Fondation Scelles, Charpenel Y. (sous la direction de),
Prostitutions: Exploitations, Persécutions, Répressions,
Ed. Economica, Paris, 2016.

Cybervulnérabilité des usagers des réseaux sociaux

Aujourd'hui, l'explosion d'internet et de ses multiples usages a bouleversé les relations humaines, notamment avec les réseaux sociaux qui sont des communautés virtuelles tenant désormais une place prépondérante dans le quotidien de presque tous les internautes. Ils peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des centres d'intérêts communs. Plus de 700 sont recensés dans le monde[1].

Ces médias incitent les utilisateurs à fournir des données à caractère personnel permettant de présenter une description ou un «profil». Les réseaux sociaux mettent également à disposition des outils permettant aux usagers de mettre leur propre contenu en ligne et une liste de contacts pour chaque utilisateur avec une possibilité d'interaction entre eux (*AJ Pénal*, mai 2012).

Si ces réseaux sociaux permettent une libre interaction entre les internautes, le maintien de liens positifs et la possibilité de nouvelles rencontres, il existe des dérives. Depuis les phénomènes d'addiction aux atteintes sur la vie privée, les vulnérabilités découlant des réseaux sociaux n'ont rien de virtuel. Aussi, il convient à chacun de bien en mesurer tous les risques, ce qui est loin d'être évident au vu de l'actualité quotidienne qui relate de nombreuses affaires où des internautes deviennent des « cybervictimes » (*Quemener*, 2013). En effet, on n'y rencontre pas que des amis mais aussi des ennemis qui peuvent appartenir à des réseaux organisés pratiquant le recrutement de futures victimes vulnérables et souvent mineures.

Incontestablement, la liberté d'internet ou son illusion est propice à l'offre de services de prostitution sur des sites mettant ainsi des usagers, parfois fragiles, en risque de proxénétisme. Les réseaux sociaux n'ont fait qu'accentuer ce phénomène car ils favorisent une stratégie d'approche avec prises de contact progressives, conviviales voire ludiques, avec les futures victimes.

L'anonymat relatif que procure internet, la volatilité des échanges qui circulent par ce biais, le caractère mondial et planétaire a en effet incité des délinquants comme des proxénètes et des réseaux organisés à recourir à ces moyens plus discrets pour développer leurs activités illégales.

De plus, la relation des usagers des réseaux sociaux qui peuvent en être aussi les victimes peut apparaître moins risquée et violente par le recours à une communication progressive

[1] *Avis 512009 sur les réseaux sociaux en ligne*, adopté le 12 juin 2009, Groupe de travail « article 29 sur la protection des données ».

© Fondation Scelles, Economica, 2016

ayant souvent largement recours à la séduction. Le prédateur n'est-il pas d'abord un ami avant de devenir un ennemi ?

Ces internautes vulnérables n'ont-ils pas des raisons de culpabiliser davantage que d'autres victimes puisqu'ils ont participé d'une certaine façon à leur perte en échangeant avec leur futur agresseur ? Tous ces questionnements révèlent d'emblée la complexité des rapports de vulnérabilité que génèrent les réseaux sociaux pour des usagers fragiles en raison de leur jeunesse et leurs difficultés personnelles.

Il convient de cerner la nature de ces menaces, présenter les modes opératoires visant ces cybervictimes de prostitution et d'exploitation sexuelle et, enfin, de présenter les réponses législatives tant nationales qu'internationales en ce domaine.

Les cybermenaces sur la liberté individuelle et sur la vie privée

Il faut tout d'abord admettre que le réseautage social est, pour ses nombreux adeptes, l'une des manières les plus pratiques de communiquer, permettant d'utiliser d'innombrables fonctionnalités communautaires.

Les internautes ont tendance à communiquer souvent par jeu et phénomène d'entraînement. Ceci aboutit à la réalisation en quelque sorte d'une *désintimité* (moment de dépossession de l'intimité à l'écran) (*Adolescence*, 2013), à la perte d'un fragment de soi qui implique un véritable mal-être dans la réalité pour certains adolescents, par exemple.

La large exposition de la vie privée est également à considérer comme une autre vulnérabilité découlant d'un accès trop fréquent aux réseaux sociaux. Dans cette optique, les utilisateurs sont demandeurs de services qui proposent un maximum de confidentialité. Les géants du secteur rivalisent ainsi de créativité pour séduire les internautes. Google, Twitter et Facebook du côté logiciel, Research in Motion, Samsung et Apple du côté matériel. Tous affirment détenir le système de cryptage le plus pointu, dont l'infaillibilité est censée garder à l'abri de toutes indiscrétions, les correspondances de ses membres et/ou utilisateurs. En la matière, la sensibilisation et l'éducation sont essentielles.

