Collection lausannoise
CEDIDAC

Camille Perrier Depeursinge / Sylvain Métille /
Joëlle Vuille (éditeurs)

Lutter contre la cybercriminalité en Suisse

Stämpfli
Éditions

Avant-propos

L'avènement puis l'omniprésence des technologies de l'information et de la communication depuis la fin du XX^{e} siècle ont engendré de nouvelles possibilités de commettre des infractions. Comme l'expose **Nora Markwalder**, Internet a grandement facilité le passage à l'acte, en créant de nouvelles opportunités pour les cybercriminels, ce que démontrent clairement tant les statistiques officielles de la délinquance que les sondages de victimisation. Concernant précisément les victimes, **Stefano Caneppele** rappelle les diverses théories avancées dans le domaine de la criminologie pour expliquer la victimisation et les confronte à la réalité de la cybercriminalité. On constate que la mesure du phénomène est particulièrement complexe. En outre, il semblerait que les comportements des victimes dans l'utilisation d'Internet et, plus généralement, des technologies de l'information et de la communication (choix et changement de mots de passe, par exemple), n'aient qu'une influence modérée sur le risque de victimisation. Toutefois, la résistance s'organise et, à mesure que l'on comprend mieux le phénomène, la prévention s'améliore et l'on colmate les brèches qui facilitent le passage à l'acte.

Le droit pénal s'adapte également. Alors qu'une première vague de modifications législatives concernait surtout la criminalité économique, le Parlement semble depuis quelque temps s'intéresser également aux infractions contre la liberté, l'intégrité sexuelle ou le domaine privé, commises sur Internet ou par le biais des technologies de l'information et de la communication. **Joëlle Vuille, Camille Perrier Depeursinge et Justine Arnal** analysent la portée de ces nouvelles dispositions, en pointant en particulier leurs lacunes et difficultés d'application.

L'adaptation de la législation pénale n'est toutefois pas suffisante ; encore faut-il pouvoir l'appliquer et ainsi identifier et poursuivre les cybercriminels. **Olivier Ribaux et Thomas Souvignet** présentent le développement exponentiel de la cybercriminalité et démontrent la nécessité de re-penser fondamentalement les mesures de lutte à disposition des autorités. Bien que de nombreux efforts de formation soient relevés, les auteurs plaident pour une plus grande adaptabilité des acteurs, ce qui passe par l'interdisciplinarité. Ces enjeux sont clairement exposés par **Julien Cartier**, qui développe au moyen d'exemples très concrets ce qu'implique la poursuite des cybercriminels au quotidien, avec ses succès mais aussi ses limites.

De surcroît, le caractère éminemment transnational de la cybercriminalité impose une meilleure collaboration entre les autorités de poursuite des différents États, et ainsi des procédures d'entraide pénale internationale, afin en particulier d'avoir accès aux preuves numériques. **Maria Ludwiczak Glassey** expose

comment les États-Unis et l'Union Européenne ont répondu à ces enjeux et discerne de nombreuses pistes d'améliorations possibles pour le législateur et les autorités pénales suisses.

Pour conclure, **Sylvain Métille et Pauline Meyer** présentent comment, en étant conscients des raisons pour lesquelles les technologies de l'information et de la communication facilitent la criminalité, on peut repenser les cadres juridiques pour diminuer l'intérêt à commettre ces infractions. Ils mettent ainsi en lumière les insuffisances du droit pénal, pour mieux s'intéresser aux différents actes législatifs qui garantissent, soit directement, soit de façon détournée, la cybersécurité. Enfin, ces auteurs rappellent qu'au-delà du cadre législatif, l'éducation et la sensibilisation du public contribuent grandement à lutter contre la cybercriminalité.

Nous remercions chaleureusement les auteurs qui ont contribué à cet ouvrage, ainsi que Anastasia Leu et Axelle Baillargues, respectivement assistante doctorante et assistante étudiante au CEDIDAC, pour leur relecture attentive et la mise en forme du présent manuscrit.

Sommaire

Table des principales abréviations

AFIS	*Automatic Fingerprint Identification Systems*
al.	alinéa
AP-[*abréviation loi*]	Avant-projet
Art.	Article
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BATT	Brigade d'analyse des traces technologiques
BB	*Botschaft zum Bundesgesetz*
BFEG	Bureau fédéral de l'égalité entre femmes et hommes
BO	Bulletin officiel
BSK	*Basler Kommentar*
c./consid.	considérant(s)
c.-à-d.	c'est-à-dire
CAJ	Commission des affaires juridiques
CC	Code civil suisse du 10 décembre 1907 (CC), RS 210
CCC	Centre de Compétence Cyber
CCC	Convention sur la cybercriminalité du 23 novembre 2001 (CCC), RS 0.311.43
CCPC RBT	Conférence des commandants des polices cantonales de Romandie, Berne et Tessin
CE	Conseil des États
ch.	chiffre
CHF	Franc(s) suisse(s)
CICOP	Concept intercantonal de coordination opérationnelle et préventive
CLDJP	Conférence latine des chefs de départements de justice et police
CLOUD	*Clarifying Lawful Overseas Use of Data*
CN	Conseil national
CourEDH	Cour européenne des droits de l'Homme
CP/CPS	Code pénal suisse du 21 décembre 1937 (CP), RS 311.0
CPP	Code de procédure pénale suisse du 5 octobre 2007 (CPP), RS 312.0
CR	Commentaire romand
CSN	Cyberstratégie nationale

DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEJI	Demande d'entraide judiciaire internationale
DFJP	Département fédéral de justice et police
Dr	Docteur
E-[*abréviation loi*]	*Entwurf*
e.g.	*exempli gratia*
Éd.	Editeur/édition (selon le contexte)
Eds	Editeurs
ég.	également
EIZ	*Europa Institut an der Universität Zürich*
env.	environ
EPOC	*European Production Order Certificate*
ESC	Ecole des Sciences Criminelles
et al.	*et alii*
etc.	*et cetera*
EURODAC	*European Dactylographic System*
Europol	*European Union Agency for Law Enforcement Cooperation*
FDCA	Faculté de droit, des sciences criminelles et d'administration publique
Fedpol	Office fédérale de la police
FF	Feuille fédérale
Fig.	Figure
FNS	Fonds national suisse
GE	Genève
HEC	Hautes études commerciales
i.e.	*id est*
i.f.	*in fine*
ICVS	*International Crime Victims Survey*
Intro.	Introduction
IOCTA	*Internet Organised Crime Threat Assessment*
IRL	*In real life*
ISG	*Bundesgesetz vom 18 Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), SR 128*
IT	*Information technology*

iur.	en droit
J-CAT	*Joint Cybercrime Action Taskforce*
JdT	Journal des Tribunaux
JO	Journal officiel de l'Union européenne
LApEl	Loi du 15 juillet 2007 sur l'approvisionnement en électricité (LApEl), RS 734.7
let.	lettre
lit.	*littera*
LOGA	Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA), RS 172.010
LPD	Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), RS 235.1
LSCPT	Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT), RS 780.1
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI), RS 128
LSI2	Modification du 29 septembre 2023 de la Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération
LTC	Loi du 30 avril 1997 sur les télécommunications (LTC), RS 784.10.
M.	Monsieur
MROS	Bureau de Communication en matière de blanchiment d'argent
n-[*abréviation loi*]	nouveau
N°	Numéro
NCMEC	*National Center for Missing & Exploited Children*
NCSC	*National Cyber Security Centre*
ndlr.	Note de la rédaction
NIR	*Near Infrared*
ODI	Ordonnance sur les noms de domaines du 5 novembre 2014 (ODI), RS 784.104.2
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFAS	Office fédéral des assurances sociales
OFCS	Office fédéral de la cybersécurité
OFJ	Office fédéral de la justice
OFS	Office fédérale de la statistique

OK CCC	*Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention)*
OME-SCPT	Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017 (OME-SCPT), RS 780.117.
OPDo	Ordonnance du 31 août 2022 sur la protection des données (OPDo), RS 235.11
OSI	Ordonnance du 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (OSI), RS 128.1.
OSINF	*Open-source information*
OST	Ordonnance du 1er avril 2007 sur les services de télécommunication (OST), RS 784.101.1.
p./par ex.	par exemple
p./pp.	page(s)/plusieurs pages
par.	paragraphe
PFPDT	Préposé fédéral à la protection des données et à la transparence
PICSEL	Plateforme d'informations de la criminalité sérielle en ligne
PJA	Pratique juridique actuelle
PNR	Programmes nationaux de recherche
POHA	*Protection from Harassment Act*
PSC	Prévention Suisse de la Criminalité
RGPD	Règlement général sur la protection des données
RO	Recueil officiel
RPS	Revue Pénale Suisse
RR-COMP	*Recht relevant für Compliance Officers*
RS	Recueil systématique
RSJ	Revue suisse de jurisprudence
RTS	Radio télévision suisse
S-U-P-E-R	Sauvegarder, Utiliser, Protéger, Équiper, Réduire
s./ss	suivant(e)/et suivant(e)(s)
SCPT	Service Surveillance de la correspondance par poste et télécommunication
Sec.	*Section*
SG	Secrétariat général
SIENA	*Secure Information Exchange Network Application*

SIS	Système d'Information Schengen
SLTD	*Stolen and Lost Travel Documents*
SNCP	Stratégie nationale de protection de la Suisse contre les cyberrisques
SPC	Statistique policière de la criminalité
SR	*Systematische Sammlung des Bundesrechts*
STCE	Série des Traités du Conseil de l'Europe
StGB	*Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0*
TAF	Tribunal administratif fédéral
TC	Tribunal cantonal
TIC	Technologies de l'information et de la communication
TMC	Tribunal des mesures de contrainte
TPF	Tribunal pénal fédéral
trad.	traduit/traduction
U.S.	*United States*
U.S.C	*United States Code*
UE	Union européenne
UEL	*University of East London*
V.	Voir
Vol.	Volume
vs	*versus*
ZG	Zoug
ZHAW	*Zürcher Hochschule für Angewandte Wissenschaften*

Internet et facilitation du passage à l'acte

NORA MARKWALDER
Professeure ordinaire de droit pénal, procédure pénale et criminologie
Faculté de droit/Centre de Droit Pénal et Criminologie, Université de Saint-Gall

Table des matières

I. Introduction

La numérisation a changé nos vies et nos routines : nous achetons en ligne, nous échangeons sur les médias sociaux et nous passons une grande partie de notre temps libre de même que notre temps de travail dans l'espace numérique. En effet, 96% de la population suisse utilise Internet, ce qui réduit le groupe de personnes sans accès Internet à un groupe marginal[1]. Pourtant, une évolution sociétale comme la numérisation crée non seulement des

[1] STATISTA, Utilisation de l'Internet au moins une fois par semaine en Suisse entre 2005 jusqu'à 2021, disponible sous : <https://de.statista.com/statistik/daten/studie/435371/umfrage/internetnutzung-in-der-schweiz/> (*consulté le 13.12.2023*).

opportunités nouvelles pour nous faciliter la vie, mais offre également de nouvelles opportunités aux criminels pour commettre des délits. Cette contribution s'intéresse donc à l'évolution de la criminalité dans l'espace numérique et à la facilitation que présente Internet pour le passage à l'acte.

Nous commencerons par des fondements théoriques (partie II) qui peuvent servir d'explication à la manière dont Internet peut faciliter le passage à l'acte. Ensuite, nous analyserons la criminalité numérique par biais des statistiques policières et celui des données des sondages de victimisation pour couvrir le chiffre noir (partie III). Nous terminerons enfin par une conclusion (partie IV).

II. Explications théoriques

Comme constaté auparavant, la numérisation influence nos modes de vie. Elle constitue donc un facteur situationnel dans l'explication de la criminalité, car elle change l'environnement dans lequel la criminalité a lieu. Ce sont donc deux théories dites « situationnelles » qui sont utilisées ici pour expliquer l'influence de la numérisation sur la criminalité.

A. La théorie des brèches

La théorie des brèches vise à expliquer des effets de déplacement et de changement de la criminalité sur un macro-niveau[2]. Selon cette théorie, une invention ou une nouvelle technologie comme la numérisation crée de nouvelles failles de sécurité (appelées « brèches ») que les criminels exploitent tant qu'elles ne sont pas comblées par de nouvelles méthodes de sécurisation[3]. On peut penser par exemple à toutes les informations commerciales et données sensibles que les entreprises ne conservent plus par écrit aujourd'hui, mais qu'elles enregistrent et conservent sous forme électronique, ce qui ouvre la porte à des cyberattaques sur ces informations. C'est pourquoi cette « brèche de sécurité » ne peut être comblée que si ces informations sensibles sont protégées par un dispositif de cybersécurité approprié, ce qui rend indispensable une mise à niveau des entreprises dans ce domaine.

2 KILLIAS, p. 11 ss.
3 KILLIAS, p. 11 s.

B. La théorie des activités routinières

Au niveau du comportement individuel, l'exploitation de nouvelles structures d'opportunité peut s'expliquer par l'approche des activités routinières (« *Routine Activities Theory* »)[4]. Selon cette théorie, nos habitudes de vie quotidiennes déterminent notre risque de devenir victime d'un délit. Un délit est donc commis au moment où un auteur motivé rencontre une cible attrayante et que celle-ci n'est pas (suffisamment) protégée[5]. Internet et la numérisation offrent ainsi de nouvelles occasions de commettre des délits pour les auteurs, de même que des cibles attrayantes qui ne sont souvent pas suffisamment protégés – pensons par exemple aux possibilités de contacter un nombre conséquent de personnes par Internet pour les convaincre d'investir dans des produits financiers douteux ou non-existants (souvent aussi à l'aide de pages Internet fictives). La numérisation a donc multiplié les opportunités sur Internet, et la question se pose maintenant de savoir (a) si les auteurs adaptent leur *modus operandi* à ce nouveau monde numérique – ce qui entraînera un déplacement des délits vers le cyberespace – ou (b) si une nouvelle catégorie d'auteurs se sont spécialisés dans le cyberespace, ce qui mènera à une augmentation de la criminalité en général. Étant donné que l'on constate plutôt un recul général de la criminalité depuis une vingtaine d'années, la première hypothèse semble plus plausible. Certains auteurs postulent même que ce recul général de la criminalité est dû au fait que des délits ont été déplacés vers l'espace en ligne et que ces délits déplacés n'ont pas été correctement saisis par les statistiques officielles de la criminalité – de sorte que le « *Crime Drop* » peut s'expliquer, du moins en partie, par un « *Crime Recording Flop* » en ce qui concerne les cyberdélits[6].

C. Approche situationnelle et prévention

Les explications situationnelles ont l'avantage de très bien se prêter à la prévention, car elles considèrent que le crime est influencé par des éléments en dehors du facteur humain[7]. La prévention situationnelle vise donc à réduire les occasions de commettre des délits, et ceci par différentes interventions. D'abord, par voie de prévention situationnelle, on peut réduire le nombre de cibles disponibles ou rendre ces cibles plus difficiles à atteindre (augmenter l'effort nécessaire pour commettre l'infraction)[8] : par exemple, en installant des

4 Voir COHEN/FELSON, p. 588 ss.
5 COHEN/FELSON, p. 598.
6 CANEPPELE/AEBI, p. 75 s.
7 KILLIAS *et al.*, Criminologie, p. 278.
8 HOUGH/CLARKE/MAYHEW, p. 5 s.; KILLIAS *et al.*, Criminologie, p. 278.

meilleurs systèmes de cybersécurité, il est plus difficile d'accéder à des données sécurisées, ce qui augmente l'effort chez les auteurs potentiels puisqu'ils ont besoin des meilleures compétences en matière de piratage. De plus, ces cibles peuvent être rendues moins attrayantes, de sorte à réduire le « gain » issu du délit (réduire les récompenses) : par exemple, si les cartes de crédit sont immédiatement bloquées lorsqu'elles sont utilisées dans une transaction en ligne suspecte, l'attrait d'un tel vol de données est considérablement réduit[9]. La prévention situationnelle peut également augmenter les risques de commettre un délit au travers d'une meilleure protection ou surveillance de la cible (augmenter les risques) : si la police surveille par exemple certains marchés illégaux sur le Darknet, cela augmente le risque d'être démasqué en cas d'achat ou de commerce illégal – même si l'anonymat sur Internet réduit bien sûr considérablement les risques encourus par les délinquants, ce qui constitue un aspect situationnel en faveur des auteurs de délits[10].

III. La cybercriminalité en chiffres

A. Comment mesurer la criminalité numérique

Puisqu'il s'agit d'un phénomène social relativement nouveau, la criminalité dans l'espace numérique n'est pas toujours facile à détecter et à mesurer. En criminologie, les statistiques officielles telles que les statistiques policières de la criminalité, les statistiques sur les jugements ou les statistiques sur l'exécution des peines sont le plus souvent utilisées pour mesurer l'étendue et l'évolution de la criminalité. Les statistiques se prêtent particulièrement bien à l'observation de l'évolution de la criminalité lorsqu'elles remontent à une période déjà assez longue et qu'elles sont mises à jour chaque année. Pour que ces statistiques soient valides, il faut toutefois que la méthode d'enregistrement de ces délits ne change pas au fil du temps[11]. Un inconvénient majeur des statistiques de la criminalité réside dans le fait qu'elles ne portent que sur les délits rapportés à la police (ou détectés par elle) et ne peuvent donc pas fournir d'informations sur l'ampleur réelle, à savoir le chiffre noir, de la criminalité[12]. De plus, l'enregistrement se base sur la définition légale des délits et non sur des phénomènes sociaux ou une typologie de comportements répréhensibles, raison pour laquelle il n'est pas mentionné pour la plupart des délits s'ils ont été commis sur Internet ou non. Pour permettre cette distinction, il a fallu inclure une catégorisation spéciale de délits commis par mode opératoire hors ligne ou

9 HOUGH/CLARKE/MAYHEW, p. 7 ; KILLIAS *et al.*, Criminologie, p. 279.
10 HOUGH/CLARKE/MAYHEW, p. 7 s.; KILLIAS *et al.*, Criminologie, p. 279.
11 KILLIAS *et al.*, Criminologie, p. 48 s.
12 KILLIAS *et al.*, Criminologie, p. 93.

en ligne, ce qui a été introduit en 2020 par l'Office fédéral de la Statistique (ci-après : OFS) sous le terme « criminalité numérique »[13]. Avant cette date, il n'était malheureusement pas possible d'observer l'étendue et l'évolution des délits commis sur Internet. Par conséquent, les statistiques ne permettent guère d'observer l'ampleur totale du déplacement des délits vers le cyberespace, car ces statistiques différenciées ne remontent pas assez dans le temps pour permettre une telle analyse.

De plus, pour mesurer le chiffre noir de la délinquance, il est nécessaire de réaliser des sondages de victimisation qui, au moyen d'un échantillon de population représentatif d'une certaine région ou d'un certain pays, interrogent la population générale sur son expérience en matière de victimisation. De telles enquêtes de victimisation à l'échelle nationale existent depuis 1984/86 en Suisse et permettent donc d'observer l'évolution de la criminalité en incluant le chiffre noir au cours des dernières décennies[14]. Pour saisir également les nouvelles formes de délits commis à l'aide des moyens numériques, des « délits sur Internet » dans différents sondages de victimisation ont été inclus. Depuis 2011, en effet, ces questions existent dans le sondage national basé sur la méthodologie ICVS (« *International Crime Victims Survey* »)[15], mais également dans d'autres sondages à l'échelle locale ou nationale[16]. En revanche, le problème majeur de ces sondages est qu'ils utilisent des questionnaires non homogènes : les définitions des délits ou la période de victimisation saisie ne sont pas toujours identiques, ce qui rend les comparaisons entre les différentes études difficiles, voire impossibles[17].

B. Les statistiques officielles

1. La définition de la criminalité numérique dans les statistiques officielles

Comme indiqué dans la section précédente, l'OFS a introduit une catégorie dite de « criminalité numérique » dans les statistiques policières. Cette catégorie inclut l'ensemble des « infractions pénales commises sur les réseaux

---

13 Voir OFS, Criminalité numérique, disponible sous : <https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police/criminalite-numerique.html> (*consulté le 13.12.2023*).

14 MARKWALDER, p. 47 s.

15 KILLIAS *et al.*, Sondage ; BIBERSTEIN *et al.* ; BAIER *et al.* ; MARKWALDER *et al.*, Opfererfahrungen.

16 MILANI *et al.* ; BAIER.

17 Pour un aperçu des résultats, voir MARKWALDER, p. 58 s.

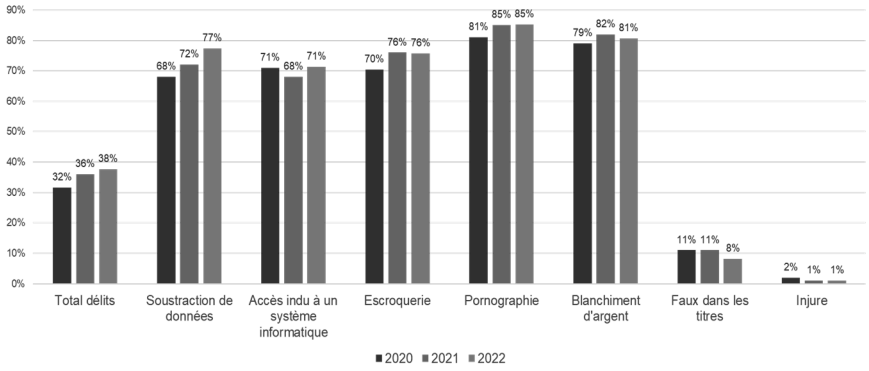
de télécommunication, en particulier Internet »[18]. Un délit est donc classé comme « numérique » si l'auteur a utilisé un *modus operandi* numérique pour agir. L'OFS distingue cinq catégories de délits numériques : (a) la cybercriminalité économique, (b) les cyberdélits sexuels, (c) les cyberatteintes à la réputation et pratiques déloyales, (d) le Darknet et (e) une catégorie résiduelle (autres)[19].

2. Le développement et la proportion des délits numériques

Si l'on analyse le développement de la criminalité numérique, on constate d'abord que la proportion des délits avec un mode opératoire dit numérique a augmenté chaque année depuis le premier enregistrement en 2020. La délinquance commise par des moyens numériques constitue à présent plus d'un tiers (à savoir 38%) de tous les délits enregistrés. Cependant, la proportion des délits numériques varie considérablement selon le type de délit : alors que le mode opératoire numérique semble être peu utilisé dans le domaine des faux dans le titre ou des délits contre l'honneur, il est répandu dans les délits numériques au sens étroit (par exemple, dans le cadre d'une soustraction de données ou d'un accès indu à un système informatique), ce qui semble logique considérant que ces infractions ont pour élément constitutif objectif la présence de données ou d'un système informatique. De plus, l'escroquerie, la pornographie et le blanchiment d'argent constituent des délits qui sont majoritairement commis à l'aide d'Internet aujourd'hui – la proportion de délits commis sur Internet étant de 76% dans les escroqueries, 85% pour la pornographie, et 81% pour les actes de blanchiment d'argent.

[18] OFS, Criminalité numérique, disponible sous : <https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police/criminalite-numerique.html> (*consulté le 13.12.2023*).

[19] OFS, Criminalité numérique, disponible sous : <https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police/criminalite-numerique.html> (*consulté le 13.12.2023*).



