al. 1, let. b et i, LCD. Lors de la dernière révision en date de la LCD, l'art. 3, al. 1 a été pourvu d'une lettre s[195] sous laquelle est prévue une obligation d'information visant à renforcer la transparence en matière de commerce électronique.

Si des particuliers rémunérés en espèces ou en nature sont chargés par une entreprise d'utiliser leur profil sur des réseaux sociaux afin de donner une image négative des concurrents de celle-ci, l'art. 3, al. 1, let. a, LCD peut être applicable pour autant que la concurrence, ses marchandises, ses œuvres, ses prestations, ses prix ou ses affaires soient dénigrés par des allégations inexactes, fallacieuses ou inutilement blessantes[196]. Dans ce domaine, la difficulté pourrait consister à mettre en évidence le caractère publicitaire d'un profil privé sur les réseaux sociaux et à prouver le lien unissant le particulier en question à une entreprise donnée.

4.5.6 Manipulation de la formation de l'opinion publique (sur les sujets politiques)

4.5.6.1 Contexte

Des méthodes similaires à celles observées dans la vente peuvent être appliquées dans le domaine de la formation de l'opinion publique afin d'influencer la rhétorique politique, ce qui peut se révéler particulièrement problématique à l'approche de votes et d'élections. Des profils de réseaux sociaux, des groupes de réseau ou des blogs sont ainsi utilisés – de manière prétendument indépendante – pour promouvoir un ou une candidat(e) ou une opinion. Ce phénomène a été baptisé "astroturfing".

Des logiciels en cours de développement permettront bientôt à des individus de gérer plusieurs comptes sur des blogs, des forums Internet et des réseaux sociaux pour donner l'apparence d'une opinion majoritaire[197].

---

[190] Les directives recommandent par ailleurs aux annonceurs d'informer pleinement les blogueurs et autres célébrités faisant de la publicité pour eux sur les propriétés du produit qu'ils vantent et sur la situation juridique afin de prévenir les allégations trompeuses. Elles les invitent aussi à vérifier l'exactitude et la pertinence des messages publicitaires véhiculés par les tiers engagés par eux. L'annonceur est, au même titre que les tiers agissant pour leur compte, tenu pour responsable des allégations fausses et mensongères concernant ses produits.

[191] Loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD), RS 241

[192] Jöhri Yvonne, Werbung im Internet, Zürich 2000, p. 59

[193] Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, p. 180 ss; Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, p. 52

[194] Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011, p. 71 s.

[195] RO 2011 4910

[196] Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, p. 226 s.

[197] "Security-Firma entwirft Tools zur Meinungsmache mit Kunstfiguren", heise online du 20 février 2011; consultable à l'adresse: http://www.heise.de/newsticker/meldung/Security-Firma-entwirft-Tools-zur-Meinungsmache-mit-Kunstfiguren-1193436.html

4.5.6.2 La législation en Suisse

La liberté de vote garantie par l'art. 34, al. 2, Cst. protège également, dans une certaine mesure, contre l'intervention d'acteurs privés dans la libre formation de l'opinion. L'Etat est tenu de se montrer particulièrement vigilant à l'approche de scrutins. Si, peu avant un vote, des acteurs privés diffusent des contenus manifestement faux ou mensongers, les autorités doivent en informer les électeurs ou apporter les rectifications qui s'imposent. Un nouveau vote peut être organisé s'il paraît vraisemblable que le comportement d'acteurs privés a influencé de manière décisive l'issue du scrutin ou si les autorités ont failli à leur devoir d'information.

En ce qui concerne la propagande électorale déguisée sur les réseaux sociaux, l'Etat ne peut donc agir que dans la mesure où la dissimulation des véritables motivations sous-tendant des propos tenus sur les réseaux sociaux est susceptible d'induire les électeurs en erreur et où ces manœuvres se produisent peu avant un vote. Pour invalider un vote, il faut qu'il paraisse probable que les résultats ont été influencés de manière décisive par des méthodes opaques de cet ordre. Si la preuve de cette influence ne peut être apportée ou si les méthodes en cause ne sont pas mises en œuvre durant la période précédant tout juste un scrutin, les propos faux ou mensongers tenus par des tiers doivent être rectifiés dans le cadre des débats publics[198].

4.5.7 Publicité illicite pour certains produits ou services

4.5.7.1 Contexte

Afin de protéger certains intérêts publics, la Suisse connaît diverses interdictions de publicité qui ne sont pas toujours respectées lors des échanges sur les réseaux sociaux. Ces interdictions portent en particulier sur la publicité pour le tabac ou pour certains médicaments.

A cet égard, les règles édictées par la loi fédérale sur l'alcool (RS 680) sont en première ligne. Le Service Coordination commerce et publicité[199], qui veille au respect de la loi sur l'alcool, est de plus en plus amené à examiner des pages Facebook. En l'occurrence, le problème qui se pose est que les contributions non liées à un produit n'émanent bien souvent pas de l'administrateur de la page, mais d'utilisateurs ("amis") qui les publient volontairement à sa demande.

4.5.7.2 La législation en Suisse

Les campagnes publicitaires axées sur la Suisse qui sont diffusées via les réseaux sociaux doivent notamment se conformer aux limitations énoncées à l'art. 42*b* de la loi sur l'alcool, lesquelles incluent des prescriptions visant à protéger la jeunesse. L'art. 42*b*, al. 3, let. e interdit ainsi la publicité pour les boissons distillées "lors de manifestations auxquelles participent surtout des enfants et des adolescents ou qui sont organisées principalement pour eux". La question de savoir si ces manifestations peuvent également avoir pour cadre les réseaux sociaux n'a pas été tranchée à ce jour.

Dans la pratique, la Régie fédérale des alcools n'emploie pas seulement les moyens découlant du droit pénal administratif pour faire appliquer les prescriptions en matière de publicité; elle recourt aussi à des décisions de droit administratif. Leur application soulève diverses interrogations quant aux propos tenus sur les médias sociaux: à qui faut-il attribuer un message posté sur une plateforme? Comment poursuivre des fournisseurs à l'origine d'une campagne sur les réseaux sociaux lorsqu'ils sont basés à l'étranger?

---

[198] A ce sujet, voir: Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, p. 618 ss et Häfelin Ulrich/Haller Walter/Keller Helen, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich 2012, N. 1392 s., p. 443 s.

[199] Ce service vérifie uniquement les publicités se rapportant de manière explicite à la Suisse (par exemple du fait de la langue, de la monnaie, de la diffusion ou du produit).

4.6 Personnes nécessitant une protection particulière

4.6.1 Enfants et adolescents

4.6.1.1 Contexte

Les risques encourus par les enfants et les adolescents sur les réseaux sociaux sont de diverses natures et vont au-delà des atteintes aux intérêts individuels décrites ci-dessus, qui concernent globalement tous les utilisateurs. En la matière, le problème vient surtout des contenus pour adultes ou des manœuvres d'approche de tiers à des fins sexuelles[200]. Faute de connaissances techniques et de conscience du problème, les enfants et les adolescents ne sont pas toujours capables de se protéger contre les risques liés à des prises de contact dangereuses ou à la transmission de données personnelles[201]. Bien souvent, les adultes qui les encadrent, tels que les parents ou les enseignants, manquent eux aussi de l'expérience et des connaissances techniques nécessaires pour mettre en garde les enfants et les adolescents contre les risques que recèlent les réseaux sociaux. Les amitiés entre des élèves et des enseignants sur les réseaux sociaux sont également à considérer avec prudence en ce qu'elles peuvent se traduire par une proximité inappropriée. En mettant au jour certains pans de la vie privée des élèves et des enseignants, ces contacts sont en outre susceptibles de nuire au bon déroulement des cours.

La mise en œuvre technique d'une protection efficace de la jeunesse sur les réseaux sociaux butte notamment contre le manque de fiabilité des systèmes de vérification de l'âge. Ceux-ci sont en effet incapables de s'assurer que l'internaute indique son âge réel lorsqu'il se connecte sur un site[202].

4.6.1.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

La Recommandation du Conseil de l'Europe sur les services de réseaux sociaux exige qu'une protection particulière soit accordée aux enfants et aux jeunes utilisant les réseaux sociaux. Les exploitants sont à cet égard appelés à prévoir des mesures préventives, à créer des mécanismes visant à signaler tout contenu inapproprié et à lutter contre la cyberintimidation et la manipulation psychologique par Internet.

Le Conseil de l'Europe demande par ailleurs aux Etats membres d'étudier des moyens visant à supprimer les contenus Internet créés par des enfants et susceptibles de porter atteinte à leur dignité, à leur sécurité ou à leur sphère privée[203] et à former les enfants à l'utilisation de ces médias[204]. Il préconise également la création sur Internet d'espaces sûrs adaptés aux enfants et la mise en place d'un label paneuropéen et de systèmes de certification des contenus en ligne[205].

---

[200] D'après une récente enquête, les agressions sexuelles entre jeunes par le biais des médias électroniques sont un phénomène très répandu en Suisse. 9,5% des garçons et 28% des filles ont indiqué en avoir été victimes. La cybervictimisation constitue dès lors une sous-catégorie importante des agressions sexuelles sans contact physique. Les données couvrent toutefois les médias électroniques d'une manière générale. Elles ne se limitent donc pas aux réseaux sociaux, mais englobent aussi la téléphonie mobile ou le courrier électronique, par exemple. Voir l'Etude Optimus "Violences sexuelles envers des enfants et des jeunes en Suisse", février 2012, p. 9, 39 ss et 95 ss.

[201] Selon l'étude UE Kids en ligne 2011, menée dans 25 pays européens, 64% des enfants et des adolescents savent bloquer des messages indésirables et 56% savent modifier les paramètres de sécurité des réseaux sociaux. Ces chiffres montrent qu'une importante minorité d'enfants et de jeunes manque des connaissances requises pour prendre ces mesures de sécurité. Par ailleurs, 29% des 9-12 ans et 27% des 13-16 ans ont un profil public, et un cinquième d'entre eux y ont fait figurer des informations comme leur adresse ou leur numéro de téléphone. Voir EU Kids Online Final Report, September 2011, p. 17.

[202] Selon l'étude UE Kids en ligne 2011, 27% des 9-12 ans n'indiquent pas leur véritable âge sur les réseaux sociaux et 38% des 9-12 ans possèdent un profil sur un réseau social. Voir EU Kids Online Final Report, September 2011, p. 18.

[203] Déclaration du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur Internet

[204] Recommandation Rec(2006)12 sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication

[205] Recommandation MC/Rec(2009)5 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication

La Proposition de règlement général de l'UE sur la protection des données[206] contient elle aussi des dispositions relatives à la protection des enfants. S'agissant de l'offre de services de la société de l'information aux enfants, elle prévoit notamment que le traitement de données à caractère personnel relatives à un enfant *de moins de 13 ans* ne soit licite que si le consentement est donné par un parent de l'enfant ou par une personne qui en a la garde[207]. L'art. 11 stipule que les informations relatives au traitement des données à caractère personnel doivent être fournies en des termes clairs et simples, adaptés à la personne concernée, en particulier lorsqu'il s'agit d'un enfant.

A travers le programme "Internet plus sûr" 2009-2013[208], l'UE entend sensibiliser le public, promouvoir la création de points de contact pour le signalement des contenus illicites et des comportements préjudiciables en ligne (manipulation psychologique, harcèlement etc.), encourager les initiatives d'autorégulation et la participation des enfants à la création d'un environnement en ligne plus sûr et établir une base de connaissances sur les utilisations actuelles et émergentes des technologies en ligne et sur leurs conséquences pour les enfants[209].

L'un des volets du programme porte sur la *promotion de l'autorégulation au sein de la branche Internet*. C'est dans ce cadre que les principaux réseaux sociaux actifs en Europe ont signé, en 2009, les "principes de l'UE pour des réseaux sociaux plus sûrs"[210]. Ces principes incluent le paramétrage par défaut en mode "privé" des profils de mineurs et la mise en place de mécanismes de signalement et de suppression pour les contenus illicites et les prises de contact indésirables. A cela s'ajoutent la mise à disposition par les exploitants de paramètres de confidentialité bien conçus et d'informations intelligibles au sujet de la sécurité et de la sphère privée sur les réseaux sociaux, ainsi que des mesures visant à empêcher que des inconnus prennent contact avec des enfants et que les profils d'enfants soient accessibles par le biais des moteurs de recherche.

4.6.1.3 La législation en Suisse

Les prescriptions générales présentées plus haut concernant la protection contre les risques liés aux réseaux sociaux, telles que la loi sur la protection des données ou les dispositions civiles et pénales relatives à la protection de la personnalité, s'appliquent également aux enfants et aux jeunes. Les instruments de protection les plus pertinents à cet égard sont ceux contre la cyberintimidation et le harcèlement en ligne (point 4.4.2), contre l'usurpation d'identité (point 4.4.3) contre la pornographie (point 4.5.2) et contre les risques en matière de santé (point 4.5.4).

Au-delà de ces prescriptions générales, le droit suisse comporte de nombreuses dispositions portant spécifiquement sur la protection des enfants et des jeunes. Les besoins des enfants sont ainsi abordés dans la Constitution fédérale et dans plusieurs conventions internationales signées par la Suisse[211]. Au niveau des lois et des ordonnances, des règles de protection spécifiques sont

---

[206] Proposition de règlement général sur la protection des données, COM(2012) 11 final. En ce qui concerne les efforts déployés par l'UE dans le domaine de la protection des enfants, voir également la Communication de la Commission "Stratégie européenne pour un Internet mieux adapté aux enfants" COM (2012) 196 final, qui recense les exigences et recommandations formulées par la Commission en la matière.

[207] Art. 8 de la Proposition de règlement général de l'UE sur la protection des données, COM(2012) 11 final

[208] Décision n° 1351/2008/CE instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication

[209] Voir http://europa.eu/legislation_summaries/information_society/internet/l24190d_fr.htm et la Communication de la Commission "relative à l'évaluation intermédiaire du programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication", COM(2012) 33 final.

[210] Pour des liens vers les "principes de l'UE pour des réseaux sociaux plus sûrs" et vers les rapports de mise en œuvre de la Commission européenne, voir:
http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm . Autre initiative d'autorégulation à l'échelle de l'UE, la "CEO Coalition to make the Internet a better place for kids", créée en décembre 2011. Pour des documents de référence et des informations à ce sujet:
http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm .

[211] Voir les art. 11, 19, 41, 62, 67, 123*b* Cst. S'agissant des conventions internationale, voir notamment la Convention du 20 novembre 1989 relative aux droits de l'enfant (RS 0.107) et ses protocoles facultatifs ou la Convention n° 182 du 17 juin 1999 concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination

notamment prévues dans le droit pénal[212], le code civil[213], la législation sur la radio et la télévision[214], le droit du travail[215] ou la réglementation relative aux denrées alimentaires (consommation d'alcool)[216]. Le législateur fédéral s'est également penché sur le thème de la promotion de la jeunesse[217].

Il n'existe en revanche aucune disposition fédérale de protection de la jeunesse qui régisse spécifiquement les réseaux sociaux. Le champ d'application de certaines prescriptions visant à protéger les enfants et les jeunes inclut toutefois les réseaux sociaux; c'est le cas notamment de l'interdiction de la publicité pour le tabac ou l'alcool auprès des jeunes[218] ou de l'interdiction de rendre de la pornographie accessible aux moins de 16 ans.

A eux seuls, les instruments légaux ne suffisent néanmoins pas à protéger les enfants et les jeunes. En la matière, le comportement des parents est primordial. Dans le cadre de l'autorité parentale, ils peuvent décider de l'utilisation que font leurs enfants des réseaux sociaux et de leurs données personnelles si ceux-ci ne sont pas capables de discernement quant à leurs activités sur les réseaux sociaux ou si leur capacité de discernement peut être mise en doute. Notons que la capacité de discernement d'un enfant ne se jauge pas de manière abstraite, mais uniquement à l'aune d'actes concrets[219].

Lorsque les actes d'un enfant capable de discernement relèvent de ses droits strictement personnels, le pouvoir de représentation dont disposent ses parents atteint ses limites[220]. Les enfants capables de discernement exercent en effet de manière autonome leurs droits strictement personnels sauf dans les cas où la loi exige le consentement du représentant légal (art. 19*c* CC). Cette règle a toute son importance en ce qui concerne les activités sur les réseaux sociaux, car celles-ci relèvent précisément des droits strictement personnels des utilisateurs. Par conséquent, les enfants capables de discernement n'ont en principe pas besoin du consentement de leur représentant légal pour publier des données personnelles les concernant, notamment des photos, ou des contenus créés par eux sur les réseaux sociaux. De même, le consentement d'un enfant capable de discernement à une atteinte à sa personnalité est normalement valable (art. 13, al. 1, LPD; art. 28, al. 2, CC)[221].

