Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

19 octobre 2022

Compléter le code pénal par des dispositions relatives au cyberharcèlement

Rapport du Conseil fédéral donnant suite au postulat 21.3969 de la Commission des affaires juridiques du Conseil national du 25 juin 2021

BJ-D-15663401/110

Compléter le code pénal par des dispositions relatives au cyberharcèlement

Table des matières

Compléter le code pénal par des dispositions relatives au cyberharcèlement

1 Contexte et structure du rapport

1.1 Postulat

Le postulat 21.3969 de la Commission des affaires juridiques du Conseil national (CAJ-N) du 25 juin 2021[1] intitulé « Compléter le code pénal par des dispositions relatives au cyberharcèlement » a la teneur suivante :

> **Texte déposé :** Le Conseil fédéral est chargé d'établir un rapport présentant les possibilités de compléter le code pénal par des dispositions punissant le cyberharcèlement et la violence digitale.
>
> **Développement :** Pour les personnes concernées, le cyberharcèlement est insupportable. Le code pénal (CP) comporte déjà plusieurs articles permettant de punir le cyberharcèlement (art. 173 - diffamation, art. 177 - injure, art. 180 - menaces, art. 181 - contrainte, et bien d'autres).
>
> L'inscription de la notion de cyberharcèlement dans le code pénal ne permet pas à elle seule de soulager la détresse des personnes concernées.

1.2 Historique et structure du rapport

1.2.1 Initiative parlementaire Suter sur le cyberharcèlement

Le 11 juin 2020, la *conseillère nationale Suter* a déposé *l'initiative parlementaire 20.445 « Inscrire le cyberharcèlement dans le code pénal »*[2] pour demander que le code pénal (CP)[3] soit complété d'une disposition érigeant le cyberharcèlement en infraction. Elle indique que le phénomène du cyberharcèlement (les anglophones parlent de cybermobbing, mais aussi de cyberbullying, d'Internetmobbing ou de e-mobbing) a fortement gagné en importance avec l'arrivée des smartphones. *À la différence du harcèlement traditionnel*, poursuit-elle, l'auteur peut rester anonyme, les contenus peuvent rapidement devenir viraux et une fois en ligne, ces contenus sont accessibles en permanence et quasiment impossibles à supprimer. Elle estime que les victimes subissent ainsi une attaque psychologique particulièrement violente. Il est cependant difficile de *poursuivre pénalement* les auteurs, car la jurisprudence associe les éléments constitutifs de l'infraction à des *actes particuliers* aboutissant à un certain résultat, alors que le cyberharcèlement consiste plutôt en une série d'actes et de comportements ayant ensemble un effet sur la victime. Les actes répréhensibles devraient dès lors être décrits *aussi précisément que possible* dans le CP, qui doit définir de manière claire les infractions liées aux nouveaux phénomènes sociaux pour pouvoir avoir un effet préventif.

Lorsque la CAJ-N a discuté de l'initiative parlementaire, le 25 juin 2021, elle a jugé bon de commencer par faire établir un rapport pour voir quelle est la meilleure réponse pénale à apporter au phénomène du cyberharcèlement. Elle a estimé que le CP contient déjà plusieurs articles permettant de punir l'auteur de cyberharcèlement ; inscrire la notion dans le CP ne suffira pas pour réduire la détresse des victimes. La commission a de plus étendu la problématique à la « violence numérique » en général en déposant le même jour le *postulat 21.3969 « Compléter le code pénal par des dispositions relatives au cyberharcèlement »*. Elle a néanmoins donné suite à l'initiative parlementaire 20.445 par 19 voix contre 0 et 4 abstentions pour souligner que les dispositions légales en vigueur ne suffisent pas pour protéger effectivement les victimes[4]. Le Conseil fédéral a proposé le 8 septembre 2021

---

1 www.parlament.ch > Objet 21.3969

2 www.parlament.ch > Objet 20.445

3 RS **311.0**

4 www.parlament.ch > Objet 20.445 > Communiqué de presse > Communiqué de presse de la CAJ-N du 25 juin 2021

d'accepter le postulat, proposition à laquelle le Conseil national s'est rallié sans discussion le 27 septembre 2021[5].

La Commission des affaires juridiques du Conseil des États (CAJ-E) s'est penchée sur l'initiative parlementaire 20.445 le 20 janvier 2022. Elle a décidé par 8 voix contre 5 de ne pas approuver la décision de donner suite à l'initiative pour le moment, souhaitant attendre la publication du rapport que le Conseil fédéral doit établir en réponse au postulat. Elle espère que ce rapport dressera un vaste état des lieux et montrera clairement s'il y a lieu ou non de prendre des mesures en la matière[6].

1.2.2 Interventions parlementaires traitant de la « violence numérique »

Plusieurs interventions parlementaires ont été déposées récemment au sujet de la *« violence numérique ».* Le *postulat 22.3201 Bellaiche « Enrayer la violence numérique »* du 17 mars 2022, que le Conseil fédéral a recommandé d'accepter le 18 mai 2022, demande un rapport sur l'ampleur de la violence numérique en Suisse et sur les mesures à prendre pour la combattre[7]. *L'interpellation 21.3684 Gysin Greta « Violence en ligne. Les bases légales sont-elles adéquates ? »* du 10 juin 2021 présente elle aussi un intérêt dans le contexte du présent rapport. À la question de savoir quelles bases légales protègent les victimes de violence, de haine et de harcèlement en ligne, le Conseil fédéral a répondu en renvoyant aux différentes infractions du CP[8] et aux dispositions prévues contre les atteintes à la personnalité aux art. 28 ss du code civil (CC[9]). Mais il a aussi souligné que le problème qui se pose dans le domaine des poursuites pénales ne réside généralement pas dans l'absence de dispositions matérielles et que la principale difficulté consiste à appliquer le droit[10]. Le *postulat (Quadranti) Siegenthaler 19.4111 « Protéger les enfants et les jeunes et empêcher les criminels de les inciter ou de les forcer à se livrer à des actes sexuels sur eux-mêmes en se filmant avec leur téléphone »* du 24 septembre 2019[11] demande un rapport étudiant les mesures juridiques, techniques ou autres qui permettraient d'empêcher que les enfants et les jeunes ne soient incités ou forcés à réaliser des enregistrements relevant de la pédophilie. Le Conseil national l'a accepté le 20 décembre 2019. Il faut aussi évoquer les *interpellations Gysin Greta 21.3683 « Prévention de la violence en ligne »* du 10 juin 2021[12] et *22.3156 « Prévenir et lutter contre la violence numérique, conformément aux recommandations du Grevio sur la convention d'Istanbul »* du 16 mars 2022[13].

D'autres interventions parlementaires traitent des *différentes formes* de « violence numérique ». Comme le *postulat 21.3450 « Discours de haine. La législation présente-t-elle des lacunes ? »* du 25 mars 2021, par lequel la *Commission de la politique de sécurité du Conseil des États (CPS-E)* a chargé le Conseil fédéral de présenter d'ici à mi-2023 un rapport indiquant les lacunes éventuelles de la législation. Le rapport commandé à l'Office fédéral de la communication (OFCOM) du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) pointera les mesures législatives à prendre et exposera l'ampleur et les formes des discours de haine sur les plateformes en ligne[14]. À la

---

5 BO **2021** 1935

6 www.parlament.ch > Objet 20.445 > Communiqué de presse > Communiqué de presse de la CAJ-E du 20 janvier 2022

7 Il s'agira notamment d'examiner pourquoi rien ne freine la propagation de la violence numérique, pourquoi les poursuites pénales échouent, qui est particulièrement touché et quelles sont les mesures à prendre ou les points de contact à créer pour enrayer le phénomène : www.parlament.ch > Objet 22.3201.

8 Il a cité notamment les délits contre l'honneur (art. 173 ss CP), les menaces (art. 180 CP), la contrainte (art. 181 CP), la pornographie (art. 197 CP) et l'extorsion et chantage (art. 156 CP).

9 RS **210**

10 www.parlament.ch > Objet 21.3684 ; l'interpellation a été liquidée suite à la réponse du Conseil fédéral du 1 septembre 2021.

11 www.parlament.ch > Objet 19.4111.

12 www.parlament.ch > Objet 21.3683 ; l'interpellation a été liquidée avec l'avis du Conseil fédéral du 1 septembre 2021.

13 www.parlament.ch > Objet 22.3156 ; l'interpellation a été liquidée avec l'avis du Conseil fédéral du 18 mai 2022.

14 www.parlament.ch > Objet 21.3450 ; le Conseil des États a accepté le postulat le 8 juin 2021.

suite du rapport établi par l'OFCOM avec la participation de la Chancellerie fédérale, intitulé « Intermédiaires et plateformes de communication »[15], le Conseil fédéral a chargé le DETEC (OFCOM) de lui présenter une note de discussion indiquant si et comment les plateformes de communication doivent être réglementées. Cette note traitera aussi du sujet du postulat. L'OFCOM a en outre invité des chercheurs à soumettre des esquisses de projets sur le thème du discours de haine en ligne. Le Conseil national s'est rallié à la proposition du Conseil fédéral en acceptant le 9 mai 2022 le *postulat 21.4531 Gysin Greta « Transparence sur les cas de discours haineux dans les médias sociaux »* du 16 décembre 2021[16].

L'initiative parlementaire 19.433 de la CAJ-N « Étendre au harcèlement obsessionnel ("stalking") le champ d'application des dispositions du CP relatives aux délits » du 3 mai 2019 vise, comme le dit son développement, à trouver des solutions relatives à l'application du droit en cas de cyberharcèlement[17]. L'*initiative parlementaire 18.434 Amherd (Bregy) « Punir enfin le pédopiégeage en ligne »* du 14 juin 2018, à laquelle les deux chambres ont donné suite[18], sera discutée dans le cadre de l'harmonisation des peines et de l'adaptation du droit pénal accessoire au nouveau droit des sanctions, révision du droit pénal en matière sexuelle (projet 3)[19]. Le Conseil des États a rejeté la création d'une infraction spécifique de pédopiégeage comme le lui proposait la commission chargée de l'examen préalable. Il estime que le droit en vigueur réprime déjà le pédopiégeage au sens étroit[20] lorsque celui-ci constitue la tentative d'un acte punissable. Une nouvelle disposition pénale distincte n'élargirait que peu le champ d'application actuel et n'aurait de ce fait qu'une valeur symbolique. Elle soulèverait en outre de délicats problèmes de concours entre les infractions définies dans le droit en vigueur et la nouvelle infraction. Comme il paraît malaisé de fixer avec précision un seuil à partir duquel un acte serait objectivement punissable, on risque de mettre davantage l'accent sur l'élément subjectif, à savoir l'intention, et de basculer dans le domaine inacceptable du droit pénal réprimant les opinions et les intentions. Le projet est maintenant discuté au Conseil national[21].

1.2.3 Nouvelle infraction de pornodivulgation

Dans le cadre de la *révision du droit pénal en matière sexuelle*, la CAJ-E a proposé par 11 voix contre 1 d'ériger en infraction le phénomène de *pornodivulgation* (« revenge porn »)[22]*.* Quelques participants à la consultation organisée sur le projet de loi étaient d'avis que les dispositions en vigueur ne tiennent pas assez compte du phénomène[23]. La disposition proposée par la CAJ-E (art. 197*a* P-CP) sanctionne la transmission indue d'un contenu non public à caractère sexuel. Il s'agit typiquement de photos ou de vidéos enregistrées dans le cadre d'une relation de couple, avec le consentement des personnes concernées, qui sont ensuite publiées sans le consentement des personnes qui y sont identifiables[24].

Une minorité de la commission proposait de renoncer à pareil article : la disposition ne concerne pas des infractions contre l'intégrité sexuelle, mais plutôt contre l'honneur et contre le domaine secret ou le domaine privé. La minorité estimait aussi qu'il convient de viser d'autre

---

15 Rapport OFCOM Intermédiaires et plateformes de communication

16 www.parlament.ch > Objet 21.4531

17 www.parlament.ch > Objet 19.433

18 www.parlament.ch > Objet 18.434

19 www.parlament.ch > Objet 18.043. Les deux autres projets ont été adoptés par le Parlement le 17 décembre 2021 ; FF **2021** 2996 et 2997.

20 Est considérée comme pédopiégeage en ligne au sens étroit toute prise de contact concrète avec un enfant dans le but de le rencontrer. Voir FF **2022** 687 68.

21 FF **2022** 687 69 s.

22 www.parlament.ch > Objet 18.043 > Communiqué de presse > Communiqué de presse de la CAJ-E du 18 février 2022 ; FF **2022** 687 54 ss

23 Rapport consultation droit pénal en matière sexuelle, ch. 6.3

24 www.parlament.ch > Objet 18.043 > Communiqué de presse > Communiqué de presse de la CAJ-E du 18 février 2022

comportements comme la publication de photos qui, même si elles ne sont pas à caractère sexuel, sont compromettantes[25]. Le Conseil fédéral a soutenu la proposition de la minorité en invoquant les mêmes arguments. Il juge en outre problématique la formulation de la disposition proposée. Il a signalé en particulier que le phénomène en question est une forme de cyberharcèlement qui sera analysée dans le cadre du présent rapport[26]. Le Conseil des États, conseil prioritaire, s'est néanmoins rallié à la majorité de la commission le 13 juin 2022 par 37 voix contre 6 et a accepté l'infraction de pornodivulgation[27].

1.2.4 Interventions traitant de l'application du droit

La *motion 16.4082 Levrat « Faciliter l'accès des autorités de poursuite pénale aux données des réseaux sociaux »* du 15 décembre 2016 demandait qu'un réseau social proposant des services destinés aux consommateurs suisses et traitant des données personnelles à ces fins doive disposer d'une représentation en Suisse. Dans son avis du 15 février 2017, le Conseil fédéral a indiqué qu'il serait difficile d'imposer pareille obligation, tout en signalant les initiatives voyant le jour à l'échelon international pour améliorer la coopération. La motion a été retirée le 22 mars 2018. La *motion 18.3379 CAJ-E « Accès des autorités de poursuite pénale aux données conservées à l'étranger »* du 23 mars 2018, que le Conseil fédéral proposait d'accepter, a en revanche été adoptée par le Parlement[28]. Contrairement à ce que laisse penser son titre, la motion demande que soit instaurée une obligation générale, pour les cyberentreprises, de créer un domicile de notification en Suisse. À la demande du Conseil fédéral, la *motion 18.3306 Glättli « Renforcer l'application du droit sur Internet en obligeant les grandes plates-formes commerciales à avoir un domicile de notification »* du 15 mars 2018 a elle aussi été adoptée[29]. Elle charge le Conseil fédéral de renforcer l'application du droit sur Internet en obligeant les grandes plateformes commerciales à avoir un domicile de notification. Lors des délibérations parlementaires, la conseillère fédérale compétente a déclaré que le Conseil fédéral acceptait cette motion et la motion 18.3379, dans l'idée que des solutions réalisables et efficaces soient recherchées[30].

1.3 Mandat

Le mandat issu du postulat 21.3969 de la CAJ-N « Compléter le code pénal par des dispositions relatives au cyberharcèlement » et de son interprétation à la lumière de l'initiative parlementaire 20.445 Suter « Inscrire le cyberharcèlement dans le code pénal » ainsi que des préoccupations exprimées par la CAJ-E lors des délibérations sur la révision du droit pénal en matière sexuelle est le suivant :

Le rapport devra dresser un vaste état des lieux sur le cyberharcèlement et la violence numérique et montrer clairement s'il y a lieu ou non de prendre des mesures en la matière, autrement dit de compléter le cadre juridique[31]. Il abordera aussi la question de la pornodivulgation, qui est une forme de cyberharcèlement[32]. L'auteur du postulat constate qu'il est difficile dans la pratique de sanctionner le cyberharcèlement, les infractions classiques visant des actes particuliers tandis que le cyberharcèlement consiste en une série d'actes et de comportements ayant ensemble un effet sur la victime. Les actes répréhensibles devraient dès lors être décrits *aussi précisément que possible* dans le CP, qui doit définir de manière

[25] FF **2022** 687 55

[26] FF **2022** 1011 4 s.

[27] BO **2022 E** 499 ss

[28] www.parlament.ch > Objet 18.3379

[29] www.parlament.ch > Objet 18.3306

[30] BO **2018** N 1400.

[31] www.parlament.ch > Objet 21.3969 > Communiqué de presse > Communiqué de presse de la CAJ-E du 21.01.22 > Lutte pénale contre le cyberharcèlement : nécessité d'attendre le rapport du Conseil fédéral.

[32] FF **2022** 1011. 4 s.

claire les infractions liées aux nouveaux phénomènes sociaux pour pouvoir avoir un effet préventif[33].

1.4 Structure du rapport

Le rapport commence par familiariser le lecteur avec les *notions* de cyberharcèlement et de « violence numérique » et tenter de les définir pour les besoins du code pénal (ch. 2), puis il expose la punissabilité de ce phénomène social dans le *droit matériel* en vigueur. Il présente aussi les réglementations adoptées par quelques pays choisis et les lacunes du droit en vigueur, et analyse ses avantages, avant de signaler les possibilités d'action dont dispose le législateur (ch. 3). Le rapport se consacre ensuite à *l'application du droit*. Après une présentation détaillée de la problématique, il expose le mandat législatif issu des interventions parlementaires en suspens (ch. 4). Il se termine par un résumé des conclusions à tirer des études réalisées (ch. 5).

2 Définitions

2.1 Notion de cyberharcèlement

2.1.1 Description du phénomène

Le Conseil fédéral a adopté le 26 mai 2010 le *rapport « Protection contre la cyberintimidation » en réponse au postulat Schmid-Federer 08.3050*. Selon ce rapport, on entend par cyberintimidation « la publication de textes, d'images ou de films diffamatoires par le biais de moyens de communication modernes […] dans le but de dénigrer, de compromettre ou de harceler une personne, sachant que ces attaques sont généralement des actes répétitifs ou commis au cours d'une période relativement longue, et que les victimes se caractérisent par une grande vulnérabilité[34]. » Le terme est défini de manière analogue dans le *rapport du Conseil fédéral du 9 octobre 2013 « Cadre juridique pour les médias sociaux »*[35]*.* L'autrice de l'*initiative parlementaire 20.445* entend par cyberharcèlement le fait « d'insulter, menacer, ridiculiser ou importuner une personne par voie numérique »[36]. Le *rapport de l'OFCOM « Intermédiaires et plateformes de communication »* intègre en outre l'aspect de l'incapacité de la victime à se défendre[37].

Dans la perception qu'en ont aussi bien le public que les juristes qui discutent du phénomène, c'est en particulier au cyberharcèlement entre *adolescents* que les gens pensent[38]. Mais le cyberharcèlement concerne aussi les adultes, et notamment les *personnes qui occupent une position publique*.

Le cyberharcèlement est un *phénomène social* qui peut englober une *multitude de comportements*. Il se définit principalement par les effets qu'il produit sur la victime et sur la perception qu'elle en a. En anglais, le terme de *mobbing* est dérivé du verbe *to mob*, qui signifie assaillir, agresser ou brimer quelqu'un. Le substantif *mob* (bande en anglais) présuppose aussi

---

[33] www.parlament.ch > Objet 20.445 > Développement

[34] www.parlament.ch > Objet 08.3050 ; Rapport cyberintimidation. Le rapport traite de la fréquence et de l'ampleur du phénomène et des mesures possibles pour le combattre, en particulier de la prévention. Le Conseil fédéral avait rejeté la motion Freysinger 10.4054 « Norme pénale contre le harcèlement psychologique », qui demandait l'ajout dans le code pénal d'une disposition condamnant le harcèlement au travail, estimant que le droit en vigueur régule déjà largement ce type de comportement et qu'une norme pénale n'apporterait d'amélioration guère vu qu'elle ne remédierait pas aux problèmes centraux que sont l'administration des preuves et les inhibitions qu'ont les victimes à engager des poursuites. Le Conseil national l'avait suivi par 130 voix contre 33 et 11 abstentions : www.parlament.ch > Objet 10.4054.

[35] Rapport postulat médias sociaux 2013 ; voir aussi le rapport complémentaire médias sociaux 2017.

[36] www.parlament.ch > Objet 20.445 > Développement

[37] Rapport OFCOM Intermédiaires et plateformes de communication, ch. 5.1, avec renvoi à CAMPBELL/BAUMAN, 3

[38] Il n'existe pas de données solides sur l'ampleur de ce phénomène chez les adolescents. La forte hausse évoquée par l'étude JAMES, à laquelle renvoie le développement de l'initiative parlementaire 20.445 Suter « Inscrire le cyberharcèlement dans le code pénal » du 11 juin 2020 (www.parlament.ch > Objet 20.445 > Développement), concerne le harcèlement sexuel, qui peut certes se présenter lors de cyberharcèlement, mais indépendamment de lui. Voir à ce sujet l'étude JAMES 2020 de la Haute école zurichoise des sciences appliquées, www.zhaw.ch > Forschung > Mediennutzung > JAMES > Ergebnisbericht JAMES-Studie 2020, 54.

que plusieurs auteurs s'en prennent ensemble à la même victime[39]. Il y a mobbing – harcèlement en français – dès lors qu'une personne se sent *insultée, chicanée, persécutée ou rabaissée*[40]*.* Les jeunes en particulier ne sont souvent pas conscients des effets de leur comportement, du moins au début. Tout peut même commencer sur le mode de la plaisanterie ; la frontière avec un comportement blessant est souvent floue[41]. Les attaques doivent également être *réitérées* : selon les définitions, il est supposé qu'elles se répètent sur une longue période[42] ou à maintes reprises[43], fréquemment et systématiquement[44]. Le harcèlement peut aussi être *dynamique*, c'est-à-dire que le comportement s'intensifie avec le temps.

Le préfixe *cyber-* vise à indiquer que les auteurs de harcèlement *utilisent les technologies de l'information et de la communication (TIC)*[45], et plus particulièrement les *courriels, services de messagerie, réseaux sociaux, chats, forums, blogs ou portails vidéo*. De nos jours, une part considérable des interactions sociales passe par Internet. Avec la multiplication des smartphones, nombreux sont ceux qui sont en ligne toute la journée. Les conflits se déplacent vers Internet[46]. Il est plus facile d'y rester anonyme[47], chose qui abaisse le seuil d'inhibition des auteurs. De plus, les textes ou images publiés sur des conversations de groupe, les réseaux sociaux, les forums ou les blogs sont accessibles à un large cercle de personnes, parfois incontrôlable. Comme ces messages peuvent déclencher des émotions chez le lecteur, ils se diffusent vite[48]. Le dénigrement est d'autant plus intense qu'il est perçu par un grand nombre de personnes. Et il agit plus longtemps, car les données publiées par des tiers sur Internet ou ailleurs échappent à tout contrôle[49].

Le cyberharcèlement se définit donc comme le *harcèlement en général* – avec la condition supplémentaire qu'il est pratiqué au moyen des TIC[50]. On peut aussi penser à des *formes mixtes*, associant harcèlement dans le monde réel et cyberharcèlement, dont les effets sont globalement dévalorisants.

Il faut noter que le *sens du terme a évolué*. Tandis qu'on l'utilisait au départ avec retenue, le réservant exclusivement aux attaques d'une certaine gravité, le terme de harcèlement désigne de plus en plus souvent des situations conflictuelles telles que des altercations dans la vie professionnelle ou des scènes de dénigrement ponctuelles. Le danger est que les comportements de harcèlement graves soient pris moins au sérieux du fait qu'ils se diluent dans cet usage général[51], alors qu'en droit pénal, domaine qui rattache les effets les plus graves possibles à un comportement clairement défini, il est précisément important de s'en tenir à des éléments conceptuels clairs.

---

39 Voir la définition figurant sous www.skppsc.ch > Thématique Internet > Cyberharcèlement ; voir aussi le rapport OFCOM Intermédiaires et plateformes de communication, ch. 5.1, avec renvoi à CAMPBELL /BAUMAN, 3 : « Groupes ou individus ».

40 Voir www.skppsc.ch > Thématique Internet > Cyberharcèlement > Victimes, auteurs et causes > Les liens victime-harceleur ; www.jeunesetmedia.ch > Thèmes > Cyberharcèlement > Bon à savoir > Le cyberharcèlement est-il un phénomène répandu ?

41 www.jeunesetmedia.ch > Thèmes > Cyberharcèlement > Bon à savoir > Le cyberharcèlement est-il un phénomène répandu ?