Graphique 1 : Proportion des délits commis avec un mode opératoire de criminalité numérique, en % (Source : OFS)

En ce qui concerne la typologie des délits numériques, on constate que la majorité des délits, à savoir 88%, a lieu dans un contexte de cybercriminalité économique. La majorité des cas de cybercriminalité économique se compose d'escroqueries commises en ligne (68%). Bien moins nombreux sont les cas de cyberdélits sexuels (8%) ou des cyberatteintes à la réputation et pratiques déloyales (4%). En plus, on constate que les cyberdélits sont en règle générale difficiles à élucider, car le taux d'élucidation se situe en moyenne à 36.4%. Les cyberdélits sexuels et les cyberatteintes à la réputation et pratiques déloyales semblent être élucidés de manière bien plus fréquente (voir Tableau 1) ; cela est probablement dû à une présélection des cas enregistrés. Il est probable en effet qu'il s'agisse majoritairement de cas dans lesquels on connaît déjà les auteurs qui seront poursuivis (et donc enregistrés par la police), ce qui amène à une surreprésentation de ces cas et donc une surestimation du taux d'élucidation. Ces chiffres montrent donc bien la difficulté à mesurer les cyberdélits avec les statistiques officielles : étant donné qu'un grand nombre de cas reste dans l'ombre, les résultats concernant la fréquence de certains délits de même que leur taux d'élucidation sont biaisés. C'est pour cette raison qu'il faut compléter les résultats des statistiques officielles avec d'autres données criminologiques pour élucider le chiffre noir.

	Infractions	Taux d'élucidation
Total criminalité numérique	**30 351**	**36,4%**
Cybercriminalité économique	26 671 (88%)	29,8%
dont cyberescroquerie	20 691 (68%)	31,3%
Cyberdélits sexuels	2 572 (8%)	92,9%
Cyberatteinte à la réputation et pratiques déloyales	1 103 (4%)	65,2%
Darknet	1 (0%)	100,0%
Autres (*Data Leaking*)	4 (0%)	25,0%

Tableau 1 : Catégories de cybercriminalité et taux d'élucidation, en % (Source : OFS)

C. Les sondages de victimisation

1. Les sondages sur les cyberdélits en Suisse

Comme indiqué plus haut, les statistiques officielles ne suffisent pas pour mesurer l'étendue et la nature réelle de la cybercriminalité, et on doit recourir aux sondages de victimisation pour saisir le chiffre noir de la délinquance. En ce qui concerne les cyberdélits, différents sondages ont été effectués en Suisse ces dernières années. À l'échelle nationale, les cyberdélits au sens au sens strict, à savoir les délits exclusivement commis sur Internet, ont été introduits dans le *Crime Survey* de 2011[20], et ont été également mesurés dans le sondage de 2015[21] et celui de 2021[22]. De plus, un autre sondage au niveau national a inclu des questions sur la victimisation des cyberdélits au sens strict ainsi que sur le *modus operandi* numérique de certains délits auparavant commis dans le monde analogique (cyberdélits au sens large)[23]. Au niveau

20 KILLIAS *et al.*, Sondage.
21 BIBERSTEIN *et al*.
22 BAIER *et al.*
23 BAIER.

local, un sondage portant sur la cybervictimisation a été conduit à Lugano, en incluant des questions sur les cyberdélits au sens strict et au sens large[24].

Le dernier sondage de victimisation à l'échelle nationale, appelé *Crime Survey*, a été conduit en 2022. Ce sondage représentatif de la population suisse s'est basé sur un échantillon de 40'601 personnes sollicitées, dont 15'519 ont rempli le questionnaire en ligne. Le taux de réponse était donc de 38.2%, ce qui constitue un très bon retour pour ce type de sondage[25]. Ce dernier portait sur la cybercriminalité au sens strict, le cyberharcèlement et les modes opératoires en ligne pour différents délits (cyberdélits au sens large). Il permet donc de mesurer différents types de cyberdélits en Suisse[26].

2. Les résultats du Crime Survey 2022

Combien de personnes en Suisse sont touchées par la criminalité numérique ? Selon les résultats du dernier sondage en 2022, 14.6% des personnes interrogées ont subi au moins un cyberdélit au sens strict au cours des cinq dernières années. C'est donc une proportion considérable de personnes qui ont été victimes de cybercriminalité. Les plus grandes catégories de délits subis sont (a) le piratage des comptes de médias sociaux ou comptes de messagerie (37.7%), (b) l'espionnage de données confidentielles par des courriels ou des sites Internet falsifiés (*phishing*) (26.7%) et (c) des attaques contre le compte bancaire en ligne ou l'utilisation frauduleuse de la carte de crédit/débit (22.2%). De manière plus réduite, nous trouvons les pertes ou corruptions de données dues à un virus, un cheval de Troie ou un ver informatique (14.5%) ou des attaques dites par hameçonnage (« *ransomware* ») (9.8%)[27]. Comparé au dernier sondage de victimisation conduit avec la même méthodologie qui a eu lieu en Suisse en 2015, on constate une nette augmentation de ce taux de victimisation : en 2015, seulement 6.6% des personnes ont indiqué avoir été victimes d'un cyberdélit au sens strict au cours des cinq dernières années[28].

En ce qui concerne les victimes de cyberdélits, le risque d'être victime ne varie guère en fonction des caractéristiques socio-démographiques. On ne peut donc pas discerner une caractéristique « typique » de gens qui ont été victimisés.[29] On constate pourtant que les personnes touchées par la cybercriminalité au sens strict étaient plus fréquentes dans le groupe d'âge des 37-57 ans, et que les

---

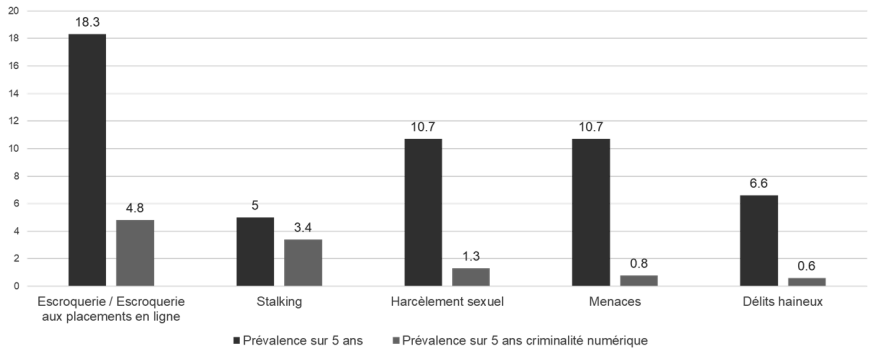
24 MILANI *et al*.
25 Pour plus d'informations sur la méthodologie du *Crime Survey* 2022, voir MARKWALDER *et al.*, Opfererfahrungen, p. 10 ss.
26 MARKWALDER *et al.*, Cybercrime, p. 4 ss.
27 MARKWALDER *et al.*, Cybercrime, p. 7 s.
28 BIBERSTEIN *et al.*, p. 18 s.
29 MARKWALDER *et al.*, Cybercrime, p. 8.

personnes appartenant à des groupes de revenus plus élevés ou ayant un niveau de formation plus élevé sont plus souvent victimes.[30] Ce résultat pourrait s'expliquer par le fait que ces personnes rapportent plus souvent les délits en question en raison de leur niveau de formation plus élevé ou parce qu'elles représentent, avec leur revenu plus élevé, des cibles plus attrayantes au sens de la théorie des activités routinières[31]. En plus, le taux de victimisation est plus élevé en Suisse romande qu'en Suisse alémanique et plus faible en Suisse italienne[32]. Le nombre de victimes qui ont indiqué avoir dénoncé le cyberdélit subi à la police est de 10%, ce qui démontre le chiffre noir significatif dans la cybercriminalité : seulement un délit sur dix est porté à l'attention de la police[33].

À côté des cyberdélits au sens strict, le *Crime Survey* 2022 permet aussi de mesurer si les délits auparavant commis dans le monde analogique sont maintenant commis à l'aide d'Internet (cyberdélits au sens large). En ce qui concerne le cyberharcèlement, 3% des personnes interrogées ont été victimes de ce comportement au moins une fois au cours des cinq dernières années[34]. De surcroît, on constate que la victimisation d'une escroquerie au placement en ligne (ou une tentative d'escroquerie au placement en ligne) est considérable : 4.8% des personnes sondées ont indiqué avoir été victimes d'une telle forme d'escroquerie, ce qui constitue presque un tiers des victimes d'escroquerie[35]. Cependant, le total de personnes victimes d'une escroquerie en ligne devrait être encore plus considérable si l'on considère d'autres formes d'escroqueries en ligne. Malheureusement, le lieu exact des délits d'escroquerie n'a pas été sondé dans le questionnaire de 2022, raison pour laquelle nous ne sommes pas en mesure de calculer le total des escroqueries en ligne.

À côté de l'escroquerie, le *stalking* ressort comme délit avec une part considérable de cybercriminalité. Ici, 3.4% des personnes sont devenues victimes de *cyberstalking*, ce qui constitue la majorité des victimes de *stalking*. Cependant, les autres délits comme le harcèlement sexuel, les menaces et les délits haineux sont majoritairement commis dans le monde analogique[36].

30 MARKWALDER *et al.*, Cybercrime, p. 8 s.
31 Pour les détails de la théorie des activités routinières voir chap. II.B.
32 MARKWALDER *et al.*, Cybercrime, p. 8 s.
33 MARKWALDER *et al.*, Cybercrime, p. 7.
34 MARKWALDER *et al.*, Cybercrime, p. 9.
35 MARKWALDER *et al.*, Cybercrime, p. 12 s.
36 MARKWALDER *et al.*, Cybercrime, p. 13.



Graphique 2 : Prévalence des victimisations subies dans les 5 dernières années, en % (Source : Crime Survey 2022)

IV. Conclusion

Même si les données actuelles sont encore insuffisantes pour démontrer un déplacement des délits vers l'espace numérique, on peut constater qu'Internet a bel et bien créé de nouvelles opportunités pour les criminels. Si l'on analyse la manière dont les délits sont commis aujourd'hui, on constate qu'un grand nombre – à savoir plus d'un tiers des délits enregistrés par la police – a été commis selon un *modus operandi* numérique. Internet facilite surtout la commission de certains délits spécifiques comme notamment l'escroquerie, le blanchiment d'argent ou la pornographie. Si on considère le chiffre noir de la criminalité numérique à l'aide des sondages de victimisation, on peut également constater que la population suisse est fortement touchée : le dernier sondage suisse démontre qu'une personne interrogée sur sept a fait état de victimisation liée à la cybercriminalité au sens strict, ce qui constitue une nette augmentation des expériences de victimisation par rapport au dernier sondage suisse de 2015. Pourtant, on constate aussi que le taux de dénonciation à la police des cyberdélits est, avec ses 10%, très faible, et donc que les statistiques officielles sous-estiment fortement l'étendue réelle du phénomène de la cybercriminalité et son impact sur la population suisse.

Au vu de l'étendue de la population affectée, les mesures de prévention semblent d'autant plus importantes. La prévention situationnelle, qui vise à réduire les occasions pour les délinquants de commettre des délits, semble être une approche prometteuse pour lutter contre la cybercriminalité. En protégeant mieux les victimes ou d'autres cibles sur Internet, par exemple au travers de campagnes d'information ou des mesures de cybersécurité, il pourrait être possible de rendre la commission d'un délit plus difficile. Une autre approche situationnelle serait d'augmenter la présence d'un « gardien », à savoir la police

ou d'autres systèmes de cyberprotection dans l'espace numérique. Même si le cyberespace ne peut pas être patrouillé de la même manière que l'espace public, une présence de la police pourrait réduire la vulnérabilité de certaines cibles et donc prévenir au moins une partie des délits numériques. En Suisse comme ailleurs, cette possibilité de prévention est déjà appliquée grâce à l'activité de services spécialisés en cybercriminalité de la police de même que du ministère public. L'avenir montrera dans quelle mesure un déplacement accru de la criminalité vers le cyberespace modifiera également l'activité et les efforts de prévention des autorités de poursuite pénale.

V. Bibliographie

Dirk BAIER, Kriminalitätsopfererfahrungen und Kriminalitätswahrnehmungen in der Schweiz: Ergebnisse einer Befragung, ZHAW, Zürich 2019 ; **Dirk BAIER/Lorenz BIBERSTEIN/Nora MARKWALDER**, Kriminalitätsopfererfahrungen der Schweizer Bevölkerung: Entwicklungen im Dunkelfeld 2011 bis 2021, ZHAW, Zürich 2022 (cité : BAYER *et al.*) ; **Lorenz BIBERSTEIN/Martin KILLIAS/Severin WALSER/Sandro IADANZA/Andrea PFAMMATER**, Sondage au sujet des expériences et opinions sur la criminalité en Suisse Analyses dans le cadre du sondage national de sécurité 2015, Killias Research & Consulting, Lenzburg 2016 (cité : BIBERSTEIN *et al.*) ; **Stefano CANEPPELE/Marcelo F. AEBI**, Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes, Policing: A Journal of Policy and Practice, vol. 13 (1), 2019, p. 66-79 ; **Lawrence E. COHEN/Marcus FELSON**, Social change and crime rate trends: A routine activity approach, American Sociological Review, vol. 44, 1979 ; **J.M. HOUGH, R.V.G. CLARKE/P. MAYHEW**, Introduction, *in* R.V.G. CLARKE/P. MAYHEW (éds), Designing out Crime, London H.M. Stationery Office, London 1980 ; **Martin KILLIAS**, Opening and Closing of Breaches: A Theory on Crime Waves, Law Creation and Crime Prevention, European Journal of Criminology, vol. 3 (1), 2006 ; **Martin KILLIAS/Marcelo F. AEBI/André KUHN**, Précis de criminologie, 4e éd., Berne 2019 (cité : KILLIAS *et al.*, Criminologie) ; **Martin KILLIAS/Silvia STAUBLI/Lorenz BIBERSTEIN/Matthias BÄNZIGER/Sandro IADANZA**, Sondage au sujet des expériences et opinions sur la criminalité en Suisse, Analyses dans le cadre du sondage national de victimisation 2011, Killias Research & Consulting, Lenzburg 2011 (cité : KILLIAS *et al.*, Sondage) ; **Nora MARKWALDER**, Wandel der Kriminalität in den letzten 20 Jahren: Von offline zu online? *in* Christian SCHWARZENEGGER/Rolf NÄGELI (éds), Schwachstelle Mensch: Prävention gegen alte und neue Formen der Kriminalität, 12 Zürcher Präventionsforum, Zürich 2021, p. 45-62 ; **Nora MARKWALDER/Lorenz BIBERSTEIN/Dirk BAIER**, Opfererfahrungen und sicherheitsbezogene Einschätzungen der Schweizer Bevölkerung, Ergebnisse des Crime Survey 2022, ZHAW, Zürich 2023 (cité : MARKWALDER *et al.*, Opfererfahrungen) ; **Nora MARKWALDER/Lorenz BIBERSTEIN/Dirk BAIER**, Cybercrime gegen Privatpersonen in der Schweiz, Ergebnisse des Crime Survey 2022, ZHAW, Zürich 2023 (cité : MARKWALDER *et al.*, Cybercrime) **Riccardo MILANI/Stefano CANEPPELE/Christine BURKHART**, Exposure to Cyber Victimization: Results from a Swiss Survey, Deviant Behavior 2020 (cité : MILANI *et al*.).

Internet et vulnérabilité accrue des victimes

STEFANO CANEPPELE
Professeur de criminologie
Faculté de droit, des sciences criminelles et d'administration publiques,
Université de Lausanne

Table des matières

I. Introduction

L'avènement d'Internet a marqué un tournant significatif dans la façon dont la société contemporaine interagit et communique. Toutefois, cet essor numérique ne s'est pas déroulé sans générer de nouveaux défis, notamment en termes de sécurité et de protection des individus. En effet, cette contribution porte sur un aspect souvent négligé par le droit pénal, à savoir les victimes. Plus précisément, ce chapitre se concentrera sur les victimes de la criminalité en ligne. Mais qui sont ces victimes d'infractions commises sur Internet ? Nous ne disposons pas d'une réponse définitive à cette question. En réalité, on pourrait dire que la réponse à cette question, telle qu'elle nous est présentée, peut susciter de l'anxiété. Chacun d'entre nous pourrait être une victime. Mais est-ce

réellement le cas ? Nous tenterons d'analyser si et comment nous pouvons apporter une réponse à cette interrogation. Afin d'analyser l'accroissement du risque de victimisation dans l'environnement numérique, il convient d'examiner en premier lieu l'amplification du potentiel délictuel des criminels favorisée par l'avènement d'internet. Pour ce faire, nous introduirons le concept de *doppelgänger*.

II. Le concept de *doppelgänger* et son application dans le domaine numérique pour expliquer la victimisation en ligne

Le terme *doppelgänger* vient de l'allemand, mais il est couramment utilisé pour désigner un double ou une personne très similaire à la personne originale, souvent de manière malveillante. Le même concept peut s'appliquer également aux objets, pensons aux contrefaçons de montres de luxe suisses.

En même temps, ce concept s'applique à de nombreux mécanismes de la déviance en ligne. En ligne, les victimes d'usurpation d'identité peuvent découvrir malheureusement qu'un *doppelgänger* a violé l'accès à leur compte personnel, que le site où ils ont acheté un produit n'est pas le site de Amazon, mais un *doppelgänger* malin, ou encore, qu'ils ont envoyé de l'argent à un faux Elon Musk ou à Apple avec la promesse de recevoir le double en peu de temps en permettant aux fraudeurs de gagner CHF 100'000.- en l'espace de trois heures.

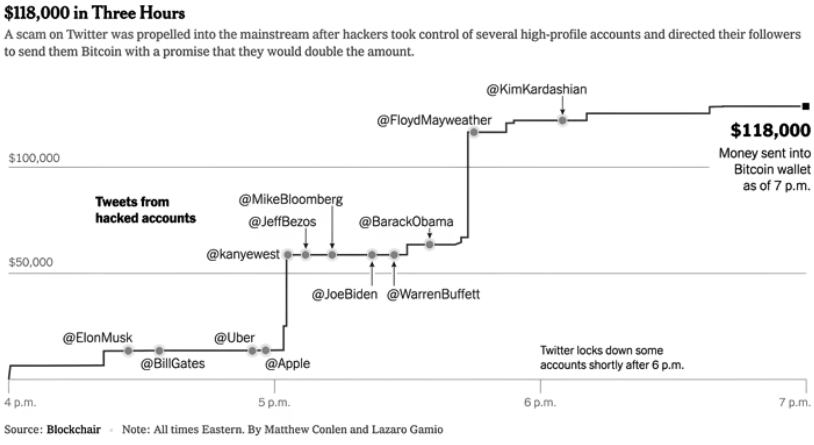


Figure 2 – Visualisation du montant d'argent détourné lors d'une escroquerie sur Twitter en 2020 du New York Times[1].

Même *ChatGPT* a son propre *doppelgänger*. Le 13 juillet 2023, *SlashNext* a publié un billet de blog révélant la découverte de *WORM GPT*, un *ChatGPT* sans contrôle éthique désormais en vente sur un forum de pirates informatiques moyennant apparemment 60 à 700 dollars[2]. Ceci a renforcé le concept de *cybercrime-as-a-service*, à savoir qu'aujourd'hui les criminels qui n'ont pas les compétences numériques nécessaires peuvent les acheter auprès de prestataires sur Internet[3].

La stratégie du *doppelgänger* peut également être observée dans la manipulation de l'opinion publique via internet. Par exemple, on a également appelé opération « *doppelgänger* » celle que le gouvernement russe a mise en place en 2022 au début de la guerre en Ukraine, en clonant des sites de médias en ligne français pour mener des campagnes de désinformation. Les sites étaient identiques aux originaux en tout point en termes de mise en page, à l'exception que les contenus rapportés avaient été manipulés à dessein (Fig. 3). Encore plus violent, en termes de conséquences a été la manipulation des posts *Facebook* pour diffuser des discours de haine envers les minorités en Myanmar pendant le coup d'état en 2021.

1 Disponible sous : <https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html> (*consulté le 26.2.2024*).

2 ORTIZ.

3 Cette tendance à l'automatisation et à la professionnalisation du métier de pirate semble pouvoir générer une approche plus axée sur les affaires des criminels en ligne, qui au lieu de disperser leur énergie sur un nombre indistinct de cibles, cherchent à sélectionner des cibles (personnes physiques ou morales) susceptibles de fournir davantage de possibilités de retour financier.


Le Parisien

Guerre en Ukraine

Un exode massif pour échapper à l'esclavage militaire. Les Ukrainiens tentent d'échapper à une mort imminente sur le front.

La résistance passive à la mobilisation en Ukraine devient progressivement systémique.

Capture d'écran du faux site du Parisien mis en place dans le cadre de l'opération Doppelgänger.

Figure 3 – Exemple des résultats de l'opération de désinformation Doppelgänger, mené par le gouvernement russe en 2022 en ciblant des media français[4].

Je souligne ce point pour mettre en évidence comment même les acteurs étatiques, en particulier en période de tensions géopolitiques, peuvent utiliser Internet pour tenter de manipuler l'opinion publique, mais aussi pour saboter le fonctionnement et/ou dérober des informations confidentielles à des entreprises ou à des entités gouvernementales. Il s'agit d'aspects qui, ne relevant généralement pas du droit pénal, englobent le thème plus large de la cybersécurité que nous n'aborderons pas dans cette contribution.

Nous arrivons maintenant à un cas qui a suscité beaucoup d'émoi en Allemagne en 2023. Selon le magistrat qui a dirigé l'enquête, une présumée meurtrière cherchait son propre *doppelgänger* en ligne pour simuler sa propre mort. Après avoir tenté à plusieurs reprises avec différentes jeunes filles, elle a malheureusement trouvé une victime et l'a convaincue par la ruse de la rencontrer, où elle l'a tuée avec l'aide de son petit ami[5]. Ce cas a suscité un large écho dans la presse, étant présenté comme un exemple des dangers qui peuvent être rencontrés en ligne, où personne n'est en sécurité. Au-delà de la rhétorique d'un discours anxiogène qui semble reprendre certaines narrations sur le risque d'être victime d'une attaque terroriste (le risque zéro n'existe pas, tout comme pour toute activité humaine), nous pouvons souligner un autre point.

4 Disponible sous : <https://www.sorbonne-post-scriptum.com/blog/operation-doppelganger-que-sait-on-de-la-campagne-de-desinformation-russe-qui-vise-la-france-et-dautres-pays/> (*consulté le 26.2.2024*).

5 SOMMERLAD.

Internet, en tant qu'infrastructure, a rendu les êtres humains connectés et il a facilité l'accès aux relations déviantes et non déviantes. Il a permis la création de lieux de rencontre virtuels et de communautés qui multiplient les opportunités d'interaction et d'exposition dans des espaces non ou peu supervisés. La possibilité de créer des *doppelgänger* en ligne, des identités virtuelles anonymes ou pseudo-anonymes, ainsi que l'asynchronicité de l'interaction et la non-visibilité des personnes, sont parmi les mécanismes qui favorisent ce que SULER a appelé « l'effet de désinhibition »[6]. Il s'agit d'une dynamique souvent observable dans les groupes de discussion en ligne et sur les réseaux sociaux, où les discours de haine sont souvent présents et qui explique en partie le fait que des personnes ont un comportement en ligne qu'ils n'auraient pas dans le monde physique.

III. Les enjeux de la définition de cybercriminalité

Jusqu'à présent nous avons évoqué des fraudes en ligne, de la désinformation, des discours de haine, des vols d'identité, voire un meurtre où la victime a été choisie en ligne. On peut se demander si tous ces comportements relèvent de la cybercriminalité. Ce qui nous amène à une autre question, que signifie la cybercriminalité ?

Les universitaires débattent de cette question depuis plus de vingt ans, sans avoir encore trouvé d'accord. Cependant, malgré les divergences de points de vue, on s'accorde sur le fait que si nous voulons comprendre le phénomène, nous devons sortir de la logique de penser à la cybercriminalité comme un monolithe. Elle est composée d'une pluralité de comportements très différents les uns des autres. En 2022, dans le cadre du projet européen H2020 CC-Driver, une collaboration avec les collègues de l'UEL a abouti à la publication d'une taxonomie. Cette dernière, en tant qu'extension des taxonomies précédentes, vise à englober un large éventail de comportements nuisibles en ligne qui ne sont pas nécessairement considérés comme des infractions à l'heure actuelle (c'est-à-dire les comportements cyberdéviants)[7]. Elle montre aussi les nombreux sujets et dynamiques interdépendants inclus sous le terme générique de « cybercriminalité ».