Les cybermenaces sur l'identité : usurpation d'identité et cyberharcèlement

La vulnérabilité des usagers des réseaux sociaux est particulièrement visible lorsque leur identité va être bafouée et violée. Les victimes potentielles d'usurpation d'identité numérique peuvent être des personnes physiques. Par ailleurs, ce n'est plus le seul nom de la victime qui est visé, mais son identité et plus largement n'importe quelle donnée « permettant de l'identifier ». Les informations relatives à l'identité d'une personne physique susceptibles d'être considérées comme des données « identifiantes » sont nombreuses et variées : nom, prénom, pseudonyme, photographie, dénomination sociale, nom commercial, sigle, marque, logo, enseigne, nom de domaine, adresse IP, adresse e-mail...

La Loi n°2011-267 du 14 mars 2011 d'orientation et programmation pour la performance de la sécurité intérieure (dite loi LOPPSI II) promulguée le 14 mars 2011 a introduit, dans le Code pénal, un délit spécifique d'usurpation d'identité s'étendant aux réseaux numériques. Ainsi, l'article 226-4-1 du Code pénal sanctionne « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de*

troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ».Cette nouvelle incrimination comble un vide juridique en permettant de répondre à des actes malveillants qui ne pouvaient jusque-là tomber sous le coup d'aucune qualification pénale. Certaines décisions avaient sanctionné l'usurpation d'identité, sur un réseau social, sur le fondement de l'article 9 du Code civil relatif au respect de la vie privée.

Il existe aussi un mode de harcèlement sur internet en particulier via les réseaux sociaux. Les personnes victimes de ce type de comportement agressif reçoivent des messages répétés. Leur contenu est teinté de menaces, d'insultes ou de chantage. Les auteurs de ces messages peuvent demander de l'argent pour arrêter de porter préjudice, exiger une rencontre en vue de relations sexuelles ou solliciter des informations privées. Ce type de harcèlement a surtout lieu sur les réseaux sociaux où l'anonymat et l'absence de contrôles d'identité permettent aux « harceleurs » d'agir en toute discrétion.

L'article 222-33-2-2 du Code pénal[2] prévoit désormais que « *Le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni d'un an d'emprisonnement et de 15 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieure ou égale à huit jours ou n'ont entraîné aucune incapacité de travail. Les faits au premier alinéa sont punis de deux ans d'emprisonnement et de 30 000 € d'amende* ». Cependant, le législateur a prévu en la matière une circonstance aggravante en raison de l'utilisation d'un service de communication au public en ligne, les faits étant alors punis de 3 ans d'emprisonnement et de 45 000 € d'amende. Les victimes vont ainsi pouvoir se défendre beaucoup plus efficacement qu'auparavant et les plaintes devraient être traitées plus rapidement par les services de police et de gendarmerie compétents.

Cybervictimes de prostitution et de traite

La plupart des réseaux organisés de traite et de prostitution utilisent désormais les fonctionnalités d'internet pour développer leur « business » et, en particulier, les réseaux sociaux (*Fondation Scelles*, 2013). Les délinquants sexuels sont présents sur les réseaux sociaux comme sur la toile en général, avec la pédopornographie, véritable plaie d'internet (*Robert*, février 2014) contre laquelle le monde entier se mobilise, qui s'accompagne parfois de passages à l'acte où l'on trouve aussi du proxénétisme organisé.

La distance apparente entre internautes facilite les comportements de séduction voire pour certains, de négociation en vue de l'achat d'un service sexuel. Ce qui est un facteur puissant de banalisation de ce qui ressemble tellement à de l'e-commerce ordinaire (*Fondation Scelles Infos*, avril 2014). Par exemple, une affaire a abouti récemment à l'interpellation de plusieurs auteurs qui s'étaient connu par le biais des réseaux sociaux et leur mise en examen pour travail dissimulé et proxénétisme.

[2] Issu de la loi n°2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes.

Les réponses du législateur

L'article 6.I.-1 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) dispose que « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens* ».

En clair, les fournisseurs d'accès à internet (FAI) doivent informer leurs abonnés de l'existence de filtres parentaux et leur en proposer un. Par ailleurs, la même loi précise également que les hébergeurs et les FAI ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Mais ils doivent concourir à la lutte contre la diffusion de ces infractions compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale, à la pornographie enfantine, à la violence, notamment aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine.