42 BRUN, 101 ; www.skppsc.ch > Thématique Internet > Cyberharcèlement > Définition

43 www.jeunesetmedia.ch > Thèmes > Cyberharcèlement > Bon à savoir > Le cyberharcèlement est-il un phénomène répandu ?

44 KUNZ, 8

45 Les TIC sont, au sens large, les technologies de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre l'information sous différentes formes : texte, musique, son, image, vidéo et interface graphique : www.wikipédia.org > TIC

46 www.skppsc.ch > Thématique Internet > Cyberharcèlement > Victimes, auteurs et causes > Déplacement vers Internet, au sujet des jeunes : la prise de risque – consciente ou inconsciente – typique de ce groupe d'âge, la recherche des limites ou leur transgression, se font toujours plus souvent en ligne.

47 Souvent, la victime connaît les auteurs du harcèlement : www.jeunesetmedia.ch > Thèmes > Cyberharcèlement > Bon à savoir > Qu'est-ce que le cyberharcèlement ?

48 Voir par ex. DEB ROY/SINAN ARAL, The spread of true and false news online, www.sience.org du 9 mars 2018.

49 www.skppsc.ch > Thématique Internet > Cyberharcèlement > Victimes, auteurs et causes > Déplacement vers Internet

50 Il n'en va donc pas des infractions numériques au sens strict (infractions commises exclusivement à l'aide des TIC), mais d'infractions dont les auteurs choisissent les TIC comme moyen d'action.

51 KUNZ, 8

2.1.2 Cas de figure

Sur le modèle de BRUN[52] et de la Prévention Suisse de la Criminalité (PSC)[53], le présent rapport se fonde sur les trois cas de figure suivants : *(1) Intimidation :* l'auteur importune sa victime, lui fait peur ou met à mal son sentiment de sécurité. *(2) Intrusion :* l'auteur trouble la sphère privée de sa victime, par exemple en la harcelant par des messages choquants ou des images à caractère sexuel. *(3) Humiliation :* l'auteur dénigre publiquement sa victime, par exemple en diffusant des informations qui portent atteinte à son honneur ou sont erronées, des rumeurs ou des photos ou vidéos embarrassantes, truquées, indécentes ou pornographiques, en créant de faux profils de la victime (au contenu blessant) ou en fondant des « groupes de haine » dans lesquels des propos négatifs sont tenus sur la personne concernée.

Comme le harcèlement consiste en des attaques répétées, les différents cas de figure ne sont pas isolés les uns des autres. Ils peuvent au contraire *se confondre et se cumuler*. C'est ce que montre l'anglais *« harrassment »*, autrement dit l'envoi répété de messages menaçants, humiliants ou insultants[54]. Les types de comportements cités peuvent passer par les TIC ou se produire dans le monde réel (ch. 2.1.1). La répartition entre les cas de figure vise uniquement à faciliter l'approche pénale du phénomène et la réflexion.

2.1.3 Définition pénale

La définition pénale du cyberharcèlement doit s'appuyer sur les **éléments** suivants :

- **Intimidation, intrusion ou humiliation**
  Voir les trois cas de figure au ch. 2.1.2.
- **Répétition**
  Les différents actes se répètent fréquemment sur une longue période.
- **Utilisation des TIC**
  En particulier de courriels, services de messagerie, réseaux sociaux, chats, forums, blogs ou portails vidéo
- **La personne concernée se sent insultée, chicanée, persécutée ou rabaissée**
  Il faut supposer que cet effet est objectivable, autrement dit qu'une personne raisonnable réagirait de la même manière dans la même situation.
- **Intention**
  L'auteur doit agir délibérément. Cela signifie qu'il doit notamment être conscient de l'effet dégradant de ses actes et le vouloir ou du moins en prendre le risque.

La frontière entre cyberharcèlement et *cyberharcèlement obsessionnel* est difficile à tracer. Le stalking ou harcèlement obsessionnel est défini comme « le fait, lorsqu'il est commis intentionnellement, d'adopter à plusieurs reprises un comportement menaçant dirigé envers une autre personne, conduisant celle-ci à craindre pour sa sécurité »[55]. Il s'agit donc d'un comportement à la fois intentionnel, menaçant et répété visant à susciter la peur chez la victime. Comme il ressort de l'exposé des cas de figure possibles (ch. 2.1.2), ces conditions peuvent aussi être réunies lors de (cyber)harcèlement. Le (cyber)stalking peut aussi consister dans des menaces ou intrusions susceptibles d'intimider la victime, de lui faire peur et d'entamer son sentiment de sécurité. L'auteur de harcèlement a généralement pour but de *déprécier ou rabaisser* sa victime.

---

[52] BRUN, 102. WENK 89 prévoit les mêmes cas de figure.

[53] www.skppsc.ch > Thématique Internet > Cyberharcèlement > Définition

[54] BRUN, 102

[55] Rapport OFJ stalking, ch. 3, avec renvoi à la FF **2017** 163 214

2.2 Autres formes de « violence numérique »

2.2.1 Origines du terme

Les notions de « violence numérique » et de « cyberviolence » *ne sont apparues que récemment*. La Convention du Conseil de l'Europe sur la cybercriminalité[56] (CCC) conclue à Budapest le 23 novembre 2001 et entrée en vigueur pour la Suisse le 1er janvier 2012, par exemple, n'évoque pas la violence à propos des infractions commises à l'aide des TIC.

La notion de « violence numérique » est entrée dans le langage juridique international avec une *recommandation du Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO)* du 20 octobre 2021 consacrée à la dimension numérique de la violence à l'égard des femmes[57]. Le GREVIO considère que la violence exercée à l'égard des femmes et la violence domestique, notamment psychologique, peuvent aussi se manifester via les canaux de communication numériques. Le GREVIO fonde ce principe sur une acception large du terme et considère bien des actes commis sur Internet comme des formes de violence à l'égard des femmes ou de violence domestique[58]. Le GREVIO ne qualifie cependant pas directement la cybercriminalité de violence dans sa recommandation. Dans le présent rapport, qui ne se focalise pas sur les formes de violence exercées à l'égard des femmes ou domestique, la conception très large de la recommandation du GREVIO n'est pas appropriée. La recommandation, qui ne reflète d'ailleurs pas la ligne officielle du Conseil de l'Europe, comme le signale l'avant-propos[59], n'a pas d'effet contraignant pour le droit suisse.

La notion de « violence numérique » a également fait son entrée dans le débat public en Suisse. Ainsi, l'interpellation Gysin 21.3684 évoquée plus haut entend par « violence numérique » les phénomènes *de violence, de haine et de harcèlement* qui se produisent *en ligne*. La définition de la violence numérique tend de plus en plus à comprendre les formes de dénigrement, d'isolement social, d'atteinte à la réputation, de contrainte, de chantage et de menaces exercées via les TIC[60].

2.2.2 La notion de violence dans le code pénal

Il est indispensable de signaler que l'inscription d'un nouveau concept de « violence numérique » dans le code pénal serait non seulement inadéquate, mais aussi dangereuse. Pareille généralisation peut conduire à une dilution du concept pénal de violence.

La notion pénale de violence couvre plusieurs aspects. On distingue aujourd'hui la *violence physique, la violence sexuelle et la violence psychologique*. Tandis que les infractions contre la vie et l'intégrité corporelle (art. 111 ss CP) et certaines infractions contre l'intégrité sexuelle (art. 187 ss CP) impliquent de toute évidence des actes de violence, d'autres infractions contiennent des éléments de violence (comme les infractions dites composites : brigandage, extorsion et chantage, art. 140 et 156 CP, mais aussi traite d'êtres humains ou séquestration et enlèvement, art. 182 s. CP).

L'art. 33 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul) conclue le 11 mai

---

56 RS **0.311.43**

57 Recommandation générale nº 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes du 20 octobre 2021, www.coe.int > Droits de l'homme > Violence à l'égard des femmes et violence domestique - GREVIO > À propos du suivi > GREVIO > Recommandation générale > Recommandation générale n° 1

58 Recommandation générale nº 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes du 20 octobre 2021, www.coe.int > Droits de l'homme > Violence à l'égard des femmes et violence domestique - GREVIO > À propos du suivi > GREVIO > Recommandation générale > Recommandation générale n° 1, § 19 s.

59 Recommandation générale nº 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes du 20 octobre 2021, www.coe.int > Droits de l'homme > Violence à l'égard des femmes et violence domestique - GREVIO > À propos du suivi > GREVIO > Recommandation générale > Recommandation générale n° 1, § 2

60 Voir FRASCH. Voir la définition qu'en donne le postulat 22.3201 Bellaiche « Enrayer la violence numérique » du 17 mars 2022, www.parlament.ch > Objet 22.3201 : cyberintimidation, cyberharcèlement, discours haineux, menaces de violence ou discrimination.

2011[61], entrée en vigueur pour la Suisse le 1er avril 2018, définit la violence psychologique comme le fait, lorsqu'il est commis intentionnellement, de porter gravement atteinte à l'intégrité psychologique d'une personne par la contrainte ou les menaces. Dans ce sens, on doit qualifier les infractions de menace (art. 180 CP) et de contrainte (art. 181 CP) d'actes de violence, y compris lorsqu'elles sont commises au moyen des TIC. Tel n'est pas le cas d'autres infractions, que le discours public englobe dans la « violence numérique ». La victime peut là être atteinte dans d'autres aspects de sa personnalité, parce qu'elle est visée par des allégations touchant à son honneur ou la diffusion d'images intimes contre sa volonté, toutes choses qui peuvent causer de grandes souffrances, mais n'impliquent pas forcément de violence (psychologique).

2.2.3 Les différentes attaques numériques

Conformément aux définitions données ci-dessus, le rapport aborde, outre le cyberharcèlement, les phénomènes sociaux que sont le discours de haine, la pornodivulgation et la sextorsion[62]. Il s'agit là d'attaques numériques commises contre la personnalité, qui peuvent comprendre de la violence psychologique (comme dans la sextorsion). Leurs définitions se recoupent partiellement.

Ces phénomènes sont en grande partie couverts par le code pénal (ch. 3.2.1.1 ss). Ils peuvent aussi constituer des actes ponctuels de cyberharcèlement.

- **Discours de haine :** selon une nouvelle recommandation du Comité des Ministres du Conseil de l'Europe[63], le discours de haine (« hate speech ») couvre tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que la race, la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle.
- **Pornodivulgation :** le terme de pornodivulgation (« revenge porn ») a d'abord été défini étroitement comme le fait de publier, après une rupture amoureuse, des photos ou des vidéos intimes de son ancien partenaire faites par la personne représentée ou avec son accord, afin de lui nuire et de se venger[64]. Avec le rôle croissant des TIC, la perception qu'a le public de ce terme s'est élargie. Il s'agit aujourd'hui pour l'essentiel d'images intimes prises sans l'accord de la personne représentée, ou avec son accord mais à destination de certaines personnes, qui sont diffusées pour l'humilier, l'insulter ou la diffamer.
- **Sextorsion :** l'auteur de sextorsion menace une personne de diffuser des photos ou vidéos intimes ou pornographiques soit pour lui extorquer de l'argent, soit pour la contraindre en envoyer d'autres.

---

61 RS **0.311.35**

62 Le rapport exclut donc les phénomènes de cyberstalking et de pédopiégeage en ligne. Le cyberstalking est le harcèlement obsessionnel exercé à l'aide des TIC. Il fait l'objet de l'initiative parlementaire 19.433 de la CAJ-N « Étendre au harcèlement obsessionnel ("stalking") le champ d'application des dispositions du CP relatives aux délits ». Est considéré comme pédopiégeage en ligne au sens étroit le fait d'entrer en contact avec un enfant dans le but de le rencontrer. La question de sa punissabilité fait partie de la révision du droit pénal en matière sexuelle. Le Conseil des États, prioritaire, s'est opposé à l'introduction d'une infraction spécifique de pédopiégeage en ligne. Voir FF 2022 687 71.

63 Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022 : « Le discours de haine est entendu comme tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que la 'race', la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle », www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres.

64 Voir l'interprétation qu'en donne l'interpellation 16.3162 Feri « Vengeance pornographique » du 17 mars 2016, www.parlament.ch > Objet 16.3162.

3 Droit matériel

3.1 Droit civil

Une personne victime de cyberharcèlement ou d'autres atteintes numériques subit en règle générale *une atteinte illicite à sa personnalité*. Elle peut donc faire appel au droit civil pour sa protection contre toute personne qui participe à cette atteinte (art. 28, al. 1, CC).

De la sorte, la personne visée peut requérir le juge *d'interdire une atteinte illicite, si elle est imminente, ou de la faire cesser, si elle dure encore* (art. 28*a*, al. 1, ch. 1 et 2, CC). Elle peut également intenter une action en *dommages-intérêts* et en *réparation du tort moral* (art. 28*a*, al. 3, CC). En cas de violence, de menaces ou de harcèlement, le demandeur peut requérir le juge d'*interdire à l'auteur* de l'atteinte, en particulier *de prendre contact avec lui, notamment par téléphone, par écrit ou par voie électronique* (art. 28*b*, al. 1, ch. 3, CC). Le moyen retenu par l'auteur pour prendre contact par voie électronique est sans importance[65]. Depuis le 1er janvier 2022, la victime peut demander la surveillance électronique de l'auteur (art. 28*c*, al. 1, CC), ce qui est toutefois plus efficace pour les mesures d'éloignement (interdiction d'approcher la victime ou d'accéder à un périmètre déterminé) que pour prévenir les atteintes à la personnalité par la voie électronique[66].

Le tribunal peut, sur demande, ordonner *d'autres mesures* à la place de l'interdiction de prendre contact, telle qu'une interdiction de publier des messages sur les réseaux sociaux.

Les règles générales de procédure civile obligent le demandeur, c'est-à-dire en l'espèce la victime de cyberharcèlement, à *produire la preuve* qu'une personne donnée a porté une atteinte illicite à sa personnalité : le fardeau de l'allégation et de la preuve lui incombe en vertu de l'art. 55, al. 1, du code de procédure civile (CPC[67]). Par ailleurs, la procédure civile permet d'*intervenir rapidement* : les mesures peuvent ordonnées *à titre provisionnel, voire superprovisionnel*, c'est-à-dire sans entendre la partie adverse. L'art. 268 CPC permet en outre de modifier la mesure en tout temps. Le tribunal peut enfin assortir la décision d'une *menace de la peine* encourue pour insoumission à une décision de l'autorité (art. 292 CP), de sorte que l'auteur soit également puni d'une amende, le cas échéant.

3.2 Droit pénal

Le CP ne contient *aucune infraction spécifique* correspondant au cyberharcèlement et aux autres atteintes numériques dont il est question ici. Il prévoit toutefois des possibilités matérielles pour poursuivre et punir le dénigrement, les menaces, la contrainte et d'autres comportements pénalement répréhensibles constitués dans chaque cas d'espèce.

Une des particularités du droit pénal suisse est qu'il respecte autant que possible le principe de *neutralité technologique* (ch. 3.5.5), ce qui signifie que chaque infraction est définie de manière *générale et abstraite*, donc indépendamment de la manière dont l'acte est commis concrètement. Des agissements dans le monde virtuel et dans le monde réel peuvent donc constituer une seule et même infraction, le critère décisif étant l'atteinte portée par un comportement donné. Seules de rares infractions échappent à ce principe, à l'instar de la détérioration de données (art. 144bis CP). Celle-ci a dû faire l'objet d'une disposition spéciale, puisque les éléments constitutifs du dommage à la propriété (art. 144 CP) ne sont pas transposables à des biens immatériels. Autre exemple, l'utilisation abusive d'une installation de télécommunication (art. 179septies CP) est elle aussi nécessairement liée à une technologie donnée.

---

65 Sur l'ensemble de la question, voir le message du 11 octobre 2017 concernant la loi fédérale sur l'amélioration de la protection des victimes de violence, FF **2017** 6913, 6926 ; interpellation 22.3157 Gysin Greta « L'interdiction de contact et l'interdiction géographique protègent-elles suffisamment les victimes de violence numérique ? », www.parlement.ch > Objet 22.3157.

66 Sur l'ensemble de la question, voir FF **2017** 6913, 6949 s.

67 RS **272**

Compléter le code pénal par des dispositions relatives au cyberharcèlement

3.2.1 Cyberharcèlement

D'après le rapport du Conseil fédéral du 26 mai 2010 en réponse au *postulat Schmid-Federer 08.3050 « Protection contre la cyberintimidation »*, les actes de harcèlement, d'intimidation ou de dénigrement à la base du phénomène peuvent faire l'objet de poursuites efficaces et de sanctions appropriées en application de l'instrumentaire pénal existant[68].

De même, le *rapport du Conseil fédéral sur les médias sociaux de 2013 et le rapport complémentaire de 2017* précisent que rien ne semble indiquer que l'arsenal pénal existant serait insuffisant. Ces deux rapports constatent que la principale difficulté réside dans l'application du droit[69].

Enfin, dans son *rapport du 22 juin 2015 sur la motion 12.4161 Schmid-Federer « Pour une stratégie nationale contre le cyberharcèlement »,* la Commission de la science, de l'éducation et de la culture du Conseil des États (CSEC-E) n'a pas non plus jugé nécessaire de créer une nouvelle norme pénale, car les dispositions en vigueur lui semblent suffire à sanctionner le cyberharcèlement[70].

Les infractions existantes qui peuvent s'appliquer au cyberharcèlement sont présentées ci-dessous plus en détail selon les cas de figure traités au ch. 2.1.2.

3.2.1.1 Intimidation

Dans ce cas de figure, le harceleur utilise les TIC pour intimider quelqu'un en l'importunant, en l'effrayant ou en le faisant se sentir en danger.

Menaces (art. 180 CP) : c'est la première infraction qui entre ici en ligne de compte. Quiconque, *par une menace grave, alarme ou effraye* une personne est puni. Cette disposition protège dans une certaine mesure la *liberté intérieure* à laquelle chacun a droit afin d'assurer la libre formation ou le maintien de son équilibre psychique. Elle protège également le *sentiment de sécurité* d'une personne contre un tiers qui chercherait à lui nuire gravement[71]. L'auteur doit annoncer ou faire redouter[72] à la victime un *dommage grave* dont la réalisation semble dépendre de sa volonté[73]. Dans le cas du cyberharcèlement, il peut s'agir de violence ou d'une communication compromettante. Quant à savoir ce qui constitue une menace grave au sens de cette infraction, la jurisprudence récente du Tribunal fédéral relativise son ancienne interprétation. S'il se fondait auparavant sur des critères objectifs, il admet aujourd'hui des exceptions. *En règle générale*, il considère qu'il faut tenir compte de la réaction qu'aurait une personne raisonnable, dotée d'une résistance psychologique plus ou moins normale[74]. Cette

---

[68] www.parlement.ch > Objet 08.3050 ; rapport cyberintimidation, p. 22. Le Conseil fédéral avait refusé la création d'une nouvelle infraction pour le harcèlement psychologique au travail, demandée par la motion Freysinger 10.4054 « Norme pénale contre le harcèlement psychologique », car il estimait que le droit en vigueur contenait déjà de nombreuses normes sanctionnant les comportements visés et que la création d'une nouvelle norme pénale ne résoudrait rien, dans la mesure où elle ne règlerait pas les problèmes centraux posés par l'administration des preuves et la crainte des victimes d'intenter une action en justice. Le Conseil national a également rejeté la motion par 130 voix contre 33 et 11 abstentions : www.parlement.ch > Objet 10.4054.

[69] Rapport postulat médias sociaux 2013, ch. 4.4.2.3 et rapport complémentaire médias sociaux 2017, ch. 5.3.2.1. Ces rapports renvoient également aux possibilités offertes par le droit civil : 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.

[70] Rapport du 22 juin 2015 sur la motion 12.4161 Schmid-Federer « Pour une stratégie nationale contre le cyberharcèlement », www.parlement.ch > Objet 12.4161 > ch. 4. Dans sa prise de position du 27 février 2013 sur cette motion, le Conseil fédéral avait indiqué que les résultats de l'évaluation du programme Jeunes et médias permettraient de définir si d'autres mesures s'imposaient. Dans le rapport précité, publié après cette évaluation, la CSEC-E n'a pas estimé pertinent de mettre en place une stratégie nationale de lutte contre le cyberharcèlement. Elle a constaté que les mesures d'encouragement et de prévention appliquées dans le cadre de ces programmes, qui avaient pour cible principale le cyberharcèlement, avaient porté leurs fruits, la priorité ayant été donnée à la protection des enfants et des jeunes contre les comportements sociaux inadéquats ou criminels liés à l'utilisation des médias numériques. Dans ce cadre, les cantons avaient déjà enregistré des succès en matière de prévention. Quant aux offres de conseil, elles se sont largement développées depuis.

[71] DELNON/RÜDY, BSK II StGB, Art. 180 N 5

[72] STRATENWERTH/BOMMER, BT I, § 5 N 98

[73] DELNON/RÜDY, BSK II StGB, Art. 180 N 14 ; TRECHSEL/MONA, PK StGB, Art. 181 N 4 ; ATF 120 IV 17, 19 ; 106 IV 125, 128 s. ; 94 IV 111, 116 ; 81 IV 101, 105

[74] Arrêts du TF 6B_192/2012 du 10 septembre 2012, consid. 1.1 et les références citées et 6B_307/2013 du 13 juin 2013, consid. 5.1

relativisation permet d'adapter l'appréciation du seuil de gravité à la situation de personnes particulièrement vulnérables, tels que les jeunes, souvent victimes de cyberharcèlement[75]. Le Tribunal fédéral a également affirmé que toutes les circonstances du cas d'espèce doivent être examinées pour déterminer si la menace est de nature à *alarmer le lésé*[76]. Il a ainsi admis que des menaces de gravité variable, répétées sur une longue période (en l'occurrence un an) réalisaient l'infraction : la personne concernée avait d'après lui développé un sentiment de malaise à l'égard de l'auteur et avait ainsi perdu son sentiment de sécurité intérieure[77]. La victime doit craindre la réalisation du dommage annoncé ou la considérer comme plausible et d'autre part être effrayée ou alarmée par la gravité du dommage[78]. La menace est poursuivie sur plainte[79] et punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Contrainte (art. 181 CP) : la contrainte constitue une infraction contre la liberté de formation et d'exercice de la volonté. Il y a contrainte lorsque l'auteur, en usant de violence envers une personne ou en la menaçant d'un dommage sérieux, ou en l'entravant de quelque autre manière dans sa liberté d'action, l'oblige à faire, à ne pas faire ou à laisser faire un acte. Le « sérieux » dommage annoncé, dont la réalisation doit ici aussi sembler dépendre de la volonté de l'auteur (c'est du moins ce que la victime doit croire)[80], ne doit pas être de la même gravité que pour les menaces. En particulier, il ne doit pas nécessairement effrayer ou alarmer la victime. Le moyen de contrainte doit toutefois atteindre une certaine intensité pour être de nature à influencer la liberté d'action d'un tiers. Pour éviter une extension excessive de la protection pénale, le Tribunal fédéral se fonde ici en principe sur un *critère objectif* pour déterminer si le dommage annoncé est sérieux au sens de l'art. 181 : seules les menaces susceptibles de faire plier une personne raisonnable réalisent les conditions de l'infraction[81]. Le caractère absolu de ce critère doit toutefois être relativisé pour deux raisons : d'une part, la situation de chaque victime permet une certaine marge d'appréciation et d'autre part, un dommage relativement anodin doit être considéré comme « sérieux » si l'auteur exploite délibérément une faiblesse particulière de la victime, par ex. une phobie[82]. Comme pour les menaces, une partie de la doctrine suggère donc que la situation des personnes particulièrement vulnérables doit être prise en compte[83]. Quant à la formule générale « *de quelque autre manière* », son application présuppose un effet qui dépasse clairement le niveau d'influence habituellement toléré, comme de la violence ou la menace d'un dommage sérieux, expressément mentionnées par la loi[84]. L'intensité de la violence n'a cependant pas besoin d'être élevée au point de rendre la victime incapable de résister. Le critère est ici relatif : il suffit que la violence fasse plier la victime[85]. Étant donné que la définition de la contrainte est ouverte, son caractère illicite doit être particulièrement bien établi pour que l'infraction soit réalisée. En effet, ce n'est pas la liberté de l'individu qui est protégée en soi, car la liberté absolue n'existe pas. L'ordre étatique et juridique ainsi que la vie en société imposent d'emblée à chacun de nombreuses contraintes de fait et de droit. La loi ne protège donc pas toute liberté de formation et d'exercice de la volonté. Par conséquent, seule une restriction illicite de la liberté peut être punissable, ce qui ne protège que la liberté de l'individu « protégée par la loi » ou « garantie

[75] DELNON/RÜDY, BSK II StGB, art. 180 N 21 ; voir également BRUN, 103.