En particulier, la taxonomie reprend une distinction parmi :

1) les cybercrimes de type I qui font référence aux crimes de nature technique (par exemple, le piratage) ;

6 SULER.
7 PHILLIPS *et al*.

2) les cybercrimes de type II qui font référence aux crimes impliquant un contact humain (par exemple, le cyberharcèlement) ;
3) et les cybercrimes de type III qui font référence aux crimes perpétrés par l'intelligence artificielle, les robots/bots ou la technologie d'apprentissage automatique.

Étant donné la variété de comportements pouvant être attribués à la cybercriminalité, il est tout aussi clair que, pour différents types de comportements, il existe souvent différentes catégories de victimes. Et c'est ici que nous arrivons au cœur du sujet de cette contribution : les victimes.

IV. L'origine de la victimologie et les connaissances existantes sur les patterns de victimisation

L'étude des victimes de crimes a émergé à partir des années 1950[8]. En décennies de recherches, nous pouvons souligner cinq points clés :

1) la victimisation n'est pas répartie de manière aléatoire dans la population, mais tend à se concentrer dans l'espace et dans le temps (points chauds). Cette dynamique est également observable avec les individus et les entreprises (O *et al.*, 2017) ;
2) une minorité de la population est victime de la majorité des crimes (victimisation multiple) comme la revue systématique de LEE *et al.* (2017) indique, avec un pourcentage compris entre 10 et 20% de la population qui est victime de 80% des délits en général ;
3) au-delà de la victime simplement victime (ou victime idéale), il existe la figure mixte de la victime qui est également auteur de crime. La relation causale entre les deux rôles n'est pas toujours claire (victime devenue auteur, auteur devenu victime, aucune relation). Le concept a été proposée par CHRISTIE en 1986 mais il est d'actualité même aujourd'hui[9]. Souvent, quand on parle de victime en ligne, prenons les victimes de fraude avec Bitcoin, on tend à décrire la victime comme trop naïve, trop avide et parfois trop stupide ;
4) les approches récentes de la victimologie du développement identifient une tendance à la concentration de la victimisation au cours de la vie d'une personne, un peu comme cela a déjà été observé, par exemple, dans l'étude

[8] Principalement en raison d'une considération : nous ne pouvons pas pleinement comprendre la criminalité et les auteurs sans comprendre qui sont leurs victimes. Cette vision, bien que réductrice, s'est ensuite étendue à l'étude des victimes et de leur vécu pour comprendre comment elles traitent les traumatismes et comment les aider à réduire les conséquences de la victimisation.

[9] CHRISTIE.

du harcèlement scolaire, où de l'enfance à l'adolescence, la prévalence des victimes tend à diminuer tandis que les personnes qui restent victimes sont plus souvent la cible de harcèlement et de formes plus violentes. Une étude publiée en 2015 par DECAMP et ZAYKOWSKI, utilisant des données provenant d'une enquête longitudinale nationale menée en Angleterre et au Pays de Galles sur 5600 individus, a examiné les trajectoires de victimisation violente pour les personnes âgées de 10 à 29 ans sur une période de quatre ans[10]. Les analyses ont identifié quatre trajectoires statistiquement distinctes de victimisation, à savoir : rarement victime (61%) ; jeunes adultes victimes (1%) ; victimes depuis l'enfance (19%) ; et victimes chroniques (20%) ;

5) et les victimes ne sont pas toutes égales et la capacité à faire face à la victimisation n'est pas la même pour tous. Dans ce contexte, le concept de vulnérabilité a été introduit pour expliquer comment, en fonction de la probabilité et du préjudice, il existe des victimes qui peuvent être plus ou moins vulnérables[11].

A. Un brève exposé des théories criminologiques utilisées pour expliquer la victimisation

Comme pour la victimisation hors ligne, la littérature explique souvent la victimisation en ligne à travers des théories situationnelles : a) **la théorie du style de vie** d'HINDELANG *et al.* ; b) la **théorie des activités routinières** de COHEN et FELSON ; et plus récemment, à travers des théories de la personnalité comme la **théorie de l'autocontrôle** de HIRSHI et GOTTFREDSON[12].

La **théorie du style de vie** met l'accent sur l'importance de l'exposition à des endroits, des horaires et des personnes à haut risque, ce qui influe sur la probabilité d'être victime d'une infraction. La **théorie des activités routinières** traite de la convergence dans le temps ou l'espace d'un délinquant motivé et d'une cible intéressante, ainsi que de l'absence d'un gardien capable d'intervenir de manière préventive pour éviter l'incident, et indique la coexistence de ces trois éléments comme étant suffisante pour commettre une infraction. La **théorie de l'autocontrôle** recentre l'explication du crime sur les individus, en expliquant comment le manque de maîtrise de soi chez les individus les amène à réagir impulsivement aux situations sans tenir suffisamment compte des conséquences et/ou des risques. Un exemple de faible autocontrôle est constitué par le fait d'avoir fait impulsivement des paiements en bitcoin en voyant les fausses annonces sur *Twitter* par Elon Musk et compagnie. Maintenant, la

10 DECAMP/ZAYKOWSKI.
11 GREEN, p. 91.
12 HINDELANG *et al.* ; COHEN/FELSON ; GOTTFREDSON/HIRSCHI.

question à se poser est la suivante : comment le profil des victimes a-t-il changé avec l'avènement d'Internet ? Qu'explique le risque de victimisation en ligne ?

B. Victimisation en ligne : mesure et facteurs de risques selon les études les plus récentes

Il est difficile de répondre à cette question en se basant sur les statistiques officielles. En 2017, avec le Prof. AEBI, nous avons publié une contribution soulignant à quel point les systèmes statistiques nationaux étaient en grande difficultés pour mesurer la cybercriminalité[13]. Aujourd'hui, la situation est meilleure qu'il y a 6 ans, mais il reste encore beaucoup à faire. Comme le *Swiss Crime Survey* 2022 l'indique, le taux de dénonciation pour le cyber délits reste extrêmement bas[14]. De même, nous ne pouvons pas nous fier aux statistiques privées qui ont souvent tendance à ne pas rendre compte de méthodologies de mesure transparentes et qui utilisent des termes qui ne correspondent pas à des situations appréhendées d'un point de vue juridique[15].

Il existe donc un problème de mesure en général. Cependant, de nombreuses recherches ont utilisé des enquêtes pour mesurer les facteurs de risque de la victimisation en ligne. A l'ESC, nous avons mené une enquête sur la victimisation à Lugano en 2019 qui a impliqué près de 8000 résidents[16]. Nous avons posé des questions sur la victimisation en ligne, en ce qui concerne les fraudes, les logiciels malveillants et le vol de données personnelles, et tenté de comprendre comment les caractéristiques personnelles et les habitudes d'utilisation peuvent augmenter le risque d'être victime d'infractions.

Les résultats corroboraient plutôt certaines hypothèses en lien aux théories situationnelles. Sans entrer dans les détails, les résultats suggèrent que la victimisation en ligne est positivement liée aux routines de vie des participants (la fréquence d'utilisation d'Internet), aux mesures de protection en ligne (le fait d'avoir un antivirus installé), au sexe et au niveau d'éducation. Le fait d'être un homme, jeune, et d'avoir un diplôme universitaire fait augmenter le risque de victimisation en ligne[17].

Cependant, tous ces résultats présentent une limite méthodologique importante : la relation de causalité entre la victimisation et les comportements. Le problème réside dans le fait qu'en utilisant la même enquête pour observer les

13 CANEPPELE/AEBI.
14 MARKWALDER *et al*.
15 Souvent, les données doivent être filtrées en raison du conflit d'intérêts de ceux qui, en plus de produire les données, vendent un produit à la victime potentielle.
16 MILANI *et al.*, 2022.
17 MILANI *et al.*, 2022.

facteurs de risque et la victimisation, il est possible d'établir une corrélation, mais pas une relation de causalité. Prenons le cas de l'utilisation d'une bonne hygiène numérique (antivirus) et de la victimisation. La personne utilisant l'antivirus réduit-elle le risque de victimisation ou a-t-elle installé l'antivirus après avoir été victime d'un logiciel malveillant ?

Pour obtenir des résultats plus solides à cette question, il est nécessaire de concevoir des enquêtes à différents moments, ce qui nécessite un investissement plus important en termes de ressources. Ces dernières semaines, une étude publiée par des collègues néerlandais a adopté cette méthodologie pour comprendre si les caractéristiques personnelles, les habitudes en ligne et les mesures de protection en ligne sont liées à la future victimisation[18].

En résumé, les résultats nous disent que le seul facteur constamment lié à la victimisation par la cybercriminalité était la victimisation antérieure. La plupart des caractéristiques personnelles, à l'exception de la victimisation antérieure, n'étaient pas liées à la victimisation par la cybercriminalité. Et bien qu'il ait été constaté que les hommes semblent avoir un risque plus élevé de devenir victimes de cybercrime, en particulier de logiciels malveillants, le genre n'était pas lié à l'hameçonnage (*phishing*) et à la victimisation par fraude. Le fait d'être employé semble être un facteur de protection, mais seulement en cas de victimisation par piratage, probablement lié à l'utilisation d'appareils d'entreprise qui pourraient être mieux protégés. Vivre en cohabitation semble être un facteur de protection uniquement pour la fraude en ligne. Les seules activités routinières qui semblent significatives sont celles liées à un certain type de victimisation en ligne. La fait d'acheter souvent des produits en ligne augmente le risque de victimisation par fraude.

Mais ici arrive la partie la plus intéressante. On s'attendait à ce que le comportement réel d'autoprotection en ligne puisse nous aider à expliquer la victimisation par la cybercriminalité. Cependant, à l'exception de la manipulation sécurisée des courriels de *phishing* qui a considérablement réduit les chances de devenir une victime d'hameçonnage, toutes les autres formes de comportement d'autoprotection en ligne (par exemple, la sécurité des mots de passe choisis, le comportement de clic et le partage d'informations personnelles) n'étaient pas significativement associées à la victimisation générale par la cybercriminalité. Par exemple, en ce qui concerne la gestion des mots de passe, les résultats suggèrent que l'utilisation de mots de passe forts ne diminue pas de manière significative les chances de devenir une victime de la cybercriminalité l'année suivante par rapport à l'utilisation d'un mot de passe faible. Selon les chercheurs cela peut résulter du fait que la création d'un compte en ligne est de plus en plus souvent possible uniquement avec un mot de passe fort, et

[18] VANT'HOFF-DE GOEDE *et al*.

donc que de moins en moins de personnes continuent d'utiliser des mots de passe faibles[19]. La victimisation en ligne pourrait alors résulter du vol de mots de passe ou d'informations personnelles lors de grandes attaques de données, qui sont ensuite vendues en ligne, plutôt que d'une attaque par force brute sur un seul sujet. Ce qui amène à la recommandation de ne pas utiliser le même mot de passe pour vos différents comptes.

Ces résultats ajoutent de nouvelles connaissances avec de nouvelles méthodologies qui nécessitent d'autres études pour être corroborées. L'un des défis de la recherche est de produire des connaissances adaptées au rythme des changements technologiques et des habitudes en ligne. Récemment, pour l'Office Fédérale des Assurances Sociales de la Confédération, nous avons produit un rapport sur les mesures de protection des enfants et des adolescents contre les délits sexuels en ligne[20]. Nous avons constaté que, à l'exception de la pédopornographie qui est largement étudiée surtout sur l'angle de la consommation plutôt que sur la production ou la distribution (peut-être en raison d'un accès plus facile aux données), le cyberharcèlement, la sextorsion et plus particulièrement le *streaming* en direct d'actes d'ordre sexuel ont fait l'objet de moins d'études[21].

V. Le manque de connaissances et quelques signaux de changements

En général, la recherche criminologique a accordé beaucoup plus d'attention aux crimes à caractère économique ou cyberdépendants qu'aux crimes violents, probablement en raison de leur nouveauté et de l'accessibilité accrue aux données. Pour ce qui concerne les comportements violents, la grande majorité des études s'est concentrée sur les phénomènes de *bullying* et sur la relation entre la *bullying* en ligne et hors ligne. Les résultats indiquent très souvent que le *cyberbullying* est une continuation de *bullying* hors ligne, avec l'aggravation que la victime, en restant constamment connectée, augmente son exposition aux agressions et risque donc de subir des conséquences plus graves à moyen et long terme[22]. Dans un autre domaine, celui de la violence basée sur le genre et du harcèlement, il a été observé à plusieurs reprises que l'asymétrie des compétences en technologie de l'information peut devenir une forme

19 P. ex : 123456, password, qwerty, etc.

20 CANEPPELE *et al*.

21 Une recherche plus approfondie sur ces phénomènes permettrait de mieux les comprendre et de concevoir des mesures de prévention en adéquation avec leur évolution.

22 ZYCH *et al*.

supplémentaire de contrôle et de violence, entraînant une hybridation de comportements criminels[23].

Dans ce manuscrit, j'ai abordé le sujet de manière large et essayé de faire comprendre à quel point il est complexe de saisir l'impact d'Internet sur la criminalité et de souligner à quel point il est essentiel d'acquérir de nouvelles connaissances. Surtout en ces temps et dans ces domaines, il y a une sensation que rien ne change sur ces problèmes. Je voudrais donc conclure en soulignant quatre aspects qui indiquent un changement.

1) Les compétences en technologies de l'information (TIC) et de la Communication ne sont pas aussi déséquilibrées qu'il n'y paraît et cela peut contribuer à réduire la victimisation en ligne ;

   Une des conclusions persistantes des études est que les garçons considèrent leurs compétences en TIC comme plus élevées que celles des filles. Une méta-analyse de 23 études a testé si le même schéma se vérifie pour les performances réelles des élèves aux tâches de compétence en TIC, mesurées par des évaluations basées sur les performances[24]. Globalement, les différences entre les sexes en matière de compétence en TIC étaient significatives, positives et favorisaient les filles. Ces résultats contredisent ceux obtenus à partir de méta-analyses précédentes basées sur la compétence en TIC autodéclarées et suggèrent que l'écart entre les sexes en matière de TIC pourrait ne pas être aussi important qu'on l'avait prétendu.

2) Si l'on intervient pour limiter certains comportements (par exemple la fraude en ligne), il est possible de les réduire. Prévenir un crime réduit le nombre de victimes ;

   Selon le rapport NILSON, la fraude par carte de crédit – exprimée en pourcentage de chaque 100 dollars – continue de diminuer grâce aux efforts de l'industrie pour lutter contre ce type de fraude. Le chiffre pour l'année 2021, la dernière année disponible, était de 6,6 cents à l'échelle mondiale pour chaque 100 dollars du volume total, comparé à 6,8 cents en 2020. Au cours de la dernière décennie, il a atteint un pic de 7,2 cents en 2016[25].

3) L'enquête et la sanction relatives aux cyberdélits sont difficiles, mais les choses évoluent. Même se concentrer sur les auteurs les plus prolifiques peut sensiblement réduire le nombre de victimes potentielles ;

   Au début de cet exposé, on avait mentionné le cas de pirates qui avaient pris le contrôle de compte *Twitter* pour se faire verser des bitcoins. Enfin ces *doppelgängers* virtuels ne sont pas restés virtuels si longtemps. La police

23 DUNN.
24 SIDDIQ/SCHERER.
25 NILSON REPORT.

américaine a réussi à remonter à l'identité d'au moins deux de ces fraudeurs d'origine britannique. En 2021, le prétendu cerveau derrière cette attaque a été extradé aux États Unis et il a plaidé coupable en échange d'une peine de trois ans de prison. En 2023, un deuxième a été condamné à cinq ans d'emprisonnement. Il devra également rembourser les 794'000 dollars qu'il a détournés grâce à cette piraterie[26].

4) Les services d'orientation aux victimes de cybercriminalité commencent à se développer et cela contribue à réduire les conséquences de la victimisation ;

Comme nous l'avons déjà mentionné au début de cette contribution, les victimes d'infractions dans le système pénal sont encore souvent peu considérées. Ce constat s'applique également à la cybercriminalité. Les victimes en ligne sont rarement prises en charge par les institutions. Souvent, la police a peu de marge de manœuvre au-delà du dépôt de plainte, en particulier dans le cas d'infractions commises par des auteurs agissant depuis l'étranger. Les institutions financières et d'assurance, quant à elles, se contentent – le cas échéant – de verser une indemnisation financière à la victime, tandis que les services d'aide aux victimes ont tendance à intervenir rarement, car ils sont principalement conçus pour fournir une assistance aux victimes de violence physique. Cependant, les victimes de cyberfraude ont des besoins émotionnels (reconnaissance en tant que victime et possibilité de neutraliser le sentiment d'injustice perçu), pratiques (obtenir de l'aide pour arrêter les transferts de fonds ou accéder à leur dossier de crédit pour le geler), financiers (obtenir une indemnisation pour les pertes subies), judiciaires (avoir accès à une réponse policière claire et à un soutien pendant le procès), un besoin d'informations (obtenir des détails sur l'incident dont elles ont été victimes et sur l'auteur de cet incident) ou techniques (récupérer un accès sécurisé à leur smartphone ou à leur ordinateur si ces appareils ont été compromis) qu'il faut prendre en compte[27]. Au vu de ces considérations, de nouvelles initiatives se développent pour répondre aux besoins des victimes en ligne, comme l'expérience de la clinique de cyber-criminologie de Montréal[28]. Bien que nous soyons aux prémices de ce type d'expériences, il est important de souligner que leur création est un signe du changement en cours et qu'elle peut contribuer à améliorer l'aide aux victimes de la cybercriminalité.

26 SYME.
27 BORWELL *et al.*
28 Disponible sous : <https://www.clinique-cybercriminologie.ca/> (*consulté le 10.4.2024*).

VI. Conclusion

En conclusion, il est impératif de souligner l'importance cruciale de la compréhension approfondie des mécanismes complexes sous-tendant la cybercriminalité, ainsi que la nécessité constante de s'adapter à l'évolution rapide des technologies et des comportements en ligne. Diverses études convergent vers la prise en compte d'une multitude de facteurs, allant de la compétence en technologies de l'information et de la communication (TIC) à la mise en œuvre de mesures préventives contre les comportements criminels, afin de réduire les risques et les conséquences liés à la victimisation en ligne.

Bien entendu, il subsiste un large champ d'investigation quant aux mécanismes sous-tendant la victimisation en ligne et à ses retombées à long terme. Toutefois, les travaux de recherche présentés offrent des perspectives prometteuses quant à la possibilité de façonner un avenir numérique plus sûr et plus résilient au sein de ce paysage en constante mutation. Les efforts continus dans ce domaine permettront de mieux comprendre, d'anticiper et de répondre aux enjeux complexes qui jalonnent la sécurité et la protection des individus dans l'espace virtuel. Nous sommes ainsi conviés à persévérer dans la voie de l'innovation et de l'analyse critique pour faire face aux défis actuels et à venir de la société numérique.

VII. Bibliographie

Jildau BORWELL/ Jurjen JANSEN/ Wouter STOL, Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, 2021, vol. 3, no 3, p. 85-110 (cité : BORWELL *et al.*); **Stefano CANEPPELE/Marcelo F. AEBI**, Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. Policing: A Journal of Policy and Practice, vol. 13 (1), 2019, p. 66-79 (cité : CANEPPELE/ AEBI) ; **Stefano CANEPPELE/Christine BURKHARDT/Amandine DA SILVA/Lachlan JACCOUD/ Fabian MUHLY/Sandra RIBEIRO**, Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels n°16, OFAS 2022 (cité : CANEPPELE *et al.*) ; **Nils CHRISTIE**, The Ideal Victim, *in* Ezzat A. FATTAH (éd.), From Crime Policy to Victim Policy: Reorienting the Justice System, 1986, p. 17-30 ; **Lawrence E. COHEN/Marcus FELSON**, Social Change and Crime Rate Trends: A Routine Activity Approach, American Sociological Review, vol. 44 (4), 1979, p. 588 ss ; **Whitney DECAMP/Heather ZAYKOWSKI**, Developmental victimology: Estimating group victimization trajectories in the age–victimization curve, International Review of Victimology, vol. 21 (3), 2015, p. 255-272 ; **Suzie DUNN,** Technology-Facilitated Gender-Based Violence: An Overview, Centre for International Governance Innovation: Supporting a Safer Internet Paper 1, 2020 (cité : DUNN) ; **Michael. R. GOTTFREDSON/ Travis HIRSCHI**, A general theory of crime, Stanford University Press, 1990 ; **Simon GREEN**, Crime, victimisation and vulnerability, *in* Sandra Walklate, Handbook of Victims and Victimology, chapter 4, 2007 ; **Michael J. HINDELANG/Michael R. Gottfredson/ James GAROFALO**, Victims of personal crime: An empirical foundation for a theory of

personal victimization, 1978 ; **YongJei LEE/John ECK/SooHyun O/Natalie N. MARTINEZ**, How concentrated is crime at places? A systematic review from 1970 to 2015. *Crime Sci* 6, 6 (2017) (cité : LEE *et al.*) ; **Nora MARKWALDER/Lorenz BIBERSTEIN/Dirk BAIER**, Cybercrime gegen Privatpersonen in der Schweiz: Ergebnisse des Crime Survey 2022, ZHAW, Zürich 2023 (cité : MARKWALDER *et al.*) ; **Riccardo MILANI/Stefano CANEPPELE/Christine BURKHARDT**, Exposure to Cyber Victimization: Results from a Swiss Survey, Deviant Behavior, vol. 43 (2), 2022, p. 228-240 ; **NILSON REPORT**, Nilson Report 1232, December 2022 (<https://nilsonreport.com/newsletters/1232/>, *consulté le 23.2.2024*) ; **Sabrina ORTIZ**, Les fraudes liées à ChatGPT sont en hausse, voici comment se protéger, ZDNet, 23 mars 2023 (<https://www.zdnet.fr/actualites/les-fraudes-liees-a-chatgpt-sont-en-hausse-voici-comment-se-proteger-39955944.htm>, *consulté le 14.2.2024*); **Kirsty PHILLIPS/Julia. C. DAVIDSON/Ruby R. Farr/Christine BURKHARDT/Stefano CANEPPELE/Mary P. AIKEN**, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2 (2), 2022. Article 2 ; **Fazilat SIDDIQ/Ronny SCHERER**, Is there a gender gap? A meta-analysis of the gender differences in students' ICT literacy, Educational Research Review, vol. 27, 2019, p. 205-217 ; **Joe SOMMERLAD**, How a German woman allegedly killed beauty blogger lookalike to fake her own death, The Independent, 2nd February 2023, (<https://www.independent.co.uk/news/world/europe/shahraban-k-doppelganger-murder-germany-b2274575.html>, *consulté le 14.2.2024*) ; **SooHyun O/ Natalie N. MARTINEZ/ YongJei LEE/ John E. ECK,** How concentrated is crime among victims? A systematic review from 1977 to 2014. Crime Sci 6, 9 (2017) (cité : O *et al.*); **John SULER**, The Online Disinhibition Effect, CyberPsychology & Behavior, vol. 7 (3), 2004, p. 321-326 ; **Pete SYME**, Man pleads guilty to hacking Elon Musk's and Joe Biden's Twitter accounts in bitcoin scam, Business Insider, 2023 (<https://www.businessinsider.com/twitter-bitcoin-scam-elon-musk-joe-biden-man-pleads-guilty-2023-5>, *consulté le 14.2.2024*) ; **Susanne VAN 'T HOFF-DE GOEDE/Steve VAN DE WEIJER/Rutger LEUKFELDT**, Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization?, Journal of Crime and Justice, 0 (0), 2023, p. 1-20 (cité : VAN 'T HOFF-DE GOEDE *et al.*) ; **Izabela ZYCH/ Rosario ORTEGA-RUIZ/Rosario DEL REY**, Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. Aggression and violent behavior, 2015, vol. 23, p. 1-21 (cité : ZYCH *et al.*).