Lancé en 2010 par le Conseil fédéral, le programme national "Protection des jeunes face aux médias et compétences médiatiques" a pour objectif de familiariser les enfants et les jeunes avec les opportunités et les risques inhérents aux technologies en ligne et de donner aux parents, aux enseignants et aux autres chargés d'éducation les moyens d'encadrer les activités des enfants sur

---

(RS 0.822.728.2). La Convention du Conseil de l'Europe du 25 octobre 2007 sur la protection des enfants contre l'exploitation et les abus sexuels a été approuvée par le Conseil fédérale et par l'Assemblée fédérale; voir FF 2012 7051 et FF 2012 7129.

[212] Art. 5, 136, 187, 188, 195, 197, 213, 219, 220, 363 ss et 264 ss CP; loi fédérale du 20 juin 2003 régissant la condition pénale des mineurs (DPMin), RS 311.1; loi fédérale du 20 mars 2009 sur la procédure pénale applicable aux mineurs (PPMin), RS 312.1

[213] Art. 296 ss, 307-317 CC

[214] Art. 5 et 13 LRTV et art. 4 et 16 ORTV

[215] Ordonnance du 28 septembre 2007 sur la protection des jeunes travailleurs (OLT 5), RS 822.115; ordonnance du DEFR du 4 décembre 2007 sur les travaux dangereux pour les jeunes, RS 822.115.2

[216] Art. 11 de l'ordonnance du 23 novembre 2005 sur les denrées alimentaires et les objets usuels (ODAIOUs), RS 817.02

[217] Loi fédérale du 20 septembre 2011 sur l'encouragement des activités extrascolaires des enfants et des jeunes (LEEJ), RS 446.1; ordonnance du 17 octobre 2012 sur l'encouragement des activités extrascolaires des enfants et des jeunes (OEEJ), RS 446.11; ordonnance du 11 juin 2010 sur des mesures de protection des enfants et des jeunes et sur le renforcement des droits de l'enfant, RS 311.039.1

[218] Ordonnance du 27 octobre 2004 sur les produits du tabac et les produits contenant des succédanés de tabac destinés à être fumés (OTab), RS 817.06, art. 18, et ordonnance du DFI du 23 novembre 2005 sur les boissons alcooliques, RS 817.022.110, art. 4

[219] BSK-ZGB I, Bigler-Eggenberger Margrith, 4. Aufl., Basel 2010, Art. 16, N. 14 ss, p. 177 ss

[220] BSK-ZGB I, Schwenzer Ingeborg, 4. Aufl., Basel 2010, Art. 304/305, N. 6, p. 1606

[221] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 70, p. 104

Internet. Son champ d'application couvre également les médias sociaux. Le portail Internet http://www.jeunesetmedias.ch/fr.html réunit des informations et des initiatives visant à aider les parents, les chargés d'éducation et les écoles.

En 2011, le Conseil fédéral a proposé, dans son rapport d'évaluation de la LPD, d'examiner des mesures visant à mieux protéger les données des mineurs en tenant compte du fait qu'ils sont moins conscients que les adultes des risques liés au traitement de leurs données personnelles.[222]

4.6.2 Salariés

4.6.2.1 Contexte

A l'échelle internationale[223] comme en Suisse[224], l'influence que peuvent avoir des données personnelles publiées sur les réseaux sociaux sur l'examen d'un dossier de candidature par un futur employeur est un thème récurrent. Il est de notoriété publique que les recruteurs se servent des moteurs de recherche sur Internet afin de se renseigner sur de futurs employés potentiels. Mais les utilisateurs n'ont souvent pas conscience que les informations qu'ils ont postées sur une plateforme sont susceptibles, selon les paramètres de confidentialité de leur profil, d'être trouvées par les moteurs de recherche. Sans compter que les employeurs peuvent avoir accès, via des profils de tiers, à des informations que des candidats à un poste révèlent sur les réseaux sociaux.

4.6.2.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Un projet de révision de la loi fédérale allemande sur la protection des données définit jusqu'à quel point la collecte de données est admissible avant la conclusion d'un contrat de travail[225]. A cet égard, il interdit aux employeurs de collecter des données relatives aux candidats à un poste sur les réseaux sociaux même si ces données sont librement accessibles (notamment via les moteurs de recherche externes). Les réseaux professionnels (tels que Xing ou LinkedIn) ne sont pas couverts par cette interdiction. Le projet est encore appelé à évoluer, notamment du fait de la révision en cours du droit européen en matière de protection des données.

En février 2013, des élus du Congrès américain ont déposé un projet de loi[226] interdisant aux employeurs, aux universités et aux établissements d'enseignement locaux de demander aux employés, candidats à l'embauche, étudiants et élèves de leur communiquer leurs identifiants et mots de passe donnant accès à leurs comptes sur les réseaux sociaux ou à leurs comptes privés de messagerie électronique. Les personnes concernées ne doivent en outre pas être pénalisées pour avoir refusé de communiquer ces informations. Des lois similaires sont déjà en vigueur dans certains Etats fédérés, tels que la Californie, le Maryland ou l'Illinois[227].

4.6.2.3 La législation en Suisse

En Suisse, il n'existe pas de dispositions légales répondant explicitement à la question de savoir si et dans quelle mesure les employeurs sont autorisés à se renseigner sur des candidats à l'embauche en recourant aux réseaux sociaux. L'art. 328*b* CO autorise l'employeur à traiter des données relatives au travailleur dans la mesure où ces données portent sur l'aptitude du travailleur à remplir son emploi ou

---

[222] Rapport du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données, point 5.2.2 (FF 2012 268)

[223] Voir à cet égard l'avis du Conseil économique et social européen "L'utilisation responsable des réseaux sociaux et la prévention de troubles associés", 2012/C 351/07, p. 2, 7 et 10.

[224] "Schweizer Konzerne überprüfen Bewerber im Internet", Tagesanzeiger du 2 mai 2011, http://www.tagesanzeiger.ch/leben/gesellschaft/Schweizer-Konzerne-ueberpruefen-Bewerber-im-Internet/story/17153295?dossier_id=510

[225] Gesetzesentwurf Beschäftigtendatenschutz, 17/4230

[226] Social Networking Online Protection Act du 6 février 2013, H.R.537

[227] "Kalifornien schützt private Online-Kommunikation vor Arbeitgebern und Unis", heise online (2 octobre 2012), http://www.heise.de/newsticker/meldung/Kalifornien-schuetzt-private-Online-Kommunikation-vor-Arbeitgebern-und-Unis-1721503.html

sont nécessaires à l'exécution du contrat de travail. L'application de cette prescription à la phase de candidature précédant la conclusion du contrat de travail est validée par le Tribunal fédéral et par une partie importante de la doctrine, même s'il existe des avis divergents[228]. Dès lors, le libellé de l'article pose une limite objective aux données que l'employeur est autorisé à collecter au sujet d'un candidat à l'embauche. Les profils privés, par opposition aux profils professionnels, sur les réseaux sociaux peuvent contenir des informations donnant un aperçu de l'aptitude du candidat. Mais, généralement, les profils privés comportent aussi et surtout des informations exclues du champ d'application de l'art. 328*b* CO, car les données relatives à la vie privée ne peuvent qu'exceptionnellement être qualifiées de données portant sur l'aptitude du travailleur[229]. Etant donné qu'en chargeant un profil, l'employeur accède immanquablement à l'intégralité de son contenu, il est plus que légitime de se demander s'il peut se fonder sur l'art. 328*b* CO pour prétendre à un droit de consultation des profils privés de candidats à l'embauche. Une partie de la doctrine estime dès lors qu'une recherche générale sur Internet à l'aide d'un moteur de recherche ou sur les réseaux sociaux d'orientation privée contrevient à l'art. 328*b* CO[230].

Si l'employeur accède à un profil privé par un comportement illicite (en enfreignant par exemple l'art. 143bis, al. 1, l'art. 179^{novies} ou l'art. 181 CP), il enfreint par la même occasion le principe de la licéité du traitement des données (art. 4, al. 1, LPD). Les principes de la bonne foi et du traitement reconnaissable des données (art. 4, al. 2, et 4 LPD) interdisent par ailleurs une collecte de données clandestine par l'employeur. Si l'employeur accède à un profil privé sans y avoir été autorisé par le titulaire, il contrevient de surcroît à l'art. 12, al. 2, let. b, LPD. Si l'employeur sollicite l'accès au profil privé d'un candidat à l'embauche, il y a lieu de se demander si le consentement est accordé librement car le candidat peut craindre d'être pénalisé en cas de refus.

La mesure dans laquelle la loi restreint l'exploration par l'employeur des données accessibles à tout un chacun (art. 12, al. 3, LPD) sur Internet, et en particulier sur les profils publics des réseaux sociaux, suscite également des divergences. Il est en général considéré qu'il y a atteinte à la personnalité dès lors qu'un employeur qui se trouve être membre d'un réseau d'orientation privée se renseigne à propos d'un candidat à l'embauche en épluchant des données accessibles à tout un chacun mais n'ayant aucun lien avec l'activité professionnelle passée ou future du candidat. S'agissant d'un réseau mettant l'accent sur la vie privée, tel que Facebook, les informations seraient utilisées par l'employeur dans un but qui n'avait pas été envisagé par la personne concernée lorsqu'elle les a publiées[231]. Dans la pratique, il est toutefois quasiment impossible de prouver que l'employeur a consulté des données accessibles via une simple recherche sur Internet. Dans le cas des profils créés sur des réseaux sociaux professionnels (tels que Xing ou LinkedIn), il est à supposer que les utilisateurs y ont placé à dessein des informations destinées à des employeurs potentiels[232]. Mais, là aussi, bon nombre d'informations ne sont disponibles qu'aux membres du réseau.

Pour apporter une solution satisfaisante aux problèmes qui se posent dans ce contexte, les exploitants de plateformes devraient proposer des paramètres de confidentialité suffisants, les employeurs devraient respecter la sphère privée des candidats à l'embauche et les utilisateurs devraient choisir avec soin les données qu'ils publient sur les réseaux sociaux. Dans ses recommandations relatives aux médias sociaux, le préposé fédéral à la protection des données et à la transparence conseille du reste aux utilisateurs de se demander avant toute publication de données

---

[228] Voir arrêt du Tribunal fédéral 2C_103/2008 du 30 juin 2008, cons. 6.2. Positions favorables à l'application l'art. 328*b* CO à la phase de candidature: BSK-OR I, Portmann Wolfgang, 5. Aufl., Basel 2011, Art. 328b, N. 34 ss, p. 1952 et Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, N. 4, p. 580. Contre: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008, N. 25, p. 731.

[229] BSK-OR I, Portmann Wolfgang, 5. Aufl., Basel 2011, Art. 328b, N. 8, p. 1947; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, N. 5, p. 581 ss

[230] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, N. 65 ss; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012, Art. 328b, N. 10, p. 597

[231] Voir Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, N. 66 s.

[232] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, N. 70 s.

les concernant s'ils souhaiteraient y être confrontés lors d'un entretien d'embauche, même dans dix ans[233].

4.6.3 Personnes handicapées

4.6.3.1 Contexte

Les nouvelles technologies de l'information et de la communication, réseaux sociaux y compris, ouvrent aux personnes handicapées de nouvelles possibilités de prendre part à la vie sociale, de s'informer et d'échanger, à condition toutefois qu'Internet et les services d'information, de communication et de transaction proposés par son entremise soient conçus pour être accessibles.

4.6.3.2 Solutions appliquées à l'étranger ou dans le cadre du droit international

Des recommandations internationales (règles pour l'accessibilité des contenus Web [WCAG] 2.0 du World Wide Web Consortium) visent à garantir l'accessibilité des technologies en ligne pour les utilisateurs en situation de handicap[234]. La Recommandation CM/Rec(2012)4 du Conseil de l'Europe sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux exhorte également les exploitants de plateformes à faire en sorte que leurs services soient accessibles aux personnes handicapées.

4.6.3.3 La législation en Suisse

En Suisse, les collectivités publiques sont, dans les limites du principe de proportionnalité, tenues par la loi de rendre leur offre sur les réseaux sociaux accessible aux personnes handicapées. Cette obligation découle, d'une manière générale, de l'interdiction des discriminations (art. 8, al. 2, Cst.) et, dans le cas particulier de la Confédération, de la loi sur l'égalité pour les handicapés[235], dont le champ d'application couvre entre autres les services proposés via Internet[236]. Les prestataires privés qui fournissent des services au public ont uniquement l'interdiction, conformément à l'art. 6 LHand, de traiter les personnes handicapées de manière discriminatoire du fait de leur handicap. Il ne découle toutefois de cette disposition aucune obligation de concevoir une offre Internet accessible à tous.

Au vu de l'importance prise par les réseaux sociaux en général, et plus particulièrement dans l'optique de la participation des personnes handicapées à la vie sociale, il est plus que souhaitable de garantir un accès sans entrave aux offres de réseaux sociaux. Des dispositions édictées par le législateur à l'échelon national n'auraient cependant que très peu de prise sur les réseaux sociaux les plus populaires. Il paraît malgré tout judicieux d'œuvrer pour le respect des normes d'accessibilité par d'autres mesures et en concertation avec les principales parties prenantes.

4.7 Postulat Amherd 12.3545 "Accès des enfants à Facebook"

Le postulat 12.3545[237] charge le Conseil fédéral d'exposer quelles mesures sont susceptibles de protéger les enfants contre les conséquences néfastes des médias sociaux en Suisse. Outre les modifications de la législation, il s'agit également d'indiquer les mesures visant à soutenir les parents, les titulaires de l'autorité parentale et les écoles. Le Conseil fédéral doit en particulier examiner la possibilité que propose Facebook de lier le profil des enfants à ceux – s'ils en ont - de leurs parents.

---

[233] Voir à cet égard http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=fr#sprungmarke20_9

[234] http://www.w3.org/Translations/WCAG20-fr/

[235] Loi fédérale du 13 décembre 2002 sur l'élimination des inégalités frappant les personnes handicapées (LHand, RS 151.3)

[236] En ce qui concerne les services en ligne de la Confédération, l'art. 10 de l'ordonnance du 19 novembre 2003 sur l'élimination des inégalités frappant les personnes handicapées (OHand, RS 151.31) stipule que l'information et les prestations proposées sur Internet doivent être accessibles aux personnes handicapées. En la matière, les pages Internet de la Confédération sont soumises à la norme P028 – "Directives de la Confédération pour l'aménagement de sites Web facilement accessibles". Voir à ce sujet http://www.isb.admin.ch/themen/standards/alle/03237/index.html?lang=fr.

[237] Voir http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20123545.

Dans ce contexte, il faut tenir compte des possibilités qu'offre la Suisse ID. A en croire des sondages, les moins de 13 ans sont, en Suisse, très rares à posséder un profil sur les réseaux sociaux [238].

Les projets de Facebook, qui envisage de ramener à moins de 13 ans l'âge requis pour utiliser son réseau et de lier les comptes de ces enfants à ceux de leurs parents, ne sont certainement pas totalement désintéressés car la société pourra ainsi capter un nouveau groupe-cible très friand de jeux, un marché en forte croissance qui génère de lucratives recettes pour Facebook. Le lien avec le profil des parents pourrait, en cas de contrats conclus par l'enfant, avoir valeur de consentement parental (tacite ou explicite) au contrat. Il n'est en outre pas à exclure que Facebook prenne l'initiative d'attaquer en justice une réglementation nationale et tente de la faire disparaître.[239]

Comme évoqué au point 4.6.1.3, les prescriptions légales d'ordre général concernant les risques liés aux réseaux sociaux protègent également les enfants et les jeunes. De plus, de nombreuses dispositions spécifiques visant à protéger cette population s'appliquent également aux réseaux sociaux.

L'idée de lier les profils des enfants à ceux de leurs parents est problématique à plusieurs égards. Tout d'abord, elle suppose que les parents possèdent eux-mêmes un profil sur le réseau social et qu'ils l'utilisent, ce qui serait évidemment favorable au réseau social en question mais qui risque de déplaire à de nombreux parents qui, pour une raison ou une autre, ne souhaitent pas l'utiliser. De plus, ce lien entre les profils est susceptible de restreindre les droits à la personnalité des enfants capables de discernement.