[76] ATF **99** IV 212, 215

[77] Il s'agissait de menaces adressées par le mari à sa femme : arrêt du TF 6B_1121/2013 du 6 mai 2014, consid. 6.3 et 6 à 8.

[78] DELNON/RÜDY, BSK II StGB, Art. 180 N 24

[79] La poursuite a toutefois lieu d'office si la menace est proférée dans le contexte d'une relation de couple : art. 180, al. 2, CP.

[80] DELNON/RÜDY, BSK II StGB, Art. 181 N 26 et 25

[81] ATF 122 IV 325 s. ; 120 IV 17, 19 ; 115 IV 207 ; 107 IV 38 ; 106 IV 125 ; 105 IV 122 ; 101 IV 48

[82] TRECHSEL/MONA, PK StGB, Art. 181 N 5

[83] DELNON/RÜDY, BSK II StGB, Art. 181 N 35 et les références citées ; sur le cyberharcèlement, BRUN, 105

[84] ATF 119 IV 301, 305

[85] ATF 101 IV 42, 44 ; 101 IV 167, 169

par la loi »[86]. La contrainte est poursuivie d'office et punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Dans le cas de la contrainte découlant d'un harcèlement obsessionnel (s*talking*), la jurisprudence fédérale a développé la thèse selon laquelle les effets d'une multitude d'intrusions durant une longue période se cumulent. Si une certaine intensité est atteinte, chaque acte qui, pris isolément, ne constituerait pas une contrainte devient susceptible d'entraver suffisamment la liberté de la victime pour remplir les conditions de l'infraction[87]. Face à cette jurisprudence, BRUN considère que le cyberharcèlement peut constituer une contrainte, dès lors que la durée et l'intensité de la pression exercée sur la victime en viennent à entraver sa liberté d'action[88].

Extorsion et chantage (art. 156 CP) : il s'agit d'une forme de contrainte qualifiée. L'infraction consiste à user d'un moyen de contrainte afin de disposer autrui à un acte préjudiciable visant l'enrichissement illégitime de l'auteur ou d'un tiers. Cette norme protège ainsi les biens juridiques que sont la liberté et le patrimoine[89]. Elle est classée parmi les infractions contre le patrimoine, au titre 2 des dispositions spéciales du CP et sanctionne quiconque, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, détermine une personne à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, en usant de violence ou en la menaçant d'un dommage sérieux. Concernant les moyens de contrainte, on renverra au commentaire de l'infraction précédente[90]. Quant à l'acte de disposition préjudiciable, il peut s'agir de l'octroi de tout avantage pécuniaire, par exemple du versement d'une somme[91]. Infraction poursuivie d'office, l'extorsion est punie d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

La *sextorsion* et les *menaces de pornodivulgation* tombent également sous le coup des infractions susmentionnées. Ainsi, il y a *contrainte* lorsque l'auteur menace de publier une image compromettante sur Internet si la victime n'en envoie pas d'autres, par ex. Il y a *extorsion et chantage* lorsque l'auteur menace de publier l'image s'il ne reçoit pas une certaine somme en échange. Enfin, il y a *menaces* lorsque l'auteur menace simplement de la publier (pour plus de détails, voir ch. 3.2.3 et 3.2.4).

L'**injure (art. 177 CP)** est également une forme d'intimidation directe. Est coupable d'injure quiconque attaque autrui dans son honneur, par ex. par l'écriture ou l'image (et « de toute autre manière » que par la diffamation ou la calomnie, voir art. 173 s. CP), notamment en alléguant des faits entre quatre yeux, c'est-à-dire uniquement auprès de la personne lésée, ou en exprimant un jugement de valeur auprès de tiers ou en s'adressant à la personne visée. L'art. 177 CP est subsidiaire aux art. 173 s. CP, il constitue une clause générale. L'objet de l'injure est soit un pur jugement de valeur[92] (c'est-à-dire une simple absence de respect, sans que les propos incriminés ne s'appuient vraisemblablement sur des faits concrets), soit une diffamation ou une injure adressée directement au lésé[93]. Face à un fait attentatoire à l'honneur, c'est le *sentiment subjectif d'honneur* qui est protégé, c'est-à-dire le sentiment d'être une personne honnête et respectable et considérée en tant que telle par autrui[94]. Le sentiment d'honneur peut être blessé directement par des allégations adressées à la victime, mais

---

[86] DELNON/RÜDY, BSK II StGB, Art. 181 N 8 et les références citées

[87] ATF 141 IV 437, 441

[88] BRUN, 105

[89] WEISSENBERGER, BSK II, Art. 156 N 1

[90] WEISSENBERGER, BSK II, Art. 156 N 10

[91] STRATENWERTH/BOMMER, BT I, § 17 N 6 ss

[92] Également appelé injure formelle ou injure verbale.

[93] RIKLIN, BSK II StGB, Art. 177 N 1 et 4

[94] RIKLIN, BSK II StGB, Vor Art. 173 N 9 ; voir RIKLIN, 33 s. et les références citées ; dans ce sens également ATF 77 IV 94, 98 ; 80 IV 159, 164 s. ; 85 IV 182, 186 ; 92 IV 99, 101 ; 93 IV 20, 21 ; 96 IV 148, 149.

aussi indirectement lorsqu'elle a vent d'atteintes portées à sa réputation auprès de tiers[95]. L'auteur de l'injure refuse de témoigner à la personne lésée le respect qu'il lui doit objectivement[96]. On relèvera dans la jurisprudence fédérale les injures porc, charogne[97], psychopathe,[98] crapule [99] et putain[100]. Poursuivie sur plainte, l'injure est punie d'une peine pécuniaire de 90 jours-amende au plus.

3.2.1.2 Intrusion

Dans ce cas de figure, le harceleur viole la sphère privée de la victime, par ex. en lui envoyant des messages obscènes ou des images à caractère sexuel.

Pornographie (art. 197 CP) : La *pornographie* est une représentation vulgaire à outrance et primitive de la sexualité ramenée à elle-même, qui réduit les personnes au rang d'objets sexuels et a pour objectif d'éveiller le désir du spectateur[101]. Si la victime de harcèlement est importunée par des contenus pornographiques, l'infraction qui s'applique est la pornographie. Elle punit quiconque transmet de la « *pornographie dure* », c'est-à-dire en particulier des écrits, enregistrements sonores ou visuels, images ou représentations ayant comme contenu des actes d'ordre sexuel avec des animaux ou des actes d'ordre sexuel non effectifs avec des mineurs. La révision du droit pénal sexuel (ch. 1.2.3) retirera les actes de violence entre adultes de la définition de la pornographie dure[102]. Poursuivie d'office, cette infraction appelle une peine privative de liberté de trois ans au plus ou une peine pécuniaire. S'il s'agit d'actes d'ordre sexuel effectifs avec des mineurs, la sanction est une peine privative de liberté de cinq ans au plus ou une peine pécuniaire (art. 197, al. 4, CP).

Si le destinataire est âgé de *moins de 16 ans*, le fait de transmettre toute forme de pornographie, même dite « douce », est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (art. 197, al. 1, CP). En outre, proposer ou transmettre de la pornographie douce à des adultes sans y avoir été invité est puni de l'amende (art. 197, al. 2, CP).

Désagrément causé par la confrontation à un acte d'ordre sexuel (art. 198 CP) : s'il ne s'agit pas de contenu pornographique, l'infraction de désagrément causé par la confrontation à un acte d'ordre sexuel peut être réalisée. L'art. 198 CP punit notamment quiconque importune une personne par des paroles grossières (al. 2). La révision du droit pénal en matière sexuelle doit également être mentionnée ici : comme le demande la motion 18.4049 Reynard « Harcèlement sexuel. De graves lacunes à combler » du 28 septembre 2018[103] (entre-temps classée), l'infraction comportera les termes « écriture » et « image ». Dans un arrêt récent[104], le Tribunal fédéral a indiqué que l'art. 198, al. 2, portait aussi bien sur la parole que sur l'écriture ou l'image. Cette conception se retrouve également dans les développements les plus récents de la doctrine[105]. Pour satisfaire au principe de la précision de la base légale et assurer un rapprochement avec les art. 177 et 261[bis], le texte de l'art. 198 précisera que l'infraction peut également être réalisée par l'écriture. Cet ajout fera notamment de l'envoi via les TIC d'images à caractère sexuel et de messages obscènes des éléments constitutifs de

---

95 RIKLIN, BSK II StGB, Vor Art. 173 N 9

96 RIKLIN, BSK II StGB, Art. 177 N 1

97 ATF 86 IV 81, 82

98 ATF 93 IV 20, 21

99 ATF 79 IV 20, 22

100 ATF 92 IV 115

101 STRATENWERTH/BOMMER, BT I, § 17 N 4

102 FF **2022** 687, 35

103 www.parlement.ch > Objet 18.4049. La motion a été classée le 25 septembre 2020.

104 Arrêt du TF 6B_69/2019 du 4 novembre 2019, consid. 2.3.2

105 DONATSCH, § 65 588

l'infraction[106]. Le critère de la grossièreté du désagrément d'ordre sexuel par l'écriture ou par l'image vise à donner une certaine précision et signifie – dans le cas des paroles, qui constituent l'infraction dans le droit en vigueur – que seules les déclarations particulièrement vulgaires, qui constituent une sollicitation outrancière, réalisent l'infraction[107]. Celle-ci est punie sur plainte d'une amende.

L'**utilisation abusive d'une installation de télécommunication (art. 179^{septies} CP)** peut servir de *clause générale* pour les intrusions qui ne correspondent pas aux infractions susmentionnées[108]. L'enjeu est ici la protection de la sphère privée[109]. Cette infraction punit quiconque, par méchanceté ou par espièglerie, utilise abusivement une installation de télécommunication pour inquiéter un tiers ou pour l'importuner et convient donc parfaitement aux intrusions via les TIC. Les deux conditions subjectives auxquelles l'infraction est actuellement soumise, à savoir la méchanceté et l'espièglerie, seront abrogées par le projet d'harmonisation (ch. 1.2.3), ce qui permettra notamment de punir les intrusions obscènes. Le critère déterminant est que les contacts via les TIC soient objectivement pénibles ou inquiétants et atteignent une certaine fréquence ou gravité[110]. L'accumulation d'actes de moindre gravité dont l'impact s'additionne peut également réaliser l'infraction, comme l'envoi en masse de courriels[111]. La sanction prévue pour cette infraction poursuivie sur plainte a été relevée à une peine privative de liberté d'un an au plus ou à une peine pécuniaire[112].

3.2.1.3 Humiliation

Dans ce cas de figure, l'auteur dénigre publiquement la personne concernée, par exemple en la diffamant, en diffusant des informations qui portent atteinte à son honneur ou sont erronées, des rumeurs, des photos ou des vidéos embarrassantes, truquées, indécentes ou pornographiques, en créant de faux profils de la victime (au contenu blessant) ou en fondant des « groupes de haine » dans lesquels des propos négatifs sont.

Diffamation et calomnie (art. 173 s. CP) : la *diffamation* (art. 173 CP) présuppose que l'auteur, en s'adressant à un tiers, accuse une personne ou jette sur elle le soupçon de tenir une conduite contraire à l'honneur, ou de tout autre fait propre à porter atteinte à sa considération (ch. 1, al. 1). Se rend également coupable quiconque propage une telle accusation ou un tel soupçon (ch. 1, al. 2). Si l'auteur connaît la fausseté de ses allégations, il s'agit de *calomnie* (art. 174 CP).

Tout l'enjeu de ces infractions consiste à déterminer *quand le bien juridique que constitue l'honneur est violé*. La doctrine et la jurisprudence se sont longtemps fondées sur la *notion effective de l'honneur*[113]. Il s'agit ici de la *réputation et du sentiment d'être une personne honorable, d'être respecté par les tiers* – ou comme le formule le Tribunal fédéral, de la réputation de se comporter « comme un homme digne a coutume de le faire selon les idées généralement reçues[114] ». D'après le Tribunal fédéral, le droit pénal protège uniquement la *réputation morale*, soit la réputation d'être une personne honorable, qui a trait à la dimension humaine et morale de la personnalité[115]. Est notamment punissable le fait d'accuser

[106] FF **2022** 687, 60 s.

[107] ISENRING, BSK II, Art. 198 N 22

[108] BRUN, 109

[109] BRUN, 109 : utilisation des nouvelles technologies de communication ; RAMEL/VOGELSANG, BSK I StGB, Art. 179^{septies} N 1a : l'infraction couvre en particulier les courriels, les messages texte et les images.

[110] ATF 126 IV 216 consid. 2

[111] Arrêt du TF 6B_75/2009 du 2 juin 2009, consid. 3.2.1 ; ATF 126 IV 219 ; Kinzig, 3

[112] FF **2018** 2889, 2929 ; FF **2021** 2997

[113] RIKLIN, BSK II StGB, Vor Art. 173 N 12

[114] ATF 93 IV 20, 21 ; 103 IV 157, 158 ; 105 IV 111, 112 ; 105 IV 194, 195 ; 117 IV 27, 28 s. ; 131 IV 154, 157

[115] ATF 115 IV 42, 44

quelqu'un d'actes moralement répréhensibles[116]. À l'inverse, la *réputation sociale*, soit la position sociale et professionnelle de chacun[117], n'est pas protégée par le droit pénal, ce qui a été condamné par presque tous les auteurs de doctrine[118]. Cette jurisprudence a récemment été quelque peu relativisée, dans la mesure où le Tribunal fédéral a admis la possibilité que des allégations visant l'attitude professionnelle d'un individu participent de l'atteinte à la réputation morale et puissent « léser son crédit de personne honorable[119] ». Les allégations contre la réputation sociale sont donc pertinentes si elles font également paraître la personne visée moins honorable[120].

Ainsi, la jurisprudence a jugé attentatoire à l'honneur le fait d'alléguer que quelqu'un est une putain[121], entretient des relations avec des maquereaux et des prostituées et a travaillé dans ce secteur[122], a une maladie vénérienne[123], opinions politiques nazies[124], entame des procédures parce qu'il est le seul à en tirer profit en tant qu'avocat[125] ou instigue des manifestations illégales en tant que politicien[126]. En outre, employer de manière diffamatoire des termes relevant de la psychiatrie ou qui y sont associés pour présenter quelqu'un comme anormal, aliéné ou asocial constitue également une atteinte à l'honneur[127]. Le Tribunal fédéral ne considère pas que reprocher une maladie ou une anormalité porte nécessairement atteinte à l'honneur[128]. Le reproche devient une infraction lorsqu'il a trait à la capacité à assumer des responsabilités. Les diagnostics médicaux font exception[129]. L'infraction peut s'appliquer même si le trouble est avéré, il est ainsi particulièrement grave de traiter un malade mental de « cinglé »[130].

La diffamation est poursuivie sur plainte et sanctionnée d'une peine pécuniaire. Quant à la calomnie, elle est punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (art. 174, ch. 1). La peine est une peine privative de liberté de trois ans au plus ou une peine pécuniaire de 30 jours-amende au moins si le calomniateur a, de propos délibéré, cherché à ruiner la réputation de sa victime (art. 174, ch. 2).

Dans le cas du *discours de haine* (voir ch. 3.2.2) comme aspect du cyberharcèlement, les infractions applicables sont d'abord les *délits contre l'honneur* (art. 173 ss), mais aussi les *menaces* (art. 180) et la *contrainte* (art. 181). La *discrimination et incitation à la haine* (art. 261bis)[131], la *représentation de la violence* (art. 135) ou encore la *provocation publique au crime ou à la violence* (art. 259) et d'autres infractions encore peuvent également être réalisées.

---

116 ATF 76 IV 29

117 RIKLIN, 39

118 RIKLIN, BSK II StGB, Vor Art. 173 N 18 et les références citées

119 ATF 80 IV 159, 165 ; 99 IV 148, 150 entre autres ; Schwander, StGB, Nr. 600a

120 ATF 71 IV 225, 230 ; 77 IV 94, 95 ; 80 IV 159, 164 ; 92 IV 94, 96 ; 98 IV 90, 92 ; 103 IV 157, 158 ; 105 IV 111, 112 ; 105 IV 194, 195 ; 116 IV 205, 206 ; 117 IV 27 ss ; 119 IV 44, 47 ; sur l'ensemble RIKLIN, BSK II StGB, Vor Art. 173 N 18 s.

121 ATF 92 IV 115, 117 s.

122 Arrêt du TF 6B_584/2016 du 6 février 2017, consid. 3.2 et 3.2.1

123 ATF 78 IV 32 ; 80 IV 159, 168 s.

124 Arrêt de la Cour suprême du canton de Berne du 10 février 1987, in RSJ 1988, 327, n° 54

125 ATF 99 IV 148, 149

126 ATF 108 IV 94, 95

127 ATF 93 IV 20, 22 ; 96 IV 54, 55 ; 98 IV 90, 93 ; autres exemples chez RIKLIN, BSK II StGB, Vor Art. 173 N 20 ss

128 TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 8

129 TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 10

130 TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 8

131 Arrêt du TF B_627/2015 du 4 novembre 2015, consid. 2.8

Usurpation d'identité (art. 179decies nCP) : La révision totale de la loi fédérale du 19 juin 1992 sur la protection des données (LPD[132]) crée une nouvelle infraction qui sanctionne l'usurpation d'identité. L'entrée en vigueur du nouvel art. 179decies CP est prévue au 1er septembre 2023. Il punit l'utilisation de l'identité d'une autre personne sans son consentement dans le dessein de lui nuire ou de se procurer ou de procurer à un tiers un avantage illicite. L'infraction présuppose que la victime de l'usurpation subisse un dommage d'une certaine gravité, qu'il soit matériel ou non. La seule intention de causer de graves ennuis peut déjà suffire. Poursuivie sur plainte, l'usurpation d'identité sera punie d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire. Prendre l'identité d'un tiers pour créer un faux profil pourra donc réaliser cette infraction à l'avenir. L'atteinte à la réputation qui en découle sera toujours sanctionnée par les délits contre l'honneur (art. 173 ss CP)[133]. Dans le cas des faux profils, l'*accès indu à un système informatique* (art. 143bis CP), l'*utilisation frauduleuse d'un ordinateur* (art. 147 CP), la *détérioration de données* (art. 144bis CP) ou encore la *soustraction de données personnelles* (art. 179novies CP, également introduit par la révision de la LPD et en vigueur dès septembre 2023) peuvent également être applicables.

La diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes constitue une variante de la *pornodivulgation*. S'il s'agit *de photos ou de vidéos à caractère pornographique*, l'infraction pertinente est la *pornographie* (art. 197 CP ; ch. 3.2.1.2). Il est délicat de déterminer à partir de quel moment une image (non pornographique) doit être considérée comme *embarrassante*. Une photo issue de la sphère intime de la personne représentée ne porte pas en soi atteinte à son honneur[134]. En revanche, si elle est calomnieuse ou de nature trompeuse, propre à donner l'impression que la personne visée se dénigre ou s'humilie, les délits contre l'honneur peuvent être réalisés (notamment la diffamation, art. 173 CP ; ch. 3.2.1.2, voir également ch. 3.2.3).

3.2.2 Discours de haine

La punissabilité du discours de haine selon le droit en vigueur a déjà été abordée du point de vue des actes relevant du cyberharcèlement (ch. 3.2.1.3). L'infraction de *discrimination et incitation à la haine* (art. 261bis CP) s'applique à l'incitation publique à la haine ou à la discrimination envers une personne ou un groupe de personnes en raison de leur appartenance raciale, ethnique ou religieuse ou de leur orientation sexuelle (al. 1), à la propagation d'idéologies (al. 2), à l'organisation, l'encouragement et la participation à des actions de propagande (al. 3) ainsi qu'au fait d'abaisser ou de discriminer publiquement autrui d'une façon qui porte atteinte à la dignité humaine, par la parole, l'écriture, l'image, le geste, par des voies de fait ou de toute autre manière (al. 4). Cette norme pénale protège la dignité humaine et (accessoirement) la paix publique, dans la mesure où elle sanctionne l'incitation publique à la haine et la discrimination publique fondée sur des caractéristiques fondamentales de la personnalité. Le droit pénal concrétise ainsi en partie l'interdiction de la discrimination inscrite à l'art. 8 Cst. À la faveur de l'initiative parlementaire 13.407 Reynard « Lutter contre les discriminations basées sur l'orientation sexuelle » du 7 mars 2013, l'art. 261bis CP a récemment été complété par l'élément de l'orientation sexuelle. Cette modification est entrée en vigueur le 1er juillet 2020. La discrimination fondée sur l'identité de genre[135] est pour sa part sanctionnée au titre des délits contre l'honneur (art. 173 ss CP), les infractions contre l'intégrité

[132] RS **235.1**

[133] FF **2020** 7397, 7446 ; FF **2017** 6565, 6741 s.

[134] RSJ 2004, 95 s.

[135] Les comportements à poursuivre pénalement selon la Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022 (www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres) ne sont toutefois pour la plupart pas entièrement couverts par le CP. Par ex., à l'inverse de cette recommandation, l'art. 261bis CP ne protège ni le genre en tant que tel ni toutes les personnes LGBTI. Sur proposition du Conseil fédéral, le Parlement a expressément renoncé à inclure l'élément d'identité de genre dans la norme pénale : FF **2018** 5327. Voir toutefois les initiatives parlementaires 21.527 Bertschy, 21.522 Studer, 21.516 Arslan, 21.515 De Quattro, 21.514 Binder-Keller et 21.513 Marti, toutes intitulées « Pénaliser les appels à la haine et à la violence en raison du sexe » et déposées en décembre 2021. La CAJ-N y a donné suite le 23 juin 2022.

corporelle (art. 111 ss CP) et sexuelle (art. 187 ss CP), les dispositions du code civil relatives à la protection de la personnalité (art. 28 ss CC, ch. 3.1) et, en droit administratif, celles relatives à la protection contre la discrimination fondée sur le sexe au sens de la loi du 24 mars 1995 sur l'égalité[136].

L'objet d'étude du présent rapport est étroitement lié aux déclarations qui incitent à la haine envers une personne ou un groupe de personnes ainsi qu'au fait d'abaisser ou de discriminer publiquement d'une façon qui porte atteinte à la dignité humaine, par la parole, l'écriture, l'image, le geste, par des voies de fait ou de toute autre manière (art. 261bis, al. 4, CP). Il ne semble guère possible de mener une campagne de haine sans commettre de délits contre l'honneur[137]. Une fois de plus, ce sont d'abord l'*injure* (art. 177 CP), la *diffamation* (art. 173 CP) et la *calomnie* (art. 174 CP) qui s'appliquent (ch. 3.2.1.1 et 3.2.1.3). La doctrine considère que ces infractions suffisent à réagir adéquatement à ce nouveau phénomène[138]. Quant à savoir ce qui « porte atteinte à l'honneur » dans le sens pénal du terme, le Tribunal fédéral est en mesure d'adapter sa jurisprudence aux enjeux actuels[139]. Celle-ci estime déjà qu'il suffit qu'une personne soit accusée d'un manque de sens du devoir, de responsabilité et de fiabilité ou de toute autre qualité susceptible de la rendre méprisable en tant qu'être humain ou de donner une image défavorable de son caractère[140]. La disposition pertinente sera ici en priorité l'art. 174, ch. 2, CP, l'*atteinte délibérée à la réputation*, qui est une qualification de la calomnie[141]. Le succès de l'entreprise est sans importance : le seul risque de ruiner la réputation suffit.

Exceptionnellement, les articles du code pénal sur l'*extorsion et chantage* (art. 156), les *menaces* (art. 180 CPla *contrainte* (art. 181), la *représentation de la violence* (art. 135), la *provocation publique au crime ou à la violence* (art. 259), la *violence ou menace contre les autorités et les fonctionnaires* (art. 285) ou les *organisations criminelles et terroristes* (art. 260ter) peuvent s'appliquer.