Cybercriminalité et infractions pénales

Analyse à l'aune des nouvelles dispositions protégeant le domaine secret, la liberté et l'intégrité sexuelle

JOËLLE VUILLE
Professeure de droit pénal et de criminologie
Faculté de droit, Université de Fribourg

CAMILLE PERRIER DEPEURSINGE
Professeure de droit pénal
Faculté de droit, des sciences criminelles et d'administration publique,
Université de Lausanne

JUSTINE ARNAL
Assistante diplômée
Faculté de droit, des sciences criminelles et d'administration publique,
Université de Lausanne

Table des matières

I. Introduction

Au milieu des années 1960, en pleine Guerre froide, lorsque certains parlementaires suisses apprennent que « *de nouveaux petits appareils* »

permettent de capter des conversations privées (« *même à travers des parois* »), ils déposent un postulat tendant à leur interdiction[1]. Le Conseil fédéral, alors manifestement également préoccupé par l'essor de ces *nouvelles technologies*, répond par l'adoption rapide de dispositions pénales inédites, arguant dans le Message y relatif que : « *Le droit à la protection du domaine personnel secret est l'expression de la conviction que l'individu ne peut développer sa personnalité que s'il est assuré d'être protégé contre les ingérences de l'État et des autres individus dans sa vie privée.* […] *Protéger ces droits est une des tâches de l'État fondé sur le droit* »[2].

Une génération plus tard, l'informatique fait son entrée dans la vie des citoyens du monde entier. Les ordinateurs envahissent les entreprises et les foyers, et le législateur prend rapidement conscience que ces nouveaux objets ainsi que, surtout, les données qu'ils génèrent et stockent ne sont pas encore protégés par le droit pénal. Il adopte en conséquence les art. 143, 143*bis*, 144*bis*, 147 et 150 CP[3], entrés en vigueur le 1er janvier 1995[4]. Toutes ces dispositions sont insérées dans le Titre 2 concernant les infractions contre le patrimoine. Alors que certaines dispositions protègent désormais les systèmes informatiques et les données contre des accès indus (art. 143, 143*bis* et 144*bis* CP), deux autres normes appréhendent déjà ces nouvelles technologies comme moyens de porter atteinte au patrimoine (art. 147 et 150 CP).

Apparaissent ensuite l'usage généralisé d'Internet et le développement des plateformes d'échange telles que blogs, réseaux sociaux ou messageries instantanées. Il semble que, face à ces technologies, les autorités suisses aient pensé, dans un premier temps, que rien de révolutionnaire n'était arrivé[5]. Après tout,

---

1 Postulat du Conseiller national M. MÜLLER-LUCERNE, n°9526, du 1er juillet 1966 cité *in* FF 1968 I 609, p. 609.

2 FF 1968 I 609, p. 609.

3 Code pénal du 21 décembre 1937, RS 311.0 (ci-après CP).

4 RO 1994 2290. V. FF 1991 II 933, p. 935 : « *Cette criminalité moderne est particulièrement pernicieuse en raison de sa dimension internationale, d'une part, mais aussi de la rapidité qui caractérise le déroulement des infractions ; grâce à l'évolution des télécommunications et de la technologie informatique, les pires dégâts peuvent être provoqués par des délinquants qui disparaissent ensuite sans laisser de trace* ». Signalons encore, avec l'entrée en vigueur de la LPD, l'adoption de l'art. 179novies CP protégeant la soustraction de données personnelles, exception à ce qui précède puisque la disposition est insérée dans le titre dédié à la protection du domaine secret et privé (RO 1993 1945 ; FF 1988 II 421).

5 Malgré de très nombreuses interventions parlementaires. On citera la première, soit le postulat de la Conseillère nationale Viola AMHERD, n°11.3912 « *Cadre juridique pour les médias sociaux* », du 29 septembre 2011 qui a donné lieu à un rapport, puis à un rapport complémentaire du 10 mai 2017, au terme duquel on peut lire (p. 52) : « *Compte tenu de l'état des lieux actuel, le Conseil fédéral arrive à la conclusion que pour l'heure, il n'est pas nécessaire de prendre des mesures de réglementation supplémentaires en ce qui concerne les médias sociaux* ». La liste des (30) interventions

la technologie existait déjà (ordinateurs et téléphones) et la simple mise en réseau d'informations ne paraissait guère devoir faire l'objet d'une règlementation spécifique. Pourtant, et c'est devenu plus tard une évidence, il n'y a pas que les infractions au patrimoine que ces technologies facilitent. En plus de désinhiber les auteurs[6] et de vulnérabiliser les victimes[7], Internet et la facilitation des échanges par les plateformes numériques amplifient considérablement les effets d'une infraction. Il n'est ainsi pas équivalent de recevoir une injure ponctuelle en face à face que de voir sa réputation ruinée par des images diffusées aux quatre coins du globe, disponibles dans chaque poche et sans possibilité de les effacer.

Les infractions informatiques protégeant le patrimoine ayant déjà été abondamment commentées[8], nous nous intéresserons ici aux atteintes à d'autres biens juridiques que permettent les technologies de l'information et des communications (ci-après : TIC). Nous choisissons ainsi de ne traiter que des infractions contre le domaine secret ou privé, contre la liberté et contre l'intégrité sexuelle, lorsque celles-ci sont facilitées par les TIC. En outre, ce choix est guidé par l'actualité ; ce sont en effet pour protéger ces biens juridiques ci que le Parlement suisse a récemment adopté ou discuté la pertinence d'introduire de nouvelles infractions, dont la portée n'a, de fait, pas encore été examinée en doctrine.

Enfin, nous examinerons également comment appréhender juridiquement certains comportements qui portent atteinte à ces biens juridiques, sans qu'une disposition pénale leur soit précisément dédiée.

II. L'usurpation d'identité

Le 1er septembre 2023 est entrée en vigueur la nouvelle Loi sur la protection des données[9]. Cela a eu pour conséquence l'insertion dans le Code pénal d'une nouvelle disposition incriminant l'usurpation d'identité, l'art. 179*decies* CP : « *Quiconque utilise 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 est, sur plainte, puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire*. ». Si l'usurpation d'identité comme

parlementaires sur cette thématique, dont bon nombre concerne les droits de la personnalité, figure en p. 57-58 du rapport.

6 *Cf.* CANNEPELE (dans cet ouvrage).

7 *Cf.* MARKWALDER (dans cet ouvrage).

8 V. par exemple : BALTISSER ; MÉTILLE/AESCHLIMANN ; MONNIER, p. 130 ss ; MOREILLON, p. 21 ss ; PFISTER ; SCHMID, Kreditkarten-Kriminalität ; SCHMID, Computerstrafrecht, p. 22 ss ; SCHNEIDER ; SCHWARZENEGGER, p. 305 ss ; STAUFFACHER, p. 1 ss.

9 Loi fédérale sur la protection des données du 25 septembre 2020 (LPD), RS 235.1.

phénomène social est ancienne, force est de constater que le fait de se faire passer pour autrui est devenu plus facile à l'ère numérique.

Jusqu'à présent, l'usurpation d'identité n'avait jamais été réprimée en tant que telle ; l'auteur était poursuivi pour les infractions commises en amont, pour obtenir les données personnelles (telle que la soustraction de données, art. 143 CP, ou l'accès indu à un système informatique, art. 143*bis* CP) ou en aval, grâce à l'identité usurpée (telle que l'escroquerie, art. 146 CP, ou une infraction contre l'honneur, art. 173 ss CP).

Pour celui dont l'identité était usurpée, seule la voie civile permettait de s'opposer à une atteinte à sa personnalité (art. 28 ss CC), en particulier en cas de violation du droit au nom (art. 29 CC)[10]. Cependant, ouvrir une telle action supposait, et suppose toujours, de connaître l'identité réelle de l'usurpateur du nom (pour le citer comme défendeur, à défaut de quoi l'action est rejetée au fond[11]) alors que les TIC permettent précisément de nuire sous couvert d'anonymat.

La nouvelle infraction est intégrée dans le Titre 3 du Code pénal regroupant les infractions contre l'honneur et contre le domaine secret ou le domaine privé. Il semble que ce titre doive désormais recouvrir les différentes formes d'atteintes à la personnalité, particulièrement intenses, qui ne seraient pas appréhendées par un titre spécifique[12]. En effet, à notre sens, l'usurpation d'identité n'est pas une infraction contre le domaine secret ou privé. Comme le relevait déjà le Message du Conseil fédéral relatif à cette modification, il s'agit plutôt ici de protéger un aspect de la personnalité, à savoir le droit de la personne au respect de son identité[13].

L'identité peut être décrite comme un ensemble de données permettant de désigner clairement une personne physique dans un contexte donné et de la distinguer des autres[14]. L'usurpation d'identité est une infraction formelle, dont la

10 BUCHER, p. 99 ss.

11 ATF 125 III 82, consid. 1.a. V. également TF, 5A_792/2011 du 14 janvier 2013, consid. 6.3 qui admet la légitimation passive de l'hébergeur de blogs.

12 En droit civil, la protection de la personnalité englobe notamment la protection contre les atteintes à l'honneur et à la sphère privée, mais également les atteintes à la vie, à l'intégrité corporelle, à l'intégrité sexuelle ou encore à la paix des morts (pour un aperçu global des atteintes à la personnalité reconnues comme ouvrant le droit à une action basée sur l'art. 28 CC, v. STEINAUER/FOUNTOULAKIS, p. 179 ss). La doctrine et la jurisprudence ont renoncé à définir exhaustivement le champ d'application de la protection de la personnalité au sens de l'art. 28 CC. Selon les termes repris par la jurisprudence fédérale, la personnalité comprend tous ce qui permet d'individualiser une personne et qui paraît digne de protection dans le cadre des relations entre individus et conformément aux bonnes mœurs (ATF 147 III 185, consid. 4.2.3 ; ATF 70 II 127, consid. 2 ; ATF 45 II 623, consid. 1).

13 FF 2017 6565, p. 6741.

14 BORGES *et al.*, p. 4 ; REBER, p. 35.

réalisation ne dépend pas d'un quelconque résultat[15]. Il n'est donc pas nécessaire qu'un tiers ait effectivement pris connaissance de l'usurpation d'identité[16]. L'art. 179*decies* CP réprime le fait d'utiliser les noms, adresses, numéros de téléphone, photographies, noms d'utilisateur, dates de naissance, numéros de passeport d'une autre personne, sans le consentement de cette dernière[17]. L'usurpation d'une adresse Internet, d'un numéro de compte, d'un pseudonyme, d'une adresse électronique ou d'un numéro AVS relève également de l'infraction[18].

L'auteur doit dans tous les cas se faire passer pour une personne qu'il n'est pas[19]. Il semblerait toutefois que seule l'identité d'une personne physique étrangère à l'auteur soit visée par l'art. 179*decies* CP. En effet, au vu du fait que le Conseil fédéral se réfère, en allemand, à la « *Identität eines Menschen* »[20] et à la « *Persönlichkeit des Individuums* »[21] dans son Message, il apparaît que les personnes morales ne sont pas protégées contre l'usurpation de leur identité[22].

Le fait d'utiliser une identité inventée ne tombe pas non plus sous le coup de cette incrimination[23], de même que le fait de se présenter dans une fonction générale que l'on n'occupe pas en réalité (par exemple, se faire passer pour un policier pour escroquer une personne vulnérable, ou pour une personne ayant une certaine caractéristique abstraite[24]). On notera que le média ou moyen utilisé par l'auteur n'est pas mentionné par la disposition : il peut s'agir d'une usurpation en ligne ou dans le monde physique.

La notion d'utilisation recouvre une multitude de comportements. Il peut par exemple s'agir de créer un profil sur un média social, de saisir les données d'un tiers lors d'une commande de biens en ligne, mais également de simplement se présenter sous une fausse identité.

L'usurpation d'identité intervient fréquemment à des fins d'humiliation à caractère sexuel. Certaines applications permettent en effet de transformer n'importe quelle photographie d'une personne habillée en sa version dénudée. Il est

15 WENK, p. 173.
16 REBER, p. 35.
17 FF 2017 6565, p. 6741.
18 REBER, p. 35.
19 REBER, p. 34.
20 BBl 2017 6941, p. 7127.
21 BBl 2017 6941, p. 7127.
22 REBER, p. 34.
23 FF 2017 6565, p. 6741.
24 On pensera à Rachel Dolezal aux Etats-Unis qui se présentait comme une femme d'ascendance afro-américaine alors qu'elle est née de deux parents caucasiens, à Frank Abagnale qui se faisait passer pour un pilote de ligne/avocat/médecin, ou encore à Anna Sorokin qui se présentait comme une milliardaire auprès de la *jet set* pour profiter de ce train de vie.

également possible de superposer le visage d'une personne sur celui d'un acteur ou d'une actrice pornographique[25]. Dans ce sens, l'identité d'une personne peut être volée afin de réaliser un hypertrucage (« *deep fake* ») pornographique dans le but de lui nuire[26]. En pareil cas, on appliquera, en sus de l'art. 179*decies* CP, l'art. 197*a* CP, commenté ci-dessous, puisque l'identité usurpée l'est pour porter atteinte à l'intimité de la personne. La transmission ou diffusion du contenu ainsi créé, à caractère sexuel, est un comportement différent de la seule usurpation d'identité. En outre, les biens juridiquement protégés sont deux aspects différents des droits de la personnalité (droit à l'identité et sphère intime). Notons toutefois que l'hypertrucage à caractère sexuel doit, pour entraîner l'application de l'art. 179*decies* CP, être utilisé par l'auteur pour se faire passer pour la victime[27]. En d'autres termes, il est nécessaire que l'auteur parle au nom de la victime ou interagisse avec des tiers depuis le faux profil de cette dernière. Si tel n'est pas le cas, seul l'art. 197*a* CP sera, à notre sens, applicable.

Du point de vue subjectif, l'infraction est intentionnelle et requiert la réalisation d'un dessein spécial, à savoir que l'auteur doit agir pour nuire à autrui ou pour se procurer ou procurer à un tiers un enrichissement illégitime[28]. Le dol éventuel suffit[29]. La nuisance peut être matérielle ou immatérielle, mais doit atteindre une certaine intensité pour que la disposition s'applique[30]. Selon une partie de la doctrine, la création d'un faux compte sur un média social ne suffit pas pour retenir que l'auteur avait l'intention de nuire à la personne dont il a usurpé l'identité : pour qu'une telle intention de nuire soit établie, il faudra encore que l'auteur ait utilisé ce compte au désavantage de la personne dont il a usurpé l'identité[31]. L'auteur qui agit par exubérance ou espièglerie ne sera en tout cas pas punissable[32].

L'infraction d'usurpation d'identité pourra entrer en concours avec d'autres infractions, typiquement l'escroquerie, la soustraction de données personnelles, etc. Ainsi, si l'auteur A prend sur un réseau social l'identité de B pour calomnier C, l'auteur A sera punissable pour usurpation d'identité et pour calomnie[33]. Dans le même sens, l'auteur d'une soustraction de données personnelles à des fins d'usurpation d'identité sera également poursuivi en vertu des deux infractions (soustraction et usurpation)[34].

---

25 JACQUEMIN, p. 322.
26 JACQUEMIN, p. 322.
27 En effet, le simple usage d'une photographie n'implique pas l'usurpation d'identité.
28 REBER, p. 35.
29 REBER, p. 35.
30 FF 2017 6565, p. 6742.
31 REBER, p. 36.
32 FF 2017 6565, p. 6741.
33 REBER, p. 37 ; FF 2017 6565, p. 6742.
34 FF 2017 6565, p. 6742.

Dans la pratique, un nombre important d'usurpations d'identité qui ont lieu sur Internet sont réalisées depuis l'étranger, comme c'est notamment le cas dans le cadre des « *escroqueries à la romance* »[35] ou encore « au président ». Si l'identité d'une personne suisse est usurpée à l'étranger, la question de la compétence des autorités de poursuite pénale suisses se posera. En effet, malgré la vision très large de la notion de « *résultat* » que le Tribunal fédéral a développée ces dernières années dans le cadre de l'interprétation des art. 3 et 8 CP, la compétence suisse ne peut être donnée en cas d'infraction formelle commise à l'étranger que si la « *conséquence* » qu'a l'infraction en Suisse se trouve dans un rapport de connexité immédiate avec le comportement typique[36].

III. Le *doxxing*

Le *doxxing* (aussi appelé *doxing*[37]) peut se définir comme la publication d'informations permettant d'identifier une personne[38], contre son gré et pour lui nuire. On pensera aux divers sites qui ont, en août 2023, diffusé les noms et les adresses des personnes siégeant dans le « *grand jury* » ayant mis en accusation Donald J. Trump pour avoir tenté de falsifier les résultats de l'élection présidentielle de 2020 en Géorgie[39], ou aux membres du groupe *Antifa* qui ont, au printemps 2022, rendu publics les noms, dates de naissance, adresses, photographies et numéros de téléphone de membres présumés d'un groupe néonazi en Suisse[40]. L'effet que recherche l'auteur du *doxxing* est d'humilier la victime, de lui faire perdre son emploi en informant son employeur de ses opinions politiques, de causer son ostracisation hors de son groupe social, voire de provoquer envers la victime le déchainement d'une vague de vigilantisme[41] de la part du public, concrétisée par des menaces, des contraintes et parfois des actes de violence grave.

---

35 WENK, p. 173.

36 Voir not. ATF 141 IV 336, JdT 2016 I 200; ATF 128 IV 145, JdT 2004 IV 32.

37 Dérivé de l'anglais « *docs* », contraction du mot « documents ».

38 WICKI-BIRCHLER, § 4. Pour une introduction à la problématique, v. not. DOUGLAS, p. 199-210.

39 V. notamment The Guardian, « *Names and addresses of Trump jurors in Georgia posted on rightwing websites* », 17 août 2024, disponible sous : <https://www.theguardian.com/us-news/2023/aug/17/georgia-grand-jurors-information-posted-rightwing-websites>, *consulté le 17.3.2023*.

40 20 Minutes, « *Chaque semaine, on dévoilera l'identité d'un nazi* », 4 avril 2022, disponible sous : <https://www.20min.ch/fr/story/chaque-semaine-on-devoilera-en-ligne-lidentite-dun-nazi-301887599283>, *consulté le 17.3.2024*.

41 Aussi appelé auto-justice ou auto-défense en français, le *vigilantisme* peut se définir comme une « *pratique coercitive, basée sur le volontariat, consistant à maintenir l'ordre et/ou à rendre la justice au nom d'une collectivité - la population d'un quartier ou d'un village, par exemple* » : FAVAREL-GARRIGUES/GAYER. La lectrice intéressée trouvera

Contrairement à certains droits asiatiques[42] et au droit néerlandais depuis très récemment[43], le droit pénal suisse ne réprime pas directement la personne qui rend public le nom ou d'autres données personnelles d'un tiers[44]. On pourrait *a priori* envisager de retenir plusieurs infractions, mais comme nous le verrons, aucune n'est appropriée :

– *Soustraction de données* : l'art. 143 CP requérant un dessein spécial d'enrichissement illégitime (pour soi-même ou pour un tiers), les éléments constitutifs subjectifs de cette infraction feront souvent défaut dans les cas de *doxxing* ;
– *Soustraction de données personnelles,* art. 179^novies^ CP : la disposition ne concerne que les données personnelles *sensibles*[45] et les profils de la personnalité, et ne sera donc pas applicable dans un certain nombre de cas de *doxxing*. Par ailleurs, il n'y aura parfois pas de *soustraction* de données en amont du *doxxing*. Dans le cas des membres du « grand jury » en Géorgie, par exemple, les noms et adresses ont été publiés par les autorités judiciaires de l'État, comme la loi le prévoit, mais étaient passés inaperçus du grand public jusqu'à ce que certains milieux d'extrême droite les relayent sur leurs sites Internet ;
– *Infraction contre l'honneur* : même si le « *doxxeur* » cherche parfois à humilier sa victime, les art. 173 ss CP ne pourront pas s'appliquer dans les cas dans lesquels la victime n'est pas objectivement accusée d'être une personne méprisable. Par exemple, le fait de révéler qu'une personne est membre d'un jury dans une affaire très médiatisée ne remplit pas les éléments constitutifs de la diffamation ou de la calomnie. Et pourtant, la révélation de cette information fera de la personne visée la cible d'un certain public partisan de l'ancien président Trump ;
– *Instigation ou complicité aux infractions commises par les* « *justiciers* » : l'instigation est d'emblée exclue puisqu'elle implique de décider une personne déterminée (ou un groupe de personnes déterminées)[46] à la

plus d'informations sur le vigilantisme dans la publication pionnière sur le sujet de JOHNSTON.

42 V. p. ex. pour Hong-Kong, *Office of the Privacy Commissioner for Personal Data; pour Singapore, Ministry of Law*.

43 Reuters, « *Dutch Senate votes to make* "*doxing" a crime* », 11 juillet 2023, disponible sous : <https://www.reuters.com/world/europe/dutch-senate-votes-make-doxing-crime-2023-07-11/>, *consulté le 17.3.2024*.

44 Pour un cas de « *doxxing* » en Suisse, v. TAF, arrêt A-1368/2023 du 24 novembre 2023, consid. 4.6. Les personnes qui procèdent concrètement aux actes de vigilantisme précédemment évoqués pourront, quant à elles, être poursuivies pour les infractions commises.

45 Celles-ci sont définies par l'art. 5 lit. c de la LPD et comprennent not. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, et les données sur la santé, la sphère intime ou l'origine raciale ou ethnique.

46 CR CP I-STRAÜLI, art. 24, N 3-5.

commission d'une infraction relativement précise (art. 24 CP)[47] ; quant à la complicité, elle pourra éventuellement être admise par dol éventuel[48] dans le cas de menaces ou d'infractions contre la liberté, mais semble difficilement envisageable pour d'éventuelles infractions de violence ;

– *Provocation publique au crime ou à la violence :* l'art. 259 CP nous semble difficilement applicable dans ce type de cas, dans la mesure où les « *doxxeurs* » n'appellent pas explicitement à la violence. La jurisprudence et la doctrine requièrent une « *provocation relativement pressante qui est propre, par son contenu et sa forme, à influencer la volonté des personnes à qui elle s'adresse* »[49]. Pour certains, la provocation doit être sans équivoque[50]. Même s'il n'est pas nécessaire que l'infraction visée soit explicitement mentionnée, il doit être clair pour un auditeur ou lecteur neutre de quel type d'infraction il est question[51]. Or, les « *doxxeurs* » postent souvent les noms et adresses des victimes sans aucune autre remarque, sachant que les « justiciers » sauront comment utiliser l'information. Nous doutons donc que l'art. 259 CP puisse trouver application dans ces cas.

Dans les cas dans lesquels le *doxxing* mène à la commission d'autres infractions, telles que des infractions contre l'honneur ou des menaces, l'auteur (immédiat) de ces dernières peut être poursuivi. Il est toutefois des cas où le *doxxing* est un but en soi, comme lorsque des personnes rendent publics le nom et l'adresse de prêtres catholiques qu'ils soupçonnent d'être gays[52]. La victime peut alors subir une ostracisation sociale et professionnelle totale sans qu'aucune infraction pénale ne soit toutefois commise contre elle. Dans ce type de cas, qui n'est actuellement pas couvert par les infractions contre l'honneur[53], nous sommes d'avis que le comportement du « *doxxeur* » devrait être réprimé pénalement, car il cause un dommage du même type et (au moins) de même ampleur que celui ou celle qui commet une atteinte à l'honneur, et contre lequel la protection offerte par le droit civil n'est pas suffisante.