Avant de mettre en œuvre un contrôle automatisé de l'identité permettant entre autre de vérifier l'âge des utilisateurs, les réseaux sociaux doivent créer les conditions requises dans leurs systèmes et contrôler les preuves d'identité. Or, il est pour le moment impossible de dire si la Suisse ID satisferait aux exigences de Facebook en la matière.

4.8 Tentative d'appréciation globale de la législation en vigueur

Les prescriptions légales présentées dans le présent chapitre au regard des différentes questions juridiques soulevées par les réseaux sociaux offrent un tableau très nuancé. Il est donc très difficile d'en tirer des conclusions universelles. Sur la base des expériences faites jusqu'ici, il est néanmoins possible de dire qu'en cas de litige, les dispositions des textes législatifs suisses, à la formulation souvent générale, peuvent être interprétées et appliquées de manière à permettre des solutions équilibrées. La législation ne présente par ailleurs aucune lacune frappante.

A ce stade, les tribunaux et les autorités suisses n'ont toutefois été que peu confrontés à cette thématique. Il y a dès lors lieu de se demander si le droit en vigueur est suffisamment incitatif pour amener les personnes concernées à faire valoir leurs droits. Les divers aspects du droit de la protection des données pourraient notamment receler un potentiel d'amélioration (en particulier les ressources allouées au PFPDT et le caractère non obligatoire des paramètres de confidentialité; cf. point 4.3.1.5 plus haut). Des évolutions techniques pourraient conduire à ce que la population défende plus efficacement ses droits.

Dans bien des domaines, l'incertitude règne quant à savoir si, en cas de litige porté devant les tribunaux, l'application des prescriptions générales aux nouvelles questions juridiques donnerait des résultats satisfaisants. Cette incertitude tient notamment au fait que les moyens de défense existants risquent d'être difficiles à imposer dans le contexte international qui est celui des réseaux sociaux.

---

[238] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts, 2013, point 1.4, p. 27; le problème semble plus aigu en Allemagne, où la première inscription a lieu à l'âge moyen de 12,7 ans: Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013, p. 62.

[239] Voir notamment http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html#

5 Problème de fond: l'application du droit

5.1 Généralités

Le chapitre 4 examinait si le droit suisse applicable (notamment LPD, CC, LCD et CP) répond de manière adéquate aux problèmes juridiques spécifiques des médias sociaux.

Le présent chapitre revient sur l'application du droit en vigueur, une question centrale dans les médias sociaux. En effet, les responsables d'infractions juridiques (p. ex. l'auteur de contenus illicites publiés sur une plateforme sociale) ne peuvent souvent pas être amenés à rendre des comptes. Il faut donc se demander si le droit suisse définit suffisamment les responsabilités des personnes impliquées.

De plus, les exploitants de réseaux sociaux étant fréquemment actifs au niveau international, la législation nationale atteint par essence ses limites.

5.2 Poursuite des auteurs de contenus illicites publiés sur des plateformes

5.2.1 Problème de l'anonymat

Comme expliqué au chapitre 4, les contenus publiés sur les plateformes sociales peuvent enfreindre de nombreuses dispositions du droit pénal (p. ex. diffamation, pornographie, discrimination raciale, incitation publique au crime ou à la violence) ou du droit civil (p. ex. protection de la personnalité). Dans la pratique, il est parfois difficile de faire appliquer ces dispositions. Les auteurs d'éventuelles contributions illicites ne peuvent être appelés à rendre des comptes que si leur identité est connue. Or, ce n'est pas toujours le cas, vu que les contenus anonymes (ou publiés sous un pseudonyme) sont devenus monnaie courante dans la colonne de commentaires des blogs ou sur des réseaux comme Facebook. Dans de tels cas, une identification s'avère compliquée, voire impossible.

Parfois, les autorités de procédure pénale en Suisse peuvent suivre l'une ou l'autre piste, notamment grâce aux adresses IP, c'est-à-dire les adresses de réseau internet dont les utilisateurs n'ont en général pas connaissance, mais que les exploitants du système enregistrent lorsqu'un usager navigue sur une plateforme sociale ou qu'il envoie un courriel. La possibilité d'accéder à ces adresses dépend aussi de l'exploitant de la plateforme concernée.

5.2.2 Contributions anonymes sur les plateformes de journalistes professionnels

L'ordre juridique suisse reconnaît depuis longtemps que les publications anonymes ne reposent pas systématiquement sur des motifs répréhensibles[240]. Le code pénal protège la publication anonyme dans une large mesure, même expressément. Selon l'art. 28a CP et l'art. 172 CPP, les personnes qui, à titre professionnel, participent à la publication d'informations dans la partie rédactionnelle d'un média à caractère périodique peuvent cacher l'identité de l'auteur. Elles et leurs auxiliaires ont donc le droit de refuser la remise – exigée par les autorités de procédure pénale – des adresses IP des auteurs anonymes. Ce droit vaut également pour les plateformes sociales comme les blogs, lorsqu'ils sont exploités par des journalistes professionnels. Le Tribunal fédéral a par exemple accepté le refus de la SSR de transmettre au ministère public du canton de Zoug l'adresse IP d'une personne qui avait placé sur le blog de la SSR, sous un faux nom, un commentaire prétendument diffamatoire sur l'émission "Alpenfestung"[241]. Si l'auteur ne peut pas être identifié ou traduit en justice en Suisse, une sanction du rédacteur responsable (ou, à défaut, de la personne responsable de la publication) pour défaut d'opposition à une publication constituant une infraction (art. 322bis CP) peut aussi être envisagée.

5.2.3 Contributions anonymes sur d'autres plateformes

La situation est différente pour les exploitants de plateformes qui ne sont pas journalistes professionnels. Ceux-là peuvent être obligés par les autorités compétentes à communiquer les

[240] Voir notamment ATF 55 II 94 E. 1 p. 98

[241] ATF 136 IV 145

adresses IP de personnes suspectes. Les données correspondantes doivent être enregistrées conformément à la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS 780.1). La LSCPT contraint tous les fournisseurs de services de télécommunication et d'accès à l'internet (art. 1, al. 2) à conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation (art. 15, al. 3), et à les transmettre sur demande au service chargé de la surveillance de la correspondance par poste et télécommunication (art. 15, al. 1). Selon la pratique actuelle et le texte français de l'art. 1, seuls les fournisseurs d'accès internet sont soumis à cette obligation. Les exploitants de plateformes doivent uniquement fournir des données déjà disponibles. En vertu de l'art. 22, al. 4, du projet de révision de la LSCPT[242], le Conseil fédéral doit pouvoir obliger les fournisseurs de services qui utilisent des services de télécommunication et qui permettent une communication unilatérale ou multilatérale (fournisseurs de services de communication dérivés) à conserver les données tout comme les FST. Lorsqu'un fait punissable est commis sur l'internet, le droit en vigueur habilite les autorités de procédure pénale à découvrir l'identité du titulaire du raccordement même sans décision de justice et à procéder par exemple à une perquisition au domicile de ce dernier. C'est pourquoi le Tribunal fédéral a confirmé en 2010 la punition infligée à l'exploitant d'une plateforme internet pour entrave à l'action pénale (art. 305 CP). En tant que fournisseur, celui-ci avait détruit les adresses IP d'auteurs anonymes de commentaires prétendument injurieux, pour permettre à ces suspects d'échapper aux poursuites pénales[243].

Il est plus difficile de faire appliquer la loi lorsque les adresses IP ne sont connues que de l'exploitant d'une plateforme étrangère non soumise aux dispositions de la LSCPT. Dans ce cas, les autorités suisses doivent collaborer avec l'exploitant étranger ou emprunter la voie contraignante de l'entraide judiciaire internationale en matière pénale. Les exploitants étrangers d'une plateforme ne sont pas toujours disposés à supprimer un contenu, mais consentent parfois à communiquer à l'autorité de procédure pénale, à sa demande, l'adresse IP d'une personne qui a publié un propos illicite, par exemple.

5.2.4 Le problème de la compétence territoriale

S'agissant de la poursuite des infractions perpétrées sur les plateformes de médias sociaux, il faut d'abord désigner l'autorité compétente, ce qui soulève des problèmes pratiques. Ce n'est qu'ensuite que les demandes internationales d'entraide judiciaire (p. ex. à Facebook) peuvent être adressées et les éventuelles infractions examinées. Vu que les propos publiés sur les plateformes internationales sont accessibles partout, le risque existe que ni les Ministères publics cantonaux, ni le Ministère public de la Confédération ne soient considérés comme compétents pour lancer la procédure. C'est pourquoi l'art. 27, al. 2, CPP habilite ce dernier à ouvrir une procédure lorsque la compétence n'est pas clairement établie. Si le Ministère public de la Confédération applique cette disposition avec rigueur, les infractions commises sur les réseaux sociaux peuvent aussi faire l'objet de poursuites pénales.

5.3 Responsabilité des exploitants de plateformes et des fournisseurs de services

5.3.1 Ebauches de solutions à l'étranger ou dans le droit international

Dans l'UE, la responsabilité des fournisseurs de services internet est définie par les règles spécifiques de la *directive sur le commerce électronique (CE-DR)*[244]: l'art. 12 CE-DR stipule que ni les fournisseurs d'accès à l'internet ni d'autres fournisseurs de services ne peuvent être rendus responsables des informations transmises. Selon l'art. 14 CE-DR, les prestataires qui stockent des informations de tiers (prestataires de services d'hébergement) ne sont pas non plus responsables, à

[242] FF 2013 2483

[243] Arrêt du Tribunal fédéral 6B_766/2009 du 8.1.2010

[244] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("Directive sur le commerce électronique"), JO L 178 du 17.7.2000, p. 1

condition toutefois qu'ils n'aient pas eu connaissance de l'activité illicite. Dès le moment où ils en ont, ils doivent retirer les informations concernées ou rendre l'accès à celles-ci impossible.

Il n'existe cependant aucune obligation de surveiller les informations transmises ou stockées, ou de rechercher activement des contenus illicites (art. 15 CE-DR). La Cour de justice de l'Union européenne (CJUE) a également reconnu que les fournisseurs ne doivent pas être contraints d'examiner au préalable tous les contenus qu'ils stockent ou rendent accessibles. Elle a rejeté toute obligation générale de filtrage aussi bien pour les fournisseurs d'accès[245] que pour les prestataires de services d'hébergement[246].

Toutefois, lorsque le fournisseur ne se limite pas au traitement automatique des informations fournies par sa clientèle, mais qu'il choisit ou modifie lui-même les informations transmises, le privilège de l'absence de responsabilité et d'obligation de surveillance accordé par l'art. 15, al. 1, CE-DR tombe[247]. L'exploitant de la plateforme ne joue pas un rôle actif s'il stocke les offres sur son serveur, fixe les modalités de son service, reçoit une rémunération pour ce dernier et donne des renseignements généraux à ses clients. Par contre, la CJUE estime que l'exploitant joue un tel rôle par exemple lorsqu'il optimise la présentation d'un contenu ou promeut celui-ci[248].

Au niveau des *droits de l'homme*, la question de savoir dans quelles circonstances un exploitant de plateforme peut être poursuivi civilement pour des commentaires illicites d'utilisateurs (portant atteinte à la personnalité, par exemple) et condamné au paiement d'une indemnité pour tort moral suscite la controverse. Le recours de l'exploitant estonien d'un portail d'informations jugé pour violation de la liberté d'expression (art. 10 CEDH) est pendant auprès de la Cour européenne des droits de l'homme depuis 2009[249].

5.3.2 Situation juridique en Suisse

Comme à l'étranger, il est clair en Suisse également que les auteurs de contenus illicites (fournisseurs de contenus) publiés sur des médias sociaux sont juridiquement responsables lorsqu'ils peuvent être identifiés et traduits en justice. En revanche, contrairement à la plupart des pays européens, la Suisse ne dispose d'aucune réglementation spécifique concernant la responsabilité des autres personnes impliquées dans la chaîne de communication (p. ex. les prestataires de services d'hébergement et les fournisseurs d'accès). Les dispositions générales sur la responsabilité pénale et civile s'appliquent. La critique ayant souvent été émise que, en raison de l'absence d'une réglementation spécifique, la situation juridique manque de clarté, le Conseil national et le Conseil des Etats ont exigé un cadre juridique plus strict et déposé une motion en ce sens en 2001.

Dans la foulée, une commission d'experts sur la cybercriminalité a été mise en place. En 2004, sur la base du rapport établi par celle-ci, le Conseil fédéral a mis en consultation un avant-projet de modification du Code pénal (CP) et du Code pénal militaire (CPM). Une réglementation explicite de la responsabilité pénale des fournisseurs de services et des exploitants de moteurs de recherche a été saluée, mais des controverses sur des points de détail sont également apparues. En 2008, le Conseil fédéral a décidé de renoncer à réglementer la responsabilité pénale.

---

[245] Arrêt CJUE du 24.11.2011 SABAM / Scarlet Extended, Rs C-70/10 (Injonction aux fournisseurs d'accès en vue du filtrage et du blocage de fichiers partagés contraire au droit européen)

[246] Arrêt CJUE du 16.2.2012 SABAM / Netlog NV, Rs C 360/10 (Pas d'obligation pour les prestataires de services d'hébergement qui surveillent les contenus stockés sur une plateforme de réseau social et installent un système de filtrage pour empêcher les atteintes au droit d'auteur)

[247] Arrêt CJUE du 19.7.2011 L'Oréal / E-Bay, Rs C-324/09, Rec. I-6011 (Responsabilité pour les fournisseurs jouant un "rôle actif")

[248] Arrêt CJUE du 19.7.2011Rz. 115s. L'Oréal / E-Bay, Rs C-324/09, Rec. I-6011 Rz. 115s.

[249] Requête n° 64569/09 "Delfi AS c Estonie"; l'affaire a été soumise par la Cour de justice à l'avis du gouvernement estonien le 11.2.2011.

Par la suite, le Conseil fédéral a déclaré à plusieurs reprises qu'une réglementation spécifique pour les fournisseurs d'accès et les prestataires de services d'hébergement n'était judicieuse ni en droit pénal, ni en droit civil (voir motion Riklin 09.4222 "Responsabilité juridique des fournisseurs Internet", initiative parlementaire Hochreutener 08.418 "Accroître la sécurité du droit dans le domaine de la cybercriminalité" et interpellation Stöckli 12.4202 "Swisscom. Gestion des contenus protégés par les droits d'auteur").

- Dans le domaine *pénal*, il est d'avis qu'il existe des solutions pertinentes reposant sur le droit pénal des médias (art. 28 CP) et les principes généraux sur l'identification des auteurs et la participation (art. 24ss CP).

- Dans le domaine *civil*, les fournisseurs de services sont responsables au même titre que les autres fournisseurs de prestations. Conformément au droit des obligations (CO), celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou par imprudence, est tenu de le réparer (art. 41, al. 1, CO)[250].

La responsabilité des exploitants de plateformes de médias sociaux qui n'entrent pas dans les catégories habituelles de fournisseurs n'a pas encore été clarifiée[251]. En général, les exploitants jouent un rôle plus actif que les hébergeurs, qui ne permettent que le téléchargement automatique d'informations sur leur serveur. En outre, ils ont un rapport plus étroit avec les contenus diffusés que les hébergeurs, qui se bornent à mettre à disposition un espace de stockage. Les exploitants de plateformes réglementent la mise en forme, l'étendue et la teneur des contenus générés par les utilisateurs. Contrairement aux hébergeurs traditionnels, ils sont souvent en mesure d'exercer une fonction de surveillance et d'intervenir si nécessaire. Dans leur cas, renoncer à un filtrage en effectuant des contrôles ponctuels ou en intervenant en temps utile contre des contenus manifestement illicites pourrait avoir des répercussions aux niveaux pénal et civil. Leurs obligations n'ont été jusqu'ici que vaguement esquissées par la justice et les facultés de droit[252].

En présence de délits d'opinion, on peut se demander dans quelle mesure les exploitants de plateformes doivent être soumis aux dispositions spéciales du droit pénal des médias (art. 28 CP) et si une responsabilité subsidiaire pour défaut d'opposition à une publication litigieuse (art. 322bis CP) s'applique dans leur cas aussi. L'un des problèmes est que de nombreuses plateformes proposent aussi bien des contenus s'adressant à une large audience que des publications destinées à un public restreint. Or, le droit pénal des médias en vigueur n'est pas conçu pour de telles formes mixtes. A l'inverse des éditions de presse, des radiodiffuseurs ou des exploitants de sites internet, les exploitants de réseaux sociaux ne constituent pas des entreprises de médias au sens habituel du terme.