Un grand nombre de propos qualifiés de haineux n'atteignent toutefois pas le seuil de la punissabilité. Conformément à la *recommandation du Comité des Ministres du Conseil de l'Europe du 20 mai 2022 sur la lutte contre le discours de haine*[142], seules les formes graves de discours de haines devraient être sanctionnées par le droit pénal. Il conviendrait de combattre les actes de moindre gravité par des instruments relevant du droit civil ou administratif. Le Conseil de l'Europe et la jurisprudence de la Cour européenne des droits de l'homme ne définissent pas précisément ce qui constitue un discours de haine grave. Plusieurs facteurs à prendre en compte dans l'évaluation de la gravité sont toutefois cités : le contenu du discours, le climat politique et social, l'intention, la position et le statut social de l'orateur, la méthode de diffusion du discours, la probabilité de préjudice, la nature et l'ampleur du public ainsi que les caractéristiques du groupe visé[143].

3.2.3 Pornodivulgation

Dans son acception majoritaire, le terme pornodivulgation décrit le fait de diffuser des photos ou des vidéos intimes faites sans l'accord de la personne représentée, ou certes avec son

---

136 RS **151.1**

137 SELMAN/SIMMLER, 257 ; SALMINA, 217

138 SELMAN/SIMMLER, 228 et SALMINA, 218, qui suggère toutefois une augmentation de la peine.

139 SALMINA, 218

140 ATF **105** IV 112, 113

141 SALMINA, 219, déplore que cette qualification n'existe pas également pour la diffamation.

142 Recommandation CM/Rec(2022)16 du 20 mai 2022 du Comité des Ministres aux États membres sur la lutte contre le discours de haine, www.coe.int > Droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres.

143 Recommandation CM/Rec(2022)16 du 20 mai 2022 du Comité des Ministres aux États membres sur la lutte contre le discours de haine, www.coe.int > Droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres, ch. 4.1 ; exposé des motifs CM(2022)43, N 32 s. avec renvois aux arrêts de la CourEDH.

accord, mais destinées à un cercle de personnes bien précis, ce dans l'objectif de l'humilier, de l'insulter ou de la diffamer.

S'il s'agit de *photos ou de vidéos pornographiques*, elles sont punies par l'infraction de pornographie (art. 197 CP). Les particularités de cette infraction sont présentées plus haut (ch. 3.2.1.2). La diffusion est punissable lorsqu'il s'agit de « pornographie dure » (art. 197, al. 1, CP) ou de toute pornographie, y compris « douce » mise à la disposition d'un mineur de moins de 16 ans (art. 197, al. 4, CP). C'est le cas d'une part lorsque la personne concernée appartient dans cette tranche d'âge, et d'autre part de manière générale lors d'une publication sur Internet, car l'auteur peut s'attendre à ce que le contenu soit également consulté par des mineurs de moins de 16 ans. Enfin, proposer ou transmettre de la « pornographie douce » à des adultes sans y avoir été invité est puni de l'amende (art. 197, al. 2, CP).

Il est délicat de déterminer à partir de quel moment une autre image (non pornographique) doit être considérée comme *embarrassante*. Si elle est calomnieuse ou de nature trompeuse, propre à dénigrer ou à humilier la victime, les *délits contre l'honneur* peuvent être réalisés (notamment la diffamation, art. 173 CP ; ch. 3.2.1.2). Cependant, si l'image est uniquement indécente, sa diffusion ne constitue pas un délit contre l'honneur. Une photo issue de la sphère intime de la personne représentée ne porte pas en soi atteinte à son honneur[144]. Dans le contexte du cyberharcèlement, les circonstances accompagnant la diffusion peuvent cependant causer un dénigrement suffisant à constituer l'infraction.

La menace de la publication d'images constituant un dommage sérieux pour la victime et l'alarmant ou l'effrayant est punie par l'art. 180 CP. L'enregistrement de ces images à l'insu de la victime ou sans son consentement tombe en sus sous le coup de la *violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues* (art. 179^{quater} CP). Cette disposition sanctionne quiconque, sans le consentement de la personne intéressée, observe avec un appareil de prise de vues ou fixe sur un porteur d'images un fait qui relève du domaine secret de cette personne ou un fait ne pouvant être perçu sans autre par chacun et qui relève du domaine privé de celle-ci (al. 1) ainsi que quiconque conserve une prise de vues ou la rend accessible à un tiers, alors qu'il savait ou devait présumer qu'elle avait été obtenue de cette manière (al. 3). Ces actes sont punis sur plainte d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Comme indiqué plus haut, le Conseil des États propose un nouvel *art. 197a CP* afin d'ériger en infraction le phénomène de pornodivulgation (ch. 1.2.3) :

> **Transmission indue d'un contenu non public à caractère sexuel**
>
> [1] Quiconque transmet à un tiers un contenu non public à caractère sexuel, notamment des écrits, enregistrements sonores ou visuels, images, objets ou représentations, sans le consentement de la personne qui y est identifiable, est, sur plainte, puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.
>
> [2] L'auteur est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire s'il a rendu le contenu public.

Le Conseil fédéral considère que la *formulation* proposée pour cette infraction est *problématique*. Une disposition au contenu aussi opaque placerait les tribunaux face à de *sérieux problèmes d'application*. Lorsqu'il en est ainsi, la conséquence est en règle générale que la disposition est rarement appliquée et que la poursuite pénale que le Parlement appelle de ses vœux ne peut pas être mise en œuvre. La formulation « contenu à caractère sexuel » notamment manque de clarté. Les photos de personnes nues pourraient n'y correspondre que si la pose ou le cadrage a quelque chose de sexuel. La situation pourrait également être

[144] RSJ 2004, 95 s.

ambiguë lorsque la photo montre par exemple un décolleté plongeant mettant la poitrine en évidence ou encore une personne non identifiable (parce qu'on ne voit que certaines parties de son corps ou qu'elles ont été retouchées) mais que son nom est mentionné. Enfin, la formulation « non public » est équivoque.

Une disposition qui se limiterait à des *contenus d'ordre sexuel* ne permettrait d'appréhender qu'une partie du problème. Les images embarrassantes, truquées ou indécentes ne pourraient tomber sous le coup de l'infraction que si leur contenu est d'ordre sexuel. L'infraction devrait être formulée différemment pour permettre de sanctionner le phénomène.

Elle ne devrait pas non plus figurer parmi les infractions contre l'intégrité sexuelle. L'essence du problème est que le domaine secret ou privé de la victime est violé par la diffusion d'une image qu'elle n'entendait pas montrer à des tiers, qu'elle endure une humiliation qui porte atteinte à son honneur ou qu'elle subit menaces, contrainte ou extorsion sous la menace de la diffusion. Dans le cas de contenu à caractère sexuel, la pudeur de la personne concernée est également blessée, mais le noyau de la question n'est pas la violation de l'intégrité sexuelle ni le harcèlement sexuel[145].

3.2.4 Sextorsion

Le droit en vigueur sanctionne la sextorsion : les infractions de contrainte (art. 181 CP) et d'extorsion et chantage (art. 156 CP), sinon de menaces (art. 180 CP) lui sont applicables. Il y a *contrainte* lorsque l'auteur menace de publier une image compromettante sur Internet si la victime n'en envoie pas d'autres, par ex. Il y a *extorsion et chantage* lorsque l'auteur menace de publier l'image s'il ne reçoit pas une certaine somme en échange. Enfin, si les *menaces* portent uniquement sur la publication et alarment ou effrayent la victime, ce qui constitue la menace d'un dommage sérieux, elles sont punies au titre de l'art. 180 CP.

3.2.5 Actes non pris en compte

Le *cyberharcèlement* n'est notamment pas couvert par le droit pénal en vigueur lorsque les actes ne causent qu'une faible injustice s'ils sont considérés isolément et n'atteignent donc pas le seuil requis pour constituer une infraction, mais que le comportement vu dans sa globalité est insultant, intimidant ou dénigrant pour la personne visée et paraît pénalement répréhensible. La jurisprudence du Tribunal fédéral, en particulier sur la contrainte et l'utilisation abusive d'une installation de télécommunication, admettrait toutefois une évaluation du comportement dans son ensemble (ch. 3.2.1). À notre connaissance, le Tribunal fédéral n'a toutefois pas encore examiné l'application de cette jurisprudence à des cas de harcèlement.

La législation actuelle ne permet pas non plus de sanctionner la *diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes si leur contenu n'est pas pornographique* et que les circonstances *ne permettent pas de déduire une atteinte à l'honneur*.

3.3 Législations étrangères

3.3.1 Autriche

Le code pénal autrichien (A-CP) prévoit une infraction spécifique pour le *cyberharcèlement*, qui est entrée en vigueur le 1er janvier 2016.

[145] Sur l'ensemble, voir FF **2022** 1011, 4 s.

Compléter le code pénal par des dispositions relatives au cyberharcèlement

> **Art. 107c A-CP**
> **Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems**
>
> (1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen,
>
> 1. eine strafbare Handlung gegen die Ehre einer Person für eine größere Zahl von Menschen für eine längere Zeit wahrnehmbar begeht oder
> 2. eine Tatsache oder Bildaufnahme des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen für eine längere Zeit wahrnehmbar macht,
>
> ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.
>
> (2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zur Folge, begeht der Täter innerhalb eines ein Jahr übersteigenden Zeitraums fortgesetzt gegen die verletzte Person gerichtete Tathandlungen im Sinne des Abs. 1 oder übersteigt die Dauer der Wahrnehmbarkeit nach Abs. 1 ein Jahr, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Cette infraction est constituée soit par *une atteinte répréhensible à l'honneur d'une personne*, soit par *la publication d'un fait ou d'une image relevant de la sphère intime d'une personne sans son accord*. Ce second élément relève de la *pornodivulgation* dans son acception la plus large, tout en la limitant à la cyberinfraction, c'est-à-dire que l'acte doit avoir été commis en utilisant *un moyen de télécommunication ou un ordinateur*. L'infraction prévoit également que la publication sans consentement doit avoir été visible par *un grand nombre de personnes* (à savoir au moins 10 personnes[146]) durant *une longue période*. L'acte doit avoir été commis de manière *continue*, ce qui signifie que seuls des actes réitérés réalisent l'infraction, contrairement à une occurrence unique. Un des éléments primordiaux de l'infraction, qui en fait une *infraction de mise en danger abstraite*, est que l'acte *doit être de nature à rendre intolérable la vie quotidienne de la victime*. Cette délimitation nécessaire signifie que le comportement mis en cause doit être insupportable au point qu'une personne lambda placée dans la même situation aurait pu être amenée à changer sa façon de vivre. On pensera par ex. à un changement d'école, à la rupture de liens amicaux ou à l'abandon des médias sociaux[147]. L'al. 2 relève la peine, en particulier si le cyberharcèlement a poussé la victime au *suicide* ou à une *tentative de suicide*. La sanction est également aggravée si les actes se sont étalés sur plus d'une année ou si la divulgation est restée visible plus d'un an.

De même, la pornodivulgation n'est punissable qu'au titre d'acte isolé dans le contexte du cyberharcèlement. Les comportements relevant de l'intimidation ou de l'humiliation sont en outre sanctionnés selon les mêmes critères que les délits contre l'honneur qui existaient déjà auparavant, soit en Autriche *Beschimpfen*, *Schmähen*, *Verspotten* ou *Herabwürdigen*[148] (insultes, ridiculisation, moquerie, dénigrement). On peut supposer que la différence avec le droit suisse ne porte guère sur le seuil de punissabilité, mais uniquement sur des *aspects symboliques*.

[146] WENK, 93, et les références citées

[147] *Ibid*.

[148] WENK, 93 f., et les références citées

Quant à l'application de cette infraction, les statistiques de la criminalité[149] montrent qu'un grand nombre de plaintes sont déposées au titre de l'art. 107c A-CP, mais qu'elles n'aboutissent qu'à un très faible nombre de condamnations. Ainsi, 359 plaintes ont été déposées en *2017* pour seulement 16 condamnations, une tendance qui n'a guère évolué en *2019* avec 330 plaintes et 11 condamnations. Au regard de ces chiffres, on ne saurait donc parler d'une grande importance dans la jurisprudence, mais puisque cette norme est récente, la situation peut encore évoluer[150].

Le code pénal autrichien sanctionne également le discours de haine, désigné par le terme *Verhetzung* (incitation à la haine). L'art. 283 A-CP protège les groupes ou les membres de groupes qui se distinguent par leur couleur de peau, leur langue, leur religion ou leurs convictions, leur nationalité, leur ascendance ou leur origine nationale ou ethnique, leur sexe, leur handicap, leur âge ou leur orientation sexuelle. Les actes visés sont la provocation ou l'incitation à la haine envers un groupe particulier ou l'appartenance à ce groupe, l'injure envers une personne ou un groupe et l'approbation, la négation, la banalisation grossière ou la justification de certains crimes. Dans le cas de l'injure, l'auteur doit avoir agi dans l'intention de porter atteinte à la dignité humaine du groupe ou de la personne et que l'injure soit de nature à jeter le discrédit sur le groupe ou la personne dans l'opinion publique. Étant donné qu'il s'agit d'une infraction propre, qui ne concerne que certaines personnes ou groupes, et que l'injure doit remplir des conditions supplémentaires, le simple dénigrement n'est pas sanctionné, dès lors qu'il ne porte pas atteinte à l'honneur ni ne s'apparente à une autre infraction.

3.3.2 Allemagne

Le code pénal allemand (D-CP) ne prévoit *aucune infraction spécifique pour le harcèlement ou le cyberharcèlement*. Chaque acte constituant un tel comportement est puni au titre des dispositions idoines.

La *Netzwerkdurchsetzungsgesetz* (NDG), entrée en vigueur le 1er octobre 2017, oblige les exploitants de réseaux sociaux à but lucratif à supprimer d'eux-mêmes les « contenus visiblement illégaux » dans les 24 heures suivant leur signalement. La NDG ne crée aucune obligation de suppression qui ne découle pas déjà du droit civil ou du droit pénal. Une révision de cette loi qui a récemment abouti vise à améliorer la lutte contre l'extrémisme de droite et les infractions de haine, tout en renforçant les droits des utilisateurs de réseaux sociaux.

Dans le contexte du cyberharcèlement, on citera en priorité l'infraction de *Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen* (violation de la sphère intime par des prises de vues ; § 201a D-CP). En Allemagne, la violation de la personnalité par des images relève du droit pénal, tandis que c'est le droit civil qui est déterminant en Suisse (ch. 3.1). § 201a D-CP sanctionne notamment la *pornodivulgation*, définie comme la publication sciemment non autorisée d'images initialement enregistrées avec autorisation (§ 201a, al. 1, ch. 5, D-CP). Cette disposition vise en particulier les prises de vues réalisées ou envoyées consensuellement dans le cadre d'une relation puis publiées par vengeance au terme de celle-ci[151]. Elle punit également le fait de rendre accessible à un tiers une image d'une autre personne propre à nuire gravement à sa réputation (§ 201a, al. 2, D-CP). Cette variante de l'infraction a été introduite expressément pour lutter contre le cyberharcèlement [152]. L'Allemagne punit également l'incitation à la haine publique (*Volksverhetzung*, § 130 D-CP). Il s'agit là aussi d'une infraction propre : elle protège les personnes appartenant à un groupe

[149] www.statistik.gv.at > Statistiken > Bevölkerung und Soziales > Kriminalität und Sicherheit > Verurteilungs- und Wiederverurteilungsstatistik, Publikationen > Gerichtliche Kriminalstatistik 2017 und 2018, 82 et Gerichtliche Kriminalstatistik 2019 und 2020, 86 ; Polizeiliche Kriminalstatistik 2017, www.bundeskriminalamt.at > Grafiken & Statistiken > Broschüre Sicherheit 2017, 17 ; WENK, 94

[150] WENK, 94

[151] WENK, 97 et les références citées

[152] WENK, 97 s. et les références citées

défini par la nationalité, la race, la religion ou l'origine ethnique, de même que des parties de la population ou un individu appartenant à un groupe donné ou à une partie de la population. Elle punit l'incitation à la haine, à la violence ou à des mesures arbitraires (al. 1, ch. 1), de même que le le fait de porter atteinte à la dignité humaine en insultant, en méprisant ou en calomniant un groupe ou un individu en raison de son appartenance audit groupe. L'infraction est également liée aux délits existants contre l'honneur du D-CP.

3.3.3 France

Le code pénal français (F-CP) prévoit des infractions qui sanctionnent expressément le harcèlement. Il punit notamment 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 (art. 222-33-2-2 F-CP). L'infraction est également constituée lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée, ou encore lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent qu'ils caractérisent une répétition. Le *cyberharcèlement* constitue une qualification de l'infraction.

La *pornodivulgation* est sanctionnée par l'art. 226-2-1 F-CP. L'infraction se fonde sur les atteintes à la vie privée (art. 226-1 et 226-2 F-CP) et les peines sont accrues lorsque les délits portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé. L'art. 226-2-1, al. 2, F-CP punit en outre le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu avec le consentement exprès ou présumé de la personne ou par elle-même.

L'art. R625-7 F-CP punit le *discours de haine*, compris comme la provocation non publique à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une prétendue race ou une religion déterminée (al. 1) ou à raison de leur sexe, de leur orientation sexuelle ou identité de genre, ou de leur handicap (al. 2). Le dénigrement ou l'humiliation purs ne sont donc pas sanctionnés.

3.3.4 Italie

Le droit pénal italien n'aborde pas expressément le cyberharcèlement. Il existe toutefois une disposition de droit civil qui définit ce terme. Elle garantit le droit à la suppression des contenus relevant du cyberharcèlement et prévoit un recours en cas de violation du droit à la suppression.

La diffusion d'idéologies dénigrantes, l'incitation à la discrimination et à la violence sont sanctionnées par l'art. 3, let. a et b, de la loi spéciale sur la convention contre le racisme. L'attaque doit donc porter sur la race, l'ethnie, la nationalité ou la religion. Ici aussi, la loi ne punit le discours de haine dénigrant ou humiliant que s'il constitue un délit contre l'honneur.

3.4 Avis doctrinaires

En Suisse, BRUN et WENK se sont notamment prononcés sur la question de la nécessité de créer une *infraction de cyberharcèlement* spécifique dans le CP. Les deux auteurs s'accordent à dire qu'elle n'est *pas indispensable* ni objectivement justifiée[153], les formes typiques de cyberharcèlement pouvant *en principe être adéquatement sanctionnées par les normes*

[153] BRUN, 111 ; WENK, 99 s. ; sur le droit allemand, voir PREUSS, 104.

existantes[154]. Le fait de ne punir que le cyberharcèlement, et non des cas de *harcèlement classique* de même gravité, est en outre considéré comme problématique[155], tout comme le *concours d'infractions* que créerait une telle norme[156].

WENK perçoit cependant un certain *besoin de réforme*. Étant donné que les actes relevant du cyberharcèlement sont pour l'essentiel déjà sanctionnés, il propose des modifications ponctuelles des infractions. Il estime ainsi que les délits contre l'honneur pourraient être complétés par un alinéa augmentant la peine si l'acte a été commis par l'intermédiaire des TIC et visible par un grand nombre de personnes[157]. Il voit également une lacune dans la pénalisation de la publication (malveillante) d'images intimes, embarrassantes ou dégradantes[158].

Tous les auteurs relèvent en outre l'importance de la *prévention* dans la lutte contre le cyberharcèlement[159].

3.5 Analyse

3.5.1 Comportements hétéroclites

Les actes énumérés *peuvent concrètement être commis de diverses manières*. C'est notamment le cas du cyberharcèlement, qui est défini comme le résultat de la répétition d'actes uniques, mais aussi des autres atteintes numériques traitées dans le présent rapport.

Les *biens juridiques* affectés sont de natures différentes. Il peut ainsi s'agir d'atteintes à l'honneur, à la liberté, au domaine secret ou privé, au patrimoine ou à l'intégrité sexuelle. Cet éventail de possibilités pose problème, car où intégrer une éventuelle infraction dans la systématique pénale ?

Un autre obstacle à prendre en compte ici est le *concours d'infractions*. La création d'une norme autonome contre le cyberharcèlement signifierait qu'un seul et même acte pourrait constituer à la fois la nouvelle infraction et les anciennes infractions applicables aux comportements en question. L'infraction de cyberharcèlement devrait toutefois être conçue comme une *lex specialis*. Or, une telle infraction devrait couvrir un grand nombre de comportements, des moins répréhensibles jusqu'aux plus graves. Elle devrait donc prévoir une gamme de peines très large. En application des règles du concours d'infractions, il se pourrait qu'une sanction en vertu des infractions existantes (art. 49 CP : peines de même genre et augmentation de la peine) mène parfois à une condamnation plus lourde.

3.5.2 Principe de précision

Le principe de précision de la base légale veut que *les caractéristiques d'un comportement incriminé soient décrites de manière suffisamment précise dans la loi*. En effet, chacun doit pouvoir identifier les comportements répréhensibles afin d'agir en conséquence. Il s'agit d'une manifestation du principe de la légalité inscrit à l'art. 1 CP, ce qui révèle d'ailleurs son importance.

Une infraction pour laquelle une *formulation générale et abstraite* devrait être trouvée pour des *actes extrêmement disparates* (comme ce serait le cas pour le cyberharcèlement, mais aussi pour la délimitation du discours de haine ou de la pornodivulgation) ne saurait satisfaire à cette exigence. La *limite entre les actes ou ensemble d'actes irrépréhensibles et ceux qui sont*

[154] BRUN, 111, qui n'exclut toutefois pas que les évolutions futures changent la donne.

[155] PREUSS, 104

[156] WENK, 99

[157] WENK, 95

[158] WENK, 99

[159] BRUN, 111 ; WENK, 100 ; PREUSS, 104

punissables reposerait sur des termes juridiques imprécis qui laisseraient aux autorités chargées de l'application de la norme une marge de manœuvre excessivement délicate. Cette marge serait surtout *très complexe à gérer en pratique*.

3.5.3 Effet de prévention générale

On espère d'une infraction cyberharcèlement, à la portée symbolique, qu'elle produise un effet de prévention générale. La prévention générale consiste à dissuader les personnes enclines à commettre l'infraction en les rendant conscientes de l'interdiction et de la sanction (prévention générale négative) ou à éviter l'apparition d'un tel penchant (prévention générale positive)[160].

En ce qui concerne la prévention générale négative, le fait que l'acte soit puni par une disposition spécifique ou par plusieurs n'est pas significatif pour l'auteur potentiel. La doctrine considère en outre comme acquis que la sévérité de la peine encourue n'est pas davantage déterminante. En d'autres termes, l'effet d'une norme ne semble pas dépendre de la nature ni de la sévérité de la peine. Ce qui compte est plutôt le fait que la transgression soit sanctionnée par le droit pénal[161].

Cette conclusion signifie également qu'à l'inverse, une infraction à la formulation nécessairement imprécise (ch. 3.5.2) et par là même difficile à prouver (ch. 3.5.4), qui n'aboutit que rarement à des condamnations, pourrait s'avérer contre-productive : l'absence de condamnations malgré l'existence d'une infraction (spécifique) peut pratiquement être perçue comme une invitation par les personnes enclines à passer à l'acte. Cette perspective devrait constituer une mise en garde contre l'ajout dans le CP d'infractions spécifiques à la portée essentiellement symbolique.

3.5.4 Difficultés d'administration des preuves

La création d'une infraction spécifique *ne faciliterait guère l'administration des preuves*. Cette norme *nécessiterait des actes répétés qui produisent un certain effet*. Ce résultat devrait être attesté concrètement, comme lorsqu'il s'agit de prouver que les éléments constitutifs des infractions en vigueur, toujours applicables, sont réunis. La documentation des faits serait certes plus aisée dans le cas du cyberharcèlement, captures d'écrans et historiques de conversation à l'appui, que dans le cas du harcèlement traditionnel.

N'oublions pas non plus que les *éléments constitutifs de l'infraction qui laissent une grande marge d'interprétation* – et sont donc délicats, eu égard au principe de précision (ch. 3.5.2) – sont souvent difficiles à prouver. En Autriche, c'est par ex. le cas lorsqu'il s'agit de prouver que le cyberharcèlement était de nature à rendre intolérable la vie quotidienne de la victime. Il se pourrait qu'on puisse prouver que les éléments constitutifs des infractions existantes sont réunis, sans pour autant que ce soit le cas pour la nouvelle infraction.