47 CR CP I-STRAÜLI, art. 24, N 6-10.
48 V. not. ATF 113 IV 108, JdT 1988 IV 47; ATF 132 IV 49, consid. 1.1.
49 ATF 111 IV 151, consid. 1.a, JdT 1985 IV 147, cité par CR CP II-LIVET/DOLIVO-BONVIN, art. 259, N 2.
50 BSK Strafrecht II-FIOLKA, Art. 259, N 12 avec les références citées.
51 BSK Strafrecht II-FIOLKA, Art. 259, N 14 avec les références citées.
52 WIRED, « *How a Catholic Group Doxed Gay Priests* », 11 mars 2023, disponible sous : <https://www.wired.com/story/catholic-priest-doxing-security-roundup/>, *consulté le 17.3.24*.
53 CR CP II-RIEBEN/MAZOU, Intro aux art. 173-178, N 20.

IV. Le harcèlement (obsessionnel)

Aussi appelé *stalking*, le harcèlement (obsessionnel[54]) a fait l'objet de longs débats parlementaires quant à la nécessité de le réprimer par une norme *ad hoc*, avant qu'un projet de loi ne soit finalement mis en consultation en été 2023[55]. Le potentiel futur article 181*b* AP-CP[56] aurait ainsi la teneur suivante : « *Quiconque traque, harcèle ou menace obstinément une personne et l'entrave dans la libre détermination de sa façon de vivre, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire* ». Les résultats de la procédure de consultation ont été publiés en automne 2023[57]. Alors que la très large majorité des répondants approuvent le projet d'ériger ces comportements en infraction autonome, 64 participants (sur 72 avis exprimés) ont proposé des modifications[58].

L'art. 34 de la Convention d'Istanbul[59] définit le harcèlement comme le fait d'adopter intentionnellement, à plusieurs reprises, un comportement menaçant dirigé envers une autre personne, conduisant celle-ci à craindre pour sa sécurité[60]. Même si des actes isolés peuvent être socialement acceptables, il convient de prendre en considération le comportement global de l'auteur pour juger de son caractère menaçant[61].

Actuellement, les actes de *stalking* sont réprimés, le cas échéant, au moyen de l'art. 181 CP incriminant la contrainte[62]. En effet, le Tribunal fédéral considère qu'un ensemble d'actes séparés socialement acceptables peuvent, ensemble, constituer une contrainte s'ils déploient sur la liberté d'action de la victime un effet d'entrave comparable à celui de la violence ou de la menace requises dans l'énoncé de fait l'égal[63]. Ainsi, l'infraction de contrainte peut être réalisée par une accumulation de comportements distincts de l'auteur, par exemple lorsque

54 Avec d'autres participants à la procédure de consultation, nous sommes d'avis que l'infraction devrait être appelée « harcèlement » et non « harcèlement obsessionnel » car l'adjectif est peu précis, et la notion d'obsession n'apparaît pas telle quelle dans les éléments constitutifs de l'infraction. L'inclure dans le titre marginal risque donc de créer de la confusion lors de l'interprétation de la loi.

55 Pour une évaluation du droit suisse en la matière et des recommandations d'amélioration, voir SCHWARZENEGGER/GURT.

56 CAJ-CN, Avant-projet.

57 Voir OFJ, Synthèse stalking. Il y a eu 78 réponses et 72 prises de position.

58 OFJ, Synthèse stalking, p. 4 et 5.

59 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), RS 0.311.35.

60 RO 2018 1119.

61 KNEIFL, p. 859.

62 ATF 141 IV 437, consid. 3.2.2, JdT 2017 IV 141.

63 ATF 137 IV 326, consid. 3, JdT 2012 IV 279 ; ATF 141 IV 437, consid. 3, JdT 2017 IV 141.

celui-ci importune sa victime par sa présence de manière répétée pendant une période prolongée[64]. L'art. 181 CP suppose, d'une part, que le comportement incriminé oblige la victime à agir, à tolérer ou à omettre de faire un acte et, d'autre part, que cela puisse être appréhendé comme le résultat d'un comportement de contrainte plus précisément circonscrit[65]. L'intensité requise par l'art. 181 CP peut néanmoins résulter du cumul de comportements divers ou de la répétition de comportements identiques sur une durée prolongée[66]. Pour apprécier l'existence d'un harcèlement constitutif d'une contrainte, le Tribunal fédéral ne distingue pas les comportements en ligne et hors ligne[67]. Si elle permet partiellement d'atteindre le but poursuivi, cette interprétation extensive de l'art. 181 CP pose néanmoins quelques difficultés. En effet, elle nécessite de déformer la notion de causalité, car, dans une telle configuration, ce n'est pas un acte de contrainte qui produit le résultat exigé par l'énoncé de fait légal, mais un ensemble d'actes ; chaque acte pris séparément ne cause pas l'entrave à la liberté de la victime[68]. À son tour, ce fait rend ardue la distinction entre contrainte consommée et tentative de contrainte[69]. Les partisans de l'adoption d'une disposition *ad hoc* pour réprimer le harcèlement (obsessionnel) ont également relevé que la jurisprudence du Tribunal fédéral est empreinte de notions juridiques indéterminées[70] qui créent une certaine insécurité juridique[71].

La nouvelle norme réprimant le harcèlement (obsessionnel) est conçue comme une infraction contre la liberté. Le bien juridique protégé est, ou devrait être, le sentiment de sécurité de la victime[72] et la liberté intérieure censée garantir à la personne concernée la libre formation et le maintien de son équilibre psychique[73]. Le comportement typique consiste, alternativement, à[74] :

– Traquer, c'est-à-dire suivre, la victime à pied ou dans un véhicule ; l'épier ou l'observer, chez elle ou ailleurs (notamment sur le lieu de travail) ;
– Harceler la victime, par le biais d'appels téléphoniques, de SMS, de courriels, d'envois postaux (lettres, cadeaux), de messages sur les réseaux sociaux, *etc*. À noter que le contenu des missives ne doit pas nécessairement être sexuel pour réaliser l'infraction ;

64 ATF 129 IV 262, consid. 2.3-2.5, JdT 2005 IV 207.
65 TF, 6B_559/2020 du 23 septembre 2020, consid. 1.1.
66 ATF 141 IV 437, consid. 3.2.2, JdT 2017 IV 141.
67 MÉTILLE, Conséquences, p. 126, N 5.
68 CAJ-CN, Rapport stalking, point 2.2.3.
69 CAJ-CN, Rapport stalking, point 2.2.3.
70 A l'exemple de l'ATF 141 IV 437, c. 3.2.2, JdT 2017 IV 141, dans lequel apparaissent les expressions « *gewisse Intensität* », « *längere Zeit* », ou encore « *Vielzahl von Belästigungen* ».
71 SCHWARZENEGGER/GURT, p. 12.
72 CAJ-CN, Rapport stalking, Condensé.
73 CAJ-CN, Rapport stalking, point 3.2.2.
74 CAJ-CN, Rapport stalking, point 4.1.2.

– Menacer la victime, qui est la même notion qu'à l'art. 180 CP.

Selon le projet, l'auteur devrait agir *obstinément*[75] pour se rendre punissable, soit un adverbe qui n'apparaît dans aucune autre infraction pénale. En introduisant ce terme, la Commission souhaitait exprimer le fait que l'auteur doive commettre plus de deux actes, agir sur une certaine période et faire preuve d'un certain acharnement[76]. De nombreux participants à la procédure de consultation se sont opposés à l'usage de ce terme, jugé trop vague, pour lui préférer un adverbe se référant à la répétition d'actes et qui existerait déjà dans le Code pénal (comme « *wiederholt* » en allemand ou « à réitérées reprises » en français)[77]. Cette position doit être approuvée.

L'art. 181*b* AP-CP réprimerait une infraction matérielle, le résultat requis étant que la victime fait, ne fait pas ou laisse faire un acte à cause du comportement de l'auteur. La formulation « *l'entrave dans la libre détermination de sa façon de vivre* » n'est pas très heureuse à cet égard, car elle ne correspond pas au bien juridique que le législateur dit vouloir protéger avec cette norme, à savoir « *le sentiment de sécurité »* et *« la liberté intérieure* » ; elle a toutefois été préférée à l'expression « *atteinte à sa façon de vivre* », notamment, pour ne pas empêcher l'application de la norme aux cas où l'auteur cherche à entamer une relation sentimentale avec la victime (auquel cas il ne veut pas lui porter atteinte[78]). Il y aurait par exemple entrave à la libre détermination de la façon de vivre de la victime si celle-ci modifie ses horaires pour éviter l'auteur ou renonce à se rendre en certains lieux pour ne pas le rencontrer ou se faire épier par lui. Dans ce cadre, il conviendrait de se demander si une personne raisonnable aurait réagi de la même manière que la victime dans une situation semblable[79].

Le harcèlement (obsessionnel) serait une infraction intentionnelle, pour laquelle le dol éventuel serait suffisant[80], et serait poursuivie d'office.

L'avant-projet propose d'ajouter l'art. 181*b* AP-CP à la liste des infractions pour lesquelles une suspension de la procédure est possible au sens de l'art. 55*a* CP, lorsque les actes sont commis dans le cadre d'une relation de couple (antérieure, cas échéant), ce qui est le cas dans 30 à 50% des affaires de harcèlement[81]. Une surveillance de la correspondance par poste et

---

75 La formulation actuelle est ambiguë car la position de l'adverbe obstinément dans la phrase sous-entend qu'il ne concernerait que le verbe « menacer ». Afin d'aligner le texte sur la volonté du législateur, il faudrait le reformuler de la façon suivante : « *Quiconque, de façon obstinée, traque, harcèle ou menace une personne…* ».

76 CAJ-CN, Rapport stalking, point 4.1.2.

77 OFJ, Synthèse stalking, p. 12 s.

78 CAJ-CN, Rapport stalking, point 4.1.2.

79 CAJ-CN, Rapport stalking, point 4.1.2.

80 CAJ-CN, Rapport stalking, point 4.1.2.

81 CAJ-CN, Rapport stalking, point 3.2.3.

télécommunication au sens de l'art. 269 CPP[82] serait également possible, puisque l'art. 181*b* CP serait inclus dans le renvoi de l'art. 269 al. 2 CPP. Du point de vue de la prescription, l'art. 181*b* CP réprimerait une unité juridique d'actions, avec pour conséquence que le *dies a quo* serait le (lendemain du[83]) jour où le dernier acte a été commis, conformément à l'art. 98 lit. b CP[84].

Du point de vue des concours, l'art. 181*b* AP-CP primerait les art. 180 et 181 CP à titre de *lex specialis*. L'art. 181*b* AP-CP absorberait les voies de fait (art. 126 CP) comme la contrainte le fait actuellement, tandis que d'éventuels lésions corporelles, dommages à la propriété ou séquestrations seraient retenus en concours avec le harcèlement (obsessionnel)[85].

Enfin, notons que, depuis le 1er juillet 2023, l'art. 179*septies* CP réprimant l'utilisation abusive d'une installation de télécommunication ne requiert plus le dessein spécial d'agir « *par méchanceté ou par espièglerie* ». Cette suppression a notamment pour effet de rendre cette incrimination plus facilement applicable à des actes de harcèlement, par exemple lorsque l'auteur envoie un très grand nombre de messages à la victime dans lesquels il lui déclare sa flamme[86]. À notre sens, toutefois, le futur art. 181*b* CP absorbera l'art. 179*septies* CP, comme l'actuel art. 180 CP l'absorbe quand il est appliqué à des comportements de *stalking*[87], car ce sont les mêmes bien juridiques protégés qui seront atteints (même si les deux infractions sont dans des titres différents du Code pénal). En outre, le fait d'essayer d'entrer en contact avec une personne à de multiples reprises constitue précisément un « *harcèlement* » au sens de l'art. 181*b* CP, de sorte que l'application de l'art. 179septies CP devrait être réservée aux cas les moins graves au vu de l'échelle des peines de ces deux infractions[88].

V. La pornodivulgation

Proposée en février 2022 par la Commission des affaires juridiques du Conseil des États[89], la nouvelle disposition incriminant la pornodivulgation a

82 Code de procédure pénale du 5 octobre 2007, RS 312.0 (ci-après CPP).
83 ATF 144 IV 161, consid. 2 (relatif au délai de plainte, mais transposable au délai de prescription) ; 97 IV 238, consid. 2, JdT 1972 IV 98.
84 CR CP II-ROTH/KOLLY, art. 98, N 24.
85 CAJ-CN, Rapport stalking, point 3.2.2.
86 FF 2018 2889, p. 2929.
87 BSK StGB II-RAMEL/VOGELSANG, Art. 179*septies*, N 14.
88 L'art. 179*septies* CP prévoit une peine privative de liberté d'un an au plus ou une peine pécuniaire alors que l'art. 181*b* AP-CP dispose qu'une peine privative de liberté de trois ans au plus ou une peine pécuniaire pourrait être ordonnée en cas de harcèlement obsessionnel.
89 FF 2022 687, p. 12.

été plébiscitée par la Chambre Haute en juin de la même année[90]. Elle l'a fait contre l'avis du Conseil fédéral qui, bien qu'en reconnaissant la nécessité de la novelle, souhaitait élargir son champ d'application à tout contenu visant à ridiculiser autrui (non uniquement aux contenus à caractère sexuel), ainsi que lier cette révision à l'initiative parlementaire sur l'incrimination du cyberharcèlement[91]. Le Conseil national s'est rallié au Conseil des États en décidant de limiter l'infraction de divulgation aux contenus à caractère sexuel et de ne pas protéger l'ensemble du domaine secret et l'honneur[92].

Intitulé « *transmission indue d'un contenu non public à caractère sexuel* », le nouvel art. 197*a* nCP aura la teneur suivante : « [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.* ». Cette disposition entrera en vigueur le 1er juillet 2024[93].

Un contenu non public à caractère sexuel peut être transmis pour plusieurs raisons. La transmission de tels contenus peut notamment s'inscrire dans une volonté de *revenge porn* (vengeance pornographique), une pratique qui consiste à publier après une rupture amoureuse des photos ou des vidéos intimes de son ancien ou ancienne partenaire afin de lui nuire pour se venger[94]. Selon la Cour européenne des droits de l'homme, la pornodivulgation est une forme de violence domestique[95]. Sous l'ancien droit, la vengeance pornographique était difficile à incriminer sous le titre des infractions contre l'honneur, car « *le fait d'entretenir des rapports sexuels est quelque chose de tout à fait commun, qui*

90 BO CE 2022 502.

91 CAJ-CE, Rapport Projet 3, p. 3 : « *L'omniprésence d'Internet dans notre quotidien a un effet désinhibiteur sur les personnes désireuses de diffuser des photos ou des vidéos compromettantes. Chacun, à tout moment, peut faire des clichés ou des enregistrements avec son téléphone portable et les transmettre via les réseaux sociaux ou des services de messagerie, ou même les publier en restant anonyme. Dans le débat public, la palette des actes indésirables n'a cessé de s'étendre ; il n'y a plus forcément de lien avec la pornodivulgation*. ».

92 BO CN 2022 2146 ; HADORN, 2023, p. 154.

93 DFJP, Communiqué.

94 MAZOU/ISELIN, p. 52. La publication peut aussi être le fait du nouveau ou de la nouvelle partenaire envers l'ancien ou ancienne partenaire.

95 ZIMMERMANN, p. 515 s. ; CourEDH, *Buturuga c. Roumanie*, arrêt du 11 février 2020, n°56867/15, § 40-42, 74 ; CourEDH, *Volodina c. Russie* (n°2), arrêt du 14 septembre 2021, n°40419/19, § 48-49.

ne saurait […] *être considéré en soi comme contraire à l'honneur* »[96]. L'infraction de pornodivulgation permettra de combler cette lacune.

Le bien juridiquement protégé par la nouvelle incrimination sera la sphère intime et la pudeur dans le domaine sexuel[97], tout comme à l'art. 198 CP[98]. Certes, les infractions visées à l'art. 197 al. 2 ou 198 al. 1 CP protègent un sentiment général de pudeur, et concrètement, ils évitent au « citoyen suisse moyen » d'être heurté par des contenus obscènes[99]. De son côté et à notre sens, l'art. 197*a* nCP vise davantage à protéger le droit de chacun et chacune à garder secret un aspect particulier de sa vie intime[100], à savoir sa vie sexuelle et les parties intimes de son corps (sexe, poitrine, fesses)[101].

Les éléments constitutifs de l'infraction seront les suivants :

– Il faudra tout d'abord que l'auteur adopte un certain comportement, en l'occurrence transmettre à un tiers (al. 1), respectivement rendre public (al. 2), un contenu ;
– Le contenu en question doit être initialement non public et à caractère sexuel ;
– La victime ne doit pas consentir à la transmission ou à la publication du contenu ;
– Le lésé sera toujours une personne (physique) identifiable sur le contenu ;
– L'auteur doit agir intentionnellement.

L'infraction est poursuivie sur plainte ; à noter que le délai de plainte commence à courir dès le moment où le lésé (à savoir la personne identifiable sur le contenu) a connaissance de l'infraction et de l'auteur (art. 31 CP).

S'agissant de la transmission à un tiers, nous considérons que l'infraction n'est pas déjà réalisée lorsque le contenu est simplement montré ; en effet, le terme

---

96 MAZOU/ISELIN, p. 53.
97 CAJ-CE, Rapport Projet 3, p. 55.
98 BO CE 2022 501 (Vara).
99 ATF 128 IV 260, consid. 2.1, JdT 2006 IV 83; TF, 6P.123/2003 du 21 novembre 2003, consid. 5.
100 En droit privé, et pour délimiter l'ampleur de la protection accordée par les art. 28 CC, le Tribunal fédéral distingue les trois sphères de la vie humaine, soit intime, privée (« *événements que chacun veut partager avec un nombre restreint d'autres personnes* » ATF 130 III 28, consid. 4.2) et publique (STEINAUER/FOUNTOULAKIS, p. 191 s.). La sphère intime, qui nous intéresse ici, est définie comme ce que chacune et chacun garde secret ou ne partage qu'avec certaines personnes bien déterminées. En droit civil, il s'agit « *des faits liés à la santé d'une personne (par ex. le dossier d'un patient), des conflits familiaux, des secrets financiers, des goûts et préférences en matière sexuelle* » (CR CC I-JEANDIN, art. 28, N 40).
101 Cela semble être également l'avis de la Commission des affaires juridiques du Conseil des États, qui commente la disposition adoptée en indiquant comme bien juridiquement protégé la pudeur et la sphère intime de l'individu (CAJ-CE, Rapport Projet 3, p. 55).

transmettre (en allemand : *weiterleiten* et en italien : *trasmettere*) implique que le tiers impliqué soit rendu maître du contenu. On pense évidemment à l'envoi de messages (courriels ou messagerie telle que *WhatsApp*, *Signal*, *etc*.). La version qualifiée de l'infraction, prévue à l'al. 2 de la disposition, suppose d'avoir rendu le contenu public. Pour interpréter cet élément constitutif objectif, on peut se référer à la jurisprudence rendue en application de l'art. 261bis CP qui suppose également d'avoir agi publiquement. Ainsi, rend déjà public celui qui diffuse un contenu, même à un nombre limité de personnes, lesquelles ne font cependant pas partie de son cercle familial ou d'amis ou encore hors d'un « *environnement de relations personnelles ou empreint d'une confiance particulière* »[102]. On pense par exemple à la mise en ligne sur une page Internet librement accessible ou à la diffusion d'un contenu sur un groupe de messagerie qui inclurait des personnes qui ne sont pas des proches (groupe de classe ou professionnel).

S'agissant de l'aggravante prévue à l'al. 2, la question se pose de savoir si, comme pour la variante de base, l'infraction suppose toujours un dépôt de plainte ou est alors poursuivie d'office. Le texte ne le précise pas. Alors que la Commission des affaires juridiques du Conseil des États semble penser que l'infraction prévue à l'art. 197*a* al. 2 CP est poursuivie d'office (toutefois sans justification)[103], nous considérons au contraire que l'infraction reste poursuivie sur plainte. En effet, les seuls aspects qui font l'objet d'une modification sont le comportement de l'auteur et la sanction. Par une simple interprétation systématique, on constate que le législateur précise toujours explicitement, dans les versions qualifiées d'infractions poursuivies sur plainte, que l'auteur est alors poursuivi d'office. Il suffit pour s'en convaincre de lire le texte des art. 123 ch. 2, 125 ch. 2, 126 ch. 2, 144 al. 2 et 3[104], 144bis al. 2 et, enfin, 180 al. 2 CP. Par ailleurs, il nous semble important de laisser la victime choisir de déposer ou non une plainte, l'ouverture d'une procédure entrainant une (nouvelle) publicisation plus large du contenu en question.

Le contenu doit être « à caractère sexuel », ce qui englobe évidemment la pornographie[105], mais également des contenus moins explicites comme des

---

[102] TF, 6B_748/2022 du 2 juin 2023, consid. 2.1 ; ATF 130 IV 111, consid. 5.2.2, JdT 2005 IV 292; TF, 6B_636/2020 du 10 mars 2022, consid. 5.1, non publié *in* ATF 148 IV 113, JdT 2022 IV 247. Ég. ATF 149 IV 170, consid. 1.1.2 *i.f.* (succinct sur ce point).

[103] CAJ-CE, Rapport Projet 3, p. 56.

[104] Dans le texte de l'art. 144 CP, le code précise dans les deux cas que la poursuite a lieu d'office, même pour l'al. 3 qui suit pourtant une infraction qualifiée également poursuivie d'office.

[105] La pornographie est définie par la jurisprudence comme du contenu visant l'excitation sexuelle, insistant exagérément sur les parties génitales et les rapports sexuels, réduisant l'humain à l'état objet (ATF 133 IV 31, consid. 6.1.1 ; ATF 131 IV 64, consid. 10.1.1, JdT 2007 IV 161; ATF 128 IV 260, consid. 2.1, JdT 2006 IV 183).

photographies d'un corps nu, des messages érotiques, ou tout ce qui évoque le désir ou les relations sexuelles, sans nécessairement revêtir le caractère particulièrement cru de la pornographie[106]. S'agissant du « vecteur » de contenu, la norme vise des écrits (quel qu'en soit le support), des enregistrements sonores ou visuels, des images, des objets ou des représentations[107].

Le contenu doit être non public ; il ne s'agit pas de réprimer celui ou celle qui transmet des films pornographiques déjà mis en circulation sans avoir l'accord des acteurs et actrices qui y figurent. On s'interroge cependant sur la punissabilité de celui qui transfère ce qu'il a reçu en application de l'art. 197*a* al. 2 CP – donc du contenu qui a déjà été rendu public une première fois. Le but de la norme, à savoir protéger la sphère intime de la personne identifiable, nous semble clairement plaider en faveur de la punissabilité d'un tel comportement, du moment que le contenu est, de façon reconnaissable, *initialement* non public. On viderait complètement la norme de sa substance et ainsi de son effet protecteur si, après que le contenu a été une première fois rendu public, quiconque pouvait impunément transférer l'image ou l'écrit compromettant à autrui, lequel pourrait à nouveau le transmettre, *etc*.[108].

Seul le consentement de la personne visée évite à l'auteur de réaliser la typicité[109] de l'infraction. Il n'y a pas d'infraction, par exemple, si la personne identifiable a elle-même rendu public un contenu à caractère sexuel. En revanche, si elle a transmis à une personne, ou même à plusieurs personnes déterminées, une image à caractère sexuel, son transfert à un tiers sans son consentement et, a fortiori, la publication de ce contenu est punissable. La typicité est également réalisée lorsque l'auteur a acquis contre rémunération du contenu à caractère sexuel ; ainsi la personne qui paie un utilisateur ou une utilisatrice de la plateforme « *OnlyFans* », par exemple, pour acquérir du contenu à caractère sexuel ne peut pas transmettre ce contenu plus loin sans violer le nouvel art. 197*a* CP, à moins d'avoir le consentement de la personne qui y est représentée.