La protection spécifique des cybervictimes mineures

L'importance croissante des réseaux sociaux alimente un autre phénomène en constante progression, à savoir la sollicitation d'enfants en ligne à des fins sexuelles (*grooming*). Cette infraction a pour ressort la manipulation. Un adulte profite de l'état de vulnérabilité ou d'un point faible de l'enfant pour lui proposer, via un moyen de communication électronique, une rencontre visant à commettre un abus sexuel. Cette pratique se traduit par une mise en confiance progressive du mineur incité à envoyer des photos intimes. Il est ensuite pris en otage par l'adulte qui menace d'envoyer ces photos à ses parents, à l'école ou à ses amis. Une enquête révèle qu'un enfant sur cent indique que, durant l'année qui précède, on lui a déjà demandé une photo, une vidéo montrant son intimité ou qu'il a été invité à parler d'actes sexuels.

L'infraction est punie de 2 ans d'emprisonnement et de 30 000 € d'amende. Ces peines sont portées à 5 ans d'emprisonnement et 75 000 € d'amende lorsque les propositions ont été suivies d'une rencontre (article 227-22-1 du Code pénal).

La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance contient des dispositions destinées à réprimer certains comportements déviants dans l'usage d'internet au préjudice des mineurs (*AJ Pénal*, mars 2009) qui s'applique pleinement lorsque les faits ont été commis par le biais des réseaux sociaux.

Ainsi, l'infraction de proposition sexuelle à un mineur (C. pén., art. 227-22-1) réprime « *le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique, comportement appelé 'grooming'* ». Ce délit spécifique relatif aux propositions adressées à des mineurs par internet ou par SMS, est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Les peines sont d'ailleurs aggravées à cinq ans d'emprisonnement et 75 000 € d'amende lorsque les propositions aboutissent à une rencontre. Ce délit vise à mieux « traquer

» les adultes au comportement de « prédateurs » qui approchent des mineurs par le biais des réseaux sociaux, en se faisant passer eux-mêmes pour des mineurs.

La circonstance aggravante de recours à un réseau de communication

La traite des êtres humains est un délit puni de sept ans d'emprisonnement et de 150 000 € d'amende (article 225-4-1 du Code pénal). Cependant, des pénalités aggravées sont prévues par les articles 225-4-2 et suivants du Code pénal. L'article 225-4-2 prévoit en effet une peine de 10 ans d'emprisonnement et de 1,5 millions € d'amende lorsque l'infraction est commise dans deux des circonstances mentionnées aux 1° à 4° du I de l'article 225-4-1 du Code pénal. Les mêmes peines sont prévues lorsqu'elle est réalisée avec l'une des circonstances suivantes: 1°) à l'égard de plusieurs personnes ; 2°) à l'égard d'une personne qui se trouvait hors du territoire de la République ou lors de son arrivée sur le territoire de la République ; 3°) lorsque la personne a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique.

L'indispensable prévention et sensibilisation

Les internautes, s'ils sont parfois victimes d'infractions, en sont souvent les facilitateurs involontaires (*Robert*, février 2014), notamment lorsqu'ils dévoilent aux réseaux sociaux des données très personnelles sans être conscients qu'elles pourront un jour se retourner contre eux, et l'on sait que ce risque concerne, tout particulièrement, les mineurs. Plus que tous autres, les mineurs ont besoin d'être sensibilisés aux risques numériques et informés de la protection réelle dont ils peuvent bénéficier, ce que la *Commission nationale consultative des droits de l'homme* (CNCDH) qualifie de nécessaire « culture de la prudence et de la sécurité ». La spécificité de ces questions comme la multiplicité des acteurs conduisent la Défenseure des Enfants à suggérer la création d'une plate-forme spécifique de réflexion, de proposition et d'intervention, rassemblant l'ensemble des acteurs publics et privés, afin d'instaurer une co-régulation des politiques du numérique en direction des mineurs. Ceci rejoint les préoccupations de nombreux autres acteurs, qui souhaiteraient plus de coordination et d'impulsion de la part des Pouvoirs publics, de véritables formations aux médias pour les personnels travaillant avec les jeunes, une modification de la classification des contenus sur le web, une meilleure prise en compte des chartes européennes spécifiques, une incitation à la recherche... (*Robert*, février 2014). Ce constat souligne l'importance d'une réelle pédagogie de l'usage d'internet avec le rappel des valeurs communes susceptibles de justifier que la loi pénale cherche une limitation des libertés multiples offertes par le numérique.