3.5.5 Neutralité technologique du droit pénal

Le principe de neutralité technologique des infractions du CP offre *plusieurs avantages*. La description générale et abstraite des conditions de la punissabilité permet aux infractions de couvrir les évolutions (en particulier technologiques) encore inconnues au moment de la rédaction de la disposition. Dans la mesure du possible, les infractions sont donc formulées de manière à être réalisées par des actes du monde réel comme du monde virtuel.

Par ex., le Parlement a appliqué ce principe à *l'usurpation d'identité* (art. 179^{decies} CP, en vigueur au 1er septembre 2023). Dans son message, le Conseil fédéral observe que le phénomène de l'usurpation d'identité s'est aggravé avec la démocratisation de la communication électronique, et que la disposition doit être applicable, quels que soient les

[160] WENK, 99

[161] STRATENWERTH, AT I, § 2 N 21

moyens employés pour commettre l'acte. Celle-ci couvre donc l'usurpation d'identité traditionnelle : il n'y a pas lieu d'incriminer uniquement l'usurpation d'identité commise au moyen d'un ordinateur ou d'un téléphone[162].

La question se pose également dans le cas du harcèlement : faut-il réellement créer une disposition réservée aux actes commis à l'aide des TIC ? Il ne fait aucun doute que le cyberharcèlement a des conséquences particulièrement graves pour la personne concernée. Il semble néanmoins problématique de créer une infraction spéciale pour le cyberharcèlement, mais pas pour les cas de harcèlement classique d'une gravité comparable[163] : cela serait incohérent et difficilement justifiable objectivement.

En outre, il ne faut pas oublier qu'il existe des *formes hybrides* : dans un même cas de harcèlement, certains actes peuvent être commis dans le monde virtuel et d'autres dans le monde réel (ch. 2.1). Si une infraction spécifique est créée pour le cyberharcèlement, le traitement de ces cas sera complexe.

Au vu de ce qui précède, la possibilité de renoncer à l'infraction spécifique au profit d'une *qualification* des infractions existantes (comme les délits contre l'honneur, art. 173 ss CP), lorsque l'acte a été commis à l'aide des TIC et visible par un grand nombre de personnes (ch. 3.4) peine également à convaincre[164]. Une telle modification pourrait donner à penser que ces circonstances ne sont à prendre en compte que pour certaines infractions.

Les *règles de fixation de la peine* permettent déjà de tenir compte de la gravité supérieure d'un acte commis via les TIC. Par ailleurs, une modification de cet ordre pourrait mener à des velléités immodérées de révision en ajoutant un alinéa *déclaratoire* de même portée à d'autres infractions.

3.5.6 Définition fondée sur la perspective de la victime

La définition du harcèlement et du cyberharcèlement repose largement sur le ressenti de la personne concernée. Elle présuppose que *la victime se sent insultée, chicanée, persécutée ou rabaissée* (ch. 2.1.3).

Cette définition présente un *obstacle de taille pour la formulation de l'infraction*. Accorder une protection pénale au ressenti n'est résolument pas souhaitable. La description du comportement incriminé doit donc se fonder sur le point de vue d'une personne de sensibilité moyenne placée dans la même situation. Une infraction spécifique pour le cyberharcèlement devrait être conçue soit comme une *infraction de résultat* et nécessiter que les conditions de vie d'une personne raisonnable aient changé, soit comme une *infraction de mise en danger abstraite* (selon l'exemple autrichien), pour laquelle il suffit que l'acte soit *de nature* à changer les conditions de vie d'une personne raisonnable. C'est ici la seule manière de définir objectivement l'acte incriminé et de fixer assez haut le seuil de *punissabilité*.

Cela ne résout toutefois pas le problème de la preuve de la modification des conditions de vie ni celui de l'application de la disposition dans la pratique.

3.5.7 Actes multiples

Le cyberharcèlement est le résultat d'un cumul d'actes. Cet état de fait est pris en compte dans le droit en vigueur par les règles du concours d'infractions, notamment lors de la fixation de la peine[165]. Une disposition spécifique de harcèlement ou de cyberharcèlement pourrait toutefois apporter un changement dans la mesure où elle *sanctionnerait également les cas de*

[162] PREUSS, 104

[163] FF **2017** 6565, 6741 s.

[164] WENK, 95

[165] PREUSS, 104

harcèlement dont les conséquences sont graves pour la personne concernée, même si les actes individuels n'atteignent pas à eux seuls le seuil de punissabilité des différentes infractions.

Le tribunal fédéral a admis à plusieurs reprises que le comportement global de l'auteur doit être pris en compte pour déterminer si l'infraction est réalisée (par ex. dans le cas de la contrainte issue du harcèlement obsessionnel (art. 181 CP) ou de l'utilisation abusive d'une installation de télécommunication (art. 179^{septies} CP ; ch. 3.2.1). La création d'une infraction spécifique ne ferait que transposer cette pratique dans la loi.

3.5.8 Auteurs multiples

Dans le cas du (cyber)harcèlement, les actes ne sont pas les seuls à s'additionner. Il s'agit souvent aussi d'une *interaction dynamique entre plusieurs personnes*. Ainsi, *l'ancienne définition* du harcèlement présupposait l'action de plusieurs personnes contre la même victime (ch. 2.1).

Cette particularité peut être prise en compte à la fois par l'application de plusieurs dispositions et par le recours à une disposition spécifique au cyberharcèlement. En particulier, plusieurs auteurs peuvent agir en tant que *coauteurs*. Ce terme désigne une personne qui collabore intentionnellement et de manière déterminante avec d'autres personnes dans la décision de commettre une infraction, dans son organisation ou son exécution, au point d'apparaître comme l'un des participants principaux, ce qui revient à déterminer si la contribution de cette personne est capitale au point que l'infraction repose sur cette personne, en tenant compte des circonstances concrètes et du plan d'action[166]. Si deux personnes entreprennent ensemble d'intimider, d'importuner ou d'humilier une personne donnée (par le biais des TIC) ou si elles commettent chacune un tel acte en gardant la maîtrise de fait, elles sont toutes deux punissables pour les actes commis.

L'*instigateur* décide intentionnellement autrui à commettre l'infraction. En d'autres mots, il suscite la décision de commettre l'acte. Ce serait par exemple le cas si quelqu'un créait un groupe de haine et persuadait d'autres personnes d'y participer, celles-ci tenant par ex. également des propos portant atteinte à l'honneur. L'instigateur est puni de la même peine que l'auteur (art. 24, al. 1, CP).

Le *complice* prête intentionnellement assistance à l'auteur pour commettre l'infraction. Dans le cas du cyberharcèlement, c'est surtout la complicité psychologique qui est pertinente, par ex. le fait de faire partie du groupe de haine sans y participer activement. La loi prévoit une *peine atténuée* pour la complicité (art. 25 CP).

3.6 Mesures législatives possibles

3.6.1 Infraction spécifique pour le harcèlement

Le législateur peut agir de plusieurs manières. Eu égard au *principe de neutralité technologique*, une infraction propre à la variante virtuelle du harcèlement ne semble ni indiquée, ni justifiable objectivement. Si une infraction spécifique est créée, elle devrait être rédigée de manière technologiquement neutre et couvrir le harcèlement en ligne comme dans le monde réel. On pourrait alors éventuellement réfléchir à ajouter une *qualification*, donc prévoir une peine plus lourde, si l'auteur a agi en utilisant les TIC et a rendu l'intimidation ou l'humiliation visible pour un grand nombre de personnes. Il appartiendrait à la jurisprudence de choisir comment aborder les cas hybrides (en ligne et hors ligne).

Une telle disposition permettrait notamment de sanctionner le harcèlement lorsque les *actes individuels* ne causent qu'une faible injustice s'ils sont considérés isolément et n'atteignent

[166] ATF 135 IV 152, 155 consid. 2.3.1 ; 133 IV 76, 82 consid. 2.7 ; 130 IV 58, 66 consid. 9.2.1 ; 126 IV 84, 88 consid. 2c/aa ; 125 IV 134, consid. 3a ; 120 IV 265, 271 s. consid. 2c/aa

donc pas le seuil requis pour constituer une infraction, mais que le comportement vu dans sa globalité est insultant, intimidant ou dénigrant pour la personne visée et paraît pénalement répréhensible.

La place de cette infraction dans la *systématique légale* serait également problématique. Elle pourrait à la rigueur être classée parmi les crimes ou délits contre la liberté (intimidation) ou contre l'honneur (humiliation). Définir avec assez de précision ses éléments constitutifs serait également une gageure. Elle devrait être conçue soit comme une infraction de résultat, soit (à l'instar de l'Autriche) comme une infraction de mise en danger abstraite pour laquelle il suffit que l'acte soit de nature à changer les conditions de vie d'une personne raisonnable dans la même situation.

3.6.2 Renoncer à une infraction spécifique

Divers arguments plaident en faveur de la renonciation à une disposition spécifique pour le harcèlement ou le cyberharcèlement, par ex., le principe qui veut que le *droit pénal, le glaive le plus tranchant de l'État*, ne soit employé que là où il est nécessaire. Une législation à la portée *purement symbolique* n'a pas sa place.

Les dispositions déjà en vigueur permettent de sanctionner le harcèlement pratiquement dans la même mesure qu'une disposition spécifique. L'application par analogie de la jurisprudence du Tribunal fédéral sur la contrainte (art. 181 CP)[167] et sur l'utilisation abusive d'une installation de télécommunication (art. 179^{septies} CP)[168] pourrait même permettre de tenir compte de l'ensemble des actes et de sanctionner en conséquence des cas de harcèlement, c'est-à-dire des comportements ressentis par la victime comme intimidants, intrusifs ou humiliants, qui n'atteindraient pas sinon le seuil de punissabilité des infractions existantes.

3.6.3 Pénalisation de la diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes

Les dispositions actuelles ne sanctionnent pas toujours la diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes, notamment si *leur contenu n'est pas pornographique* (art. 197 CP), que les circonstances ne permettent *pas de déduire une atteinte à l'honneur* (art. 173 ss CP) et qu'elles ne fixent pas sur un support d'images, sans le consentement de la personne concernée, des faits qui relèvent du domaine secret de celle-ci ou des faits ne pouvant être perçus sans autre par chacun et qui relèvent de son domaine privé (art. 179^{quater}, al. 3, CP).

Ce type de comportement, s'il est considéré comme pénalement répréhensible et que les dispositions du droit civil sur la protection de la personnalité ne suffisent pas à l'appréhender, peut être puni soit en tant qu'infraction distincte (sur la base d'une disposition spécifique formulée de manière technologiquement neutre), soit en tant que variante du harcèlement. Dans le cadre de la révision du droit pénal en matière sexuelle, le Conseil des États propose cette seconde solution avec une nouvelle disposition punissant la *transmission indue d'un contenu non public à caractère sexuel* (art. 197*a* P-CP ; ch. 3.2.3). Contrairement à cette proposition, une éventuelle nouvelle disposition *ne saurait toutefois être limitée aux contenus à caractère sexuel*, mais devrait également couvrir les *autres types d'images compromettantes*. Par conséquent, elle ne devrait pas non plus être classée parmi les infractions contre l'intégrité sexuelle, mais parmi les délits contre l'honneur et contre le domaine secret ou le domaine privé (livre 2, titre 3, CP).

[167] ATF 129 IV 262, 265 ss ; 141 IV 437, 441

[168] Arrêt du TF 6B_75/2009 du 2 juin 2009, consid. 3.2.1 ; ATF 126 IV 219

3.7 Synthèse

Le droit en vigueur ne *punit pas le cyberharcèlement lorsque les actes ne causent qu'une faible injustice s'ils sont considérés isolément et n'atteignent donc pas le seuil requis pour constituer une infraction, mais que le comportement vu dans sa globalité est insultant, intimidant ou dénigrant pour la personne visée*. La jurisprudence du Tribunal fédéral permettrait d'évaluer le comportement dans son ensemble, en particulier pour la contrainte et l'utilisation abusive d'une installation de télécommunication (ch. 3.2.1). À notre connaissance, elle n'a toutefois jamais été appliquée au cyberharcèlement.

Parmi les pays voisins, seule *l'Autriche* a créé une *infraction spécifique pour le cyberharcèlement*. Eu égard au *principe de neutralité technologique du droit pénal*, une telle disposition ne serait ni indiquée, ni justifiable objectivement en Suisse. La doctrine se montre elle aussi critique à l'égard de cette solution, certains auteurs suggérant des modifications ponctuelles.

Il serait envisageable de créer une *infraction spécifique pour le harcèlement*. Elle pourrait éventuellement être qualifiée, c'est-à-dire appeler une peine plus importante, si l'auteur a agi en utilisant les TIC et a rendu l'intimidation ou l'humiliation visible pour un grand nombre de personnes.

Une disposition pénale spécifique pour le cyberharcèlement soulèverait toutefois les problèmes suivants :

- Elle devrait s'appliquer aux nombreux comportements différents qui relèvent du harcèlement (actes hétéroclites). Autrement dit, il faudrait trouver une formulation générale et abstraite qui englobe le plus grand nombre possible d'actes. Une telle disposition ne respecterait guère le *principe de précision de la base légale*. La limite entre les actes ou ensembles d'actes irrépréhensibles et ceux qui sont punissables reposerait sur des termes juridiques imprécis qui laisseraient aux autorités chargées de l'application de la norme une marge de manœuvre excessivement délicate. En raison de la très large gamme de peines que devrait prévoir cette disposition et en application des *règles du concours d'infractions*, il se pourrait qu'une sanction en vertu des infractions existantes constituées dans chaque cas d'espèce mène parfois à une condamnation plus lourde. De plus, la *place d'une telle infraction dans la systématique légale* serait incertaine, eu égard à la variété des *biens juridiques* affectés.
- Quant à la *prévention générale négative*, l'important est que la transgression soit sanctionnée par le droit pénal (que ce soit au titre des infractions existantes ou d'une disposition spécifique), tandis que la nature et l'ampleur de la sanction ne semblent guère déterminantes. Le législateur ne saurait donc se laisser guider par des *considérations symboliques*.
- L'*administration des preuves* ne serait guère facilitée. Les actes répétés, prérequis d'une infraction de cyberharcèlement, devraient être prouvés individuellement. Les éléments constitutifs de l'infraction qui laissent une grande marge d'interprétation (et sont donc délicats à appliquer face au principe de précision) sont difficiles à prouver, en particulier lorsqu'il s'agit de l'intention.

Quant aux autres *atteintes numériques à la personnalité*, le seul comportement non punissable concerne la *diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes.* Les dispositions actuelles ne sanctionnent pas toujours la diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes, notamment si *leur contenu n'est pas pornographique* (art. 197 CP), que les circonstances ne permettent *pas de déduire une atteinte à l'honneur* (art. 173 ss CP) et qu'elles ne fixent pas sur un support d'images, sans le consentement de la personne concernée, des faits qui relèvent du domaine secret de celle-ci ou des faits ne pouvant être perçus sans autre par chacun et qui relèvent de son domaine privé (art.

179^{quater}, al. 3, CP). Ce type de comportement peut être déclaré punissable s'il est considéré comme pénalement répréhensible et que les dispositions du droit civil sur la protection de la personnalité ne suffisent pas à l'appréhender. Contrairement à la proposition faite par le Conseil des États dans le cadre de la *révision du droit pénal en matière sexuelle* (transmission indue d'un contenu non public à caractère sexuel, art. 197*a* P-CP), une éventuelle nouvelle disposition ne saurait toutefois être limitée aux contenus à caractère sexuel, mais devrait également couvrir les *autres types d'images compromettantes*. Par conséquent, elle ne devrait pas non plus être classée parmi les infractions contre l'intégrité sexuelle, mais parmi les délits contre l'honneur et contre le domaine secret ou le domaine privé (livre 2, titre 3, CP).

4 Application du droit

4.1 Contexte

4.1.1 Problématique

L'absence de dispositions matérielles n'est que rarement un obstacle à la poursuite pénale d'infractions commises par le biais des TIC. Lorsque leurs *auteurs sont anonymes*, c'est plutôt *l'application du droit* qui pose problème. Les *moyens de preuves* dont les autorités ont besoin pour identifier les auteurs et établir les faits *sont souvent des données stockées à l'étranger*. Leur obtention est donc souvent très délicate techniquement et juridiquement.

La suite du rapport sera consacrée aux possibilités qui s'offrent généralement aux autorités de poursuite pénale pour accéder à des données stockées à l'étranger. Elle examinera également les possibilités pour retirer (« takedown ») et bloquer les données illicites.

4.1.2 Les acteurs du web

Dans son premier rapport sur les médias sociaux, le Conseil fédéral a présenté en détail les acteurs des plateformes de réseaux sociaux[169]. Concernant l'objet du présent rapport, on suppose que les acteurs suivants sont susceptibles de disposer de preuves.

Les exploitants de plateformes : Les exploitants de plateformes mettent à la disposition des utilisateurs un cadre destiné à l'échange de contenus créés ou repris par ces derniers. Ils 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. Ils peuvent y préciser quels contenus ou quels comportements sont interdits. Ils exercent cependant souvent un contrôle rédactionnel plus léger que celui des médias traditionnels. Les contenus non conformes aux conditions d'utilisation peuvent être retirés (« notice and takedown »).

La plupart des plateformes les plus utilisées en Suisse[170] ont leur siège à l'étranger. Les utilisateurs peuvent y apparaître sous leur vrai nom ou sous un pseudonyme. Parmi ces fournisseurs généralement domiciliés aux États-Unis figurent Facebook, Instagram, YouTube, Snapchat, Pinterest, Twitter ou TikTok.

- La plateforme **Facebook** permet de créer des profils privés et des pages d'entreprise pouvant être connectés entre eux et rendus accessibles à un nombre illimité d'abonnés. Facebook est exploité par la société Meta Platforms Inc. (États-Unis ; Facebook Inc. jusqu'en 2021). Aux yeux du Tribunal fédéral, Facebook est un fournisseur de programmes et d'applications étranger[171]. La succursale suisse de Facebook est chargée du développement du marché suisse sous l'angle de la publicité.

[169] Rapport postulat médias sociaux 2013, ch. 2.3

[170] Sur l'utilisation en Suisse, voir par ex www.mcschindler.com > Archiv > Digital 2022 Report zur Entwicklung der globalen Nutzung von Internet, Social Media und Mobile, 15.02.2022, Zahlen und Fakten in Kürze. Concernant l'utilisation des médias par les jeunes, voir par ex. l'étude JAMES de 2020 de la Haute école zurichoise des sciences appliquées : www.zhaw.ch > Forschung > Mediennutzung > JAMES > Ergebnisbericht JAMES-Studie.

[171] ATF 143 IV 270, 277

Contrairement à Meta Platforms Ireland Limited et à Meta Platforms Inc. (États-Unis), elle n'est pas détentrice des données Facebook[172].

- **Instagram** est un service gratuit de partage de photos et de vidéos appartenant à Meta Platforms Inc. (États-Unis).
- Le portail vidéo **YouTube** est une filiale de Google LLC (États-Unis). Il permet de diffuser, de regarder, de partager, d'évaluer et de commenter des vidéos gratuitement. Chaque utilisateur peut créer sa propre chaîne YouTube.
- **Snapchat** est un service de messagerie instantanée gratuit exploité par Snap Inc. (États-Unis).
- La plateforme **Pinterest**, exploitée par Pinterest Inc. (États-Unis) permet à ses utilisateurs de fixer, sur des panneaux d'affichage virtuels, des collections de photos accompagnées de commentaires.
- Twitter est un réseau social de microblogging. Ses utilisateurs y publient des messages courts destinés à un public généralement illimité ou, exceptionnellement, à un cercle de personnes défini par l'expéditeur. La plupart des utilisateurs visent à être suivis par un maximum de personnes (les *followers*)[173]. Le site est exploité par la société étasunienne Twitter Inc.
- **TikTok** est une plateforme permettant à ses utilisateurs de diffuser de courtes vidéos, de les partager et de les évaluer. TikTok est exploitée par l'entreprise chinoise ByteDance.

Les hébergeurs (« hosting providers ») : Bon nombre d'exploitants de plateformes recourent aux services d'hébergeurs, qui mettent à leur disposition *des infrastructures techniques* telles qu'espace de stockage, capacité de calcul ou bande passante. Comme la plupart des exploitants de plateformes, la majorité des grands hébergeurs ont leur siège à l'étranger. Leur responsabilité n'est généralement pas engagée sur les aspects rédactionnels, mais ils sont *techniquement en mesure, bien souvent, de supprimer des contenus de leurs systèmes*. Les services étrangers sont également très bien représentés dans le domaine du *pur stockage de données* (Google Docs, iCloud d'Apple, office.live.com de Microsoft ou Dropbox, etc.).

Les fournisseurs d'accès (« access providers ») : La liaison entre les utilisateurs et les plateformes est assurée par les fournisseurs d'accès. Les utilisateurs helvétiques optent en général pour les services d'un fournisseur établi en Suisse. Les fournisseurs d'accès ne sont généralement *pas en mesure de supprimer des contenus indésirables*, car ceux-ci ne sont pas sauvegardés sur leurs serveurs. Ils peuvent toutefois *bloquer l'accès à certains contenus*[174].

Les fournisseurs de messagerie électronique (« email providers ») : Les nombreux services de messagerie étrangers tels que gmail de Google revêtent eux aussi une grande importance pour la poursuite pénale. La succursale suisse de Google n'a toutefois aucun pouvoir sur les courriels échangés[175].

4.1.3 Gestion des données globalisée sur le nuage

Le terme « informatique en nuage » donne à penser que la communication se déroule dans des nuages virtuels, loin de toute infrastructure. Or, c'est tout le contraire : l'informatique en nuage désigne la mise à disposition, sur Internet, d'infrastructures informatiques telles que

[172] ATF 143 IV 21

[173] Arrêt du TF 5A_195/2016 du 4.7.2016, consid. 5.3

[174] Par ex. en vertu de l'art. 86, al. 1 de la loi fédérale du 29 septembre 2017 sur les jeux d'argent (LJAr ; RS 935.51) ; voir arrêt du TF 2C_336/2021 du 18.05.2022, consid. 7 et 8.

[175] TF 1B_142/2016 du 16.11.2016, consid. 3

de l'espace mémoire, de la capacité de calcul ou des logiciels d'application. L'utilisateur accède à ces ressources informatiques en ligne, sans avoir besoin de les installer sur son ordinateur local. Parmi les services les plus connus, citons Amazon Web Services, l'iCloud d'Apple, Dropbox, Google Docs et Microsoft Office 365.

Les géants du web sont des multinationales qui planifient et construisent leurs infrastructures avant tout en fonction de la rationalité économique. Ils doivent à cet égard exploiter d'importants centres de données. Facebook/Meta, par exemple, exploite actuellement, pour autant qu'on sache, trois centres de données en Europe (en Suède, au Danemark et en Irlande).

Les exploitants de plateformes disposent certes fréquemment de *succursales* dans différents pays, mais leur seule mission consiste à *commercialiser* localement la plateforme en question. Elles n'ont aucune influence sur la conception technique et l'exploitation de la plateforme ni sur le stockage de ses données.

Par conséquent, *même une communication émise en Suisse pour un destinataire suisse passe par des infrastructures étrangères et sera stockée à l'étranger*. Dans ce contexte, l'accès aux données pertinentes pour les poursuites pénales revêt souvent une dimension internationale, même si la communication en soi relie deux terminaux situés en Suisse.

4.2 Accès des autorités de poursuite pénale aux données

4.2.1 Identification de la connexion

Les internautes communiquent souvent sous un *pseudonyme*. Dans toute procédure portant sur un cyberdélit, *l'identification du suspect constitue donc la première étape et la plus décisive*. Il faut en principe pour cela disposer de *l'adresse IP*[176] avec laquelle le suspect s'est connecté à Internet. L'adresse IP fait partie des données qu'un serveur de messagerie ou de plateforme enregistre à chaque connexion. Cette information ne permet bien entendu d'identifier que le propriétaire de la connexion. Des *actes d'enquête supplémentaires* sont nécessaires (mise sous séquestre de matériel informatique, p. ex.) pour déterminer l'auteur véritable des faits.