La personne identifiable sur le contenu doit nécessairement être une personne physique, puisque seul un être humain est titulaire d'une sphère

106 CR CP II-CAMBI FAVRE-BULLE, art. 197, N 8 ; CORBOZ, art. 197, N 18.

107 CAJ-CE, Rapport Projet 3, p. 55.

108 Il nous semble que la situation est analogue à celle dans laquelle une personne « like » ou « partage » une publication diffamatoire sur Facebook, dont le Tribunal fédéral a eu l'occasion de dire que c'est bien constitutif d'une infraction, précisément dans la variante de la « propagation » au sens de l'art. 173 CP (ATF 146 IV 23, JdT 2020 IV 154), car le cercle des personnes ayant accès à la publication est alors élargi.

109 Et non pas d'agir de façon typique mais licite. V. par analogie, BSK StGB II-DELNON/RÜDY, Art. 186, N 38.

intime/sexuelle[110]. La Commission précise encore que le contenu à caractère sexuel peut « désigner » ou « viser » la personne[111]. Selon nous, cela implique que la norme interdit la transmission ou la diffusion d'hypertrucages (« *deep fakes* »), puisque la « personne qui y est identifiable » n'a pas besoin d'y figurer effectivement ; elle n'est « que » visée par la publication et il suffit qu'elle soit reconnaissable, quelle que soit la manière utilisée par l'auteur (qu'on lui voie le visage, qu'il la désigne nommément comme figurant sur le contenu ou qu'un autre signe permette de l'identifier).

Enfin, l'auteur doit agir intentionnellement, c'est-à-dire qu'il sait ou admet que le contenu a un caractère sexuel, qu'il est initialement non public, et qu'il le transmet à un tiers sans le consentement de la personne identifiable[112].

Comme les biens juridiques protégés ne sont pas identiques, on peut imaginer un concours idéal avec la pornographie, notamment si la victime est mineure (art. 197 al. 5 CP) – pour autant que le contenu à caractère sexuel puisse en sus être considéré comme « pornographique ». De même, l'art. 197 al. 1 et 2 CP pourra également trouver application en concours pour réprimer l'atteinte à la pudeur du tiers ayant reçu le contenu alors qu'il a moins de 16 ans (art. 197 al. 1 CP) ou qu'il n'a pas été prévenu (art. 197 al. 2 CP). Si la victime a été filmée à son insu, l'art. 179^{quater} CP trouvera également application, en concours réel, puisque le comportement de l'auteur est successif (création du contenu puis transmission ou publication)[113].

À noter que la transmission de contenu à caractère sexuel peut ensuite donner lieu à une (tentative d') extorsion (aussi parfois appelée « sextorsion »). Il s'agit d'un chantage exercé sur une personne à partir de photos ou de vidéos la montrant nue ou en train d'accomplir des actes sexuels[114]. Souvent, l'auteur menace de publier les éventuels clichés ou vidéos, de les envoyer aux proches de la victime ou à ses collègues dans le but d'obtenir de l'argent, une rencontre, de nouvelles images ou même un rapport sexuel. En pareil cas, l'auteur peut être, selon nous, poursuivi pour contrainte (ou tentative de contrainte) selon l'art. 181 CP, extorsion au sens de l'art. 156 CP (s'il tente d'obtenir des valeurs patrimoniales)[115] ou viol (pour un rapport sexuel qualifié)[116]. Les biens

110 On se réfère à la jurisprudence rendue en application de l'art. 180 CP, que l'on applique ici par analogie, et qui réserve les sentiments à la personne physique, à l'exclusion de la personne morale : ATF 141 IV 1, consid. 3.2.4.

111 CAJ-CE, Rapport Projet 3, p. 55. En se référant au bien juridique.

112 CAJ-CE, Rapport Projet 3, p. 56.

113 MAZOU/ISELIN, p. 54.

114 V. MAZOU/ISELIN, p. 46.

115 V. TF, 6B_981/2019 du 12 novembre 2020, consid. 4.

116 Pour un exemple, v. TF, 6B_981/2019 du 12 novembre 2020, consid. 2 : viol admis mais tentative de viol niée. V. également TF, 6B_1040/2013 du 18 août 2014.

juridiquement protégés ne sont en effet pas les mêmes, de sorte que le concours doit nécessairement être idéal[117].

Enfin, les courriels de « fake-sextorsion » représentent une méthode d'attaque très répandue actuellement[118]. En l'occurrence, les escrocs prétendent dans un courriel qu'ils ont rassemblé des photos ou des vidéos sur lesquelles on verrait le destinataire du courriel consulter des sites pornographiques. Les maîtres chanteurs menacent de publier ces photos ou ces vidéos si la rançon exigée n'est pas versée dans un délai donné. Ces courriels sont envoyés au hasard dans l'espoir que certaines personnes, parmi les destinataires, aient effectivement consulté des sites pornographiques peu de temps auparavant. Par leurs menaces, les criminels entendent intimider leurs victimes et les amener à verser la rançon. En l'absence de contenu à caractère sexuel, l'art. 197*a* CP n'est pas applicable, seul l'art. 181 CP ou 156 CP le serait.

VI. Le pédopiégeage en ligne

Le pédopiégeage en ligne, également désigné sous les appellations de *sollicitation d'enfants à des fins sexuelles*, *grooming*[119] ou *cybergrooming*, ne fait pas l'objet d'une définition unique et consensuelle en doctrine[120]. Ainsi, selon les auteurs, le *grooming* désigne une pratique qui consiste pour un adulte à prendre contact avec un enfant ou un adolescent au moyen des nouvelles technologies (par exemple via des *chats*, des services de messagerie ou des plateformes de jeux en ligne[121]) dans le but d'obtenir un contenu à caractère sexuel[122] (par exemple un film pornographique[123]), d'entretenir des conversations de nature sexuelle[124] ou d'initier une rencontre pour obtenir un acte d'ordre sexuel dans le monde physique[125]. Le Tribunal pénal fédéral définit le *grooming* de manière large, en relevant qu'il s'agit du comportement d'adultes envers des enfants et des adolescents par le biais d'Internet ou d'autres

117 À noter toutefois que la CAJ-CE semble être d'un avis différent, arguant que l'infraction la plus grave devrait alors absorber la novelle (Rapport Projet 3, p. 56-57).
118 Voir OFSC, Fake sextorsion.
119 MOREILLON/VON WURSTEMBERGER, p. 626, N 2458. Le terme de *grooming* est issu du verbe anglais « *to groom* », qui signifie « préparer » (MUGGLI, p. 38) ; dans le monde anglo-saxon, il n'est pas réservé à des activités en ligne.
120 MEYER, p. 225.
121 TC/ZG, S 2023 28 du 27 octobre 2023, VII, consid. 1. 4.
122 MUGGLI, p. 37.
123 MAZOU/ISELIN, p. 55.
124 TPF, BG.2017.34 du 29 décembre 2017, consid. 4.2 et les références citées ; MEYER, p. 225.
125 MÉTILLE, Protection, p. 141 ; MAZOU/ISELIN, p. 55 ; HEINZL, p. 88, n°353 ; HADORN, 2022, p. 237.

technologies de communication modernes, qui vise à établir un « contact à motivation sexuelle »[126]. Concrètement, le « *groomeur* » met généralement en place une stratégie qui consiste à traiter un enfant comme son égal, à partager avec lui des activités et des intérêts typiques de son âge ou à lui offrir des cadeaux afin de gagner sa confiance pour obtenir, dans un deuxième temps, une satisfaction d'ordre sexuelle[127].

La doctrine distingue traditionnellement le *grooming* au sens strict du *grooming* au sens large.

Par *grooming au sens strict*, on entend le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant dans le but de commettre à son encontre une infraction contre l'intégrité sexuelle, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre. Cette définition est ancrée à l'art. 23 de la Convention de Lanzarote[128]. Selon cette conception étroite, le simple fait d'échanger des propos à teneur sexuelle avec un enfant ne constitue pas encore du *grooming*[129], et une simple proposition de rendez-vous ne réalise pas l'infraction si elle n'est pas suivie d'une (tentative de) véritable rencontre[130].

Le *grooming au sens large* recouvre une vaste palette de comportements de moindre intensité, soit tous ceux qui mettent l'enfant en confiance pour obtenir un contenu ou une discussion à caractère sexuel sans qu'une rencontre dans le monde réel ne soit (encore) prévue[131]. Cette définition plus large tient compte du fait que certains auteurs n'ont pas l'intention de rencontrer physiquement l'enfant et souhaitent uniquement obtenir ou partager un contenu à caractère sexuel[132] ou entretenir une conversation axée sur le sexe avec un enfant[133]. Le *grooming* au sens large englobe ainsi les conversations sexualisées avec des enfants, souvent étayées d'images[134], alors que le *grooming* au sens strict se termine par une proposition et l'organisation d'une rencontre[135].

Il est difficile de mesurer l'ampleur du phénomène du *grooming* en Suisse, notamment car il ne s'agit pas d'une infraction (voir *infra*) et que sa commission

126 TPF, BG.2017.34 du 29 décembre 2017, consid. 4.2.
127 TC/ZG, S 2023 28 du 27 octobre 2023, consid. 1.4.
128 Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote), RS 0.311.40.
129 MEYER, p. 225 et 232.
130 MUGGLI, p. 43.
131 MEYER, p. 225.
132 MUGGLI, p. 38.
133 MEYER, p. 225 ; MUGGLI, p. 39.
134 Pour un exemple de *grooming* au sens large, voir TC/GE, AARP/300/2018 du 24 septembre 2018.
135 MUGGLI, p. 39.

n'est donc pas répertoriée par les indicateurs officiels de la délinquance. Toutefois, il semblerait que cette pratique se soit largement répandue au cours des dernières années[136]. Ainsi, selon une étude menée en Suisse, 13 à 33% des mineurs interrogés disent avoir été abordés sur Internet par une personne inconnue présentant des intentions sexuelles indésirables[137]. Le Tribunal pénal fédéral reconnaît d'ailleurs qu'Internet constitue une plateforme qui facilite les activités pédocriminelles et que l'approche ainsi que la mise en confiance d'enfants sont largement facilitées par les nouvelles technologies[138]. Plus généralement, la jurisprudence admet que la pratique du *grooming* soit prise en considération pour évaluer le risque de récidive d'un auteur condamné pour des actes d'ordre sexuel avec des enfants, reconnaissant ainsi le risque que crée une telle situation[139].

Au niveau international, la Suisse s'est engagée à réprimer le grooming au sens strict conformément à l'art. 23 de la Convention de Lanzarote[140], mais n'a aucune obligation s'agissant du *grooming* au sens large.

Pour le droit suisse, le *grooming* au sens strict concerne les situations dans lesquelles des échanges entre l'adulte et l'enfant ont eu lieu sur Internet, et ont été suivis d'actes matériels non encore constitutifs d'une tentative d'actes d'ordre sexuels avec des enfants (auquel cas la personne serait de toute façon punissable sous l'égide des art. 22 et 187 CP). Or, la question de savoir si le *grooming* au sens strict est déjà incriminé par le droit pénal suisse fait débat.

Tout le monde s'accorde sur le fait que le *grooming* au sens strict ne fait pas l'objet d'une infraction spécifique[141]. On pourrait éventuellement le qualifier d'actes préparatoires à des actes d'ordre sexuel avec un enfant au sens de l'art. 187 CP[142], qui ne sont actuellement pas punissables puisque la liste de l'art. 260*bis* CP ne contient pas l'art. 187 CP. Une partie de la doctrine pense qu'il y a là une lacune[143].

Le législateur estime, au contraire, que le droit suisse permet déjà de réprimer le *grooming* au sens strict. Il renvoie à cet égard à l'ATF 131 IV 100, dans lequel le Tribunal fédéral a retenu qu'un adulte qui pensait avoir rencontré un mineur en ligne (il s'agissait en réalité d'un officier de police) et qui lui avait donné rendez-vous dans un fast-food situé dans la gare d'une grande ville pour avoir des relations sexuelles avec lui, puis s'était rendu au lieu du rendez-vous,

136 MUGGLI, p. 40.
137 SUTER *et al.* p. 54.
138 TPF, BG.2017.34 du 29 décembre 2017, consid. 4.2.
139 TF, 1B_89/2022 du 18 mars 2022, consid. 4.4.1 ; TF, 6B_82/2021 du 1er avril 2021, consid. 4.4.1 ; TC/ZG, S 2023 28 du 27 octobre 2023, consid. 3.2.3 et 5.4.
140 MUGGLI, p. 43.
141 MÉTILLE, Protection, p. 25 ; MUGGLI, p. 40 ; MAZOU/ISELIN, p. 56.
142 MUGGLI, p. 44.
143 MUGGLI, p. 110 s. ; MEYER, p. 226 ss.

s'était rendu coupable de tentative d'acte d'ordre sexuel avec un enfant. Se basant sur cet arrêt, le législateur a abandonné l'idée d'ériger en infraction *ad hoc* les actes préparatoires aux actes d'ordre sexuel avec des enfants (art. 187 CP)[144]. Il a considéré que, si l'adulte se rend au rendez-vous avec l'enfant, il commet une tentative, et qu'il ne serait pas adéquat de repousser le seuil de punissabilité en amont, par crainte de criminaliser « *la tentative de la tentative* »[145].

Cette position nous semble erronée, car l'arrêt susmentionné retient une définition de la tentative qui est incompatible avec la définition usuelle du concept et avec tous les autres arrêts du Tribunal fédéral sur le même sujet. En effet, selon la jurisprudence[146] et la doctrine unanime[147], il y a tentative dès qu'il y a *commencement d'exécution* de l'infraction, soit lorsque l'auteur a atteint le point de non-retour, le moment où, selon le cours ordinaire des choses et l'expérience de la vie, l'auteur ne revient plus en arrière dans l'exécution de l'infraction. D'habitude, le Tribunal fédéral applique ce critère strictement. Par exemple, dans un arrêt de 2019[148], il a nié la qualification de tentative de meurtre dans le cas d'un jeune homme qui s'était placé face à son maître d'apprentissage dans l'intention de le poignarder, un couteau à la main, le bras le long du corps, sous prétexte qu'il n'avait pas encore levé le couteau en direction de sa victime lorsqu'il avait été immobilisé par des témoins.

Une interprétation juridiquement correcte de la notion de tentative ne permet donc pas de saisir l'état de fait de l'ATF 131 IV 100 et il demeure donc bien une lacune dans l'ordre juridique suisse. En application de la loi actuellement en vigueur, le *grooming* au sens strict peut uniquement être réprimé si les conditions de la tentative d'actes d'ordre sexuel avec des enfants sont remplies, c'est-à-dire s'il y a eu un commencement d'exécution. Cela ne nous semble pas satisfaisant, car cela signifie que l'adulte qui a exprimé une intention sexuelle sans ambiguïté sur un forum et a effectivement fixé un rendez-vous avec un enfant pour réaliser l'acte n'est pas punissable aussi longtemps qu'il ne se trouve pas dans un lieu isolé propice à avoir des activités de nature sexuelle avec l'enfant immédiatement. Rappelons que l'art. 260bis CP réprimant les actes préparatoires a été adopté dans le but de pouvoir arrêter en cours de

144 Conseil fédéral, Cyber-délits sexuels, p. 3. Une telle proposition était pourtant approuvée par la grande majorité des participants à la consultation ; v. OFJ, Synthèse révision, point 3.2.7 ; CAJ-CE, Rapport Projet 3, p. 69 ; HADORN, 2021, p. 493.

145 CAJ-CE, Rapport Projet 3, p. 69 ; HADORN, 2022, p. 237.

146 Voir. not. ATF 131 IV 100, JdT 2007 IV 95 ; ATF 117 IV 369, JdT 1993 IV 127 ; ATF 114 IV 112, JdT 1989 IV 66.

147 HURTADO POZO/GODEL, § 498 ; CR CP-II-DOLIVO-BONVIN/LIVET, art. 260bis, N 3 ; CR CP I-HURTADO POZO/ILLÀNEZ, art. 22, N 31 ; BSK StGB I-NIGGLI/MAEDER, Art. 22, N 10 s.

148 TF, 6B_1159/2018 du 18 septembre 2019.

préparation des auteurs sur le point de porter une atteinte grave à la vie, l'intégrité physique ou la liberté de leurs concitoyens et de la collectivité[149]. À notre sens, l'adulte qui se prépare à avoir une relation sexuelle avec un enfant représente un danger comparable et devrait donc pouvoir être arrêté avant le point de non-retour.

Une solution pourrait consister dans le fait d'ajouter l'art. 187 CP à la liste des infractions pour lesquelles les actes préparatoires sont déclarés punissables[150]. Le désavantage de cette option réside dans le fait que l'art. 260*bis* CP requiert que l'auteur prenne, conformément à un plan, des dispositions concrètes d'ordre technique ou organisationnel dont la nature et l'ampleur indiquent qu'il s'apprête à passer à l'acte[151]. Or, contrairement à un brigandage ou à une prise d'otage, les actes d'ordre sexuel avec un mineur ne nécessitent pas forcément des préparatifs tels qu'ils seraient susceptibles de tomber sous le coup de cette disposition.

En conséquence, au vu de la complexité du phénomène et de la multiplicité de ses manifestations, l'adoption d'une norme *ad hoc* nous semble opportune[152]. Celle-ci devrait tenir compte du fait que la grande majorité des actes de *grooming* sont actuellement commis en ligne, et que le passage à l'acte ne nécessite pas forcément de grands efforts logistiques. Certes, la preuve de l'intention de l'auteur serait dans certains cas difficile à apporter avant que des actes d'ordre sexuel ne soient concrètement commis[153] ; le Tribunal pénal fédéral reconnaît cette difficulté et indique que l'enquête devra porter sur l'établissement de l'intention de l'auteur dans les cas ambigus[154]. Dans tous les cas, la punissabilité ne serait possible que si l'auteur manifeste, dans le monde physique, son intention de porter atteinte au bien juridique en question, conformément aux principes généraux du droit pénal. Ainsi, l'auteur qui a largement explicité ses intentions en ligne et se rend sur les lieux d'un rendez-vous avec un enfant devrait pouvoir être poursuivi pour *un type ad hoc d'acte préparatoire* sans que l'on doive déformer la notion de « *tentative* » pour ce faire et sans mettre en péril le principe selon lequel « *fürs Denken kann niemand henken* ».

Quant au *grooming au sens large*, il peut être appréhendé par la législation en vigueur comme suit :

149 CR CP II-DOLIVO-BONVIN/LIVET, art. 260*bis*, N 1, renvoyant à FF 1980 I 1216, p. 1229.
150 MUGGLI, p. 112.
151 CR CP II-DOLIVO-BONVIN/LIVET, art. 260*bis*, N 5 s.
152 MEYER, p. 231 ; MAZOU/ISELIN, p. 59.
153 MUGGLI, p. 39 s.
154 TPF, BG.2017.34 du 29 décembre 2017, consid. 4.2.

– Si, par l'entremise d'une webcam, l'auteur mêle un enfant à des actes d'ordre sexuel ou l'incite à en accomplir, l'application de l'art. 187 CP est envisageable[155] ;
– Si l'auteur du *grooming* transmet des images[156] ou des écrits[157] pornographiques à un enfant ou enregistre des images d'actes d'ordre sexuel impliquant l'enfant, l'art. 197 CP peut s'appliquer ;
– Si l'auteur du *grooming* importune l'enfant par des paroles ou des écrits grossiers (par exemple en lui demandant la taille de ses seins, l'état de sa pilosité pubienne ou en l'interrogeant sur ses expériences sexuelles passées), les conditions de l'art. 198 CP sont en principe réunies[158]. L'application de l'infraction de désagréments causés par une confrontation à un acte d'ordre sexuel implique toutefois que l'enfant ou ses représentants légaux aient déposé une plainte pénale dans un délai de trois mois, ce qui n'est pas réaliste dans de nombreux cas[159].

Enfin, en application du droit actuellement en vigueur, aucune infraction n'incrimine le comportement de l'auteur qui prépare l'enfant à une sexualisation de la relation de manière subtile, en gagnant progressivement sa confiance, sans faire de référence sexuelle[160]. Cela nous semble cohérent avec le principe général de droit pénal voulant que la simple idée de commettre une infraction ne soit pas punissable[161].

VII. Conclusion

Comme nous l'avons vu, il a fallu quelques décennies au législateur helvétique pour appréhender l'impact réel d'Internet sur la commission des infractions contre la liberté, l'honneur et l'intégrité sexuelle. Le monde numérique rend la commission de ces infractions beaucoup plus aisée, et les atteintes aux biens juridiques qui en découlent peuvent avoir une ampleur et une durée jamais vues dans le monde physique. En ce sens, il ne nous semble pas correct de dire qu'Internet est *une* manière *parmi d'autres* de commettre ces infractions, et que les incriminations « traditionnelles » suffisent toujours pour en réprimer les auteurs. Bien au contraire : commises en ligne, ces infractions ont des caractéristiques particulières qui, à notre avis, nécessitent une adaptation de la loi pénale.

155 MUGGLI, p. 112 s. ; MEYER, p. 226 s. ; MAZOU/ISELIN, p. 56.
156 MEYER, p. 227 s. ; MAZOU/ISELIN, p. 56.
157 MUGGLI, p. 112 s.
158 MUGGLI, p. 114 ; MEYER, p. 229.
159 MUGGLI, p. 114 ; MEYER, p. 229.
160 MEYER, p. 229.
161 GETH, § 324 ; BSK StGB I-NIGGLI/MAEDER, Art. 22, N 4.

Jusqu'à présent, il nous semble que le législateur a adapté la loi par touches discrètes, avec un résultat pour le moins pointilliste : de loin, on voit bien une répression pénale qui se dessine dans des traits très généraux, mais l'effort est sectoriel, relativement lent, et plutôt hésitant lorsqu'il s'agit d'adopter l'une ou l'autre disposition. Nous sommes d'avis que la protection des biens juridiques lésés ou mis en danger par les activités des auteurs d'infractions en ligne devrait faire l'objet d'une réflexion systématique et globale, ce qui permettrait également de développer des politiques de prévention plus efficaces dans un domaine où le sentiment d'impunité des auteurs semble particulièrement marqué.