La littérature juridique précise que la disposition spéciale en matière de droit pénal des médias édictée à l'époque de la presse écrite (art. 28 CP) ne répond plus aux exigences actuelles du monde en ligne. Pour certains délits (p. ex. la pornographie douce) ainsi que pour les contenus publiés dans les diverses applications internet des médias de masse, son champ d'application est flou. Les limites pénales doivent donc être redéfinies dans le cadre d'une révision de la loi[253].

Le Conseil fédéral est conscient que des règles juridiques claires répondent à un souhait des fournisseurs, des clients et des autorités, mais aussi de la justice. Cependant, vu le grand nombre

---

[250] Avis du Conseil fédéral du 5.3.2010 sur la motion 09.4222 – Responsabilité juridique des fournisseurs Internet

[251] Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: medialex 2009, p. 21s.

[252] Voir toujours Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: medialex 2009, p. 19ss

[253] Christian Schwarzenegger, Der Anwendungsbereich des Medienstrafrechts (Art. 28, 322bis StGB), in: Cavallo u.a. (Ed.), FS-Donatsch, Zürich 2012, p. 187

d'acteurs impliqués et leurs divers besoins ou problèmes, tout projet de loi relatif à la responsabilité des fournisseurs de services internet et à la poursuite des infractions juridiques sur la toile est placé devant un défi de taille: trouver une solution qui réponde si possible à toutes les exigences. Le risque est alors grand de réglementer trop ou pas assez.

Dans sa réponse à des interventions parlementaires récentes (motion Riklin 13.3215; Régler la responsabilité des fournisseurs de prestations Internet, et question Glättli 13.5059, Responsabilité des fournisseurs d'hébergement et des services de blogs et de forums), le Conseil fédéral a reconnu un besoin de légiférer au niveau civil. Dans l'intervalle, le Tribunal fédéral s'est penché pour la première fois sur la responsabilité civile des fournisseurs de services d'hébergement relative aux contenus illicites (portant atteinte à la personnalité)[254]. Dans le cadre d'une action en suppression et en identification, il a refusé un privilège de responsabilité à un fournisseur qui met des blogs de tiers à disposition sur son serveur pour consultation. La Suisse n'ayant jusqu'ici pas prévu de règles spéciales, les dispositions générales de l'art. 28 CC s'appliquent[255]. Il appartient dès lors au législateur, et non à la justice, de corriger les éventuels effets indésirables de cette situation juridique[256]. Le Tribunal fédéral a expressément renvoyé au présent rapport, alors en cours d'élaboration.

Dans la jurisprudence actuelle, la justice considère les dispositions générales sur la responsabilité civile insuffisantes et espère que le législateur clarifiera les choses dans ce domaine. Les déclarations de la justice et de la doctrine[257], ainsi que les développements à l'étranger[258], suggèrent d'examiner en profondeur la nécessité de légiférer au niveau civil. Le Conseil fédéral est d'ailleurs prêt à s'engager dans cette voie (voir ci-après point 7.2.4).

5.4 Suppressions et décisions de blocage

5.4.1 Suppression de contenus problématiques sur la plateforme

Lorsqu'un contenu illégal publié sur une plateforme de médias sociaux présente un lien quelconque avec la Suisse, l'autorité de poursuite pénale peut entreprendre des démarches en vue de sa suppression. Au niveau juridique, elle peut se baser sur les dispositions relatives au séquestre (art. 263 CPP), pour autant que le contenu incriminé serve de moyen de preuve ou soit confisqué d'une autre manière. En outre, fedpol peut, conformément à l'art. 13e de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS 120), ordonner la suppression d'un site internet si celui-ci est utilisé à des fins de diffusion de matériel de propagande incitant à faire usage de la violence et si le matériel de propagande se trouve sur un serveur suisse. Lorsque ce matériel se trouve sur un serveur étranger, fedpol peut recommander aux fournisseurs d'accès suisses de bloquer le site concerné. Dans le domaine de certaines infractions aux dispositions sur la publicité (p. ex. loi sur l'alcool), l'autorité administrative compétente (p. ex. Régie fédérale des alcools) peut en outre faire respecter le droit au moyen d'une décision administrative. Ici aussi, l'exécution du droit risque d'être problématique dans le cas de propos venant de l'étranger.

---

[254] Arrêt 5A_792/2011 du 14 janvier 2013

[255] Arrêt 5A_792/2011 du 14 janvier 2013, E. 6.1

[256] Arrêt 5A_792/2011 du 14 janvier 2013, E. 6.3

[257] Kernen Alexander, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, in: Jusletter 4. März 2013, Rz 20ff.; Bühlmann Lukas, Blog-Hoster sind mitverantwortlich für persönlichkeitsverletzende Blogbeiträge, in: Digitaler Rechtsprechungs-Kommentar Weblaw, 13. März 2013, Rz 10f.; Schoch Nik / Schüepp Michael, Provider-Haftung „de près ou de loin"?, in: Jusletter 13. Mai 2013, Rz. 43ss; Hürlimann Daniel, Replik: Das Leistungsschutzrecht für Presseverlage, in: Jusletter 13. Mai 2013, FN 30

[258] Par exemple la requête n° 64569/09 "Delfi AS c Estland" susmentionnée (note de bas de page *250) déposée auprès de la CEDH, relative à l'obligation d'un portail d'informations de payer une indemnité pour tort moral en raison de la diffusion automatisée de contenus illicites étrangers (commentaires portant atteinte à la personnalité)

Lors de la suppression, seuls les contenus illicites doivent être éliminés. Les propos conformes au droit devront rester accessibles, afin de ne pas restreindre de manière exagérée et disproportionnée la liberté d'opinion (art. 16 Cst.) (voir aussi ci-après point 4.2.2).

Selon l'expérience du SCOCI, la suppression de contenus illicites est facile à réaliser sur les plateformes sociales – Facebook par exemple – qui agissent de leur propre initiative après une communication dans ce sens. Les exploitants de plateformes ayant leur siège en Suisse n'ont pas encore établi d'autoréglementation valable pour toute la branche. Les exploitants allemands, par exemple, y ont aussi renoncé jusqu'ici[259], en raison notamment des imbrications au niveau international.

Des tentatives d'autoréglementation de la branche existent toutefois du côté des fournisseurs de services d'hébergement qui proposent aux exploitants de plateformes (et à d'autres intéressés) un espace de stockage pour la publication automatisée de leurs offres. En 2013, après trois ans de travaux préparatoires, plusieurs grands fournisseurs suisses de services d'hébergement[260] ont élaboré un "Code of Conduct"[261] – sous la direction de l'association professionnelle simsa –, qui clarifie leur rôle dans la poursuite de contenus illicites sur l'internet, soit les infractions perpétrées dans le domaine de la pornographie, de la représentation de la violence, du racisme et de l'atteinte à l'honneur, mais aussi les violations des droits d'auteur et de la personnalité. Si l'exploitant d'un site internet ou d'une plateforme sociale ne parvient pas à être identifié, qu'il ne réagit pas aux demandes ou encore qu'une plainte pénale semble avoir peu de chances d'aboutir, les personnes lésées peuvent adresser leur réclamation au fournisseur de services d'hébergement. Conformément au "Code of Conduct", ce dernier doit transmettre les griefs formulés à l'exploitant du site internet (ou plateforme) concerné et l'enjoindre à clarifier la situation puis, cas échéant, à supprimer les contenus illicites. Dans les cas évidents, le fournisseur de services d'hébergement peut même bloquer provisoirement l'accès au site internet incriminé.

En Allemagne, des recherches ont montré que les modèles d'autoréglementation (et l'autoréglementation régulée par l'Etat) présentent certains avantages par rapport à une réglementation étatique étrangère, mais que leur fonctionnement est aussi complexe que fluctuant. L'autoréglementation parvient à ses limites notamment avec des fournisseurs externes (p. ex. étrangers) qui ne font pas partie de l'association professionnelle[262].

5.4.2 Blocage de l'accès à des contenus problématiques par le fournisseur d'accès

Lorsque la suppression du contenu problématique sur la plateforme de médias sociaux concernée (en général étrangère) ne peut être effectuée, ou effectuée à temps, un blocage de l'accès peut être envisagé. S'agissant de la pornographie enfantine ou d'abus commis sur des enfants, le SCOCI met à disposition des fournisseurs suisses d'accès à l'internet une liste des sites étrangers qui contiennent de toute évidence de la pornographie enfantine et qui restent accessibles depuis la Suisse malgré l'envoi d'une demande de suppression à l'étranger. Sur la base de leurs conditions générales, les fournisseurs sont habilités à bloquer ces sites et leur contenu, et à afficher à la place un avis de blocage du SCOCI. Cette coopération volontaire entre les autorités et l'économie privée a fait ses preuves. Elle permet de bloquer chaque année des centaines de milliers de requêtes de pages ayant des contenus illicites et de protéger au mieux les droits des victimes.

Il arrive aussi que de tels blocages soient ordonnés par les autorités suisses de poursuite pénale; un juge d'instruction vaudois a pris par exemple une telle mesure en réaction à des contenus injurieux

---

[259] http://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html

[260] En font partie, selon Simsa, les principaux fournisseurs suisses de services d'hébergement, à savoir Cyon, Green, Hostpoint, Metanet, Nine, Swisscom et Webland

[261] Code of conduct hosting (CCH); http://static.simsa.ch/1362151411/130201_simsa_cch_public_web.pdf

[262] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts, 2013, chiffre 2.2.2.1.4. p. 45

publiés sur le site internet "Appel au peuple"[263]. La littérature juridique critique toutefois le fait que les décisions correspondantes ne reposent sur aucune base juridique dans la législation suisse[264].

Il faut garder à l'esprit que les mesures de blocage sont susceptibles de condamner aussi des contenus conformes au droit. Par exemple, lorsque l'accès à certains noms de domaine est bloqué, d'autres offres légales proposées par ces ressources disparaissent elles aussi[265]. Fin 2012, dans un cas turc[266], la Cour européenne des droits de l'homme a ainsi contesté le blocage de toute la plateforme de sites Google ordonné en réaction à un seul site internet litigieux. De telles mesures doivent donc reposer sur une base juridique suffisamment stricte et précise, et faire l'objet d'un contrôle particulièrement sévère de la part de la justice nationale, de sorte à éviter toute mesure arbitraire.

Vu les bases légales existantes et l'efficacité de la coopération entre les autorités et les fournisseurs d'accès à l'internet, le Conseil fédéral a estimé, dans sa réponse à la question Schwaab (12.1128 – Accès aux contenus sur Internet. Concept "effacer au lieu de bloquer"), qu'il n'était pas nécessaire de créer des dispositions juridiques spécifiques.

5.5 Problèmes de l'application du droit dans un contexte transfrontalier

L'application des dispositions juridiques suisses existantes sur les réseaux sociaux est délicate notamment parce que les exploitants des plateformes incriminées sont le plus souvent étrangers et qu'il s'agit de communication transfrontalière. Dans de nombreux domaines, le droit suisse dispose d'une réglementation face aux problèmes posés par les médias sociaux, laquelle pourrait également s'appliquer aux affaires transfrontalières. Toutefois, même dans le cas où il existe un jugement exécutoire prononcé par un tribunal suisse, il n'est pas garanti que celui-ci soit appliqué à l'étranger.

5.5.1 Application du droit par les autorités chargées des enquêtes et des poursuites

5.5.1.1 Collaboration internationale

Dans la pratique, l'application du droit dépend essentiellement de la volonté de collaborer de l'exploitant (étranger) de la plateforme. Cette disposition peut être encouragée par des interventions des autorités de poursuite pénale. Ainsi, certains exploitants de réseaux sociaux ont créé leurs propres services, auxquels les autorités étrangères peuvent s'adresser sans devoir engager une procédure d'entraide judiciaire[267].

En cas de conflit, les autorités de procédure pénale devraient procéder selon les règles de l'entraide judiciaire internationale, ce qui peut considérablement retarder la poursuite pénale. Vu le grand nombre d'affaires transfrontalières, il n'y a souvent pas d'autre alternative que la collaboration internationale entre les autorités d'enquête[268]. Pour les autorités suisses de poursuite pénale, une procédure pénale lancée à l'étranger pour cause de comportement jugé répréhensible également

---

[263] Voir l'état de fait de l'arrêt du Tribunal fédéral 1B_242/2009 vom 21.10.2009

[264] Schwarzenegger Christian, Sperrverfügungen gegen Access-Provider - über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter Oliver/Jörg Florian (Ed.), Internet-Recht und Electronic Commerce Law, Bern 2003, p. 249ss

[265] Rosenthal David, Internet-Provider-Haftung – ein Sonderfall? in: Peter Jung (Ed.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf, 2007, p. 158

[266] Arrêt CEDH "Ahmet Yildirim c. Türkei" (recours n°3111/2010) du 18.12.2012 relatif au blocage contraire à la Convention de la plateforme des sites Google

[267] Selon Facebook, toute demande émanant d'une autorité est examinée sous l'angle de sa recevabilité juridique et de sa conformité avec les conditions d'utilisation de Facebook et avec la loi. Pour le premier semestre 2013, Facebook indique que dans 13% des demandes suisses, il a fourni les données requises sur certains utilisateurs. https://www.facebook.com/about/government_requests

[268] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, projet du rapport final, 2013, chiffre 2.2.2.2.1, p. 48

dans le pays concerné (p. ex. cyberpiratage ou vol de données) facilite l'échange d'informations avec leurs collègues étrangers.

Depuis l'entrée en vigueur de la Convention sur la cybercriminalité (Cybercrime Convention, CCC) le 1er janvier 2012, le SCOCI a constaté une nette augmentation des échanges d'informations entre les polices criminelles[269]. Le SCOCI transmet aux autorités compétentes, par Interpol ou Europol, des données sur les contenus illicites stockés sur des serveurs étrangers, afin que les pays concernés puissent supprimer ces contenus conformément aux dispositions légales et entreprendre des poursuites. Bien que ces contenus interdits par le droit suisse peuvent être consultés en Suisse, le SCOCI n'a pas d'influence directe sur leur suppression ou leur blocage à l'étranger.

5.5.1.2 Limites des mesures prises contre les émissions de télévision étrangères

Les mesures de blocage sont soumises à des limites en matière de droit international lorsqu'elles visent des programmes de télévision proprement dit. Conformément à la Convention européenne sur la télévision transfrontière, contraignante pour la Suisse, les mesures relèvent exclusivement de la compétence du pays émetteur.

La diffusion de véritables programmes de télévision (c'est-à-dire de contenus audiovisuels intégraux assemblés sous forme de programmes et émis [en "streaming"] simultanément) est encore assez rare sur les plateformes de médias sociaux, qui proposent plutôt des contenus audiovisuels isolés (vidéo à la demande ou télévision non linéaire). S'agissant de telles offres, le droit de l'UE prévoit également le principe du pays émetteur (ou principe du pays d'origine). La directive correspondante 2010/13/UE sur les services de médias audiovisuels n'est actuellement pas contraignante pour la Suisse en ce qui concerne les services à la demande, mais il n'est pas exclu qu'elle le devienne un jour.

5.5.2 Application du droit par les particuliers (p. ex. aux fins de protection des droits de la personnalité)

Lorsque des contenus problématiques sont diffusés sur les réseaux sociaux, l'application du droit est difficile non seulement pour les autorités, mais aussi pour les particuliers, dont les droits de la personnalité peuvent être violés par la publication d'images ou de textes[270]. La personne qui souhaite la suppression de contenus illicites publiés par un utilisateur sur un réseau social a la possibilité de procéder de la manière suivante: tout d'abord prendre contact avec l'auteur de la violation, puis avec l'exploitant du réseau social, et enfin, si nécessaire, étudier les mesures juridiques à prendre. Cette manière de faire a souvent porté ses fruits.