4.2.2 Le principe de la territorialité appliqué à la collecte de preuves

4.2.2.1 Principe

Le principe de la territorialité veut que toute personne qui se trouve sur le territoire suisse soit soumise aux lois suisses. Les règles du code de procédure pénale (CPP)[177] et de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[178] concernent par conséquent les personnes se trouvant en Suisse. Il en découle que *les autorités suisses ne peuvent en principe recueillir des preuves que si celles-ci se trouvent en Suisse* (art. 1 et 54 CPP en relation avec l'art. 1, al. 1, let. b, de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale [EIMP[179]] et l'art. 3 CP) [180].

4.2.2.2 Données stockées en Suisse

Les autorités de poursuite pénale qui ont besoin de données comme moyens de preuve peuvent *sommer le détenteur d'opérer un dépôt* (art. 265 CPP), *perquisitionner les systèmes informatiques de particuliers* (art. 246 CPP) et *mettre sous séquestre des données ou des*

[176] Adresse de protocole Internet. Concernant la fonction des adresses IP, voir ATF 136 II 508, consid. 3.3.

[177] RS **312.0**

[178] RS **780.1**

[179] RS **351.1**

[180] ATF 141 IV 108

supports de données (art. 263 ss CPP)[181]. Les autorités peuvent aussi exécuter ces mesures directement en cas de perquisition[182]. La mise sous séquestre et la fouille de smartphones revêtent aujourd'hui une importance capitale. Le Tribunal fédéral se montre à cet égard relativement exigeant s'agissant du droit de faire valoir des intérêts liés au maintien du secret (secret professionnel, p. ex.) susceptibles de s'opposer à une levée des scellés[183].

L'*obligation de conserver les données relatives au trafic Internet* n'est pas réglementée d'une façon homogène et dépend largement de l'appartenance ou non des exploitants de serveur au champ d'application de la LSCPT. La surveillance du trafic Internet relève de la surveillance de la correspondance par télécommunication. Elle constitue un cas particulier de la mise sous séquestre et fait l'objet de règles plus strictes, notamment parce que les preuves sont recueillies en secret (Art. 269 ss CPP[184]). Les modalités d'exécution de la surveillance de la correspondance par télécommunication sont réglées dans la LSCPT.

La recherche de preuves au moyen de *GovWare* constitue un cas particulier de la surveillance de la correspondance par télécommunication. Un GovWare est un programme informatique qui permet d'exercer une surveillance directe (à la source) sur la correspondance par télécommunication (art. 269ter CPP[185]). Son utilisation dans une procédure pénale est strictement encadrée. La liste des infractions, en particulier, est nettement plus courte que pour une surveillance de la correspondance par télécommunication ordinaire. Le recours à des GovWare n'est pas autorisé pour élucider la plupart des délits d'expression (en particulier les atteintes à l'honneur, la discrimination raciale et la provocation publique au crime ou à la violence) ni les atteintes au droit d'auteur (art. 269ter en relation avec l'art. 286, al. 2, CPP).

4.2.2.3 Seul le détenteur des données peut être sommé d'opérer un dépôt

En Suisse, quiconque est sommé par les autorités de poursuite pénale de procéder au dépôt de données n'est tenu de collaborer à la procédure que s'il a la *possibilité de maîtriser les données* en question. Conformément à la jurisprudence du Tribunal fédéral, les *succursales suisses* de Google et de Facebook ne sont pas détentrices des données des utilisateurs, car elles sont uniquement chargées de la commercialisation des services et non de leur exploitation[186]. De ce point de vue, les collaborateurs d'entreprises de ce type ne sont donc *pas tenus de collaborer*. Cela contraint les autorités de poursuite pénale de recourir à *l'entraide judiciaire* pour se procurer les données stockées ailleurs qu'en Suisse.

4.2.2.4 Application du principe de l'accès

Selon la jurisprudence du Tribunal fédéral, quiconque accède à un service d'une entreprise étrangère par l'intermédiaire d'une connexion Internet en Suisse n'agit pas « à l'étranger ». Le simple fait que les données du service en ligne soient gérées sur des serveurs situés à l'étranger *ne permet pas de considérer une recherche en ligne légale, menée de Suisse, comme un acte d'instruction illicite en territoire étranger* (selon la pratique du Tribunal fédéral)[187].

---

[181] Voir BOMMER/GOLDSCHMID, BSK StPO II, Art. 263 N 27. Les autorités peuvent provisoirement mettre en sûreté les données s'il y a risque de suppression de moyens de preuve ou d'autres actes de dissimulation (art. 263, al. 3 et 265, al. 4, CPP). Lorsque les preuves sont collectées auprès d'autorités, le Tribunal fédéral considère (arrêt 1B_26/2016 du 29 novembre 2016, consid. 4.1) qu'il faut suivre non pas les art. 263 ss CPP, mais les règles de l'entraide judiciaire nationale (art. 43 ss CPP).

[182] Une décision judiciaire est requise, le cas échéant. Voir art. 248, al. 3, ou 264, al. 3, CPP.

[183] Voir arrêt du TF 1B_342/2017 du 11.12.2017, consid. 3.3 (rejet d'une plainte contre une demande de levée de scellés) et, plus généralement, THORMANN/BRECHBÜHL, BSK StPO II, art. 248 N 22 ss et les références citées.

[184] Notamment, la compétence du juge est réservée pour l'autorisation de mesures de surveillance de la correspondance par télécommunication.

[185] Pour plus de détails, voir FF 2013 2379 2466 ss et HANSJAKOB, N 10 ss.

[186] ATF 143 IV 21, 25 s. et TF 1B_142/2016 du 16.11.2016, consid. 3

[187] ATF 143 IV 270, 287 s.

Par conséquent, si les données d'accès ont été recueillies sous une forme autorisée par le droit de procédure[188], les autorités de poursuite pénale en Suisse peuvent les consulter et les exploiter en passant par le compte de l'utilisateur[189]. Étant donné que cette consultation n'a rien de secret, le prévenu peut demander la mise sous scellés des données afin de protéger des secrets[190].

Cette pratique du Tribunal fédéral fait l'objet de critiques au motif qu'elle porterait atteinte aux principes de la territorialité et de la souveraineté[191]. On rétorquera que l'accès par l'intermédiaire du compte de l'utilisateur est possible sans le concours de quiconque se trouvant à l'étranger et qu'aucune contrainte n'est exercée à l'encontre de personnes se trouvant à l'étranger[192]. Il s'agit d'une situation très différente des exemples qui sont cités pour étayer la thèse selon laquelle l'accès aux données violerait les principes de la territorialité ou de la souveraineté, voire serait punissable[193].

Du point de vue technologique, il ne paraît pas absurde de *nuancer l'interprétation du principe de la territorialité en cas d'administration de preuves sur Internet* : lorsqu'une application ou un serveur de fichiers repose sur une architecture informatique en nuage, il est souvent difficile d'établir dans quel pays les données sont stockées. Qui plus est, le lieu de stockage peut, pour des raisons techniques, changer rapidement sans que l'utilisateur s'en aperçoive. Il y a donc fréquemment doute sur le pays auquel adresser une éventuelle demande d'entraide judiciaire[194]. De là à considérer que l'exploitation des preuves est admissible du moment qu'il existe en Suisse une possibilité légale de maîtriser les données en question et que les délits d'une certaine gravité y sont poursuivis, il n'y a qu'un pas[195].

Une application restrictive du principe de la territorialité ne laisse généralement pas d'autre choix à la poursuite pénale que de lancer une fastidieuse procédure d'entraide judiciaire (ch 4.2.4), avec le risque de voir expirer certains délais légaux et donc de devoir mettre fin à la poursuite[196]. L'accès à distance désormais jugé admissible par le Tribunal fédéral constitue en revanche un moyen d'obtention de preuves efficace, qui devrait encore gagner en importance[197].

Des collaborateurs d'autorités de poursuite pénale qui accéderaient en Suisse à des données situées à l'étranger risqueraient bien sûr de se rendre punissables aux yeux de la législation

---

188 Exemple : mise sous séquestre de PC, de smartphones ou de documents en cas de risque de collusion lors des enquêtes sur des infractions graves, voir ATF 143 IV 270, 279 ss.

189 ATF 143 IV 270, 285 s.

190 AT 143 IV 270, 280

191 GRAF, N 21 ss ; plus généralement : AEPLI, p. 130 s. Les atteintes aux droits souverains étrangers lors d'enquêtes transfrontalières sur les réseaux sociaux sont également traitées, sous l'angle du droit allemand, par BAUER, p. 62 ss. Opinion divergente : WICKER, p. 356. Concernant le débat en Allemagne, voir IHWAS, p. 289 ss.

192 La même question de droit international se pose en miroir (du « point de vue de la victime » suisse) concernant l'art. 271 CP : à propos de l'élément de contrainte ou du caractère volontaire et de la nécessité de recourir à l'entraide judiciaire, voir l'arrêt du Tribunal pénal fédéral (TPF) RR.2015.196-198 du 18.11.2015, consid. 2.2.1 s. et HUSMANN, BSK StGB II, Bâle 2013, art. 271 N 15 s. ; voir également ch. 4.2.3 sur l'ensemble de la question.

193 GRAF, N 22 s. et 25 s.

194 Voir arrêt du TF 1B_142/2016 du 16.11.2016, consid. 3.3 et ATF 143 IV 21, 25. Concernant la notion de perte de localisation, voir SIEBER ULRICH / NEUBERT CARL-WENDELIN, Transnational Criminal Investigations in Cyberspace : Challenges to National Sovereignty, in: Lachenmann / Röder / Wolfrum (éd.), Max Planck Yearbook of United Nations Law, Volume 20 (2016), Leiden / Boston 2017, p. 249.

195 Sur le fond : SCHMID, p. 108 s. ; plus en détail : BANGERTER, p. 280 ss

196 Par ex. le délai de conservation et d'exploitation d'adresses IP, qui constituent des données secondaires au sens de l'art. 273, al. 3, CPP ; voir aussi ATF 139 IV 98 (exposé complet des faits : arrêt du TF 1B_481/2012 du 22.01.2013, consid. 2 et 3).

197 GRAF, N 3 et 9 ss ; IHWAS, p. 263. Concernant la mise sous séquestre de téléphones portables en général, voir arrêt du TF 1B_342/2017 du 07.12.2017 (en particulier consid. 6.1 s.).

étrangère[198]. En cas d'action unilatérale, un tel risque n'est jamais exclu. Seule une convention bilatérale ou multilatérale régissant l'accès transfrontalier des parties permet de le réguler.

4.2.3 Limite prévue par le CP : violation de la souveraineté territoriale étrangère

La collecte de preuves à l'étranger en dehors de toute procédure d'entraide judiciaire peut constituer une infraction non seulement dans le pays en question, mais aussi en Suisse. Si les autorités de poursuite pénale suisses s'avisaient de lancer une procédure directe, comme l'ont fait les autorités belges contre Yahoo Inc. aux États-Unis ou contre Skype Communications SARL au Luxembourg[199], cela serait pour le moins problématique au regard du droit suisse[200]. Ce dernier punit en effet le recours à la contrainte ainsi que la menace d'y recourir contre une entreprise ou une personne située à l'étranger.

Celui qui aura violé la souveraineté territoriale d'un État étranger, notamment en procédant indûment à des actes officiels sur le territoire de cet État, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (art. 299, ch. 1, al. 1, CP). L'art. 299 CP est le pendant de l'art. 271, ch. 1, CP (actes exécutés sans droit pour un État étranger)[201]. C'est la raison pour laquelle les actes possibles sont symétriquement identiques. Ils comprennent la notification de décisions de justice contraignantes, surtout si elles contiennent des menaces de contrainte (par ex. décisions de tribunaux suisses à l'encontre de cyberentreprises étasuniennes[202]). Ce délit ne peut être poursuivi que sur décision du Conseil fédéral (art. 302, al. 1, CP).

Contrairement aux actes exécutés sans droit pour un État étranger (art. 271 CP), la violation de la souveraineté territoriale étrangère n'a joué aucun rôle en pratique jusqu'à présent. Du point de vue de la procédure, il convient toutefois de souligner que des preuves obtenues par des moyens répréhensibles sont inexploitables (art. 141, al. 2, CPP). Par ailleurs, l'exécution d'un acte officiel fondé sur le droit étranger peut tout à fait être punie s'il y existe une norme comparable à l'art. 271 CP.

4.2.4 Entraide judiciaire

Lorsque les autorités de poursuite pénale suisses n'ont pas le droit de recueillir elles-mêmes des données auprès de fournisseurs ayant leur siège à l'étranger, elles peuvent tenter de se les procurer au moyen de l'entraide judiciaire. Lorsqu'il y a entraide judiciaire en matière pénale, des mesures d'instruction pénale sont exécutées dans l'État requis comme pour une procédure pénale nationale. Elles se fondent généralement sur des dispositions du droit international[203] ou du droit administratif. La procédure se fonde sur l'EIMP[204]. Les procédures d'entraide sont fastidieuses et plusieurs mois peuvent s'écouler avant que les autorités de poursuite pénale n'obtiennent des données. Certaines législations étrangères ne prévoient en outre aucune mesure provisoire immédiate de mise en sûreté et de blocage des données, ce

198 GRAF, N 32 ; voir aussi l'étude de cas de SIEBER / NEUBERT, p. 248 s.

199 Cour de cassation de Belgique, arrêt P.13.2082.N du 1.12.2015 (Yahoo Inc., États-Unis) et Cour d'appel d'Anvers, arrêt C/1288/2017 du 15.11.2017 (Skype Communications SARL, Luxembourg)

200 Voir GRAF, N 28. Voir aussi Jurisprudence des autorités administratives de la Confédération (JAAC) 1985 51.5, consid. III (affaire Marc Rich) : tout ordre de production émis directement à l'encontre d'une entreprise suisse par des autorités étasuniennes et lié à des peines disciplinaires est contraire au droit international ; l'exécution de cet ordre contrevient au droit suisse (art. 273 CP). En l'occurrence, l'autorisation d'engager la poursuite pénale n'a pas été accordée.

201 STRATENWERTH/BOMMER, BT II, § 51 N 12

202 STRATENWERTH/BOMMER, BT II, § 47 N 14. À propos de l'effet miroir concernant l'art. 271 CP, voir l'arrêt du TPF RR.2015.196-198 du 18.11.2015, consid. 2.2.1 s. et JAAC 2016.3, ch. II 9.

203 Traités multilatéraux ou bilatéraux

204 À propos du principe de l'accès, voir ch. 4.2.2.4; à propos de l'accès direct au sens de la CCC, voir ch. 4.2.5.

qui complique encore le travail des autorités suisses. Nombre d'enquêteurs considèrent que l'entraide judiciaire est une solution trop lente et ardue[205].

4.2.4.1 Demandes d'entraide judiciaire adressées aux États-Unis

Un grand nombre de cyberentreprises ont leur siège aux États-Unis. Comme elles revendiquent souvent la maîtrise des données à leur siège, la recherche de moyens de preuve dans le cadre de l'entraide judiciaire se fonde fréquemment sur le traité conclu le 25 mai 1973 entre la Confédération suisse et les États-Unis d'Amérique sur l'entraide judiciaire en matière pénale (TEJUS)[206].

Pour qu'une administration de preuves soit ordonnée de manière contraignante, il faut notamment que l'acte incriminé soit punissable tant en vertu du droit étasunien que du droit suisse (principe de la double incrimination, art. 4, ch. 2, TEJUS). Il doit en outre figurer sur la liste des infractions permettant l'application de mesures de contrainte annexée au TEJUS. Les délits contre l'honneur (art. 172 ss CP) et la discrimination raciale (art. 261bis CP) n'y figurent pas. Autrement dit, ces délits ne permettent pas de demander aux États-Unis l'application de mesures de contrainte par la voie de l'entraide judiciaire.

Lorsque des autorités de poursuite pénale adressent néanmoins une demande d'entraide judiciaire aux États-Unis pour de tels délits, ceux-ci sont jugés selon le droit étasunien exclusivement, en particulier s'agissant des conditions d'application de mesures de contrainte. Les autorités étasuniennes ne donnent suite à pratiquement aucune des demandes d'entraide judiciaire portant sur des délits contre l'honneur ou des violations de la norme pénale contre la discrimination raciale. La Constitution étasunienne protège en effet, au titre de la liberté d'expression, bon nombre de déclarations qui constitueraient en Suisse une infraction. Faute de double incrimination, les autorités étasuniennes sont souvent dans l'incapacité de recueillir les moyens de preuve demandés auprès des entreprises concernées, car cela leur serait interdit dans une procédure nationale.

Les entreprises ont la possibilité de régler le dépôt de données dans leurs conditions générales de vente (CGV). Or, elles le lient généralement à un ordre judiciaire, lequel ne peut justement pas être donné par les tribunaux étasuniens dans ces cas de figure. Le dépôt volontaire de données (à la suite d'une sollicitation directe par les autorités de poursuite pénale suisses) dépend donc du bon vouloir de l'entreprise concernée. Plus celle-ci a d'utilisateurs, moins elle y sera encline, car le traitement de grandes quantités de demandes mobilise des ressources coûteuses. Il faut souligner que le dépôt volontaire doit respecter les lois nationales de protection des données et de la personnalité.

Pour d'autres délits (par ex. infractions contre le patrimoine ou pornographie), le TEJUS permet théoriquement l'application de mesures de contrainte par la voie de l'entraide judiciaire. Cependant, le droit étasunien déterminant est très pointilleux sur les demandes d'entraide judiciaire. Les autorités étasuniennes rejettent parfois de telles demandes au motif que la présentation des faits ne correspond pas aux exigences du droit étasunien. Or, il faut exposer très précisément non seulement les faits, mais aussi l'infraction présumée, ainsi que l'existence d'un lien étroit entre l'acte délictueux et les données demandées.

[205] Voir SIEBER/NEUBERT, 46 et « Die Schweiz zapft Google und Apple an », Aargauer Zeitung du 06 décembre 2017, 2.

[206] RS **0.351.933.6**

Compléter le code pénal par des dispositions relatives au cyberharcèlement

Les demandes d'entraide judiciaire n'aboutissent souvent pas non plus, faute de ressources, lorsque le montant du délit est faible (fraude à la commission sur des locations de vacances, contrats de vente d'appareils numériques d'usage courant, etc.).

Étant donné que les autorités étasuniennes font elles aussi face à un nombre croissant de problèmes lorsqu'elles veulent recueillir des données qui constituent des moyens de preuves dans le cadre de procédures pénales[207], le législateur étasunien a adopté en 2018 le Clarifying Lawful Overseas Use of Data Act (**CLOUD Act**). Cette loi oblige les fournisseurs de services informatiques et cyberentreprises établis aux États-Unis à donner accès aux autorités étasuniennes, dans le cadre de procédures pénales locales, aux données qu'elles stockent à l'étranger. Sont également visées les données hébergées par des filiales étrangères, et ce quelle que soit la législation locale. Le CLOUD Act ne se fonde pas sur le critère de la territorialité, habituellement déterminant en droit pénal, mais uniquement sur la question de la possibilité d'accès : si l'autorité étasunienne peut forcer l'accès à des données, le fournisseur de service doit en principe permettre cet accès. Ce faisant, la protection juridique relève exclusivement du droit étasunien, ce qui signifie par exemple que la filiale suisse d'une entreprise étasunienne peut s'opposer à l'injonction des autorités en formant un recours devant le tribunal étasunien compétent dans lequel elle montre que le droit du lieu auquel sont stockées les données s'oppose à la divulgation de celles-ci. Le droit suisse de la protection des données, les droits fondamentaux suisses ou encore le secret professionnel et bancaire sont alors pris en compte au cours d'une procédure aux USA devant un *comity*[208].

Les USA proposent aux États étrangers qui remplissent à leurs yeux certaines exigences en matière de garanties procédurales et de droits fondamentaux de conclure un *executive agreement* en vertu de la deuxième partie du CLOUD Act. En signant cet accord, l'État partenaire tolère que les USA aient accès aux données hébergées sur son territoire et gagne en échange lui-même un accès aux données stockées par des entreprises aux États-Unis. Sur les avantages et les inconvénients d'un *executive agreement*, voir le rapport de l'Office fédéral de la justice sur l'US CLOUD Act[209].

4.2.4.2 Demandes d'entraide judiciaire adressées à des États européens

L'entraide judiciaire entre la Suisse et les États européens repose avant tout sur la Convention européenne du 20 avril 1959 d'entraide judiciaire en matière pénale[210] et sur ses protocoles additionnels. Elle laisse aux États parties la possibilité de subordonner l'application de mesures de contrainte à la condition de la double incrimination. Outre la Suisse, l'Irlande (qui abrite de nombreux centres de données, comme la Suisse) a fait usage de cette possibilité.

Quelles que soient les dispositions pénales nationales concrètes (par ex. irlandaises) sur les atteintes à l'honneur ou sur les déclarations racistes, ces actes sont soumis à une appréciation des libertés marquée par une vision locale de la société, dont le droit pénal national (par ex. irlandais) constitue la limite. Des publications ou des commentaires considérés en Suisse comme discriminatoires ou portant atteinte à l'honneur sont, ailleurs, protégés par la liberté d'expression. Ces différences d'appréciation ont une influence directe sur l'évaluation de la double incrimination.

---

[207] Voir United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

[208] Voir DODGE, 2071 ss.

[209] Rapport OFJ US CLOUD Act, ch. 5.6

[210] RS **0.351.1**

Par conséquent, outre le fait que ces délits sont largement considérés comme des bagatelles ne justifiant pas une poursuite pénale complexe, l'entraide judiciaire ne donne parfois aux autorités suisses qu'un accès limité aux données à l'intérieur de l'Europe.

Un système de reconnaissance mutuel des décisions de justice au sein de l'UE s'est imposé ces dernières années[211]. L'UE a développé un arsenal d'outils (par ex. le mandat d'arrêt européen ou la décision d'enquête européenne) visant à remplacer l'examen de la double incrimination par une confiance réciproque dans le système juridique des autres États. Contrairement à la Norvège et à l'Islande, elles aussi membres de l'AELE, la Suisse ne s'est pour l'instant pas ralliée à ces instruments. L'UE développe actuellement sur cette base son propre système d'accès transfrontalier aux données pertinentes pour les procédures pénales. Ce projet, nommé E-evidence, en est encore au stade de trilogue et devrait être adopté au cours de l'année 2022[212]. Cette réglementation européenne ne concerne pas réellement les « États tiers », mais bien les droits d'accès réciproques des membres de l'UE. L'objectif déclaré de l'UE est toutefois d'avoir accès aux données de tous les fournisseurs de services actifs sur son marché intérieur. Selon le projet de règlement, l'accès au marché serait lié à l'établissement d'un « legal seat » dans l'UE. Grâce à la nouvelle injonction européenne de production, les autorités de poursuite pénales des États de l'UE pourraient donc adresser leurs décisions directement à ce « legal seat » dans l'UE. Le système E-evidence aura probablement des répercussions sur les fournisseurs de services suisses, dès lors qu'ils ont des clients dans l'UE.

4.2.4.3 De nouveaux traités d'entraide judiciaire pour simplifier la collecte de données

La révision du TEJUS est régulièrement évoquée lors de consultations entre les autorités d'entraide judiciaire suisses et étasuniennes. Les États-Unis y sont favorables en principe, tout comme à la conclusion d'un *executive agreement*. L'obligation de stocker des données de réserve en vue de procédures pénales est cependant radicalement différente dans les deux pays : en Suisse, la LSCPT oblige certains fournisseurs de services à conserver pendant six mois au moins les données permettant d'identifier un usager. Cette obligation légale n'a pas d'équivalent aux États-Unis. Les normes et les procédures en matière de protection des données et de protection juridique sont également très différentes. Il semble donc difficile de trouver un consensus sur des formes de coopération plus directes en dehors de l'entraide judiciaire fondée sur la souveraineté et la territorialité, dont les procédures peuvent être contraignantes, mais qui garantissent la protection des principes juridiques locaux dans le cadre de la coopération transfrontalière.

Tous les États de l'UE ne connaissent pas non plus d'obligation de conserver analogue à celle inscrite dans la LSCPT. Quant à savoir si et dans quelle mesure la Suisse pourrait se raccorder au système E-evidence de l'UE, tout dépend des possibilités et des intérêts des deux parties, qui ne sont pas connus à l'heure actuelle.

Étant donné que le système de l'UE ne mise pas sur des accès extraterritoriaux, contrairement au CLOUD Act, mais vise au contraire à établir la territorialité par la présence (forcée) du fournisseur de services, il semble à première vue plus compatible avec les principes suisses en matière de protection des données et de protection juridique.