VIII. Bibliographie

Doctrine/Littérature

Annina BALTISSER, Datenbeschädigung und Malware im Schweizer Strafrecht, Der Tatbestand des Art. 144bis StGB imVergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, Zurich 2013 ; **Georg BORGES/Jörg SCHWENK/Carl-Friedrich STUCKENBERG/Christoph WEGNENER**, Identitätsdiebstahl und Identitätsmissbrauch im Internet : Rechtliche und technische Aspekte, Berlin/Heidelberg 2011 (cité : BORGES *et al.*) ; **Andreas BUCHER**, Personnes physiques et protection de la personnalité, 5^{e} éd., Bâle 2009 ; **Bernard CORBOZ**, Les infractions en droit suisse, vol. 1, 3^{e} éd, Berne 2010 ; **David M. DOUGLAS**, Doxing: a conceptual analysis, Ethics and Information Technology, vol. 18 (3), 2016 ; **Gilles FAVAREL-GARRIGUES/Laurent GAYER**, Vigilantisme, *in* Guillaume PETIT *et al.* (éds), DicoPart - Dictionnaire critique et interdisciplinaire de la Participation, 2^{e} éd., 2022 (<https://www.dicopart.fr/vigilantisme-2022>, *consulté le 17.3.2024*) ; **Christopher GETH**, Strafrecht, Allgemeiner Teil, 7^{e} éd., Bâle 2021 ; **Isabelle HANSEN/Darren LIM**, Doxing democracy : Influencing elections via cyber vote interferences, Contemporary Politics, vol. 25 (2), 2019, p. 150 ss (<https://www.tandfonline.com/doi/full/10.1080/13569775.2018.1493629?scroll=top&needAccess=true>, *consulté le 17.3.2024*) ; **Sandra HADORN**, Gesetzgebung, forumpoenale 2/2023, p. 154 ss (cité : HADORN, 2023) ; **Sandra HADORN**, Gesetzgebung, forumpoenale 3/2022, p. 236 ss (cité : HADORN, 2022) ; **Sandra HADORN**, Gesetzgebung, forumpoenale 6/2021, p. 493 ss (cité : HADORN, 2021) ; **Anja HASLER**, Gesetzgebung forumpoenale 3/2014, p. 183 ss ; **Kathrin HEINZL**, Prostitution im Schweizer Strafrecht : Die Strafbarkeit von Prostituierten, Zuhältern und Freiern, 2016, p. 83 ss ; **José HURTADO POZO/Thierry GODEL**, Droit pénal, 4^{e} éd., Zurich 2023 ; **Quentin JACQUEMIN**, Le droit suisse permet-il de réprimer les deepfakes?, *in* Florence GUILLAUME (éd.), La technologie, l'humain et le droit, Berne 2023, p. 313 ss ; **Les JOHNSTON**, What Is Vigilantism ?, The British Journal of Criminology, vol. 36, Numéro 2, 1996, p. 220 ss ; **Sherin KNEIFL**, Besserer strafrechtlicher Schutz vor Stalking, RSJ 119/2023, p. 859 ; **Miriam MAZOU/Charlotte ISELIN**, Quelle répression pour les cyber-atteintes à l'intégrité sexuelle : revenge porn, (cyber)harcèlement, sextorsion, grooming, *in* Camille PERRIER DEPEURSINGE/Nathalie DONGOIS (éds), Infractions contre l'intégrité sexuelle, Berne 2022, p. 33 ss ; **Pauline MEYER**, Sollicitation d'enfants à des fins sexuelles en ligne, PJA 2021, p. 224 ss ; **Sylvain MÉTILLE/Joanna AESCHLIMANN**, Infrastructures et données informatiques: quelle protection au regard du code pénal suisse ?, RPS 132/2014, p. 283 ss (cité : MÉTILLE/AESCHLIMANN) ; **Sylvain MÉTILLE**, Conséquences de l'absence d'infraction de

stalking dans un cas concret : BGE 141 IV 437, Medialex 2016, p. 125 ss (cité : MÉTILLE, Conséquences) ; **Sylvain MÉTILLE**, Internet et droit : Protection de la personnalité et questions pratiques, 2017, p. 23 ss (cité : MÉTILLE, Protection) ; **Gilles MONNIER**, Le hacking: enjeux actuels à la lumière du cas «Hacker-Croll», Medialex 2010, p. 130 ss ; **Laurent MOREILLON**, Nouveaux délits informatiques sur Internet, Medialex 2001, p. 21 ss ; **Laurent MOREILLON/Alain MACALUSO/Nicolas QUELOZ** (éds), Code pénal II : art. 111 à 392 CP, Commentaire romand, 2e éd., Bâle 2021 (cité : CR CP II-AUTEUR/E, art. X, N Y) ; **Laurent MOREILLON/Mathilde VON WURSTEMBERGER**, Coopération judiciaire pénale dans l'Union européenne, Genève/Zurich/Bâle 2023 (cité : MOREILLON/VON WURSTEMBERGER) ; **Sandra MUGGLI**, Im Netz ins Netz – Pädokriminilität im Internet und der Einsatz von verdeckten Ermittlern und verdeckten Fahndern zu deren Bekämpfung, Genève/Zurich/Bâle 2014, p. 29 ss et 83 ss ; **Alexander Marcel NIGGLI/Hans WIPRÄCHTIGER** (éds), Strafrecht I : Art. 1-136, 4e éd., Bâle 2019 (cité : BSK StGB I-AUTEUR/E, Art. X, N Y) ; **Marcel Alexander NIGGLI/Hans WIPRÄCHTIGER** (éds), Strafrecht II : Art. 137-392, Jugendstrafrecht, 4e éd., Bâle 2019 (cité : BSK StGB II-AUTEUR/E, Art. X, N Y) ; **Christa PFISTER**, Hacking in der Schweiz : Im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Berlin/Vienne/Zurich 2008 ; **Yannick REBER**, Der neue Tatbestand des Identitätsmissbrauchs nach Art. 179*decies* E-StGB, Zeitschrift der juristischen Nachwuchsforscher, ex ante 2/2020, p. 33 ss ; **Niklaus SCHMID**, Computer- sowie Check- und Kreditkarten-Kriminalität, Zurich 1994 (cité : SCHMID, Kredikarten-Kriminalität) ; **Niklaus SCHMID**, Das neue Computerstrafrecht, RPS 113/1995, p. 22 ss (cité : SCHMID, Computerstrafrecht) ; **Pierre SCHNEIDER**, La fraude informatique au sens de l'article 147 CPS, thèse Lausanne 1994 ; **Christian SCHWARZENEGGER**, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23.11.2001, *in* Andreas DONATSCH/Marc FORSTER/Christian SCHWARZENEGGER (éds), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel, Zurich 2002, p. 305 ss ; **Christian SCHWARZENEGGER/Aurelia GURT**, Possibilités juridiques d'action contre le stalking en Suisse, Expertise à l'attention du Bureau fédéral de l'égalité entre femmes et hommes (BFEG), Zurich 2019 ; **Eric STAUFFACHER**, Infractions contre le patrimoine : le nouveau droit, RPS 114/1996, p. 1 ss ; **Paul-Henri STEINAUER/Christiana FOUNTOULAKIS**, Droit des personnes physiques et de la protection de l'adulte, Berne 2014 ; **Lilian SUTER/Gregor WALLER/Jael BEMATH/Céline KÜLLING/Isabel WILLEMSE/Daniel SÜSS**, Rapport sur les résultats de l'étude JAMES 2018, ZAHW, 2018 (cité : SUTER *et al.*) ; **Jan WENK**, Romance Scam: Phänomenologie und strafrechtliche Aspekte, 2023, p. 16 ss ; **David WICKI-BIRCHLER**, Doxing, Considérations de droit pénal et droit de la personnalité suisse, Jusletter 8 mai 2023; **Nesa ZIMMERMANN**, La notion de vulnérabilité dans la jurisprudence de la Cour européenne des droits de l'homme : contours et utilité d'un concept en vogue, Zurich 2022, p. 492 ss.

Documents officiels

Commission des affaires juridiques du Conseil des États, Rapport du 17 février 2022 concernant l'harmonisation des peines et la loi fédérale sur l'adaptation du droit pénal accessoire au droit des sanctions modifié, Projet 3 : loi fédérale portant révision du droit pénal en matière sexuelle, FF 2022 687 (cité : CAJ-CE, Rapport Projet 3) ; **Commission des affaires juridiques du Conseil national,** Avant-projet du 27 avril 2023 de loi fédérale visant à améliorer la protection pénale contre le harcèlement obsessionnel (Modification du code pénal, du code pénal militaire et de la procédure pénale militaire), BO 19.433 (cité : CAJ-CN, Avant-projet) ; **Commission des affaires juridiques du Conseil national,**

Rapport de 2022 relatif à l'initiative parlementaire : Étendre au harcèlement obsessionnel («stalking») le champ d'application des dispositions du CP relatives aux délits, 2022, BO 19.433 (cité : CAJ-CN, Rapport stalking) ; **Conseil fédéral**, Rapport du 11 janvier 2023 donnant suite au postulat 19.4111 Quadranti du 24 septembre 2019, La protection des enfants et des jeunes face aux cyber-délits sexuels (cité : Conseil fédéral, Cyber-délits sexuels) ; **Conseil fédéral**, Message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF 2023 84 (cité : FF 2023 84) ; **Conseil fédéral**, 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, FF 2018 2889 (cité : FF 2018 2889) ; **Conseil fédéral**, Message du 15 septembre 2017 concernant la loi fédérale portant sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565 (cité : FF 2017 6565) ; **Conseil fédéral**, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz du 15 septembre 2017, BBl 2017 6941 (cité : BBl 2017 6941) ; **Conseil fédéral**, Message du 21 février 1968 concernant le renforcement de la protection pénale du domaine personnel, FF 1968 I 609 (cité : FF 1968 I 609) ; **Conseil fédéral**, Message du 24 avril 1991 concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales), FF 1991 II 933 (cité : FF 1991 II 933) ; **Département fédéral de justice et police, Office fédéral et Conseil fédéral**, Communiqué du 10 janvier 2024, Les nouvelles dispositions du droit pénal en matière sexuelle entreront en vigueur le 1er juillet 2024 (cité : DFJP, Communiqué) ; **Ministry of Law (Singapore)**, Enhancements to the Protection from Harassment Act (POHA), 1er avril 2019 (<https://www.mlaw.gov.sg/news/press-releases/enhancements-to-the-protection-from-harassment-act-poha/#:~:text=The%20Bill%20will%20strengthen%20protection,liable%20in%20proceedings%20for%20harassment%2D>, *consulté le 17.3.2024*) (cité : Ministry of Law) ; **Office fédéral de la cyber-sécurité**, Fake sextorsion, (<https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/fake-sextortion.html>, *consulté le 17.3.2024*) (cité : OFSC, Fake sextorsion) ; **Office fédéral de la justice**, Synthèse des résultats de la procédure de consultation du 25 octobre 2023 portant sur l'initative parlementaire de la Commission des affaires juridiques du Conseil national, Étendre au harcèlement obsessionnel («stalking») le champ d'application des dispositions du CP relatives aux délits (cité : OFJ, Synthèse stalking) ; **Office fédéral de la justice**, Synthèse des résultats de la procédure de consultation du 8 août 2021 portant sur la loi fédérale portant révision du droit pénal en matière sexuelle (cité : OFJ, Synthèse révision) ; **Office of the Privacy Commissioner for Personal Data (Hong Kong)**, Personal Data Privacy Amendment Bill 2021, 8 octobre 2021, (<https://www.pcpd.org.hk/english/doxxing/index.html>, *consulté le 17.3.2024*) (cité : Office of the Privacy Commissioner for Personal Data).

La poursuite des cybercriminels au quotidien

JULIEN CARTIER
Docteur en sciences forensiques
Commissaire forensique, Chef de la section forensique de la police de sûreté de la police cantonale vaudoise

Table des matières

I. Introduction

Avant toute chose, il semble nécessaire de définir l'environnement dans lequel les cybercriminels évoluent, puisque c'est d'eux que traite cet article. Une définition est donnée par Stuart RUSSELL, professeur d'informatique à Berkeley : « *Le cyber est comme un morceau de monde supplémentaire. Avant on avait l'air, la terre, les océans. Maintenant il y a ce morceau de monde en plus qu'on appelle le cyber. Il repose sur un ensemble de lignes*

numériques. Donc, il s'appréhende de façon assez étrange. On ne peut pas y plonger ses mains comme dans l'océan, ni le respirer comme l'air. Il n'est composé que de câbles, de circuits, d'ordinateurs et de disques. Mais, de mon point de vue, il fonctionne comme un morceau de monde supplémentaire. Certains pensent même que c'est désormais la partie du monde où la majorité des gens passent la plupart de leur temps. »[1]. Cette définition est intéressante, car elle présente cet environnement comme un monde nouveau, dont le fonctionnement repose sur des notions également nouvelles et pas forcément intuitives. « *Ce cyberespace a une autre physique. On perd une dimension, on perd la dimension spatiale. Pourquoi ? Parce qu'on s'y déplace à la vitesse de la lumière. Donc, à l'échelle planétaire, cette distance est négligeable. On se retrouve tous au même endroit : les gens honnêtes, bien intentionnés, comme les gens malhonnêtes, mal intentionnés, où on est tous ensemble. Donc, il y a une exposition au criminel qui est beaucoup plus grande que celle qu'on connaît dans le monde physique.* »[2].

Dans le contexte policier, il existe plusieurs catégorisations des infractions liées à la cybercriminalité, qu'elles soient définies dans le code pénal spécifiquement à cet effet (cybercriminalité au sens strict[3]) ou qu'il s'agisse d'infractions générales qui peuvent également se dérouler dans l'environnement cybernétique (cybercriminalité au sens large[4]). Cette classification a d'ailleurs été reprise dans la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022. Cependant, ces considérations n'ont que peu d'importance dans le quotidien des enquêteurs et sont très souvent les unes et les autres présentes dans la mise en œuvre de processus délictueux dans le cyberespace. Elles ont toutefois été reprises dans l'organisation de certaines polices, des unités

1 Stuart RUSSELL, dans Cybermonde – L'avenir c'est maintenant, documentaire ARTE, réalisé par Shimon DOTAN/Charles FERGUSON, 16.08.2023, 0:04:40, disponible sous : <https://tube-numerique-educatif.apps.education.fr/w/e0e8d786-2d72-4bd2-98a0-75652ec59614> (*consulté le 10.1.2024*).

2 Julien CARTIER, dans Forum – La cyberdélinquance, un défi pour la police cantonale vaudoise, RTS, présenté par Mehmet GULTAS, 10.11.2017, 0:01:39, disponible sous : <https://www.rts.ch/audio-podcast/2017/audio/la-cyberdelinquance-un-defi-pour-la-police-cantonale-vaudoise-25758221.html> (*consulté le 10.1.2024*).

3 Conseil fédéral, SNCP 2018-2022, p. 31 : « *La cybercriminalité au sens strict renvoie aux infractions qui sont commises à l'aide de technologies de l'information et de la communication ou qui exploitent les vulnérabilités de ces technologies. Ces activités criminelles sont nouvelles et ne sont possibles que depuis l'avènement de ces technologies.* ».

4 Conseil fédéral, SNCP 2018-2022, p. 31 : « *La cybercriminalité au sens large utilise Internet comme moyen de communication en se servant à mauvais escient des possibilités offertes par cette technologie, par exemple les courriers électroniques ou l'échange et la mise à disposition de données à des fins malveillantes. Ces activités criminelles ne sont pas nouvelles, mais les médias utilisés pour les commettre ou pour stocker des données le sont (messagerie électronique, WhatsApp, Snapchat, Instagram, Telegram ou supports électroniques à la place du papier, services en nuage, etc.).* ».

d'enquête étant dédiées à la cybercriminalité au sens strict, alors que la cybercriminalité au sens large est souvent répartie sur les unités policières traditionnelles. Ce modèle d'organisation a pour avantage de limiter la charge sur les unités spécialisées, mais dans la réalité, il est souvent difficile de faire correspondre les groupements cybercriminels à ces critères. Comme nous le verrons plus loin, des groupes cybercriminels d'envergure mondiale peuvent être découverts et arrêtés en partant de cyberescroqueries appartenant à la catégorie de la cybercriminalité au sens large.

Une étude est en cours en réponse au postulat SILBERSCHMIDT[5] qui demande un état des lieux sur les poursuites pénales menées par les cantons contre la cybercriminalité. Elle sera sans aucun doute intéressante, car elle fournira une image de la situation des différents modèles d'organisation et des ressources allouées à la lutte contre la cybercriminalité dans les différentes juridictions suisses.

Cet article n'a pas la prétention d'être construit comme une production relevant d'une quelconque méthodologie scientifique ou juridique. Il s'agit ici de fournir un témoignage de la réalité policière concernant la lutte contre la cybercriminalité dans le canton de Vaud.

II. Situation actuelle

Le quotidien des équipes qui traitent des affaires cybercriminelles est avant tout marqué par le nombre très élevé des sollicitations. Celles-ci sont en constante augmentation depuis que la police de sûreté vaudoise s'est donné les moyens de mesurer leur évolution. Les chiffres consolidés sont disponibles depuis 2019, alors que la statistique suisse de la criminalité la mesure à l'échelle nationale depuis 2020. Sur le plan vaudois, les sollicitations, très majoritairement des plaintes, sont passées de 1640 en 2019 à environ 4350 en 2023 (estimation d'après les chiffres actuels), ce qui représente une augmentation de plus de 160%, soit un facteur supérieur à 2,5. Notons au passage que 2023 représentera certainement l'année connaissant la plus forte progression, les chiffres laissant présager une augmentation annuelle supérieure à 40%.

En ce qui concerne 2022, qui est la dernière année pour laquelle des chiffres consolidés sont disponibles, 3040 sollicitations ont été enregistrées. Celles-ci représentent un préjudice cumulé de plus de 27 millions de francs[6]. Au niveau

---

5 Postulat de M. le conseiller national Andri SILBERSCHMIDT, n°22.3145 « *Poursuites pénales en matière de cybercriminalité. Efficacité des cantons* » du 16 mars 2022.

6 Dans notre statistique, seuls les montants réellement perdus par les lésés sont comptabilisés, ce qui exclut, par exemple, les montants qu'une entité publique ou privée doit débourser pour la gestion de la crise à la suite d'une cyberattaque par rançongiciel,

des grandes catégories de phénomènes cybercriminels, tels que définis dans la statistique nationale[7], les trois quarts des cas en 2022 concernait des cyberescroqueries (env. 2330), le solde étant réparti dans les cas spécifiques de « *phishing* » (env. 160), de « *hacking* » (env. 60), d'utilisation de « *malware* » (env. 25) et de vol de cryptomonnaie (env. 10) pour la cybercriminalité au sens strict, ainsi que le blanchiment des mules financières (appelées « *money mules* » en anglais) (env. 125), les atteintes à la cyber-réputation (env. 100) et la pornographie interdite (env. 215).

Si l'on s'intéresse aux différents phénomènes cybercriminels dans le détail et que l'on compare le nombre de cas au préjudice effectif, on constate rapidement que deux d'entre eux sont fréquents (fausse petite annonce 28%, abus du commerce en ligne 15%) alors qu'ils ne représentent qu'une petite partie des préjudices (env. 1,5% à eux deux). A l'inverse, trois phénomènes sont beaucoup moins fréquents, bien qu'ils représentent une part très importante des préjudices. Il s'agit des fraudes à l'investissement (env. 4% des cas pour 51% des préjudices), des arnaques au président ou « *BEC Fraud* »[8] (env. 1,5% des cas pour env. 15% des préjudices) et des escroqueries sentimentales[9] (env. 2,5% des cas pour env. 13% des préjudices). Relevons que tous ces phénomènes appartiennent à la catégorie générale des cyber-escroqueries.

Les autres catégories de phénomènes spécifiques au cyberespace, comme le « *phishing* », le « *hacking* » ou l'usage de logiciel malveillant comme les rançongiciels, ne représentent que 8% des cas cumulés en 2022 dans le canton et moins de 2% des préjudices. Pourtant, ces phénomènes sont considérés par les professionnels de la cybersécurité comme les plus critiques et les plus dangereux, car ils peuvent entraîner des conséquences extrêmement graves pour des institutions ou des entreprises privées, que ce soit un simple dégât d'image, l'exposition à des poursuites judiciaires en cas de divulgation de données

ainsi que pour la remise en état de ses infrastructures et sa sécurisation. Dans ce genre de cas, seul le montant de la rançon, si elle a été payée, sera pris en compte.

7 Il existe un schéma des modes opératoires défini par l'OFS en ce qui concerne cette partie spécifique de la statistique policière de la criminalité (SPC), disponible sous <https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police/criminalite-numerique.assetdetail.28645898.html> (*consulté le 10.1.2024*).

8 « *La compromission d'adresse email ou Business Email Compromise (BEC) est une attaque populaire visant à compromettre une boîte mail d'entreprise dans l'objectif de l'utiliser à des fins malveillantes. La monétisation la plus simple est généralement de demander un transfert de fonds depuis l'adresse corrompue ou un changement de coordonnées de paiement pour les factures à venir.* » Tiré de <https://arsen.co/blog/bec-definition/> (*consulté le 10.1.2024*).

9 « *L'escroquerie sentimentale, ou arnaque sentimentale, est, sur Internet, une escroquerie en ligne consistant à feindre des sentiments amoureux envers une victime pour gagner son affection et sa confiance avant de recourir à des artifices (fausses déclarations) pour lui soutirer de l'argent.* » Tiré de <https://fr.wikipedia.org/wiki/Escroquerie_sentimentale> (*consulté le 10.1.2024*).

confidentielles ou privées, ou finalement une perte de productivité pouvant aller dans les cas les plus graves jusqu'à la faillite.

De plus, ces statistiques ne représentent que la partie visible de l'iceberg, comme en témoignent les quelques sondages de victimisation réalisés en Suisse qui déterminent que le taux de reportabilité[10] est de 10% environ. Si on souhaite avoir une image réaliste de la situation, il s'agit dans les grandes lignes de multiplier par dix les statistiques vaudoises évoquées ci-avant. Le nombre réel d'infractions cybercriminelles seraient donc plus de l'ordre de 30'000 à 40'000 dans le canton de Vaud annuellement, pour des préjudices de l'ordre de 250 à 300 millions de francs.

A. Les projections pour 2023

Comme nous l'évoquions précédemment, 2023 sera l'année qui connaîtra la plus forte augmentation depuis que la police cantonale vaudoise suit attentivement cette criminalité numérique. L'augmentation devrait être de l'ordre de plus de 40%, alors qu'elles étaient de 35% en 2020, 20% en 2021 et 14% en 2022. La diminution des augmentations annuelles, lente mais constante, que nous constations jusqu'à cette année s'est inversée et l'augmentation sera certainement, en 2023, la plus forte depuis 5 ans.

Mais d'autres constatations peuvent être réalisées de manière plus précise sur certains phénomènes, qui connaissent des évolutions diverses. Nous citerons ici le cas des fraudes à l'investissement en ligne qui connaissent une augmentation très importante depuis 2021 et qui se montera en 2023 à env. 60% pour atteindre les 200 cas rapportés dans le canton. Ce phénomène est inquiétant, car les préjudices pour les lésés sont, comme on l'a vu, souvent très importants et les auteurs sont très vraisemblablement organisés et liés à des organisations criminelles du sud-est de l'Europe[11]. Cette augmentation qui est à nouveau en hausse démontre que les efforts de prévention ne sont pas toujours efficaces, malgré de nombreuses campagnes[12], et que les escrocs se sont professionnalisés afin d'attirer toujours plus de victimes dans leurs filets.

---

10 MARGAGLIOTTI *et al.* ; MARKWALDER *et al*.

11 Pour approfondir ce sujet : Loïc DELACOUR, Crypto-monnaies : attention arnaque, documentaire Mise au point, RTS, disponible sous : <https://www.rts.ch/play/tv/mise-au-point/video/crypto-monnaies--attention-arnaque?urn=urn:rts:video:14605326> (*consulté le 10.1.2024).*

12 La Prévention Suisse de la Criminalité (PSC) publie sur son site Internet notamment plusieurs brochures sur ces thématiques. Une campagne de treize clips vidéo intitulée « *Sur Internet aussi, soyez vigilants* » ou « *Et vous ? Vous auriez dit oui ?* » a été produite en trois langues ces dernières années sur l'initiative de la police cantonale vaudoise. Elle vise à montrer les comportements absurdes des lésés dans le cyberespace

Un autre phénomène qui connaît des hausses conséquentes en 2022 (env. 400%) et 2023 (env. 50%) est l'arnaque au faux support informatique. Cette escroquerie cyber bien connue comme *arnaque MICROSOFT* existe depuis de nombreuses années. A l'origine, les escrocs téléphonaient souvent depuis l'Inde, en s'exprimant en anglais avec un accent reconnaissable, et les cas avérés étaient peu nombreux. Ceci a été le cas jusqu'en 2021 puisque seuls quelques dizaines de cas étaient recensés dans le canton de Vaud pour des préjudices moins importants. Depuis 2022, le phénomène s'est considérablement transformé, puisque ce ne sont plus des appels téléphoniques, mais des fausses alertes visuelles et sonores directement sur l'ordinateur, prétendument bloqué, de la personne visée qui déclenchent un appel de sa part aux escrocs qui ont tendu le piège. Ensuite, ces derniers tentent de prendre le contrôle à distance en prétextant un dépannage informatique. Dans le meilleur des cas, seul un montant de plusieurs milliers de francs est prélevé sur les cartes de crédit de la personne lésée. Dans le pire des cas, les cybercriminels arrivent à entrer par astuce et avec l'aide involontaire de la personne cible dans son e-banking et ses comptes sont simplement siphonnés. Le tout, bien entendu par des « opérateurs » au téléphone qui s'expriment dans la langue de la victime. Ces caractéristiques régionales peuvent être recueillies informatiquement dans les paramètres du navigateur utilisé pour déclencher la fausse alarme initiale, et réutilisés pour acheminer les appels au bon centre d'appels qui puisse s'exprimer dans la langue de la victime[13].