5.5.2.1 Droit applicable

Pour les particuliers, le droit applicable en cas de litige est très important. Les conditions d'utilisation des médias sociaux renvoient généralement, dans leurs clauses de droit applicable, au droit national ou local du fournisseur (p. ex. le droit californien). D'ordinaire, ce dernier n'a pas son siège en Suisse, même si des sociétés du groupe y sont présentes. En ce qui concerne le for également, les conditions d'utilisation attribuent d'habitude une compétence aux tribunaux étatiques au siège du fournisseur. Il faut toutefois se demander dans quelle mesure ces clauses déterminant le droit applicable et la désignation du for sont applicables. Les dispositions contraignantes du droit international privé suisse fournissent quelques pistes:

Le choix de règles juridiques n'est applicable que si un contrat a été conclu. L'enregistrement de l'utilisateur suffit certes; mais lorsqu'une plateforme enfreint les droits de "non-utilisateurs", le fournisseur ne peut se référer au droit applicable énoncé dans les conditions d'utilisation. S'il porte par

---

[269] Rapport annuel SCOCI 2012, chiffre 4, p. 20

[270] Les explications données au point 5.5.2 se basent sur un texte rédigé en février 2013 sur mandat de l'Office fédéral de la communication par David Rosenthal, chargé de cours en droit de l'information et des télécommunications à l'Université de Bâle. La version complète du texte figure à l'adresse http://www.infosociety.admin.ch.

exemple atteinte à la personnalité d'un individu, ce dernier peut intenter une action auprès d'un tribunal suisse selon les règles générales de détermination du for pour les droits découlant d'un acte illicite au niveau international et, conformément aux dispositions générales du droit international privé, demander l'application du droit suisse. Il en va de même pour les infractions au droit de la concurrence. Dans ce cas, il faut, pour invoquer un rattachement au droit suisse, que le marché suisse soit touché; dans la pratique, il suffit qu'un fournisseur commette un acte illicite (également) contre des clients suisses (art. 136 LDIP[271]). Le fournisseur étranger d'une plateforme de médias sociaux destinée à des clients suisses doit donc respecter les dispositions de la loi sur la concurrence (y compris l'art. 8 LCD, qui réglemente le contenu autorisé des conditions générales), quelle que soit la teneur des conditions d'utilisation. Dans le domaine de la protection des données aussi, les utilisateurs enregistrés peuvent, indépendamment des conditions d'utilisation et de la référence à un droit étranger, invoquer devant un tribunal suisse le fait que les violations de la protection des données soient jugées selon les dispositions de la LPD s'ils le souhaitent (art. 139 LDIP).

Par ailleurs, les clauses de désignation du for et celles déterminant le droit applicable inscrites dans les conditions d'utilisation ne jouent aucun rôle là où le droit international privé, y compris d'éventuels accords de droit international, prescrivent de manière impérative ou semi-impérative le for et le droit des contrats applicable entre les utilisateurs et les fournisseurs. Les consommateurs sont ainsi protégés également lorsqu'ils concluent des contrats depuis la Suisse par le biais d'un site internet et que le fournisseur se trouve à l'étranger. Dans de tels cas, le consommateur domicilié en Suisse peut en principe faire valoir ses prétentions devant un tribunal suisse (art. 15, chiffre 1, let. c, Convention de Lugano[272]; art. 114, al. 1, let. a, LDIP), qui appliquera le droit suisse (des contrats) (art. 120 LDIP).

5.5.2.2 Reconnaissance et exécution des prétentions

L'applicabilité du droit suisse et la compétence des tribunaux suisses par rapport aux conditions d'utilisation ne garantissent pas à elles seules que les prétentions envers les fournisseurs étrangers (américains notamment) de médias sociaux soient effectivement exécutées. Les personnes lésées doivent en plus mener une procédure de reconnaissance et d'exécution devant les tribunaux du pays du fournisseur concerné. Même si la reconnaissance et l'exécution d'un arrêt de tribunal suisse sont en principe possibles à l'étranger et partiellement facilités par les accords internationaux[273], une telle procédure permet souvent (à nouveau) au fournisseur de s'opposer par exemple à la compétence du tribunal suisse (qui a généralement pris une décision en dérogation aux clauses de désignation du for). La reconnaissance et l'exécution peuvent s'en trouver empêchées ou du moins retardées. Les possibilités dont dispose le fournisseur dépendent notamment du droit étranger. Dès lors, il est parfois plus judicieux pour les personnes lésées de faire valoir d'éventuelles prétentions directement sur place et de renoncer à la protection du droit suisse.

Dans les deux cas de figure, les frais de procédure ont un effet dissuasif. Les litiges judiciaires découlant des conditions d'utilisation des plateformes de médias sociaux sont rares en Suisse.

Il existe également des plateformes étrangères de médias sociaux qui acceptent et exécutent "volontairement" les décisions prononcées en Suisse, même sans procédure d'exécution à l'étranger. La plupart refusent non seulement les contenus illicites (donc également ceux qui contreviennent à la LPD), mais aussi les propos diffamatoires à l'encontre d'autres utilisateurs ou de tiers. Il leur arrive même d'aller au-delà de ce que le droit interdit (voir ci-dessus point 4.2.2). Chez les principaux exploitants, des collaborateurs s'occupent spécifiquement des réclamations, qui leur parviennent chaque jour en grand nombre.

---

[271] Loi fédérale du 18 décembre 1987 sur le droit international privé (LDIP), RS 291

[272] Convention du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (CL), RS 0.275.12

[273] P. ex., pour les Etats de l'UE et de l'AELE, la Convention de Lugano La Convention de Lugano susmentionnée concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale

De nombreux exploitants ne veulent cependant pas effectuer eux-mêmes d'appréciation juridique. Ils demandent à une autorité compétente de l'Etat concerné de prendre une décision exécutoire. Lorsque celle-ci leur est présentée, ils bloquent les contenus reconnus illicites, même si la décision ne les met pas en cause (c'est-à-dire sans qu'ils soient poursuivis en justice) ou que l'entraide judiciaire n'est pas requise. La personne concernée doit certes agir en justice, mais dans une mesure raisonnable, vu qu'il suffit de lancer une procédure en Suisse. Il existe diverses possibilités, dépendant de deux questions: Premièrement, s'agit-il d'une procédure de nature pénale (une violation de la sphère privée peut certes être illicite, mais ne relève en général pas du droit pénal (punissable) et ne peut être poursuivie "que" par un tribunal civil). Deuxièmement, l'identité de l'auteur de la violation est-elle connue avec certitude.

S'il s'agit d'une atteinte à la personnalité perpétrée par un auteur inconnu, il n'est pas possible en Suisse de déposer plainte "contre inconnu" auprès d'un tribunal civil. Dans de tels cas, il convient d'agir formellement en justice contre l'exploitant de la plateforme, pour autant qu'aucune autre personne ne soit impliquée dans l'atteinte à la personnalité (p. ex. le responsable du site sur lequel figure un propos portant atteinte à la personnalité) et que l'exploitant ne soit pas disposé à révéler l'identité de la personne responsable. En Suisse, le droit sur la protection de la personnalité permet d'entreprendre une action civile contre quiconque "participe" à une atteinte à la personnalité. Selon la doctrine dominante, l'exploitant d'un réseau social (p. ex. d'un blog) est aussi concerné, même s'il n'a joué qu'un rôle secondaire dans la publication [274]. Contrairement au cas où l'exploitant consent à coopérer, mais veut avoir en main une décision judiciaire ou une décision des autorités avant de bloquer un contenu, une plainte contre un exploitant récalcitrant n'a véritablement de sens que si ce dernier se trouve en Suisse ou dans un pays où il est simple et rapide de faire reconnaître et exécuter un jugement provenant de Suisse.

La personne lésée peut aussi porter plainte au siège de l'exploitant à l'étranger. Le processus n'est pas forcément plus onéreux qu'une procédure menée devant un tribunal suisse; cependant, il nécessite en général le recours à un avocat et occasionne donc des frais.

5.5.2.3 Protection juridique provisionnelle

Pour garantir le respect des droits de la personnalité, la législation prévoit notamment la demande de suppression, la demande en cessation du trouble, la demande en constatation, la réparation et le dédommagement. Vu le risque de diffusion rapide sur les médias sociaux des propos portant atteinte à la personnalité, une protection juridique rapide est nécessaire. Dans la pratique, le prononcé judiciaire de mesures provisionnelles est fréquent. Il permet d'empêcher qu'un contenu illicite reste en ligne pendant la procédure judiciaire normale, susceptible de durer plusieurs années. Au début de la procédure, ou même avant, la suppression préalable du contenu est donc exigée et une interdiction provisoire de publication ordonnée. Pour les mesures superprovisionnelles, l'intervention a lieu en général immédiatement et sur la seule base des explications du requérant, sans audition d'autres personnes concernées ou de tiers. Pour d'autres mesures provisionnelles, une audition est réalisée, ce qui peut prendre quelques semaines.

Une procédure menée en vue d'une mesure provisionnelle vise à déterminer si la plainte a des chances d'aboutir (donc si, par exemple, un contenu précis est effectivement illicite), si le prononcé de la mesure provisionnelle est défendable vu les conséquences qu'elle entraîne en terme de durée de procédure pour le défendeur (p. ex. les inconvénients causés par le blocage provisoire ou la suppression du contenu) et s'il pourrait résulter, pour le demandeur, un préjudice difficile à réparer (par exemple avec de l'argent). Lorsqu'une mesure provisionnelle a été prononcée, le demandeur doit déposer une plainte contre le défendeur dans un certain délai, faute de quoi la mesure s'éteint.

[274] Voir par exemple TV 5A_792/2011 du 14.1.2013 E. 6.2 (pour l'exploitant de la plateforme blog de la Tribune de Genève); approuve Fanti Sébastien, Remarques, in: medialex 2013, S. 80

Compliquée, l'exécution de mesures provisionnelles dans le contexte international n'est parfois possible que différée dans le temps. Certaines décisions superprovisionnelles sont exclues du champ d'application de la Convention de Lugano[275], de sorte qu'elles ne peuvent pas bénéficier du mécanisme facilité de reconnaissance et d'exécution prévu dans ce dispositif. Il s'écoule parfois plusieurs mois entre l'édiction des mesures provisionnelles et l'exécution à l'étranger[276].

5.5.2.4 Autres aspects d'une protection efficace des intérêts privés

Parallèlement à l'action judiciaire, il existe d'autres moyens de protéger efficacement les intérêts privés. Même si un contenu a été supprimé d'une plateforme, il peut s'avérer nécessaire d'épurer les moteurs de recherche pour empêcher le contenu litigieux d'être retrouvé (si l'enregistrement intermédiaire n'a pas été bloqué par l'exploitant, l'ancienne page est potentiellement accessible dans la mémoire tampon). Il est recommandé d'utiliser une fonction spécifique – souvent proposée – qui permet de demander au robot du moteur de recherche d'analyser à nouveau une page donnée et de la supprimer de l'index de recherche (pour ce faire, il faut entrer l'adresse internet de la page à effacer).

Autre problème: Des contenus publiés une fois (p. ex. des vidéos) peuvent être téléchargés par d'autres utilisateurs et rediffusés ("effet viral"). La personne lésée peut finalement se trouver dans l'impossibilité de supprimer efficacement une publication indésirable, même avec les droits et instruments juridiques existants.

Dans certaines situations, il peut s'avérer judicieux qu'une personne lésée agisse elle-même pour défendre sa réputation. Une telle attitude peut inciter l'exploitant de la plateforme à intervenir avec détermination contre certains contenus illicites. En effet, les exploitants n'ont aucun intérêt à avoir mauvaise presse ou à susciter la colère des utilisateurs; ils ne veulent pas, en tant que réseaux sociaux, être présentés comme des espaces de cybermobbing ou d'appels au meurtre. Par expérience, en cas de pression publique, ils suppriment rapidement, ou plus rapidement, les contenus litigieux – dans le but aussi de protéger leur propre réputation –, alors qu'ils traitent avec moins de célérité un cas qui n'attire pas l'attention du public. A l'inverse, l'attention du public accroît aussi la pression sur la victime et peut contribuer a fortiori à une diffusion incontrôlée des contenus litigieux

[275] Arrêt CJUE du 21.5.1980 Denilauler / Couchet, Rs. C-125/79: les mesures provisionnelles qui peuvent être exécutées sans notification ou signification préalable ne sont pas transmissibles).

[276] Pour un exemple à ce sujet, voir Schneider-Marfels Karl-Jascha, Facebook, Twitter & Co: „Imperium in imperio“, in: Jusletter du 20 février 2012.

6 Questions juridiques non approfondies dans le rapport

En dehors des points traités dans les chapitres 4 et 5, les médias sociaux posent encore, sous les aspects les plus divers, toute une série de questions. Le présent chapitre se contente de les évoquer dans les grandes lignes.

6.1 Respect du droit d'auteur

A l'ère numérique, les difficultés rencontrées pour l'application du droit d'auteur et des droits connexes se présentent aussi avec les médias sociaux. Le groupe de travail AGUR12, mis en place par le DFJP, discute actuellement des mesures envisageables pour lutter contre les infractions au droit d'auteur sur l'internet (p. ex. par l'échange sans licence de fichiers de musique, de films ou de textes, par le partage de fichiers ou par la diffusion en flux (*streaming*)). Lors de leurs réunions, les membres se sont accordés à dire qu'il fallait combattre fermement les modèles commerciaux reposant sur une violation du droit d'auteur, que celle-ci soit le fait de tiers ou des créateurs de ces modèles d'activité. Les exploitants d'infrastructures (fournisseurs de services), qui utilisent ces modèles, doivent apporter leur aide dans les limites du raisonnable et des possibilités techniques et légales[277].

Par ailleurs, le SECO a mis sur pied en 2012 une table ronde dont l'objectif est d'examiner, dans le cadre de la législation en vigueur, comment les infractions au droit d'auteur sur l'internet peuvent être identifiées de manière conforme à la protection des données et poursuivies au niveau pénal[278].

6.2 Concurrence

Les aspects liés à la position dominante de certains réseaux sociaux et aux conséquences sur les intérêts des utilisateurs sont évoqués dans le présent rapport (effets de verrouillage, droit d'accès aux plateformes, notamment aux plateformes en position dominante).

Les instruments usuels du droit général de la concurrence (entre autres la loi sur les cartels) permettent aussi de remédier à un abus de position dominante dans les médias sociaux.

6.3 Les offres des diffuseurs radio-TV dans les médias sociaux

A l'instar des autres entreprises de médias, les diffuseurs de programmes de radio et de télévision sont de plus en plus présents dans les médias sociaux. En principe, le droit ne leur impose aucune restriction dans ce domaine. Le législateur a en effet renoncé intentionnellement à une réglementation spécifique dans la LRTV.

Une exception existe néanmoins pour la SSR. Sa présence sur les médias sociaux, qui est aussi financée par le produit de la redevance, entre dans la catégorie des autres offres journalistiques, dont le volume doit être fixé dans la concession, conformément à l'art. 25, al. 3, let. a, LRTV. Le Conseil fédéral propose de définir en détail les responsabilités en cas de déclarations problématiques ainsi que le pouvoir de surveillance. Il convient donc de préciser au niveau de la loi que les contributions de la rédaction de la SSR – mais pas les contenus produits par les utilisateurs – doivent répondre à certaines exigences minimales (soit: le respect de la dignité humaine, l'interdiction de toute représentation de la violence, la protection de la jeunesse ainsi que, dans certaines offres, les principes de l'objectivité et de la diversité). Ces exigences s'appliquent d'ailleurs aussi aux contributions de la rédaction publiées dans les blogs et les forums de discussion[279].

---

[277] Pour plus de détails: https://www.ige.ch/fr/droit-dauteur/agur12.html

[278] http://www.steigerlegal.ch/wp-content/uploads/2013/04/20130419_seco_roundtable.pdf/

[279] Message du 29 mai 2013 relatif à la modification de la loi fédérale sur la radio et la télévision (LRTV), chapitre 2.2, FF 2013 5017

6.4 Communication entre criminels dans des réseaux fermés

Le présent rapport ne traite que des réseaux sociaux décloisonnés et ouverts ainsi que des problèmes qui en résultent. Les réseaux de communication secrets, créés dans le but de commettre des actes délictueux (par exemple l'échange de pornographie sur des réseaux P2P) posent des problèmes spécifiques[280].

On peut lutter en partie contre de tels actes sur la base du droit en vigueur en menant des investigations secrètes. Ainsi, des collaborateurs du service national de coordination de la lutte contre la criminalité sur l'internet (SCOCI) peuvent, en vertu de l'ordonnance schwytzoise sur la police, agir en tant qu'agents infiltrés contre les pédocriminels sur les forums de discussion, les plateformes en ligne ou les réseaux privés de partage P2P[281]. Le SCOCI effectue par exemple une surveillance des réseaux P2P dans le but de repérer toute forme de pédocriminalité[282].