La Recommandation n°3 du rapport du groupe interministériel sur la lutte contre la cybercriminalité (*Robert*, février 2014), souligne les nécessités suivantes :

1- Impliquer davantage l'Etat en terme d'impulsion, de synergie, de définition des objectifs, de pilotage à long terme dans la politique de prévention de la cybercriminalité prise au sens large par :

- des campagnes de sensibilisation, destinées au grand public, sur la protection des données notamment sur les mobiles ou la vigilance contre les escroqueries,

- l'organisation de campagnes-relais en direction de publics plus spécifiques, en mobilisant, voire en organisant, des pôles de compétence,
- la création d'un 17 de l'internet ouvert au grand public,
- la réalisation systématique d'études de risque précédant toute nouvelle ouverture de service dans les domaines réglementés.
2. Faire de l'internaute le premier acteur de sa propre sécurité et de la lutte contre les propos, images et comportements illégaux par :
- l'éducation au numérique à l'école comme la mobilisation des professionnels qui opèrent dans les 5 000 espaces publics numériques et assurent déjà un important effort de formation,
- le développement d'espaces d'information en ligne ou par téléphone,
- l'harmonisation et la généralisation des différents supports préventifs utilisés dans le cadre public,
- la mise en ligne d'un moteur de recherche facilitant la détection de sites, de sociétés ou de spams associés à des cyber-infractions,
- la rationalisation des points d'accès pour les signalements à des fins d'une meilleure visibilité,
- une meilleure association des structures d'aide aux victimes ou de consommateurs,
3. Mobiliser les professionnels en assurant une meilleure cohérence des actions de sensibilisation(…)

Des orientations de politiques pénales strictes

Une circulaire récente définit des orientations de politique pénale afin de renforcer la lutte contre ces phénomènes. Pour la première fois, le terme de cyberprostitution est employé dans un tel document (*ministère de la Justice*, 22 janvier 2015). La traite des êtres humains à des fins d'exploitation sexuelle est la forme d'exploitation humaine la plus ancienne et la plus répandue. En France, cette forme de traite est aujourd'hui principalement le fait de réseaux étrangers. Grâce à une gestion et une logistique opérationnelles éprouvées, les réseaux de prostitution internationaux déplacent très rapidement leurs victimes sur le territoire et assure la logistique grâce à internet et aux réseaux sociaux. Si la prostitution de voie publique se maintient à un niveau constant assez élevé et concerne principalement les personnes d'origine roumaine, bulgare, africaine et chinoise, une prostitution plus discrète, dissimulée derrière des activités telles que les salons de massage, se développe fortement. Cette activité peut s'articuler avec une cyberprostitution sur le point de devenir une institution banalisée. Sa discrétion, son ampleur et la difficulté de détecter l'existence d'un réseau de prostitution derrière la Toile tendent à faire disparaître la traite des êtres humains de l'espace public et rendent le travail d'enquête souvent plus complexe et difficile.

A cet égard, il faut souligner que la lutte contre ce phénomène est désormais une priorité gouvernementale[3] et que la CNCDH lance une vaste démarche de consultation pour définir les priorités de son nouveau mandat de Rapporteur national sur la traite et l'exploitation des êtres humains qui devra notamment déterminer les tendances en matière de traite des êtres

[3] Le Plan d'action national contre la traite des êtres humains, adopté en Conseil des ministres le 14 mai 2015, vise à mettre en œuvre ladirective 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011. Ce Plan a fait l'objet d'une annonce par le Président de la République.

humains. Nul doute que la « cybertraite » par le biais des réseaux sociaux fera l'objet de développements dans le cadre cette étude.

Sources

- Bailly E., Daoud E., « Cybercriminalité et réseaux sociaux, la réponse pénale », *AJ Pénal*, n° 5, mai 2012.
- Charpenel Y., « La prostitution sur internet, au cœur de l'actualité », *Fondation Scelles Infos*, n°28, avril 2014.
- *Circulaire du 22 janvier 2015 de politique pénale en matière de lutte contre la traite des êtres humains*, Bulletin officiel du ministère de la Justice, NOR : JUSD1501974C, 22 janvier 2015.
- CRIDES/Fondation Scelles, *Revue de l'actualité internationale de la prostitution*, 2013.
- CRIDES/Fondation Scelles, *Revue de l'actualité internationale de la prostitution*, 2014.
- Fondation Scelles, Charpenel Y. (sous la direction), *Exploitation sexuelle - Une menace qui s'étend*, Ed. Economica, Paris, 2013.
- Gozlan A., Masson C., « Le théâtre de Facebook : réflexion autour des enjeux psychiques pour l'adolescent », *Adolescence*, 2/2013 (T.31 n° 2), 2013.
- Quemener M., « Réponses pénales face à la cyberpédopornographie », *AJ Pénal*, n°3, mars 2009.
- Quemener M., *Cybersociété - Entre espoirs et risques*, Ed. L'Harmattan, Coll. « Justice et Démocratie », 2013.
- Robert M., ministère de la Justice, ministère de l'Economie et des Finances, ministère de l'intérieur, ministère des petites et moyennes entreprises, de l'innovation et de l'économie numérique, *Protéger les internautes - Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014.

© Fondation Scelles, Economica, 2016