---

[211] Voir par ex. la fiche thématique du Parlement européen, disponible sous www.europarl.europa.eu/factsheets > Citoyens > L'espace de liberté, de sécurité et de justice > Coopération judiciaire en matière pénale.

[212] Voir les informations sur le site de la Commission européenne sous : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

Compléter le code pénal par des dispositions relatives au cyberharcèlement

4.2.5 Accès direct en vertu de la Convention du Conseil de l'Europe sur la cybercriminalité

La CCC est *le plus important des accords internationaux dans le domaine de la cybercriminalité*. Son premier chapitre oblige les parties à ériger certains comportements en infractions pénales[213]. Le second définit des règles de droit procédural en se focalisant sur la collecte et la préservation de preuves sous forme de données informatiques. Le troisième règle la coopération internationale entre les parties, qui doit privilégier la rapidité et l'efficacité en vue de la réussite de la procédure, tout en respectant les principes de l'État de droit.

Parmi les 56 États parties[214] figurent, outre la Suisse, presque tous les membres du Conseil de l'Europe et des pays tels que les États-Unis, le Canada, le Japon, l'Australie ou Israël, acteurs majeurs de la lutte commune contre la cybercriminalité. D'autres États se sont déclarés intéressés par une adhésion[215].

La CCC prévoit deux cas dans lesquels l'accès transfrontière des parties à des données informatiques est autorisé **sans concertation préalable avec l'État** où se trouvent les données ni besoin de recourir à l'entraide judiciaire internationale :

- Accès par une des parties à des *données accessibles au public*[216] : l'exploitation de données de ce genre, récupérées sur un serveur étranger, est possible sans l'autorisation de l'autre partie, même si un enregistrement comme utilisateur est requis.
- Accès par une des parties à des *données stockées à l'étranger* et utilisation de celles-ci comme *moyens de preuve*, à condition d'avoir obtenu le *consentement légal et volontaire* de la personne légalement autorisée à divulguer ces données (à une autorité de poursuite pénale ; art. 32, let. B, CCC). C'est par exemple le cas lorsqu'une personne possède un compte de messagerie chez un fournisseur étranger et met ces données à la disposition d'un ministère public national à des fins d'instruction ou de preuve[217].

Le **2e protocole additionnel** à la CCC vise à *renforcer la coopération internationale* dans la lutte contre la cybercriminalité et à *faciliter l'échange rapide d'informations et de moyens de preuve électroniques* entre les parties à la convention.

L'élaboration de ce protocole est achevée et le texte a été ouvert à la signature le 12 mai 2022. La signature par un État membre du Conseil de l'Europe (ou une mise en œuvre directe du contenu avec ratification) restera possible ultérieurement.

Le 2e protocole additionnel, qui n'est pas encore entré en vigueur, fera l'objet d'une **évaluation approfondie** de la part de la Suisse avant d'être ratifié. Le but est avant tout de déterminer ses *chances de succès* (c'est-à-dire d'être largement mis en œuvre par la communauté internationale), sa *valeur ajoutée* d'un point de vue pratique (notamment pour les autorités de poursuite pénale) ainsi que les risques qui en découlent (par ex. pour la protection des données et la souveraineté étatique). Répondre à ces questions nécessitera d'observer la situation : *dans quelle mesure les futurs États parties peuvent-ils garantir une coopération à la fois efficace, réglementaire et sûre ?*

En cas de mise en œuvre étendue du 2e protocole additionnel, les **modifications législatives** fondamentales suivantes devront être étudiées en premier lieu en Suisse :

---

213 Notamment le piratage, la fraude informatique et la pornographie enfantine

214 Situation au 01.06.2022

215 Pour plus de détails: www.coe.int > Explorer > Bureau des Traités > Liste complète > Convention sur la cybercriminalité (STE n° 185)

216 Dites « sources ouvertes », voir art. 32, let. a, CCC.

217 Voir FF **2010** 4275 4313.

Compléter le code pénal par des dispositions relatives au cyberharcèlement

- Nouvelle disposition permettant aux autorités de poursuite pénale suisses de *transmettre directement leurs demandes de renseignements aux exploitants (de domaines) sis dans un autre État partie*.
- Base légale permettant aux *exploitants suisses (de domaines) de livrer directement les informations requises aux autorités étrangères.*
- Nouvelle disposition permettant aux autorités de poursuite pénales suisses de *transmettre directement leurs demandes de renseignements sur des clients (subscriber information) aux fournisseurs sis dans un autre État partie*.
- Base légale permettant aux *fournisseurs suisses de livrer directement les informations requises sur leurs clients (subscriber information) aux autorités étrangères.*

Un **dilemme cornélien** subsiste néanmoins. L'extension des instruments visant à renforcer la coopération internationale et la confiance mutuelle entrera toujours en contradiction avec la *volonté de globalisation de la Convention sur la cybercriminalité*. L'abandon prévisible des garanties nationales au cas par cas se heurte à l'extension de la convention aux États qui, dans les faits, ne veulent ou ne peuvent pas appliquer les valeurs du Conseil de l'Europe (*en particulier la protection des données, le droit à un procès équitable et le respect des garanties de procédure*).

Les **possibilités juridiques actuelles** de l'accès transfrontière direct à des données par des autorités de poursuite pénale sont pour l'instant considérées comme *insatisfaisantes et surannées*, d'où une **multiplication des efforts** pour que la coopération internationale relève les défis du développement technologique et de l'évolution de la société afin de permettre une poursuite pénale efficace sur Internet.

4.3 Responsabilité pénale des prestataires de services

4.3.1 Insoumission punissable et infractions aux dispositions sur l'administration de la justice

Toute personne qui, malgré sommation, refuse de communiquer aux autorités des données devant servir de preuve dans une procédure pénale, se rend punissable (art. 265, al. 3, CPP).[218]

Quiconque contrevient à une obligation de collaborer prévue par le droit procédural pénal[219] peut être puni pour insoumission à une décision de l'autorité (art. 292 CP). Les personnes ayant une obligation de collaborer en vertu de la LSCPT[220] font l'objet d'une disposition spéciale analogue dans cette loi (art. 39, al. 1, let. a, LSCPT)[221].

Les délits énumérés au titre 17 du CP protègent l'administration de la justice d'influences injustifiées. Quiconque soustrait une personne à une poursuite pénale est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire pour entrave à l'action pénale (art. 305 CP). Le Tribunal fédéral[222] a confirmé la punissabilité du directeur d'un fournisseur pour ce motif précisément : en effaçant des adresses IP, cet individu avait contrevenu à son obligation de renseigner prévue par l'art. 22 LSCPT. Il était en outre tenu de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation (art. 26, al. 5, LSCPT). Le Tribunal fédéral a estimé qu'au fond, peu

[218] Le prévenu n'a pas l'obligation de déposer contre lui-même (principe *nemo tenetur*, art. 113 CPP) ; les personnes qui ont le droit de refuser de témoigner constituent une autre exception, voir art. 264 s. CPP.

[219] En particulier l'obligation de témoigner (art. 163, al. 2, CPP) ou l'obligation de dépôt (art. 265 CPP)

[220] En particulier les fournisseurs de services de télécommunication (FST), mais aussi les fournisseurs de services de messagerie, les exploitants de plateformes, etc.

[221] L'auteur qui agit par négligence est également punissable (art. 39, al. 3, LSCPT).

[222] Arrêt du TF 6B_766/2009 du 8.1.2010, consid. 3

importe sur quelles dispositions légales repose une obligation de conserver les adresses IP : ce qui compte, c'est que le directeur ait voulu soustraire les utilisateurs de son site à d'éventuelles poursuites pénales.

Si l'objet constitutif de la preuve et son détenteur se trouvent à l'étranger, ni le dépôt, ni la mise sous séquestre, ni la sanction d'une violation d'obligations ne peuvent être imposés ni ordonnés directement. Dans ce cas de figure, c'est l'EIMP qui s'applique[223].).

4.3.2 Complicité du fournisseur de services dans l'acte principal d'un utilisateur

Conformément à la jurisprudence du Tribunal fédéral, quiconque met à disposition une infrastructure technique dont un utilisateur se sert pour commettre des délits peut théoriquement être puni pour complicité[224] dans l'acte principal de l'utilisateur. Dans ce cas concret, le directeur général des PTT a été puni pour complicité de publication de contenus pornographiques illégaux : il mettait à disposition l'infrastructure technique en sachant qu'elle servait à commettre des délits concrets[225].

Dans l'affaire « Appel au peuple[226] », le Tribunal cantonal du canton de Vaud a jugé, dans un arrêt non officiellement publié du 2 avril 2003, que l'obligation de bloquer l'accès à un site Internet faite à un fournisseur d'accès était illicite du point de vue de la procédure pénale, faute de base légale, mais qu'il fallait signaler aux fournisseurs d'accès qu'ils risquaient d'être punis pour complicité dans l'acte principal (en l'occurrence, des délits d'atteinte à l'honneur) s'ils ne procédaient pas au blocage.

Il existe des règlements de référence dans ce domaine, notamment le Code de conduite hébergement (CCH) de la représentation des branches TIC et Internet[227]. Le CCH est un instrument d'autorégulation volontaire des fournisseurs d'hébergement suisses qui contient des instructions sur la manière de gérer les avis de contenus potentiellement illicites[228]. Il définit une procédure de notification et de retrait (*notice and takedown*) de contenu illicite sans pour autant donner aucun droit à la suppression du contenu contesté[229]. Un fournisseur qui respecte le CCH a peu de risques d'être poursuivi au pénal.

Conformément à la jurisprudence exposée plus haut, il serait possible d'ouvrir contre le CEO d'une plateforme de réseau social non coopérative à l'étranger une procédure pénale pour complicité de délit d'expression d'un utilisateur de la plateforme. Il faudrait pour cela que le CEO sache que des délits sont commis sur la plateforme de son entreprise sans rien faire contre. L'atteinte aux droits d'une victime suisse peut aussi être jugée au pénal en Suisse si le prévenu se trouve à l'étranger et ne se présente pas aux débats en Suisse (procédure par défaut conformément à l'art. 366 CPP). La juridiction pénale suisse découle du principe de la personnalité passive[230]. Dans la procédure contre le participant d'un acte principal, il peut être constaté sommairement que l'acte principal commis est illicite et conforme à l'énoncé de fait légal, même si l'auteur principal (l'utilisateur de la plateforme, p. ex.) est inconnu.

---

[223] Voir ch. 4.2.4.

[224] Art. 25 CP

[225] ATF 121 IV 109, consid. 3 (« télékiosque »)

[226] À ce propos, voir arrêt du TF 1B_242/2009 du 21.10.2009.

[227] Consultable sur www.swico.ch > Connaissances > Normes et standards > Code de conduite hébergement (CCH). Pour plus de détails sur le CCH (anciennement Code Simsa), voir FF **2018** 559, ch. 1.2.1.1.

[228] Ch. 1 CCH

[229] Ch. 7.1 CCH

[230] POPP/KESHELAVA, BSK StGB I, Vor Art. 3, N 21

4.3.3 Applicabilité du droit pénal des médias

Le droit pénal des médias est un droit pénal spécial favorable aux personnes associées à la publication d'un produit médiatique. Dans ce contexte en effet, contrairement à ce que prévoient les règles ordinaires, l'auteur est seul punissable (art. 28, al. 1, CP). Ce privilège est bien entendu limité à des délits typiques relatifs au contenu des médias (atteintes contre l'honneur, violations de secret, etc.). Selon la jurisprudence du Tribunal fédéral, en cas de discrimination raciale, de pornographie dure et de représentation de la violence, les règles normales s'appliquent (complicité, voire instigation et complicité) [231].

Si l'auteur ne peut être découvert ou traduit en Suisse devant un tribunal, une cascade de responsabilités pénales particulière se met en place : sont alors punissables le rédacteur ou, à défaut, la personne responsable de la publication (art. 28, al. 2, CP). Ces personnes ne seront bien entendu pas punies pour le délit d'expression de l'auteur, mais pour défaut d'opposition, intentionnel ou par négligence, à une publication constituant une infraction (art. 322bis CP).

Les réseaux sociaux tels que Twitter et Facebook peuvent en principe être considérés comme des médias au sens de l'art. 28, al. 1, CP[232]. Il va de soi que le privilège relatif aux médias ne concerne que la communication publique sur les plateformes des réseaux sociaux, non la communication privée[233]. Mais où s'arrête l'une et où commence l'autre sur les réseaux permettant de fixer le degré de confidentialité de manière individuelle et progressive[234] ? Le droit pénal des médias ne s'applique pas aux fournisseurs de messagerie, faute de publication. Il devrait en aller de même pour les plateformes qui fournissent de pures prestations de stockage sans publier les informations au sens du droit pénal des médias.

Lorsqu'un délit d'expression est commis sur la plateforme d'un réseau social, le principe des responsabilités en cascade permet d'envisager la punissabilité de l'exploitant de la plateforme à condition que celui-ci ait un devoir de surveillance et un pouvoir d'opposition[235]. S'il est impossible d'identifier l'auteur d'une publication sur une plateforme (parce que l'entraide judiciaire a été refusée, p. ex.), le droit pénal des médias permet de punir le responsable de la plateforme pour défaut d'opposition, intentionnel ou par négligence, à une publication constituant une infraction. Une procédure par défaut est également possible ici (art. 366 CP).

4.4 Retrait et blocage de contenus illicites

4.4.1 Mesures fondées sur le droit pénal

Si une décision définitive a été rendue, les contenus illicites[236] doivent être supprimés d'Internet. Ce retrait (« takedown ») des données en Suisse s'appuie, en droit pénal, sur les règles de la confiscation. Si, dans le cas de la « pornographie dure » et de la représentation de la violence, la confiscation est réglée spécifiquement (art. 197, al. 6, et 135, al. 2, CP), dans le cas de la pornographie douce (art. 197, al. 1 et 2, CP), de la discrimination raciale (art. 261 CP) et des délits contre l'honneur (art. 173 ss CP), il faut se référer à la norme fondamentale de l'art. 69 CP (confiscation d'objets dangereux). Cependant la loi ne parle que d'« objets », sans citer explicitement les « données ». La notion de donnée en droit pénal est donc sujette à

[231] ZELLER, BSK StGB I, art. 28 N 64 ss (N 68 en particulier) et les références citées ; TRECHSEL/ JEAN-RICHARD, PK StGB, art. 28 N 7

[232] Arrêt GG150250 du tribunal de district de Zurich du 26 janvier 2016, reproduit dans forum poenale 2017, 290 ss (avec rem. de ROTH SIMON) ; voir aussi ZELLER, BSK StGB I, art. 28 N 96 ss. Avis contraire: SCHWAIBOLD, p. 113 ss. Voir aussi ATF 136 IV 145: protection des sources admise concernant un commentaire sur un blog diffusé sur une page Internet de la Télévision suisse.

[233] ZELLER, BSK StGB I, art. 28 N 49

[234] À titre d'illustration: ATF 141 IV 215 concernant les menaces alarmant la population (art. 258 CP) sur Facebook, et ATF 126 IV 176 et 130 IV 111 concernant la nécessité de la publicité en cas de discrimination raciale (art. 261bis CP).

[235] TRECHSEL / JEAN-RICHARD (n. 231), art. 28 N 14

[236] Pornographie, atteinte à l'honneur ou discrimination raciale, p. ex.

discussion et l'interdiction de l'interprétation par analogie suscite des questions quant à l'applicabilité de cette norme[237].

Le retrait est difficile, sinon impossible, lorsque le fournisseur d'hébergement a son siège à l'étranger et qu'aussi bien lui-même que l'auteur refusent de coopérer. On envisage par conséquent de prendre des décisions de blocage contre les fournisseurs d'accès en Suisse, afin de rendre certains contenus inaccessibles au public suisse. Il existe deux types de blocage d'accès :

- le blocage d'*adresse IP*, par lequel le fournisseur d'accès empêche ses clients d'accéder à un serveur donné (ou à son adresse IP) ;
- le blocage de *DNS*, par lequel le fournisseur d'accès bloque l'attribution d'un nom de domaine à l'adresse IP correspondante[238].

Ces deux mesures étant relativement faciles à contourner, leur efficacité n'est pas garantie. En outre, le blocage d'adresse IP, en particulier, présente un risque de surblocage, c'est-à-dire le blocage de tous les contenus correspondant à la même adresse IP, et non uniquement les contenus illicites[239]. Dans ce genre de situation, la question de la proportionnalité est donc d'une importance capitale[240]. Pour ce qui est des délits pornographiques figurant dans le CP, le blocage auparavant volontaire procède depuis le 1er janvier 2021 d'une base légale contraignante (art. 46*a*, al. 2, de la loi du 30 avril 1997 sur les télécommunications[241])[242].

La loi allemande *Netzwerkdurchsetzungsgesetz* (ch. 3.3.2) vise à renforcer la lutte contre la haine et le harcèlement sur Internet. Elle ne fonde aucune obligation de suppression nouvelle par rapport aux prescriptions de droit pénal ou civil existantes. Son but premier est donc le retrait des contenus. Ce n'est évidemment pas l'État, mais les entreprises qui jugent de la légalité des contenus. On peut se demander si les mesures prévues par cette loi renforceront la poursuite pénale (voir également ch. 3.3.2).

4.4.2 Instruments de droit privé

Conformément à l'art. 28, al. 1, du code civil (CC), celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe. Comme exposé plus haut (ch. 3.1), le demandeur peut notamment requérir de faire cesser une atteinte illicite (action en cessation de l'atteinte conformément à l'art. 28*a*, al. 1, ch. 2, CC). Cette règle est neutre au point de vue technologique. On peut donc imaginer que tant la suppression que le blocage de contenus illicites sur Internet soient ordonnés sur cette base. Lorsque l'utilisateur en infraction n'est pas identifiable, la possibilité de recourir contre des complices devient particulièrement intéressante. C'est la raison pour laquelle le Conseil fédéral a examiné entre autres, dans le rapport « La responsabilité civile des fournisseurs de services Internet » du 11 décembre 2015, la possibilité d'intenter des actions en cessation de l'atteinte contre différents cyberacteurs.

---

[237] TRECHSEL/JEAN-RICHARD, PK StGB, art. 69 N 1 ; plus en détail: BOMMER, p 172 s. et 178 s. À propos de l'interdiction de l'interprétation par analogie, voir POPP/BERKEMEIER, BSK StGB I, art. 1 N 31 ss, en part. N 42.

[238] Comme si le fournisseur d'accès biffait, dans son exemplaire de l'annuaire, le numéro de téléphone d'un abonné. Le numéro resterait disponible dans les autres exemplaires.

[239] Pour plus de détails, voir le rapport du Conseil fédéral «La responsabilité civile des fournisseurs de services Internet», p. 46 s. et arrêt du TF 1B_294/2014 du 19.3.2015, consid. 4.5.

[240] Sur la fonction et l'admissibilité du blocage au sens de l'art. 86, al. 1, LJAr, voir arrêt du TF 2C_336/2021 du 18 mai 2022 (publication prévue), consid. 7 et 8.

[241] RS **784.10**

[242] Voir également FF 2017 6185 ss.

Compléter le code pénal par des dispositions relatives au cyberharcèlement

Le rapport précise que le cercle des personnes qui peuvent faire l'objet d'une action en cessation de l'atteinte ne peut pas être illimité. Même si une contribution subordonnée suffit pour justifier une telle action, cette contribution n'est pertinente juridiquement que si elle présente un lien de causalité adéquat[243]. Il faut aussi respecter le principe de la proportionnalité. S'agissant de la responsabilité civile à l'égard des contenus mis en ligne, le Conseil fédéral estime que le critère déterminant est la proximité du fournisseur avec le contenu[244]. Pour garantir la protection des droits des personnes concernées, il souhaite que les fournisseurs ayant une certaine maîtrise des contenus, comme les exploitants de réseaux sociaux, puissent être obligés, dans le respect du principe de la proportionnalité, à éliminer des contenus illicites. Quant aux fournisseurs d'accès à Internet, ils ne sont pas en mesure de consulter les contenus transmis, selon toute vraisemblance chiffrés. On ne peut donc pas raisonnablement attendre d'eux qu'ils exercent une influence directe sur le transport des contenus enregistrés. Par conséquent, les actions défensives dirigées contre ces fournisseurs risquent généralement d'être vouées à l'échec, faute d'un lien de causalité adéquate entre leur participation et l'atteinte[245]. Il faut également tenir compte du fait que, comme nous l'avons dit, le seul moyen dont disposent les fournisseurs d'accès pour empêcher l'accès aux contenus illicites est le blocage (d'adresse IP ou de DNS), qui suppose à chaque fois un examen scrupuleux de la proportionnalité des mesures techniques (ch. 4.4.1)[246].

L'application du droit à l'étranger présente fréquemment des difficultés, y compris dans le domaine du droit privé. Le rapport évoqué a examiné de manière approfondie la question de savoir s'il serait possible d'obliger les fournisseurs à indiquer un domicile de notification en Suisse, afin de faciliter l'exécution des décisions de droit civil les concernant. Le Conseil fédéral a toutefois conclu dans ce rapport qu'il n'est pas prioritaire de donner suite à cette question. Il souhaite au contraire mettre l'accent sur la conclusion de traités bilatéraux ou multilatéraux d'entraide judiciaire en matière civile prévoyant la transmission directe par voie postale des actes devant être notifiés à l'étranger. Des traités de ce type ont déjà été conclus avec quelques États qui accueillent le siège social d'exploitants de plateformes bien connus[247].

4.4.3 Mesures volontaires mises en place par les cyberentreprises

Les entreprises telles que Google, Facebook/Meta et Twitter proposent spontanément des procédures de notification et de retrait permettant de signaler, de bloquer[248], ou de supprimer des atteintes au droit par-delà les frontières. De plus, tout utilisateur a en principe le droit d'émettre des notifications pouvant conduire à un retrait.

Les notifications émanant de certaines sources sont traitées en priorité. Citons par exemple le programme « Trusted Flagger » de Youtube. Un « trusted flagger » est un utilisateur particulièrement digne de confiance dont l'entreprise traite les notifications et les alertes plus rapidement que celles des utilisateurs ordinaires. Cela permet de supprimer rapidement des contenus indésirables, en particulier des vidéos traitant du terrorisme ou du djihadisme. fedpol est l'un de ces « trusted flaggers »[249].

---

[243] Rapport « La responsabilité civile des fournisseurs de services Internet », ch. 3.2.2 ; sur la nécessité d'un lien de causalité entre le comportement des contributeurs et l'atteinte à la personnalité, voir ATF BGE 141 III 513, consid. 5.3, et sur la pertinence de la contribution à l'acte, voir l'arrêt du TF 5A_658/2014 du 6 mai 2015, consid. 4.2.

[244] Rapport « La responsabilité civile des fournisseurs de services Internet », ch. 3.2.2 et 7.1

[245] Sur le droit d'auteur, voir ATF 145 III 72.

[246] À ce propos, voir ch. 4.4.1 et rapport « La responsabilité civile des fournisseurs de services Internet » du 11.12.2015 (n. 2), ch. 7.1.2.

[247] États-Unis, Irlande, voir rapport « La responsabilité civile des fournisseurs de services Internet », ch. 6.2.4.

[248] Au sens du géoblocage (blocage de contenus pour certaines régions)

[249] Bühler Stefan, So stoppt der Bund Jihad-Videos, NZZ am Sonntag du 14 août 2016

4.5 Mandat législatif : obligation de désigner un domicile de notification

La *motion 18.3379 CAJ-E « Accès des autorités de poursuite pénale aux données conservées à l'étranger »* du 23 mars 2018 a été proposée pour acceptation par le Conseil fédéral et adoptée par le Parlement[250]. Son titre est incomplet, voire prête à confusion : il s'agit d'obliger les cyberentreprises à créer une possibilité de notification. La motion demande notamment la création d'une base légale pour que les réseaux sociaux soient tenus de désigner une représentation ou un domicile de notification en Suisse, et ce afin de faciliter leur communication avec les autorités comme avec les consommateurs. Si une entreprise étrangère refuse de désigner une représentation en Suisse, cette obligation ne peut toutefois pas être imposée, car les autorités suisses ne peuvent pas utiliser de moyens de contrainte dans un État étranger.