6.5 Espionnage TI (par des services secrets étrangers ou des particuliers)

Suite aux révélations d'Edward Snowden (ancien collaborateur des services extérieurs de renseignement américain, la National Security Agency NSA) en 2013, le grand public a pris davantage conscience de la surveillance des communications en ligne exercée par des services secrets[283]. La NSA utilise des interfaces pour surveiller, rassembler et conserver des contenus provenant de plateformes de médias sociaux.

Le phénomène de l'espionnage TI – par des services secrets étrangers ou des particuliers – ne touche pas uniquement les plateformes sociales mais plus encore les communications en lignes exclusivement privées. Dans sa réponse à l'IP 13.3558 Eichenberger "Cyberspionnage. Evaluation et stratégie"[284] du 20 juin 2013, le Conseil fédéral a renvoyé à la "Stratégie nationale de protection de la Suisse contre les cyberrisques" (SNPC) du 27 juin 2012 et au plan de mise en œuvre[285] de cette stratégie. Approuvé le 15 mai 2013, ce dernier concerne les 16 mesures prévues dans la stratégie. Il vise à détecter suffisamment tôt les menaces pesant sur le cyberespace, à augmenter la capacité de résistance des infrastructures d'importance vitale, à réduire les cyberrisques et à prévenir les incidents.

Dans sa réponse à l'IP 13.3033 Schwaab "Comment protéger les données personnelles des citoyens suisses détenues par des entreprises américaines?"[286] du 6 mars 2013, le Conseil fédéral s'est exprimé sur diverses questions relatives à la situation juridique et à la pratique suisses concernant la demande par les autorités américaines de données personnelles sur les citoyens d'Etats tiers stockées dans le nuage de données. Il souligne la responsabilité de chacun dans la gestion des données personnelles et mentionne le programme de sensibilisation "Jeunes et médias" ainsi que la fonction de conseil exercée par PFPDT. De plus, le Conseil fédéral donne des explications sur le droit

---

[280] En 2012, grâce à une surveillance active, le SCOCI a pu identifier 417 personnes ayant échangé des fichiers de pédopornographie; voir Rapport annuel 2012 du SCOCI, p. 1

[281] Rapport annuel SCOCI 2012, p. 13

[282] Voir à ce sujet Lentjes Meili Christiane, Präventiv oder Repressiv? Das Verwirrspiel um verdeckte polizeiliche Operationen, in Festschrift Donatsch, Zürich, 2012, p. 437ss

[283] Depuis 2007 au moins, les Etats-Unis ont surveillé une grande partie des télécommunications, notamment l'internet, au niveau mondial et indépendamment de tout soupçon; ils ont enregistré les données ainsi recueillies.

[284] http://www.parlament.ch/f/suche/seiten/geschaefte.aspx?gesch_id=20133558.

[285] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=fr

[286] http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20133033

des contrats et l'applicabilité éventuelle de la LDIP[287] et de la CL[288]. Enfin, il renvoie à la révision en cours de la LPD[289], qui doit notamment vérifier si le droit en vigueur dans ce domaine suffit ou non.

[287] Loi fédérale du 18 décembre 1987 sur le droit international privé (LDIP), RS 291

[288] RS 0.275.12.

[289] RS 235.1.

7 Principales recommandations

Cette partie du rapport propose des pistes de réponses aux problèmes identifiés aux chapitres 4 et 5. Comme exposé ci-avant, le droit matériel en Suisse est souvent suffisant. Toutefois, dans la pratique, beaucoup de problèmes ne peuvent pas être résolus seulement – et peut-être pas d'emblée – à l'aide d'instruments juridiques. L'information et la sensibilisation des utilisateurs notamment jouent également un rôle non négligeable.

7.1 Nécessité de créer de nouvelles prescriptions légales

7.1.1 Risque de surréglementation

Il est probable, mais pas certain, que les prescriptions légales en vigueur et leur application (judiciaire) dans des litiges particuliers ne permettent pas d'apporter une réponse satisfaisante aux questions soulevées par les médias sociaux. Il n'est donc pas exclu de devoir légiférer ponctuellement, tout en veillant cependant à ne pas tomber dans un activisme législatif tous azimuts, ni tendre à une surréglementation. Comme pour d'autres domaines soumis à un rapide changement, une intervention précipitée – par exemple en édictant des dispositions sur des bases hypothétiques – risque de provoquer des effets indésirables.

Dans chaque cas, il convient d'examiner au préalable si les mécanismes d'autorégulation existants – notamment le code de conduite des fournisseurs d'hébergement membres de l'association simsa évoqué au point 5.4.1 ou les conditions d'utilisation de certaines plateformes étrangères, dont Facebook et Twitter – sont suffisants.

7.1.2 Marge de manœuvre juridique des Etats entravée par des aspects internationaux

Le législateur suisse est aussi freiné en raison du contexte qui dépasse largement les frontières nationales. De nombreux problèmes ne peuvent pas être résolus au moyen de dispositions légales édictées isolément par un seul pays. Rappelons que la plupart des plateformes utilisées activement en Suisse ont leur siège à l'étranger.

Dans ce domaine, au lieu d'une activité réglementaire nationale, complexe et de portée limitée, un renforcement de la collaboration internationale s'impose. Le Conseil de l'Europe remarque à juste titre que des mesures de réglementation prises dans un système juridique peuvent fortement entraver l'accès et l'utilisation de l'internet dans d'autres systèmes juridiques, voire détériorer la fiabilité de l'infrastructure internet[290]. Par conséquent, l'échange transfrontalier d'informations sur l'internet nécessite une coopération sur une base multilatérale, avant tout pour les aspects qui impliquent différents systèmes juridiques. Avec le développement des nuages informatiques et des plateformes transfrontalières telles que les réseaux sociaux, un tel cas de figure survient toujours plus fréquemment[291].

7.1.3 Cohérence de l'ordre juridique dans son ensemble

Si un besoin de réglementation au niveau national se fait sentir dans des cas particuliers, il ne faut pas perdre de vue la cohérence de l'ordre juridique dans son ensemble. Beaucoup d'aspects problématiques en lien avec les médias sociaux se retrouvent dans d'autres domaines: le droit à l'oubli et la perte de contrôle sur ses propres données concernent aussi d'autres formes de communication en ligne et, plus généralement, la vie quotidienne[292]; certaines déclarations dans les médias de masse traditionnels (presse et radiodiffusion) peuvent aussi poser problème en termes de protection de la

[290] Voir la Déclaration sur les principes de la gouvernance de l'internet ainsi que la recommandation CM/Rec(2011)8 sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet

[291] En ce qui concerne ce problème, le Groupe Consultatif ad hoc sur l'Internet transfrontalier mis en place par le Conseil de l'Europe recommande de se référer à la participation multi-parties approuvée par le Conseil.

[292] Voir Flückiger Alexandre, L'autodétermination en matière de données personnelles :un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP/PJA 2013, p. 837ss

personnalité; la protection de la jeunesse peut également être mise à mal avec certains jeux à l'ordinateur; la pornographie ne se limite pas à l'internet, etc.

Sur un grand nombre de questions, il existe déjà une réglementation légale dans des lois générales (notamment le code pénal, le code civil ou la loi sur la protection des données) ne se rapportant pas spécifiquement aux médias sociaux. Des dispositions isolées régissant uniquement les médias sociaux risquent de provoquer un morcellement et d'aller à l'encontre de la cohérence de l'ordre juridique. Dès lors, mieux vaut chercher à développer le cadre légal existant et se demander si un problème donné concerne exclusivement les réseaux sociaux ou s'il ne touche pas d'autres domaines de la vie en société.

7.2 Examen d'une loi spécifique pour les réseaux sociaux

7.2.1 Contexte

Le postulat "11.3912 – Donnons un cadre juridique aux médias sociaux" demande s'il est possible, comme on l'a fait pour la radio et la télévision, d'élaborer une loi spécifique pour répondre à l'évolution des médias sociaux.

7.2.2 Compétence de la Confédération en matière de réglementation

Il s'agit en premier lieu de vérifier si la Confédération a effectivement la compétence d'édicter des dispositions régissant les contenus des médias sociaux. En ce qui concerne la communication publique sur les plateformes, la Confédération peut s'appuyer sur l'art. 93 Cst., qui lui confère la compétence de légiférer sur la diffusion publique d'offres et d'informations au moyen de techniques de télécommunication. Elle peut donc aussi édicter des dispositions relatives aux contenus véhiculés sur les médias sociaux. Pour ceux-ci, les mandats de prestations ne découlent certes pas directement de la Constitution, comme c'est le cas pour la radio et la télévision (art. 93, al. 2, Cst.). Néanmoins, la Confédération est libre d'édicter par voie législative des exigences sur les contenus d'autres formes de diffusion publique d'offres et d'informations au moyen de techniques de télécommunication[293]. Sur cette base, elle peut faire valoir son devoir fondamental de garantir un échange libre et pluraliste des informations et des opinions.

En ce qui concerne les contenus non destinés au public et échangés sur les médias sociaux, la Confédération ne peut évidemment pas se baser sur l'art. 93 Cst., mais plusieurs dispositions constitutionnelles prévoient des compétences en matière de réglementation. Ainsi, l'art. 92, al. 1, Cst., énonce que les télécommunications relèvent de la Confédération. La LTC réglemente donc non seulement la transmission au moyen de techniques de télécommunication, mais aussi le spamming ou les services à valeur ajoutée par exemple[294]. Le législateur fédéral peut en outre se baser sur l'art. 122 pour les dispositions de droit civil et sur l'art. 123 Cst. pour les dispositions de droit pénal. Au besoin, il aurait aussi la compétence d'établir des règles spéciales pour les médias sociaux.

7.2.3 Nécessité d'une réglementation spécifique

Une réglementation spécifique des médias sociaux, comme cela a été fait pour la radio et la télévision, ne se justifie que si une communication publique libre ne peut pas être pleinement garantie et stimulée. Vu l'offre variée des différentes plateformes sociales, cette hypothèse est a priori moins probable que dans le secteur de la radio et de la télévision, marqué traditionnellement par une rareté de l'offre due à des ressources en fréquences limitées. Là encore toutefois, la nécessité de définir des mandats de prestations est moins manifeste avec plusieurs canaux de diffusion que dans une situation de monopole ou face à un diffuseur de programmes (public) occupant une position dominante sur le marché.

---

[293] BO 1983 N 1353 (vote du conseiller national Schüle)

[294] Message relatif à la modification de la loi sur les télécommunications (LTC) du 12 novembre 2003, FF 2003 7966, 8003.

Il convient de légiférer seulement lorsque, sans l'activité correspondante, une communication libre nécessaire à l'épanouissement individuel et au débat démocratique n'est pas garantie. Cela peut être le cas, par exemple, si la diversité indispensable aux processus sociaux et démocratiques n'est plus reflétée dans les médias, notamment parce que certaines minorités n'ont pas de réelles chances de faire entendre leurs points de vue.

Certes, il se peut aussi que certaines plateformes acquièrent une importance prépondérante et que la régulation par le libre jeu des forces du marché ne soit plus suffisante. Une intervention de l'Etat permettrait dès lors de garantir la diversité des opinions indispensable aux processus sociaux et démocratiques, par exemple si certains groupes de la population n'avaient aucune chance réelle de participer à la communication sur des plateformes sociales importantes. Rien n'indique toutefois que cela soit le cas actuellement. Au contraire, les minorités peuvent probablement mieux se faire entendre grâce aux réseaux sociaux. Par ailleurs, la plupart des plus importants fournisseurs étant établis à l'étranger, des mandats de prestations du législateur suisse n'auraient aucune portée significative. Vu la situation actuelle, l'élaboration d'une loi spécifique sur les médias sociaux n'apparaît pas nécessaire.

7.2.4 Nécessité d'adapter les normes légales existantes

Face aux nouveaux problèmes engendrés par les médias sociaux, il convient de réagir non pas en élaborant une loi spécifique ou des règles isolées au cas par cas, mais en adaptant les prescriptions légales existantes, souvent formulées de manière générale. Si, sur un point précis, une adaptation s'avérait insuffisante, les textes légaux en vigueur peuvent éventuellement être complétés.

7.2.4.1 Examen approfondi des questions relevant de la loi sur la protection des données

Dans le chapitre 4, de nombreux problèmes en lien avec l'utilisation des médias sociaux ont été identifiés dans le domaine de la protection des données. Ils concernent en particulier le droit à l'oubli et, plus généralement, la perte de contrôle des utilisateurs sur leurs propres données.

En tant que loi cadre, l'actuelle loi suisse sur la protection des données (LPD) est formulée de manière très générale. Appliquée de manière judicieuse, elle permet aux autorités et aux tribunaux compétents d'examiner aussi les nouveaux problèmes en matière de protection des données. Dans certains cas, il n'est pas exclu toutefois que les dispositions en vigueur doivent être adaptées. Une évaluation approfondie de la situation – tenant aussi compte des révisions en cours des directives sur la protection des données pour l'UE et le Conseil de l'Europe – est actuellement menée sous la direction du DFJP. Un groupe d'accompagnement élargi est en train d'analyser la loi sur la protection des données et ses mesures d'application. Il se penchera également sur les problèmes engendrés par les médias sociaux.

Le DFJP est chargé de soumettre au Conseil fédéral fin 2014 au plus tard des propositions sur la suite à donner à ce processus.

7.2.4.2 Nécessité de déterminer et de réglementer la responsabilité

Vu les développements récents et les signaux donnés par la justice dans le domaine du droit civil, il paraît judicieux – comme nous l'avons déjà exposé au point 5.3. – que le Conseil fédéral examine à nouveau la nécessité de réglementer la responsabilité des fournisseurs de services sur l'internet (c'est-à-dire les fournisseurs d'accès et d'hébergement ainsi que les exploitants de plateformes). Cette tâche est cependant délicate, d'autant plus qu'une jurisprudence différenciée, qu'il faudra analyser soigneusement, se développe à l'étranger. Des travaux en ce sens doivent débuter en 2013, sous la houlette du DFJP.

Ces travaux pourraient éventuellement inclure d’autres problèmes et examiner si les règles en vigueur relatives à la suppression des contenus illégaux ou au blocage de l'accès ne devraient pas être revues.

7.2.4.3 Droit des télécommunications et médias sociaux

Une qualification juridique des divers services de transmission, qui sont aussi partiellement offerts par les médias sociaux, est difficile. Le droit des télécommunications en vigueur, élaboré à une époque où les services non liés à l'infrastructure de transmission sous-jacente n'existaient pas encore, ne propose pas de réponse adéquate. Aujourd'hui, d'autres modèles d'affaires sont répandus (p. ex. financement par la publicité), les conditions techniques ont changé et les services de transmission pouvant être offerts partout dans le monde avec peu de moyens se sont multipliés. Par conséquent, les règles du droit des télécommunications applicables à ce type de services doivent être examinées de manière large, c'est-à-dire non seulement pour les médias sociaux, mais aussi pour tous les services fournis (souvent gratuitement) sur l'internet sans que l'autorisation du fournisseur de services de l'utilisateur ne soit requise au préalable (services *over-the-top*). Ces questions seront examinées de manière approfondie dans le cadre du projet de consultation sur la révision de la loi sur les télécommunications que le Conseil fédéral souhaite encore lancer durant la présente législature.

7.2.4.4 Réglementation du transfert des données

Les médias sociaux qui pourraient être tentés de retenir leurs clients en leur interdisant de transférer leurs données sur des plateformes concurrentes (voir ci-dessus point 0) doivent être suivis de près. La Confédération observe le marché et, si nécessaire, élabore une disposition légale relative au transfert des données. Il pourrait s'avérer utile, le cas échéant, de réglementer les interfaces entre les différentes plateformes et d'obliger les principaux médias sociaux à autoriser leurs utilisateurs à échanger des données, notamment des informations privées, avec les utilisateurs d'autres plateformes. Ces prochaines années, on pourra probablement aussi se baser sur les expériences réalisées à l'étranger et prendre ces dernières en considération au moment d'examiner les besoins de légiférer.

7.3 Information et sensibilisation

Tant sur le plan national qu'au niveau international, les chances et les risques des médias sociaux ne doivent pas seulement être abordés au travers de règles juridiques (et de leur application). Pour obtenir de bons résultats, il faut recourir aussi à des instruments extra juridiques, par exemple à des actions de sensibilisation.

7.3.1 Droit à l'oubli

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) relève que les solutions techniques existantes ne permettent pas actuellement de protéger convenablement les données publiées et ne peuvent pas empêcher une copie non autorisée par des tiers, ni une éventuelle rediffusion après leur suppression "officielle"[295]. Dans un système ouvert comme l'internet, des solutions purement techniques ne sont pas suffisantes pour faire appliquer le droit à l'oubli. Une approche interdisciplinaire s'impose donc pour définir le droit à l'oubli juridiquement et techniquement[296].

Dans bien des cas, le respect du droit à l'oubli sur les plateformes sociales peut être favorisé par un comportement préventif. Avant de publier des données, le PFPDT recommande par exemple de se demander systématiquement si l'on souhaiterait être confronté aux données en question dans un entretien d'embauche, et cela, même dix ans après[297]. De même, aucune donnée personnelle sur des tiers ne devrait être publiée. Ces principes sont certes connus, mais il convient de les rappeler régulièrement en recourant à des exemples éloquents. A cet égard, le programme national "Jeunes et médias" offre un cadre idéal.

---

[295] Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011; http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten?searchterm=the+right+to+be+forgotten

[296] ENISA, The right to be forgotten, p. 11ss

[297] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=fr#sprungmarke10_9

7.3.2 Atteintes à l'honneur et à la personnalité, cyberintimidation et cyberharcèlement

Quand de fausses allégations, des jugements de valeur infamants ou des révélations illicites sont publiés sur les médias sociaux, le droit suisse régit les aspects pénaux, civils et économiques (voir point 4.4.1.3). Le point 5.5.2 explique comment les particuliers peuvent agir concrètement en cas d'atteinte aux droits de la personnalité. Toutefois, le problème réside aussi dans le fait que des contenus blessants peuvent être diffusés très rapidement et à large échelle.

En ce qui concerne le cyberharcèlement et la cyberintimidation, le Conseil fédéral a constaté à plusieurs reprises que, en l'état actuel, rien ne permet de conclure à une insuffisance de l'arsenal pénal existant (voir point 4.4.2.3).

Bien que la législation matérielle soit claire en cas d'atteintes à la personnalité, de cyberharcèlement ou de cyberintimidation, rien ne permet d'affirmer que les utilisateurs de plateformes sociales en ont toujours pleinement connaissance. Il pourrait s'avérer utile de présenter la situation légale de manière aisément compréhensible et, au besoin, de formuler des recommandations. Il existe déjà des offres destinées aux écoles, par exemple les educa Guides[298] ou la plateforme "Jeunes et médias"[299]. Mais, il faudrait également examiner par quels biais atteindre les autres groupes cibles et comment mettre en place les instruments adéquats.

7.3.3 Enfants et adolescents

Comme évoqué ci-avant (point 4.6.1.3), le Conseil fédéral examinera les mesures à prendre pour améliorer la protection des données des mineurs dans le cadre de la révision de la loi sur la protection des données[300]. Les seuls instruments juridiques ne permettront toutefois pas de protéger efficacement la jeunesse. Il est essentiel de promouvoir parallèlement l'éducation aux médias chez les jeunes, les enseignants et les parents et de les rendre attentifs aux chances et aux dangers des médias numériques. Le programme national "Jeunesse et médias"[301] que le Conseil fédéral a lancé le 11 juin 2010 pour les années 2011 à 2015 va dans ce sens. Il devrait aider les parents, les enseignants et les éducateurs à acquérir les compétences nécessaires pour accompagner de manière active les enfants et les adolescents dans leur utilisation des médias. Le site http://www.jeunesetmedias.ch a notamment été conçu comme un portail de référence pour la protection des jeunes face aux médias. Il fournit un aperçu systématique des offres de formation et d'information disponibles en Suisse et présente les stratégies et mesures élaborées par les cantons. La brochure "Compétences médiatiques: conseils pour utiliser les médias numériques en toute sécurité" publiée dans le cadre du programme donne des conseils pratiques aux parents, aux enfants et aux enseignants[302]. La publication aborde différents thèmes, tels que le harcèlement en ligne, les forums de discussion, les jeux à l'ordinateur, la pornographie ou les médias sociaux. Elle répond explicitement par exemple à la question de savoir si parents et enseignants devraient devenir "amis" avec des jeunes sur des réseaux sociaux. Le programme encourage aussi la collaboration des différentes instances et groupes de contact actifs dans la protection de la jeunesse face aux médias et soutient les professionnels par le biais d'actions de sensibilisation. Il promeut en outre la qualité des offres existantes ainsi que des méthodes innovantes de transmission des connaissances dans l'utilisation des médias (éducation par des pairs, stratégies d'accès à toutes les catégories de la population).

---

[298] http://guides.educa.ch/fr/recht

[299] http://www.jeunesetmedias.ch/fr/accueil.html

[300] Rapport du Conseil fédéral du 9.12.2011 sur l'évaluation de la loi fédérale sur la protection des données, point 5.2.2 (FF 2012 269)

[301] http://www.jeunesetmedias.ch/fr/accueil.html

[302] http://www.jeunesetmedias.ch/fileadmin/user_upload/Chancen_und_Gefahren/brochure_FAQ_Medienkompetenz_fr.pdf

L'enseignement est du ressort des cantons. Les activités organisées par ces derniers en faveur de la promotion des compétences TIC sont donc importantes. La CDIP a mis en place une stratégie relative à l'intégration des TIC dans les écoles[303]. Elle a également formulé des recommandations pour la formation des enseignants dans le domaine des technologies de l'information et de la communication[304] et défini un profil des formations complémentaires destinées aux formateurs dans le domaine de l'intégration des médias dans l'enseignement[305]. Sur le serveur éducatif "educa.ch", les professionnels trouvent du matériel d'enseignement ainsi que des informations détaillées, par exemple la brochure "Safersurfing – Sécurité sur les réseaux sociaux"[306] éditée par la Prévention Suisse de la Criminalité (PSC) et consacrée à la cyberintimidation, aux violences sexuelles ou à l'utilisation de données personnelles sur les réseaux sociaux. La PSC a aussi publié en janvier 2013 la brochure "My little Safebook" pour une utilisation sécurisée des médias sociaux[307].

Outre les mesures d'encouragement énumérées ci-dessus, le Conseil fédéral a chargé l'Office fédéral des assurances sociales (OFAS) d'élaborer, dans le cadre du programme national "Jeunes et médias", des recommandations sur l'organisation future de la protection des jeunes face aux médias en Suisse.

L'OFAS a institué un groupe de projet composé de représentants de la Confédération, des cantons et de l'économie et confié quatre mandats de recherche:

Mandat 1: Evolutions et tendances d'utilisation dans le domaine des médias numériques et défis qui en résultent pour la protection des jeunes face aux médias (automne 2012 - été 2013)

Mandat 2: Recensement et contrôle des activités régulatrices des cantons (printemps 2013 - été 2014)

Mandat 3: Evaluation de la mise en œuvre et de l'effet des mesures d'autorégulation de la branche des médias en Suisse dans les domaines du cinéma, des jeux vidéo, des télécommunications et de l'internet (printemps 2013 - été 2014)

Mandat 4: Analyse des modèles de régulation d'autres pays concernant des médias spécifiques ou communs à plusieurs supports, identification des exemples de bonnes pratiques et formulation de recommandations pour la Suisse (printemps 2013 - été 2014)

L'objectif est de déterminer d'ici 2015 s'il convient de légiférer au niveau fédéral et de créer, le cas échéant, de nouvelles bases constitutionnelles.

7.3.4 Améliorer l'éducation aux médias parmi la population

Plusieurs initiatives ont été prises dans le milieu scolaire pour les enfants, les jeunes et les éducateurs afin d'améliorer leurs connaissances dans l'utilisation des médias. Comme les médias sociaux sont un phénomène très jeune et extrêmement dynamique, les sites et les publications pertinents doivent être mis à jour et revus en permanence.

---

[303] Stratégie de la CDIP du 1er mars 2007 en matière de technologies de l'information et de la communication (TIC) et de médias (http://edudoc.ch/record/30021/files/ICT_f.pdf?version=1). Voir aussi la Déclaration du 8 juin 2000 relative aux technologies de l'information et de la communication (TIC) dans le domaine de l'éducation (http://www.edudoc.ch/static/web/arbeiten/erkl_ikt_f.pdf)

[304] Recommandations du 25 avril 2004 relatives à la formation initiale et continue des enseignantes et enseignants de la scolarité obligatoire et du degré secondaire II dans le domaine des technologies de l'information et de la communication (TIC); voir http://edudoc.ch/record/24706/files/Empf_ICT_LB_f.pdf

[305] http://edudoc.ch/record/38149/files/Profil_ICT_f.pdf

[306] http://guides.educa.ch/sites/default/files/sicherheit_netzwerke_f.pdf

[307] http://news.skppsc.ch/fr/2013/01/24/neue-broschure-my-little-safebook-fur-einen-sicheren-umgang-mit-den-sozialen-medien/

Il convient aussi d'examiner dans quelle mesure l'éducation aux médias, en particulier l'utilisation des médias sociaux, doit être améliorée dans les autres groupes cibles[308]. Les médias sociaux sont en effet de plus en plus utilisés pour informer et sensibiliser les groupes cibles sur des questions particulières.

[308] Par exemple, la bande dessinée "Petites histoires d'internet" destinée à un large public http://www.geschichtenausdeminternet.ch/index_fr.html

8 Réponses aux questions du postulat

Sur la base des développements ci-dessus, on peut répondre comme suit aux questions soulevées dans le postulat:

- Quelle est la législation actuelle, en Suisse et à l'étranger, au sujet des médias sociaux?

En Suisse comme à l'étranger, jusqu'à maintenant peu de règles se rapportant spécifiquement et exclusivement aux médias sociaux figurent dans la législation. Toutefois, les normes juridiques en vigueur sont aussi applicables à la communication sur les réseaux sociaux.

- Que penserait le Conseil fédéral de l'élaboration d'une loi sur les médias sociaux qui prenne en considération les particularités de ces nouvelles plateformes de communication?

A l'heure actuelle, il n'est pas nécessaire de créer une réglementation spécifique pour les médias sociaux sur le modèle de la loi sur la radio et la télévision.

- Quelles sont les lacunes du droit et comment peut-on les combler?

Les expériences faites jusqu'ici n'ont révélé aucune lacune majeure dans le droit suisse en vigueur. Appliquées de manière judicieuse, la plupart des règles d'ordre général figurant dans les lois actuelles (p. ex. LPD, CP, CC, LCD) permettent de fournir une réponse adéquate à la majorité des problèmes que les réseaux sociaux causent ou pourraient causer aux utilisateurs ou au public. On ne peut pas affirmer toutefois que ces dispositions résisteront à l'épreuve de la pratique. Des améliorations ponctuelles paraissent envisageables dans certains domaines. Pour cette raison, des vérifications sont nécessaires ou déjà en cours sur plusieurs aspects (notamment en ce qui concerne la protection des données ou de la jeunesse). Il faut se rappeler aussi que ces vérifications ne se limitent pas aux seuls médias sociaux, mais portent sur un grand nombre d'autres questions.

9 Suite du processus

Comme évoqué ci-dessus au chapitre 7, l'administration fédérale a lancé plusieurs projets importants qui examinent entre autres l'éventualité de légiférer sur les médias sociaux.

Les questions relatives à la protection des données sont discutées dans le cadre des travaux de révision de la LPD, menés sous la houlette du DFJP. Les problèmes engendrés par les réseaux sociaux ne concernent qu'un des nombreux aspects examinés. Le droit à l'oubli et les questions juridiques autour de la perte de contrôle des utilisateurs sur leurs propres données dans les réseaux sociaux (et une certaine amélioration de la situation grâce à un paramétrage par défaut permettant de mieux protéger les données) revêtent à cet égard une importance particulière. Le DFJP a reçu le mandat de soumettre au Conseil fédéral d'ici fin 2014 des propositions sur la suite du processus.

Les questions en lien avec la protection de la jeunesse sont analysées jusqu'en 2015 dans le cadre du projet "Jeunes et médias" piloté par l'Office fédéral des assurances sociales. Ce projet examine notamment si une réglementation est nécessaire au niveau fédéral ainsi que, cas échéant, de nouvelles bases juridiques concernant la protection des enfants et des jeunes. En outre, des recommandations sur l'aménagement futur de la protection de la jeunesse dans le domaine des médias en Suisse seront élaborées.

Il s'agit aussi d'examiner la nécessité de réglementer, dans le code civil, la responsabilité des exploitants de plateformes et des fournisseurs de prestations techniques (les fournisseurs d'accès et d'hébergement). La démarche ne se limite pas aux réseaux sociaux, mais concerne plus généralement la responsabilité juridique des fournisseurs de services en ligne (fournisseurs d'hébergement). Le DFJP est chargé de traiter cette question et, en cas de besoin avéré de modification de la loi, de soumettre au Conseil fédéral un projet à mettre en consultation.

Les aspects relatifs au droit des télécommunications sont abordés dans le cadre d'un projet de révision de la LTC. Selon la planification actuelle, le Conseil fédéral devrait mettre en œuvre le projet au cours de la présente législature encore.

Il convient d'observer, en vue d'une éventuelle réglementation, l'évolution de certains médias sociaux qui seraient tentés de conserver leurs clients en interdisant à ceux-ci de transférer leurs données sur des plateformes concurrentes. Dans ce cas, on pourrait envisager d'introduire un droit au transfert des données ou de réglementer les interfaces entre les différents réseaux sociaux. Les mesures en ce sens prises à l'étranger devraient aussi servir de modèle.

Ces différentes activités et analyses ne concernent pas exclusivement les médias sociaux, mais doivent être considérées en corrélation avec le système juridique dans son ensemble. Il est important que les divers aspects forment un cadre général cohérent au niveau du contenu également en ce qui concerne les médias sociaux. A cet égard, la circulation des informations entre les offices concernés doit être assurée.

Compte tenu des nombreuses activités de réglementation connues – et des éventuelles autres – ayant un lien plus ou moins important avec les médias sociaux, on risque de perdre de vue le problème dans son ensemble. A moyen terme, il paraît donc utile de dresser un nouvel état des lieux sous l'angle des médias sociaux. Cette analyse, qui devra tenir compte à la fois de l'évolution rapide sur le plan international et de la future jurisprudence relative à de nombreux litiges, permettra de montrer les forces et les faiblesses de la réglementation en vigueur.

A l'heure actuelle, il paraît souhaitable d'établir, sous forme de bilan intermédiaire, un nouvel état des lieux afin d'examiner la base légale relative aux médias sociaux d'ici fin 2016, c'est-à-dire lorsque les travaux évoqués ci-avant auront été achevés ou que l'on saura mieux quelle direction ils prennent.

Annexe A : Abréviations

JO	Journal officiel de l'Union européenne
AGUR12	Groupe de travail chargé d'améliorer la gestion collective des droits d'auteur et des droits voisins
OPMéd	Ordonnance sur la publicité pour les médicaments
OFSP	Office fédéral de la santé publique
OFCOM	Office fédéral de la communication
FF	Feuille fédérale
LHand	Loi sur l'égalité pour les handicapés
OHand	Ordonnance sur l'égalité pour les handicapés
BGBl	Bundesgesetzblatt (bulletin d'annonces public de la République fédérale d'Allemagne)
Blog	Journal virtuel, tenu sur un site internet
Cst.	Constitution fédérale
LPD	Loi fédérale sur la protection des données
CDIP	Conférence suisse des directeurs cantonaux de l'instruction publique
PFPDT	Préposé fédéral à la protection des données et à la transparence
DFJP	Département fédéral de justice et police
CEDH	Cour européenne des droits de l'homme
CEDH	Convention européenne des droits de l'homme
UE	Union européenne
CJUE	Cour de justice de l'Union européenne (plus haute juridiction de l'Union européenne en matière de droit)
CESE	Comité économique et social européen
ENISA	European Network and Information Security Agency (Agence européenne chargée de la sécurité des réseaux et de l'information)
LTC	Loi sur les télécommunications
FTC	Federal Trade Commission (autorité de la concurrence et de la protection des consommateurs aux Etats-Unis)
LPTh	Loi sur les produits thérapeutiques
H.R.	House of Representatives (Chambre des représentants du Congrès des Etats-Unis)
Ed.	Editeur
TIC	Technologies de l'information et de la communication
LDIP	Loi fédérale sur le droit international privé
DPMin	Droit pénal des mineurs
PPMin	Procédure pénale applicable aux mineurs
LCart	Loi sur les cartels
LEEJ	Loi sur l'encouragement de l'enfance et de la jeunesse
OEEJ	Ordonnance sur l'encouragement de l'enfance et de la jeunesse
SCOCI	Service national de coordination de la lutte contre la criminalité sur Internet
ODAlOUs	Ordonnance sur les denrées alimentaires et les objets usuels
CL	Convention de Lugano
CPM	Code pénal militaire

CN	Conseillère nationale
CO	Droit des obligations
P2P	Peer to Peer
RSS	Really Simple Syndication, format de syndication de contenu permettant de diffuser les nouvelles des sites d'information
LRTV	Loi fédérale sur la radio et la télévision
ORTV	Ordonnance sur la radio et la télévision
SECO	Secrétariat d'Etat à l'économie
Simsa	Swiss Internet Industry Association (interprofession suisse pour l'internet)
PSC	Prévention suisse de la criminalité
Rec.	Recueil de la jurisprudence de la Cour de justice de l'Union européenne (CJUE)
RS	Recueil systématique du droit fédéral suisse
SSR	Société suisse de radiodiffusion et télévision
CP	Code pénal
OTab	Ordonnance sur le tabac
LDA	Loi sur le droit d'auteur
U.S.C.	United States Code (recueil et codification du droit fédéral des Etats-Unis)
LCD	Loi fédérale contre la concurrence déloyale
DEFR	Département fédéral de l'économie, de la formation et de la recherche
WLAN	Wireless Local Area Network (réseau local sans fil)
P. ex.	Par exemple
CC	Code civil

Annexe B : Bibliographie

Aguiton C./Cardon D., The Strength of Weak Cooperation: an Attempt to Understand the Meaning of Web 2.0, Communication & Strategies, no.65, 1st quarter 2007 (**cit. Aguiton C./Cardon D.**).