La *motion 18.3306 Glättli « Renforcer l'application du droit sur Internet en obligeant les grandes plates-formes commerciales à avoir un domicile de notification »* du 15 mars 2018[251] charge le Conseil fédéral de renforcer l'application du droit sur Internet en obligeant les grandes plateformes commerciales à avoir un domicile de notification. Contrairement à l'actuelle disposition potestative de l'art. 140 CPC, les entreprises visées seraient à l'avenir tenues de désigner un domicile de notification. Cette obligation devrait également être inscrite dans le CPP. Le Conseil fédéral a également proposé d'accepter cette motion, tout en précisant lors des délibérations, par l'intermédiaire de la ministre de la justice d'alors, qu'il concentrerait ses recherches – tout comme pour la motion 18.3379 – sur des solutions qui puissent bel et bien être mises en œuvre et produire des résultats[252].

4.5.1 État de la mise en œuvre

Durant les débats sur la révision de la LPD, achevés fin septembre 2020, le Parlement a ajouté une disposition obligeant les responsables du traitement privés sis à l'étranger à désigner un représentant en Suisse lorsqu'ils traitent des données personnelles concernant des personnes en Suisse et que ce traitement remplit certaines conditions (art. 14 nLPD). Ce représentant a plusieurs obligations (art. 15 nLPD). Cette nouvelle règle répond aux demandes des motions 18.3306 et 18.3379.

Les responsables du traitement privés qui offrent des produits ou des services à des personnes en Suisse ou observent le comportement de personnes en Suisse (par ex. ciblage de clients) seront tenues par le nouvel art. 14 LPD de désigner un représentant en Suisse lorsqu'il s'agit d'agit d'un traitement à grande échelle[253] et régulier[254] et qu'il présente un risque élevé pour la personnalité des personnes concernées[255]. Sont a priori visés les grandes plateformes numériques et les réseaux sociaux. Le représentant sera l'interlocuteur du Préposé fédéral à la protection des données et à la transparence (PFPDT) et les personnes concernées (art. 14, al. 2, nLPD).

Le responsable du traitement étranger doit publier le nom et l'adresse de son représentant (art. 14, al. 3, nLPD). L'art. 15 nLPD confère trois devoirs au représentant : tenir un registre des activités de traitement, fournir sur demande au PFPDT les indications contenues dans ce

[250] www.parlement.ch > Objet 18.3379

[251] www.parlement.ch > Objet 18.3306

[252] BO **2018** N 1400

[253] En d'autres termes, le traitement des données doit concerner un grand nombre de personnes en Suisse ou un gros volume de données.

[254] Cette condition serait par ex. remplie dans le domaine du commerce en ligne. Même si les données personnelles constituent la « matière première » d'une activité (comme pour les réseaux sociaux), il y a traitement régulier de données. En revanche, le critère de la régularité n'est pas rempli lorsque les données ne sont traitées que pour une durée limitée ou à titre occasionnel.

[255] Il convient d'examiner au cas par cas si le traitement des données présente un tel risque élevé. Ce dernier découle en particulier du volume et de la nature des données traitées (notamment si elles sont sensibles), du but de leur traitement, de la finalité ou du mode de traitement (par ex. pour l'utilisation de nouvelles technologies), d'une éventuelle communication des données à l'étranger et des droits d'accès (si un grand nombre, voire un nombre illimité de personnes ont accès aux données).

registre[256] et fournir sur demande à la personne concernée des renseignements concernant l'exercice de ses droits.

Le PFPDT peut ordonner au responsable du traitement étranger qui remplit les critères fixés à l'art. 14 nLPD de désigner un représentant en Suisse (art. 51, al. 4, nLPD). Étant que cette décision est un document officiel, elle doit toutefois être notifiée par la voie diplomatique (sauf si un traité international prévoit la notification directe). Le PFPDT peut signifier sa décision au responsable étranger sous la menace d'une peine s'il ne s'y conforme pas (art. 63 nLPD). Si l'amende est prononcée en vertu de cette disposition, il faudra cependant recourir à l'entraide judiciaire ou à la voie diplomatique pour en exiger le versement.

4.6 Synthèse

Les délits d'expression sur Internet sont souvent commis sous couvert d'anonymat, ce qui conditionne l'identification de l'auteur à l'obtention de preuves à l'étranger.

Les autorités suisses de poursuite pénale sont soumises aux principes de territorialité et de souveraineté, ce qui signifie qu'elles ne peuvent que rarement obtenir directement ces moyens de preuve. Le plus souvent, le droit pénal suisse n'est applicable qu'au prix de lourds efforts (par le biais de l'entraide judiciaire en matière pénale), si tant est qu'il le soit (eu égard à l'exigence de la double incrimination). De nouvelles dispositions matérielles ne changeraient rien à l'affaire et risqueraient de susciter des attentes irréalistes.

Par ailleurs, des mesures unilatérales n'auraient qu'un effet limité : les traités internationaux sont l'outil privilégié pour améliorer l'obtention de preuves à l'étranger.

L'effacement de publications attentatoires à l'honneur sur Internet devrait devenir plus facile pour les personnes concernées : la nouvelle mouture de la LPD obligera les responsables du traitement privés sis à l'étranger à désigner un *représentant en Suisse* lorsqu'ils traitent des données personnelles concernant des personnes en Suisse et que ce traitement remplit certaines conditions (art. 14 s. nLPD). Cette disposition permettra de prendre directement contact avec les exploitants de plateformes en ligne. Une victime pourra donc enjoindre directement l'exploitant de retirer une publication illicite, même si cela ne créera naturellement pas pour autant un droit à l'effacement qui puisse être mis en œuvre à l'échelle internationale.

Notons enfin que le Conseil fédéral étudie la nécessité d'agir pour améliorer l'application du droit dans le cadre du postulat 21.3450 de la CPS-E « Discours de haine. La législation présente-t-elle des lacunes ? » et d'une note de discussion indiquant si et comment les plateformes de communication doivent être réglementées. Cette dernière devrait être publiée fin 2022 et le rapport donnant suite au postulat au 2e trimestre 2023.

5 Conclusions

5.1 Droit matériel

Au vu des analyses qui précédent, il ne paraît *pas nécessaire d'agir en droit matériel*.

Le *cyberharcèlement*, soit un comportement délibérément intimidant, intrusif ou humiliant commis via les TIC à plusieurs reprises sur une longue période, et qui a pour conséquence que la victime se sent insultée, chicanée, persécutée ou rabaissée, peut être poursuivi et puni par les différentes dispositions pénales en vigueur. Il en va de même lorsque les actes ne causent qu'une faible injustice s'ils sont considérés isolément et n'atteignent donc pas le seuil requis pour constituer une infraction, mais que le comportement vu dans sa globalité est insultant, intimidant ou dénigrant pour la personne visée. L'application de la jurisprudence

[256] Dans le respect du principe de souveraineté, le PFPDT n'est pas autorisé à demander au représentant des indications ou des données personnelles stockées à l'étranger. Ces informations ne peuvent être obtenues que par la voie de l'entraide judiciaire internationale.

sur la contrainte dans le cas du stalking (art. 181 CP)[257] et de l'utilisation abusive d'une installation de télécommunication (art. 179^{septies} CP)[258] par le Tribunal fédéral permettrait de tenir compte du comportement dans son ensemble et de le sanctionner en conséquence. L'arsenal légal existant fournit donc déjà un cadre approprié pour punir le cyberharcèlement.

Si une *disposition spécifique* était néanmoins créée, le Conseil fédéral estime qu'elle devrait rester *neutre technologiquement*. Il faut en effet tenir compte du fait que des formes graves de harcèlement se manifestent également dans le *monde réel*. Il est injustifiable objectivement de sanctionner la cybervariante du harcèlement par une disposition à part tout en poursuivant ce dernier comme à l'accoutumée au titre des infractions constituées dans chaque cas d'espèce. En outre, il existe des cas hybrides, dans lesquels agissements en ligne et hors-ligne se confondent. Face à une infraction réservée au cyberharcèlement, les tribunaux seraient bien en peine de traiter ces cas. Un coup d'œil aux législations étrangères montre que seule l'Autriche a créé une infraction spécifique pour le cyberharcèlement.

Il convient en outre de ne pas placer de *trop hautes attentes dans une telle disposition*. La variété des comportements incriminés (*actes hétéroclites*) complique la recherche d'une formulation qui respecte le *principe de précision* et soit praticable. Il est par ailleurs peu probable que cette nouvelle norme facilite *l'administration des preuves*. En effet, les actes répétés, prérequis d'une infraction de cyberharcèlement, et les éléments subjectifs devraient être prouvés individuellement. Or, les éléments constitutifs de l'infraction qui laissent une grande marge d'interprétation (et sont donc délicats à appliquer face au principe de précision) sont difficiles à prouver. Il ne faut pas non plus s'attendre à ce que la disposition produise un grand *effet de prévention générale négative*, c'est-à-dire un effet dissuasif, étant donné que l'important est uniquement qu'un comportement soit sanctionné par le droit pénal (que ce soit au titre des infractions existantes ou d'une disposition spécifique). La doctrine se prononce également contre une infraction spécifique[259].

Quant aux autres *atteintes numériques à la personnalité*, le seul comportement non punissable concerne la *diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes.* Les dispositions actuelles ne sanctionnent pas toujours la diffusion de photos ou de vidéos embarrassantes, truquées ou indécentes, notamment si *leur contenu n'est pas pornographique* (art. 197 CP), que les circonstances ne permettent *pas de déduire une atteinte à l'honneur* (art. 173 ss CP) et qu'elles ne fixent pas sur un support d'images, sans le consentement de la personne concernée, des faits qui relèvent du domaine secret de celle-ci ou des faits ne pouvant être perçus sans autre par chacun et qui relèvent de son domaine privé (art. 179^{quater}, al. 3, CP). Il serait envisageable de punir ce type de comportement (dès lors qu'il paraît pénalement répréhensible et que les normes civiles visant la protection de la personnalité sont jugées insuffisantes), soit par une disposition spécifique (et technologiquement neutre), soit au titre de variante d'une infraction de harcèlement. À l'inverse de l'infraction proposée par le Conseil des États dans le cadre de la *révision du droit pénal en matière sexuelle* (transmission indue d'un contenu non public à caractère sexuel, art. 197*a* P-CP), une éventuelle nouvelle disposition ne devrait *pas être limitée aux contenus à caractère sexuel*, mais devrait couvrir les *autres images compromettantes*. De plus, elle serait à classer non pas parmi les infractions contre l'intégrité sexuelle, mais parmi les infractions contre l'honneur et contre le domaine secret ou le domaine privé (livre 2, titre 3, CP).

5.2 Application du droit

N'oublions pas que les dispositions matérielles, qu'elles soient nouvelles ou déjà en vigueur, ne peuvent produire d'effet que si le droit pénal est applicable. L'*application du*

[257] ATF 129 IV 262, 265 ss ; 141 IV 437, 441

[258] Arrêt du TF 6B_75/2009 du 2 juin 2009, consid. 3.2.1 ; ATF 126 IV 219

[259] WENK suggère toutefois des adaptations ponctuelles. Il estime ainsi que les délits contre l'honneur pourraient être complétés par un alinéa augmentant la peine si l'acte a été commis par l'intermédiaire des TIC et visible par un grand nombre de personnes : WENK, 95.

droit aux infractions commises par les TIC est difficile, voire tout bonnement impossible. Les délits d'expression sur Internet sont souvent commis *sous couvert d'anonymat*, ce qui conditionne l'identification de l'auteur et des éléments constitutifs de l'infraction à l'obtention de preuves sous forme de données fréquemment stockées à l'étranger. Leur mise en sûreté est donc complexe techniquement et juridiquement.

Une amélioration significative en la matière a déjà été réalisée avec la *règle de la future LPD* qui oblige les responsables du traitement privés sis à l'étranger à désigner un *représentant en Suisse* lorsqu'ils traitent des données personnelles concernant des personnes en Suisse et que ce traitement remplit certaines conditions (art. 14 s. nLPD). Cette disposition facilitera la prise de contact directe avec les exploitants de plateformes en ligne, notamment pour exiger l'effacement de contenus portant atteinte à l'honneur.

Le Conseil fédéral étudie en outre la nécessité d'agir pour améliorer l'application du droit dans le cadre du *postulat 21.3450 de la CPS-E « Discours de haine. La législation présente-t-elle des lacunes ? »* et d'une *note de discussion indiquant si et comment les plateformes de communication doivent être réglementées*. La problématique de l'application du droit n'appelle donc pas davantage de nouvelles mesures : les travaux d'analyse et d'amélioration de la situation sont déjà en cours.

6 Bibliographie et travaux préparatoires

Bibliographie

AEPLI MICHAEL, Die Sicherstellung von elektronisch gespeicherten Daten, Zurich/Bâle/Genève 2004 (cit. AEPLI)

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht: unter vergleichender Berücksichtigung der StPO, Zurich 2014 (cit. BANGERTER)

BAUER SEBASTIAN, Soziale Netzwerke und strafprozessuale Ermittlungen, Berlin 2018 (cit. BAUER)

BOMMER FELIX, Löschung als Einziehung von Daten, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG FLORIAN S. (Éd.), Internet-Recht und Strafrecht, Bern 2005, 172 s. et 178 s. (cit. BOMMER)

BOMMER FELIX/GOLDSCHMID PETER, in: NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196–457 StPO, 2e éd., Bâle 2014, Art. 263 StPO (cit. BOMMER/GOLDSCHMID, BSK StPO II, Art. 263)

BRUN MARCEL, Cyberbullying – aus strafrechtlicher Sicht, recht 2016, 100 ss (cit. BRUN)

CAMPBELL MARILYN/BAUMAN SHERI, Cyberbullying: Definition, consequences, prevalence, in : Reducing Cyberbullying in Schools, 2018, 3 ss (cit. CAMPBELL/BAUMAN)

DELNON VERA/RÜDY BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 180 StGB (cit. DELNON/RÜDY, BSK II StGB, Art. 180)

DELNON VERA/RÜDY BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 181 StGB (cit. DELNON/RÜDY, BSK II StGB, Art. 181)

DODGE WILLIAM S., International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, 2071 ss

DONATSCH ANDREAS, Strafrecht III, 11e éd., Zurich 2018 (cit. DONATSCH)

FRASCH DENNIS, Cybermobbing ohne Konsequenzen – warum Straftäter der Justiz oft entkommen, www.watson.ch > Digital (cit. FRASCH)

GRAF DAMIAN K., Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, in: Jusletter IT du 21 septembre 2017 (cit. GRAF)

HANSJAKOB THOMAS, Was ist GovWare?, Jusletter du 11 septembre 2017 (cit. HANSJAKOB)

HANSJAKOB THOMAS, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 du 16 décembre 2016, in: forum poenale 2017, 252 ss (cit. HANSJAKOB BGer 6B_656/2015)

HUSMANN MARKUS, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht II, Art. 137–392 StGB, 4e éd., Bâle 2019, Art. 271 StGB (cit. HUSMANN, BSK StGB II, Art. 271)

IHWAS SALEH RAMADAN, Strafverfolgung in sozialen Netzwerken, Baden-Baden 2014 (cit. IHWAS)

ISENRING BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht II, Art. 137–392 StGB, 4e éd., Bâle 2019, Art. 198 StGB (cit. ISENRING, BSK StGB II, Art. 198)

KINZIG JÖRG, Die Strafbarkeit von Stalking in Deutschland – Vorbild für die Schweiz?, in: recht 2011, 1 ss (cit. KINZIG)

KUNZ HAENNES, ZEPRA Prävention und Gesundheitsförderung, Mobbing in der Schule, Saint-Gall 2016, ch. 1.2, in: Sicher! Gsund!, abrufbar unter www.sichergsund.ch > Themen > Mobbing in der Schule (cit. KUNZ)

POPP PETER/BERKEMEIER ANNE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 1 StGB (cit. POPP/BERKEMEIER, BSK StGB I, Art. 1)

POPP PETER/KESHELAVA TORNIKE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Vor Art. 3 StGB (cit. POPP/KESHELAVA, BSK StGB I, Vor Art. 3)

PREUSS TAMINA, Erforderlichkeit der Kriminalisierung des Cybermobbings – Sinnvolle Schliessung einer Gesetzeslücke oder blosses Symbolstrafrecht?, KriPoZ 2/2019, 97 ss (cit. PREUSS)

RAMEL RAFFAEL/VOGELSANG ANDRÉ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 179septies StGB (cit. RAMEL/VOGELSANG, BSK II StGB, Art. 179septies)

RIKLIN FRANZ, Der Straf- und zivilrechtliche Ehrenschutz im Vergleich, ZStrR 1983, 29 ss (cit. RIKLIN)

RIKLIN FRANZ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Vor Art. 173 StGB (cit. RIKLIN, BSK II StGB, Vor Art. 173)

RIKLIN FRANZ, NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 177 StGB (cit. RIKLIN, BSK II StGB, Art. 177 StGB)

SELMAN/SIMMLER, Shitstorm – strafrechliche Dimension eines neuen Phänomens, ZStrR 136 (2018), 228 ss (cit. SELMAN/SIMMLER)

SALMINA EDY, Der Preis der Ehre, forumpoenale 3/2020, 215 ss (cit. SELMINA)

SCHMID NIKLAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im Allgemeinen, Schweizerische Zeitschrift für Strafrecht (ZStrR) 1993, 81 ss (cit. SCHMID)

SCHWAIBOLD MATTHIAS, Warum «Twitter» kein Medium im Sinne des Strafrechts ist, sui generis 2017, 113 ss (cit. SCHWAIBOLD)

SIEBER ULRICH/NEUBERT CARL-WENDELIN, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty, in: LACHENMANN FRAUKE/RÖDER TILLMANN/WOLFRUM RÜDIGER (Éd.), Max Planck Yearbook of United Nations Law, Volume 20 (2016), Leiden/Boston 2017, 249 ss (cit. SIEBER/NEUBERT)

SMAHEL DAVID/MACHACKOVA HANA/MASCHERONI GIOVANNA/DEDKOVA LENKA/STAKSRUD ELISABETH/ÓLAFSSON KJARTAN/LIVINGSTONE SONIA/HASEBRINK UWE, 2020, EU Kids Online 2020, Survey results from 19 countries, 2020, sous : www.eukidsonline.ch > Internationaler Ergebnisbericht (cit. SMAHEL/MACHACKOVA/MASCHERONI/DEDKOVA/STAKSRUD/ÓLAFSSON/LIVINGSTONE/HASEBRINK)

STRATENWERTH GÜNTER, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 4e éd., Berne 2011 (cit. STRATENWERTH, AT I)

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8e éd., Berne 2022 (cit. STRATENWERTH/BOMMER, BT I)

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7e éd., Berne 2013 (cit. STRATENWERTH/JENNY/BOMMER, BT II)

THORMANN OLIVIER/BRECHBÜHL BEAT, in: NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196–457 StPO, 2e éd., Bâle 2014, Art. 248 (cit.THORMANN/BRECHBÜHL, BSK StPO II)

TRECHSEL STEFAN/JEAN-RICHARD-DIT-BRESSEL MARC, Praxiskommentar Schweizerisches Strafgesetzbuch, Zurich/Saint-Gall 2018, Art. 28 StGB (cit. TRECHSEL/JEAN-RICHARD, PK StGB, Art. 28)

TRECHSEL STEFAN/LEHMKUHL MARIANNE JOHANNA in: TRECHSEL STEFAN/PIETH MARK (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4e éd., Zurich/ Saint-Gall 2021, Vor Art. 173 StGB (cit. TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173)

TRECHSEL STEFAN/FINGERHUTH, in: TRECHSEL STEFAN/PIETH MARK (Éd.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2e éd., Zurich/Saint-Gall 2013, Art. 181 StGB (cit. TRECHSEL/FINGERHUTH, PK StGB, Art. 181)

WEISSENBERGER PHILIPPE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 156 StGB (cit. WEISSENBERGER, BSK II, Art. 156)

WENK JAN, #opfer, Bedarf es eines Cybermobbing-Tatbestands?, recht 2021, 88 ss (cit. WENK)

WICKER MAGDA, Cloud Computing und staatlicher Strafanspruch, Baden-Baden 2016 (cit. WICKER)

ZELLER FRANZ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Éd.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4e éd., Bâle 2019, Art. 28 StGB (cit. Zeller, BSK StGB I, Art. 28)

Compléter le code pénal par des dispositions relatives au cyberharcèlement

Travaux préparatoires

Protection contre la cyberintimidation, rapport du Conseil fédéral du 26 mai 2010 en réponse au postulat Schmid-Federer 08.3050, www.fedpol.admin.ch > Actualité > Cyberintimidation (cit. *rapport cyberintimidation*)

FF **2010** 4275, Message du 18 juin 2010 relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité

FF **2013** 2379, Message du 27 février 2013 concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

Cadre juridique pour les médias sociaux, rapport du Conseil fédéral du 9 octobre 2013 en réponse au postulat Amherd 11.3912 « Donnons un cadre juridique aux médias sociaux » du 29 septembre 2011, www.ofcom.admin.ch > Numérisation et Internet > Communication numérique > Intermédiaires et plateformes de communication > Cadre juridique pour les médias sociaux (cit. *rapport postulat médias sociaux 2013*)

La responsabilité civile des fournisseurs de services Internet, rapport du 11 décembre 2015, www.ofj.admin.ch > Publications et services > Rapports, avis de droit et décisions > Rapports et avis de droit > La responsabilité civile des fournisseurs de services Internet (cit. *rapport « La responsabilité civile des fournisseurs de services Internet »*)

FF **2017** 163, Message du 2 décembre 2016 concernant l'approbation de la convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (convention d'Istanbul)

Rapport complémentaire du Conseil fédéral du 10 mai 2017 sur le postulat Amherd 11.3912 « Donnons un cadre juridique aux médias sociaux » du 29 septembre 2011, www.ofcom.admin.ch > Numérisation et Internet > Communication numérique > Intermédiaires et plateformes de communication > Cadre juridique pour les médias sociaux (cit. *rapport complémentaire médias sociaux 2017*)

FF **2017** 6185, Message du 6 septembre 2017 concernant la révision de la loi sur les télécommunications

FF **2017** 6565, Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales

FF **2017** 6913, Message du 11 octobre 2017 concernant la loi fédérale sur l'amélioration de la protection des victimes de violence

FF **2018** 559, Message du 22 novembre 2017 relatif à la modification de la loi sur le droit d'auteur, à l'approbation de deux traités de l'Organisation Mondiale de la Propriété Intellectuelle et à leur mise en œuvre

FF **2018** 2889, Message du 25 avril 2018 concernant la loi fédérale sur l'harmonisation des peines et la loi fédérale sur l'adaptation du droit pénal accessoire au droit des sanctions modifié

Rapport de l'Office fédéral de la justice du 12 avril 2019 sur la question de la codification de l'infraction de « harcèlement », www.parlement.ch > Objet 19.433 (cit. *Rapport OFJ stalking*)

FF **2020** 7397, Loi fédérale du 25 septembre 2020 sur la protection des données (LPD)

Loi fédérale portant révision du droit pénal en matière sexuelle. Rapport du 8 août 2021 sur les résultats de la consultation, www.parlement.ch > Objet 18.043 > Consultation pour projet 3 > Les résultats de la consultation (cit. *Rapport consultation droit pénal en matière sexuelle*)

Rapport de l'Office fédéral de la communication du 17 novembre 2021, Intermédiaires et plateformes de communication. Effets sur la communication publique et approches de gouvernance, www.ofcom.admin.ch > Numérisation et Internet > Communication

numérique > Intermédiaires et plateformes de communication (cit. *Rapport OFCOM Intermédiaires et plateformes de communication*)

Rapport de l'Office fédéral de la justice du 17 septembre 2021 sur le US CLOUD Act, www.ofj.admin.ch > Page d'accueil > Publications & services > Rapports, avis de droit et décisions > Rapports et avis de droit (cit. *Rapport OFJ US CLOUD Act*)

FF **2021** 2997, Loi fédérale du 17 décembre 2021 sur l'harmonisation des peines

FF **2022** 687, Loi fédérale portant révision du droit pénal en matière sexuelle. Rapport de la Commission des affaires juridiques du Conseil des États du 17 février 2022

FF **2022** 1011, Harmonisation des peines et adaptation du droit pénal accessoire au nouveau droit des sanctions. Projet 3 : loi fédérale portant révision du droit pénal en matière sexuelle. Rapport du 17 février 2022 de la Commission des affaires juridiques du Conseil des États. Avis du Conseil fédéral du 13 avril 2022