Bächli Marc, Das Recht am eigenen Bild. Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus der Sicht der abgebildeten Person, Basel 2002 (**cit. Bächli Marc, Das Recht am eigenen Bild, Basel 2002**).

Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010 S. 56.

Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: Medialex 2009, S. 19ff.

Boyd D.M./Ellison N.B., Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), article 11, 2007 (**cit. Boyd D.M./Ellison N.B.**)

Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011.

Elixmann Robert, Datenschutz und Suchmaschinen. Neue Impulse für den Datenschutz im Internet, Berlin 2012.

Engel C./Knieps G., Vorschriften des Telekommunikationsgesetzes über den Zugang zu wesentlichen Leistungen: Eine juristisch-ökonomische Untersuchung, Baden-Baden 1998. (**cit. Engel C./Kniwps G.**)

Epiney Astrid/Fasnacht Tobias (Ed.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, Zürich 2012.

European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011.

Epiney Astrid/Probst Thomas/Gammenthaler Nina (Ed.), Datenverknüpfung. Problematik und rechtlicher Rahmen, Zürich 2011.

Hilty Lorenz/Oertel Britta/Wölk Michaela/Pärli Kurt, Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern, Zürich 2012 (**cit. Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012**).

Jöhri Yvonne, Werbung im Internet: rechtsvergleichende, lauterkeitsrechtliche Beurteilung von Werbeformen, Zürich 2000 (**cit. Jöhri Yvonne, Werbung im Internet, Zürich 2000**).

Keller Claudia, AGB von Social-Media-Plattformen, in: Medialex 2012 p. 188ss

Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. Universität Zürich, Zürich.

Mayer-Schönberger Viktor, Delete: Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010.

Meyer Julia, Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011.

Neuberger, Christoph, „Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick“. In: Neuberger, Christoph; Gehrau, Volker (Hrsg): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, p. 33 - 96.

Schmidt, Jan, „Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen“. In: Zerfass, Ansgar; Welker, Martin; Schmidt, Jan (Hrsg): Kommunikation, Partizipation und Wirkungen im Social Web. Bd. 1. Köln 2008, p. 18 - 40.

Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 p. 108.

Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: Medialex 2011 p. 197ss

Schweizer Michael, Recht am Wort: Schutz des eigenen Wortes im System von Art. 28 ZGB, Bern 2012 (**cit. Schweizer Michael, Recht am Wort, Bern 2012**).

Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7. Aufl., Zürich 2012.

Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012

Von Rimscha M. Björn, Geschäftsmodelle für Social Media . In: Petra Grimm und Oliver Zöllner (Ed.): Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten. Stuttgart 2012, p. 297–311.

Weber Rolf, E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich 2010.

Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zürich 2011.

Annexe C : Textes de référence

1. Lois

Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (LPTh), RS 812.21.

Loi fédérale du 13 décembre 2002 sur l'élimination des inégalités frappant les personnes handicapées (LHand), RS 151.3.

Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1.

Loi fédérale du 30 mars 1911 complétant le code civil suisse (CO), RS 220.

Loi fédérale du 30 septembre 2011 sur l'encouragement des activités extrascolaires des enfants et des jeunes (LEEJ), RS 446.1.

Loi fédérale du 21 juin 1932 sur l'alcool (Lalc), RS 680.

Loi fédérale du 18 décembre 1987 sur le droit international privé (LDIP), RS 291.

Loi fédérale du 20 juin 2003 régissant la condition pénale des mineurs (DPMin), RS 311.1.

Loi fédérale du 6 octobre 1995 sur les cartels et autres restrictions à la concurrence (LCart), RS 251.

Loi fédérale du 24 mars 2006 sur la radio et la télévision (LRTV), RS 784.40.

Loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD), RS 241.

Loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins (LDA), RS 231.1.

Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.), RS 101.

Loi du 30 avril 1997 sur les télécommunications (LTC), RS 784.10.

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

Code pénal militaire du 13 juin 1927 (CPM), RS 321.0.

Loi fédérale du 20 mars 2009 sur la procédure pénale applicable aux mineurs (PPMin), RS 312.1.

Code pénal suisse du 21 décembre 1937 (CP), RS 311.0.

Code civil suisse du 10 décembre 1907 (CC), RS 210.

Convention du 23 novembre 2001 sur la cybercriminalité, RS 0.311.43.

Convention du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (CL), RS 0.275.12.

Convention du 20 novembre 1989 relative aux droits de l'enfant, RS 0.107.

Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, RS 0.235.1.

Convention n° 182 du 17 juin 1999 concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination, RS 0.822.728.2.

Ordonnance du DFI du 23 novembre 2005 sur les boissons alcooliques, RS 817.022.110.

Ordonnance 5 du 28 septembre 2007 relative à la loi sur le travail (Ordonnance sur la protection des jeunes travailleurs, OLT 5), RS 822.115.

Ordonnance du 17 octobre 2001 sur la publicité pour les médicaments (OPMéd), RS 812.212.5.

Ordonnance du DEFR du 4 décembre 2007 sur les travaux dangereux pour les jeunes, RS 822.115.2.

Ordonnance du 19 novembre 2003 sur l'élimination des inégalités frappant les personnes handicapées (OHand), RS 151.31.

Ordonnance du 17 octobre 2012 sur l'encouragement des activités extrascolaires des enfants et des jeunes (OEEJ), RS 446.11.

Ordonnance du 23 novembre 2005 sur les denrées alimentaires et les objets usuels (ODAlOUs), RS 817.02.

Ordonnance du 9 mars 2007 sur la radio et la télévision (ORTV), RS 784.401.

Ordonnance du 11 juin 2010 sur des mesures de protection des enfants et des jeunes et sur le renforcement des droits de l'enfant, RS 311.039.1.

Ordonnance du 27 octobre 2004 sur les produits du tabac et les produits contenant des succédanés de tabac destinés à être fumés (OTab), RS 817.06.

2. Liste des textes de référence abrégés

a. Conseil de l'Europe

Rapport abrégé du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE n° 108) – 29e réunion plénière du 10 décembre 2012, T-PD (2012) RAP 29 Abr_fr (**cit. Rapport abrégé du Comité consultatif de la Convention 108, T-PD (2012) RAP 29 Abr_fr**).

Groupe consultatif ad hoc sur l'internet transfrontalier, 4e réunion, résumé général des 13 et 14 octobre 2011 (**cit. Groupe consultatif ad hoc sur l'internet transfrontalier**).

Recommandation Rec(2004)16 du Comité des ministres du Conseil de l'Europe du 15.12.2004 sur le droit de réponse dans le nouvel environnement des médias (**cit. Recommandation Rec(2004)16 sur le droit de réponse dans le nouvel environnement des médias**).

Recommandation Rec(2006)12 du Comité des Ministres du Conseil de l'Europe du 27.09.2006 sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication (**cit. Recommandation Rec(2006)12 sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication**).

Recommandation CM/Rec(2007)2 du Comité des Ministres du Conseil de l'Europe du 31.01.2007 sur le pluralisme des médias et la diversité du contenu des médias (**cit. Recommandation CM/Rec(2007)2 sur le pluralisme des médias et la diversité du contenu des médias**).

Recommandation CM/Rec(2008)6 du Comité des Ministres du Conseil de l'Europe du 26.03.2008 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet (**cit. Recommandation CM/Rec(2008)6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet**).

Recommandation CM/Rec(2009)5 du Comité des Ministres du Conseil de l'Europe du 08.07.2009 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication (**cit. Recommandation CM/Rec(2009)5 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication**).

Recommandation CM/Rec(2010)13 du Comité des Ministres du Conseil de l'Europe du 23.11.2010 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (**cit. Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage**).

Recommandation CM/Rec(2011)7 du Comité des Ministres du Conseil de l'Europe du 21.09.2011 sur une nouvelle conception des médias (**cit. Recommandation CM/Rec(2011)7 sur une nouvelle conception des médias**).

Recommandation CM/Rec(2011)8 du Comité des Ministres du Conseil de l'Europe du 21.09.2011 sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet (**cit. Recommandation CM/Rec(2011)8 sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet**).

Recommandation CM/Rec(2012)3 du Comité des Ministres du Conseil de l'Europe du 04.04.2012 sur la protection des droits de l'homme dans le contexte des moteurs de recherche (**cit. Recommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche**).

Recommandation CM/Rec(2012)4 du Comité des Ministres du Conseil de l'Europe du 04.04.2012 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux (**cit. Recommandation CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux**).

Déclaration du Comité des Ministres du Conseil de l'Europe du 07.12.2011 sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés et les prestataires de services en ligne (**cit. Déclaration sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés et les prestataires de services en ligne**).

Déclaration du Comité des Ministres du Conseil de l'Europe du 21.09.2011 sur les principes de la gouvernance d'internet (**cit. Déclaration sur les principes de la gouvernance d'internet**).

Déclaration du Comité des Ministres du Conseil de l'Europe du 20.02.2008 sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet (**cit. Déclaration du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet**).

Moderniser la convention 108: nouvelles propositions du Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) du 27.04.2012, T-PD-BUR(2012)01Rev2_fr (**cit. Moderniser la convention 108, T-PD-BUR(2012)01Rev2_fr**).

b. Union européenne

Avis du groupe de travail "article 29" 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles du 22.03.2012 (00727/12/FR WP 192) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (**cit. Avis DSG art. 29 00727/12/FR WP 192**).

Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 13.09.2011 sur l'application de la recommandation du Conseil du 24.09.1998 concernant la protection des mineurs et de la dignité humaine, et de la recommandation du Parlement européen et du Conseil du 20.12.2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne – protéger les enfants dans le monde numérique –, COM(2011) 556 final (**cit. Rapport de la Commission, COM(2011) 556 final**).

Décision n° 1351/2008/CE du Parlement européen et du Conseil du 16.12.2008 instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication, JO L 348 du 24.12.2008 p. 118 (**cit. Décision n° 1351/2008/CE instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication**).

Recommandation du Parlement européen du 26.03.2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet (2008/2160(INI)), JO C 117 E du 06.05.2010 p. 206 (**cit. Recommandation du Parlement européen sur le renforcement de la sécurité et des libertés fondamentales sur Internet, (2008/2160(INI))**).

Recommandation 2006/952/CE du Parlement européen et du Conseil du 20.12.2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne, JO L 378 du 27.12.2006 p. 72 (**cit. Recommandation sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne, 2006/952/CE**).

Résolution du Parlement européen du 15 décembre 2010 sur l'effet de la publicité sur le comportement des consommateurs (2010/2052(INI)), JO C 169 E du 15.06.2012 p. 58-65 (**cit. Résolution sur l'effet de la publicité sur le comportement des consommateurs (2010/2052(INI))**).

Communication conjointe au Parlement européen et au Conseil "Les droits de l'homme et la démocratie au cœur de l'action extérieure de l'UE – vers une approche plus efficace" du 12.12.2011, COM(2011) 866 final (**cit. Communication conjointe Les droits de l'homme et la démocratie au cœur de l'action extérieure, COM(2011) 866 final**).

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions "Rapport sur la compétitivité numérique de l'Europe Principaux résultats de la stratégie "i2010" entre 2005 et 2009" du 04.08.2009, COM(2009) 390 final (**cit. Communication "Rapport sur la compétitivité numérique de l'Europe Principaux résultats de la stratégie "i2010" entre 2005 et 2009", COM(2009) 390 final**).

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions "Stratégie européenne pour un Internet mieux adapté aux

enfants" du 02.05.2012, COM(2012) 196 final (**cit. Communication de la Commission "Stratégie européenne pour un Internet mieux adapté aux enfants", COM(2012) 196 final**).

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions "Evaluation intermédiaire du programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication" du 03.02.2012, COM(2012) 33 final (**cit. Communication de la Commission "Evaluation intermédiaire du programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication", COM(2012) 33 final**).

Communication de la Commission au Conseil et au Parlement européen "Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité" du 28.03.2012, COM(2012) 140 final (**cit. Communication "Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité", COM(2012) 140 final**).

Directive 2011/83/UE du Parlement européen et du Conseil du 25.10.2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, JO L 304 du 22.11.2011 p. 64-88 (**cit. Directive 2011/83/UE relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE**).

Directive 95/46/CE du Parlement européen et du Conseil du 24.10.1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995 p. 31-50 (**cit. Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**).

Conclusions du Conseil du 11.05.2012 Renforcer le potentiel de création et d'innovation des jeunes, JO C 169 du 15.06.2012 p. 1-4 (**cit. Conclusions Renforcer le potentiel de création et d'innovation des jeunes, 2012/C 169/01**).

Avis du Comité économique et social européen sur "L'Internet des objets" du 18.09.2008, JO C 077 du 31.03.2009 p. 60-63 (**cit. Avis "L'Internet des objets" 2009/C 77/15**).

Avis du Comité des régions sur le thème "Une stratégie numérique pour l'Europe", JO C 015 du 18.01.2011 p. 34-40 (**cit. Avis "Une stratégie numérique pour l'Europe", 2011/C 15/07**).

Avis du Comité économique et social européen sur le thème "L'utilisation responsable des réseaux sociaux et la prévention de troubles associés" du 19.09.2012, JO C 351 du 15.11.2012 p. 31-35 (**cit. Avis "L'utilisation responsable des réseaux sociaux et la prévention de troubles associés", 2012/C 351/07**).

Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 25.01.2012, COM(2012) 11 final (**cit. Proposition UE Règlement général sur la protection des données, COM(2012) 11 final**).

c. Allemagne

Antwort der Bundesregierung auf die kleine Anfrage "Rechtsextremismus im Internet" vom 07.06.2010, Drucksache 17/1930 (**cit. Antwort Bundesregierung auf Anfrage "Rechtsextremismus im Internet", 17/1930**).

Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes vom 03.08. 2011, Drucksache 17/6765 (**cit. Gesetzesentwurf Änderung Telemediengesetz, 17/6765**).

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010, Drucksache 17/4230 (**cit. Gesetzesentwurf Beschäftigtendatenschutz, 17/4230**).

3. Etudes et rapports

Bernet ZHAW, étude sur les médias sociaux en Suisse 2012.

eHealth Suisse, rapport "Portail de santé publique".

ENISA Threat Landscape, rapport du 28.09.2012.

EU Kids Online, rapport final, septembre 2011.

Rapports annuels 2011 et 2012 du Service national de Coordination de la lutte contre la Criminalité sur Internet (SCOCI).

Etude Optimus "Violences sexuelles envers des enfants et des jeunes en Suisse", février 2012.

Fondation Warentest "Datenschutz bei Onlinenetzwerken", 2010.

Etude de l'Office fédéral de la statistique "Internet dans les ménages en Suisse. Résultats de l'enquête Omnibus TIC 2010".

Chiffres non publiés de l'étude netTEEN (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Université de Zurich).

Fondation Wikimedia: rapport de gestion 2010/2011.