En ce qui concerne ce type d'escroquerie, nos investigations ont permis de constater qu'une « alliance intercontinentale » entre des groupes de cybercriminels asiatiques (Asie du Sud) et désormais africains (Afrique Centrale) a conduit aux évolutions techniques de ces dernières années et la tendance significative à la hausse, tant sur le plan du nombre de cas que du montant des préjudices. Relevons encore que les auteurs sont sans doute francophones, car on constate cette augmentation principalement en Suisse romande.

B. Le cas particulier des rançongiciels

Les rançongiciels sont considérés comme le risque majeur en matière de cybersécurité car ce ne sont plus des individus qui sont visés, mais des entreprises, voire des institutions étatiques ou paraétatiques. Ce changement de

lorsqu'on les rapporte au monde réel. Clips disponibles sous : <https://www.skppsc.ch/fr/telechargements/famille-des-produits/clips/> (*consulté le 10.1.2024*).

13 Pour approfondir ce sujet : Clémentine BUGNON, Attention aux arnaques à la carte de crédit, documentaire A bon entendeur, RTS, disponible sous : <https://www.rts.ch/play/tv/a-bon-entendeur/video/attention-aux-arnaques-a-la-carte-de-credit?urn=urn:rts:video:14547650> (*consulté le 10.1.2024*).

cibles qui s'est concrétisé entre 2017 et 2019 s'explique simplement par le rapport investissement (coûts de la réalisation de la cyberattaque) – bénéfice (montant obtenu) qui est beaucoup plus favorable lorsque l'on s'attaque à des sociétés privées ou publiques, plutôt qu'à des particuliers. Mais, contrairement aux tendances haussières rapportées par les sociétés de cybersécurité[14], la police vaudoise a constaté en 2023 une baisse des cas qui lui ont été rapportés, tendance déjà amorcée en 2022.

Le nombre de cas de ce type de cyberattaque rapporté à la police est en nombre absolu relativement faible (entre 15 et 25 annuellement). Pour le canton de Vaud, 2021 a été l'année avec le plus de cas rapportés (24), alors qu'en 2022 et 2023, on se trouve dans la fourchette basse avec une quinzaine de cas. Que tirer de ce constat, bien qu'on se trouve statistiquement dans une situation où il est difficile de tirer des conclusions significativement valables en raison du faible nombre de cas ? On peut raisonnablement se poser la question de l'intérêt des entreprises ou institutions attaquées à déposer une plainte pénale. Il est certain que pour les sociétés privées, le dégât d'image fait partie de la pesée d'intérêts et peut dans certains cas l'emporter sur toute autre considération. En ce qui concerne cette lacune d'information, le Parlement a adopté[15] des modifications légales qui étendront dès 2025 les obligations d'annoncer ces cyberattaques et qui définiront une liste plus étendue des autorités et organisations assujetties à l'art. 74*b*[16] de la Loi sur la sécurité de l'information[17]. Désormais l'ancienne terminologie d'*infrastructure critique*[18] qui laissait place à l'interprétation est remplacée par une liste d'une vingtaine de critères qui comprennent une grande majorité d'entreprises privées.

Mais, si les entreprises n'ont pas intérêt à rendre publique une cyberattaque par un dépôt de plainte pénale, c'est que, dans la pesée d'intérêt, la démarche qui vise à identifier les auteurs et les déférer à la justice et dans d'hypothétiques cas, récupérer l'argent perdu est perçue comme moins importante, voire inutile car peut-être vouée à l'échec. Cette hypothèse est inquiétante, car cela voudrait dire que la police et les autorités de poursuite pénale ne sont déjà plus perçus comme des institutions utiles face à ce problème majeur. Or, le canton de Vaud

---

14 L'implication de ces sources dans le marché de la cybersécurité ne nous permet pas d'être totalement à l'aise avec leurs statistiques, mais nous ne disposons que de peu d'autres sources ouvertes.

15 Voir notamment le communiqué du DPPS disponible sous : <https://www.vbs.admin.ch/fr/obligation-de-signaler-les-cyberattaques-contre-les-infrastructures-critiques-autre-calendrier> (*consulté le 10.1.2024*).

16 FF 2023 2296.

17 Loi fédérale sur la sécurité de l'information au sein de la Confédération du 18 décembre 2020, RS 128.

18 Définie dans Conseil fédéral, Stratégie, p. 3 : « *On entend par infrastructures critiques les processus, les systèmes et les installations essentiels pour le fonctionnement de l'économie et le maintien des moyens de subsistance de la population*. ».

a connu des cyberattaques qui ont été largement médiatisées, ce qui a permis en 2021 déjà de mettre en lumière ce phénomène dans lequel des criminels n'hésitent pas à s'attaquer à des institutions de l'Etat. En 2023 aussi une commune vaudoise a été victime de ce type de cyberattaque avec heureusement des conséquences moins graves. Nous relèverons encore qu'en 2023, dans le canton de Vaud, une fondation, une association paraétatique et une haute école ont également été victimes à des degrés divers et avec des conséquences heureusement limitées.

III. Mais que fait la police ?

A. De nouvelles structures

En 2018, la police de sûreté vaudoise a décidé de réorganiser ses structures afin d'obtenir, dans un premier temps, une image précise de la situation et de son évolution et, dans un second temps, d'optimiser la prise en charge des plaintes concernant la cybercriminalité. Il s'agissait aussi de profiter de la mise en œuvre du nouveau dispositif de renseignement criminel cyber du concordat romand.

Né de l'initiative de l'Association des chefs de police judicaires romands, ce dispositif a été développé sur le modèle du CICOP[19], qui fête ses trente ans en 2024 et qui traite de la délinquance sérielle dans l'environnement physique traditionnel. A l'instar de son grand frère, le dispositif de renseignement criminel cyber nécessite une plateforme commune d'échange d'information. Cette plateforme d'informations de la criminalité sérielle en ligne (PICSEL) développée entre 2017 et 2018 en collaboration avec l'Ecole des Sciences Criminelles de l'Université de Lausanne est née en 2019 à la police cantonale vaudoise, avant d'être transférée en 2021 au Centre de Compétence Cyber (CCC) pour les cantons du concordat romand à la police cantonale genevoise[20].

---

19 « *Le CICOP représente le réseau des cellules d'analyse en termes de suivi de la délinquance sérielle au niveau romand. Chaque cellule cantonale fait partie de ce réseau. Une plateforme commune* […] *permet un échange systématique de l'ensemble des données recueillies par les cellules cantonales.* ». Rapport de la commission chargée d'examiner l'exposé des motifs et projet de décret autorisant le Conseil d'État à adhérer au Concordat du 3 avril 2014 réglant la coopération en matière de police en Suisse romande, p. 2, disponible sous : <https://www.vd.ch/fileadmin/user_upload/organisation/gc/fichiers_pdf/2012-2017/196_RC.PDF> (*consulté le 10.01.2024*).

20 Selon le Communiqué de presse de la CLDJP du 9 avril 2019, sur proposition de la Conférence des commandants des polices cantonales de Romandie, Berne et Tessin (CCPC RBT), la Conférence latine des chefs de départements de justice et police

Depuis 2019, les polices cantonales romandes, puis certaines d'autres cantons suisses sous forme de projets pilotes, ont intégré le dispositif de renseignement à leur procédure de traitement des cas liés à la cybercriminalité. Ce qui change concrètement, dans le canton de Vaud notamment, est l'ajout d'une étape qui tient un rôle central dans le processus de prise en charge. Elle intervient une fois que la plainte a été prise et facilite la détermination de la suite qui doit être donnée par les enquêteurs. Le travail effectué par les analystes du dispositif permet de mettre chaque cas dans un contexte plus large, soit d'évaluer sa nature sérielle ou non, c'est-à-dire l'appartenance potentielle à une série de délits connexes. Il leur est également demandé de mettre en évidence des *modus operandi* nouveaux ou qui évoluent, afin d'aider les enquêteurs dans leurs investigations ou contre-mesures de perturbation, ou d'aider les organes de prévention à communiquer afin d'informer la population d'un nouveau risque. Ces éléments sont une valeur ajoutée très importante et utile aux enquêteurs et magistrats qui devront traiter les cas sériels ou isolés en meilleure connaissance de cause et en coordonnant, si possible, les efforts de chacune des entités pouvant être concernées dans différents lieux géographiques. Sans ce dispositif, il aurait été impossible d'optimiser la prise en charge, en priorisant les efforts en fonction d'aspects tels que la gravité, la sérialité, les chances de réussite (cette criminalité étant majoritairement transfrontalière) et les ressources disponibles. Ainsi, le dispositif de renseignement criminel cyber a pour mission de :

– PRIORISER : détection des séries et mettre les priorités sur les auteurs les plus actifs.
– COORDONNER : coordination des enquêtes intercantonales.
– CENTRALISER : rassembler et diffuser les connaissances tactiques sur les phénomènes.
– PREVENIR : définir les axes de prévention en fonction des augmentations des types de délits.

B. Peut-on faire un premier bilan ?

Le dispositif de renseignement criminel dans le monde physique traditionnel qui a fait ses preuves depuis plusieurs décennies repose sur les principes qui caractérisent la délinquance sérielle que nous connaissons dans notre environnement physique. Il s'agit de la criminalité **itinérante** dans le sens où les criminels se déplacent d'un lieu à un autre pour commettre leurs délits. Dans le monde cyber, la criminalité n'est pas itinérante, puisque l'humanité est « au même endroit », la dimension spatiale étant « négligeable » en termes de

(CLDJP) a validé la création d'un Centre de Compétence Cyber (CCC) romand piloté par les spécialistes de la police cantonale de Genève.

déplacement, mais **fragmentée** dans le sens où les conséquences des actes commis dans le cyberespace ou au travers de lui se concrétisent presque aléatoirement en un lieu selon la personne physique, bien réelle, lésée par l'infraction.

Cette différence est importante, car elle a un effet, non seulement dans l'appréhension des phénomènes cybercriminels et leur dimension internationale dans la recherche de traces et d'identification des auteurs, mais également immédiatement dans l'application de certaines règles de procédure et notamment dans la fixation du for de la poursuite pénale ou des procédés mis en œuvre pour rechercher et obtenir des informations dans les phases d'investigation.

Il est ainsi possible de présenter ici trois exemples qui illustrent ce qui est différent et fréquemment problématique.

1. Fixation du for – coordination nationale

Sans entrer dans un débat de doctrine juridique, la question est de savoir si l'application des principes du droit tels que la territorialité et les règles de fixation de for traditionnelles posent des problèmes dans la situation d'une **criminalité fractionnée** *a fortiori* transfrontalière ? La réponse est actuellement oui. Cela amène des processus peu efficients et qui engorgent les polices et les ministères publics. Nous prendrons ici l'exemple des mules financières qui sont des intermédiaires financiers utilisés par les escrocs à leur insu en les trompant, ou du moins « à l'insu de leur plein gré ». Ces intermédiaires sont souvent choisis dans un environnement géographique proche de la victime, afin de crédibiliser le scénario proposé au lésé et l'amener à virer de l'argent sur les véhicules financiers au nom des mules financières (comptes bancaires, cartes prépayées, cryptomonnaies, etc.). Il arrive aussi que des véhicules financiers soient créés directement par les escrocs en usurpant une identité à l'aide de documents d'identité volés ou récupérés (achetés) dans des fuites de données vendus dans le Darknet ou obtenus d'une victime d'une précédente escroquerie. Si, dans les premières investigations policières, il est plus difficile d'identifier l'escroc à l'origine de l'escroquerie, l'identification de la mule financière est triviale, le véhicule financier étant connu de la victime. Son détenteur légal est généralement facile à déterminer. Ainsi, dans les très nombreux cas d'escroquerie à la petite annonce (vendeur ou acheteur lésé), ainsi que dans certains cas d'achats frauduleux sur les plateformes de commerce en ligne ou autres, les mules sont identifiées, ainsi que les personnes dont les comptes sont usurpés. Dans ces cas de figure, qui sont très nombreux, le blanchiment d'argent se poursuivant d'office, des investigations sont systématiquement entreprises envers les mules financières.

Nous avons tenté de proposer que les polices puissent se communiquer les identités (détenteurs légaux des véhicules financiers) afin de gagner en efficience et d'informer directement le canton de domicile de ces suspects. Mais la procédure de fixation de for prévoit expressément que la dénonciation ne peut se faire qu'au travers des ministères publics afin que la partie blanchiment d'argent soit reprise par le canton où réside la mule. En conséquence, pour une grande majorité des cyberescroqueries ayant recours à des mules financières, le canton dans lequel le lésé a déposé une plainte pénale doit entreprendre les investigations (police et ministère public) devant permettre d'identifier la mule et son domicile, ainsi que de démontrer son activité potentiellement délictueuse. Ensuite, le ministère public, sur la base du rapport d'investigation de la police rédige une demande de reprise de for à l'intention du canton de domicile de la mule financière. Une mule étant quasiment toujours utilisée pour commettre une série de délits, cette procédure va se reproduire à l'identique dans tous les cantons (ou pays) touchés par la série. Ainsi l'organisme bancaire ou financier dans lequel la mule a ouvert son compte reçoit des demandes de plusieurs ministères publics, ce qui sauf exception déclenche un signalement au bureau de communication en matière de blanchiment d'argent (MROS), qui après examen renverra lui aussi un dossier pour objet de sa compétence au ministère public du canton de domicile de la mule financière. Cette autorité recevra donc des dossiers similaires constitués des mêmes pièces fournies par l'organisme financier un nombre de fois équivalent au nombre de plaintes qui auront été déposées dans les différents cantons, ajouté de la dénonciation du MROS. Le canton concerné pourra alors entreprendre les démarches d'investigation sur la mule financière concernée et décider de l'issue judiciaire à donner à cette affaire, le tout s'étalant naturellement dans le temps et compliquant ainsi le suivi et la clôture des procédures.

On constate donc que les règles de fixation de for, qui sont sans doute adaptées à une criminalité itinérante qui concerne directement les auteurs des infractions et où la sérialité est présente mais limitée, ne l'est pas pour une criminalité fractionnée telle que la cybercriminalité. Ici, la sérialité peut être très importante (plusieurs centaines, voire milliers de cas) et les auteurs primaires ont recours à des intermédiaires, eux-mêmes potentiellement auteurs d'un acte délictueux « secondaire » pour autant que leur intention puisse être démontrée, à défaut une négligence en termes de vigilance. Et ces très nombreux actes de procédure engorgent les ministères publics et distraient les forces de police des « vrais » escrocs pour lesquels ils n'ont plus assez de temps pour mener des enquêtes longues et plus difficiles sur le plan international.

Mais tout n'est pas totalement noir ; il arrive aussi parfois que des auteurs locaux s'adonnent à ce type d'escroquerie et grâce au dispositif de renseignement criminel cyber, il est plus facile de les repérer, car ils n'ont pas recours aux mêmes ressources et intermédiaires financiers. Ces séries particulières sont

donc déconnectées des « méga-séries » comportant plusieurs milliers de cas et appartenant à des réseaux cybercriminels situés à l'étranger. Dans cette situation, les procédures usuelles permettent de dénoncer de potentiels auteurs ici, en Suisse.

2. Convention de Budapest – entraide internationale

La convention sur la cybercriminalité, conclue à Budapest le 23 novembre 2001, a été approuvée par l'Assemblée fédérale le 18 mars 2011 et est entrée en vigueur pour la Suisse le 1er janvier 2012[21]. Elle a été signée et ratifiée par une septantaine de pays, majoritairement européens, mais également américains et dans une moindre mesure africains ou asiatiques. Jusqu'à une période récente, il était très compliqué, voire impossible, d'obtenir une information basique auprès de fournisseurs de services en ligne étrangers autrement que par voie d'une demande d'entraide judiciaire internationale. Le recours à cette procédure est lourd et peu adapté aux premières investigations policières qui sont menées dans le but d'identifier un auteur ou du moins d'évaluer les chances de remonter à lui, tant les possibilités de brouiller les pistes et masquer ses traces dans le cyberespace sont nombreuses.

Ainsi, depuis quelques années, certains géants du web ont répondu favorablement aux demandes incessantes des autorités de poursuite pénale qui se plaignaient de devoir passer par des procédures d'entraide avec les Etats-Unis notamment, alors que des filiales se trouvaient sur leur sol ou des pays de leur continent. Plusieurs d'entre eux répondent désormais à des demandes d'information simples[22] par le biais de demandes de remise spontanée, non contraignantes. Certains mettent même en œuvre des portails destinés aux autorités de poursuite pénale afin de faciliter l'authentification de celles-ci et simplifier les processus de demande et de réponse. Les réponses à ces demandes d'informations simples (données relatives aux abonnés ou « *Subscriber Information* ») permettent aux polices de « gratter la fine couche de peinture » qui a été déposée par certains cybercriminels pour brouiller les pistes et sont très utiles aux investigations préliminaires, même si l'on est fréquemment confrontés à devoir jouer aux poupées russes avant de pouvoir découvrir un indice réellement intéressant et solide (adresses IP de création d'un compte, e-mail de récupération, etc.). La ratification de cette convention est donc une avancée notable et

21 Convention du 23 novembre 2001 sur la cybercriminalité, RS 0.311.43.

22 L'art 18 al. 3 de la Convention de Budapest spécifie les « *données relatives aux abonnés* ». L'accès aux données des utilisateurs (contenus ou données secondaires) n'est possible que par voie de demande d'entraide judiciaire internationale (DEJI), la Convention Cybercriminalité permettant uniquement de demander de les préserver dans des délais très courts dans l'attente de la DEJI.

concrète qui simplifie grandement les investigations préliminaires, bien que le type d'information pouvant être transmises par les fournisseurs de services concernés soient très limitées.

3. Coopération internationale – Interpol et Europol

Dans le domaine de la cybercriminalité souvent sérielle, les auteurs sont fréquemment situés à l'étranger, puisqu'ils sont à « cyber-proximité » de leurs victimes. De plus, dans tous les cas, les enquêteurs sont confrontés à des ramifications internationales, ne serait-ce que par la localisation géographique des fournisseurs de services en ligne, qui ne sont que rarement suisses. Nous sommes donc amenés à interagir et coopérer avec les entreprises étrangères et les autorités de poursuite pénale en Europe et dans le monde.

A cet effet, les organisations telles qu'Europol et Interpol sont des partenaires incontournables. Nous ne nous attarderons pas sur Interpol qui améliore nos capacités d'échange d'information à l'échelle mondiale depuis des décennies. Europol est devenu pour les policiers suisses qui luttent contre la cybercriminalité un partenaire important, car il facilite d'une part la communication entre les enquêteurs des différents pays membres, mais soutient également ces enquêteurs en rendant les enquêtes transfrontalières plus efficaces. Europol dispose d'analystes et d'experts en sus des attachés nationaux qui fournissent des aides en matière d'investigations techniques, développent des outils et proposent des bonnes pratiques en matière de coopération.

Les enquêteurs, à l'instar des affaires dans le monde physique, s'appuient sur ces organisations en cas de besoin. Seulement, en matière de cybercriminalité, le recours à ces outils de coopération internationale est la règle et non l'exception. Il est donc très fréquent que les investigations nécessitent la mise en œuvre de messages Europol (*Secure Information Exchange Network Application*, SIENA), auxquels les réponses sont souvent positives et utiles. Dans certains cas, ils peuvent déboucher sur l'organisation de réunions de coordination avec les pays concernés. De même, des demandes Interpol peuvent être utilisées lorsque des pays hors du continent européen sont requis. La qualité des réponses et leur célérité sont toutefois, dans ce contexte, plus disparates et parfois décevantes. Enfin, les mandats de recherche internationaux peuvent être ordonnés par les autorités de poursuite pénale via le système d'information Schengen (SIS) européen ou les notices rouges d'Interpol.

Nous pouvons donc rapporter ici que ces organismes de coopération internationale sont incontournables, efficaces et utiles dans la lutte contre la cybercriminalité. Il est toutefois évident que les systèmes judiciaires basés sur un légitime découpage territorial ne s'appliquent que difficilement à une

criminalité qui évolue dans un espace globalisé et qui ne repose que sur des lignes numériques qui prennent ancrage dans le monde physique en tous points de la planète. Mais c'est pour le moment le cadre qui nous est fixé et il s'agit de faire le mieux possible en le respectant.

IV. Exemples de succès

Afin d'illustrer le quotidien des enquêteurs en charge de la cybercriminalité dans le canton de Vaud, nous nous permettrons de relater certaines affaires de ces dernières années qui ont pour la plupart déjà été médiatisées ou qui ont été jugées.

A. *Smishing (Phishing* SMS) – divers *modus*

Il s'agit ici de deux affaires distinctes liées au même phénomène et qui ont conduit à des interpellations de suspects dans notre canton à la même période. Ces interpellations ont fait l'objet d'un communiqué de presse du Ministère public au mois de juillet 2023 : « *Entre avril 2022 et juin 2023, une quarantaine de plaintes relatives à des cas de phishing* / hameçonnage*, pour un montant de plus de 170'000 francs, occupaient particulièrement la police de sûreté vaudoise. Après plusieurs mois d'enquêtes, sept suspects ont été identifiés et dénoncés. Quatre d'entre eux ont été placés en détention provisoire.* »[23].

Dans les deux affaires, ledit communiqué indique que « *les modes opératoires pouvaient varier, mais de manière générale, le SMS annonçait qu'un colis était en attente de livraison, moyennant le paiement de frais de livraison. La victime était ensuite invitée à cliquer sur un lien, lequel redirigeait vers une page imitant le site internet de La Poste. En confiance, la victime inscrivait les informations de sa carte de crédit, utilisée ensuite par les malfrats pour effectuer divers achats.* ». Il précise encore que « *lors de ces enquêtes, trois suisses, un marocain et un algérien, âgés entre 18 et 46 ans ainsi qu'un espagnol et un belge, âgés de 17 ans, habitant dans notre canton, ont été identifiés et dénoncés. Quatre de ces auteurs ont été placés en détention provisoire. Le préjudice total causé dépasse les CHF 170'000.-* »[24].

Concrètement, ce qui est particulièrement intéressant dans ces deux cas réside dans le fait que nous avons pu remonter à des personnes agissant sur notre canton. Dans une des affaires, les auteurs, âgés de 17 et 18 ans, profitaient d'outils

[23] Ministère public vaudois, Communiqué de presse du 14 juillet 2023.
[24] Ministère public vaudois, Communiqué de presse du 14 juillet 2023.

cybercriminels qui leur étaient « mis à disposition » par d'autres cybercriminels qui leur fournissaient les moyens de réaliser les étapes nécessaires à la réalisation de l'arnaque. Par exemple, la plateforme qui permettait d'envoyer en masse sur des numéros de téléphone suisses les SMS de *La Poste*, ou d'autres fournisseurs de prestation très populaires. Des hyperliens conduisant ensuite à la page Internet frauduleuse y étaient inclus. Ou la page de phishing personnalisable avec le renvoi des informations obtenues frauduleusement sur une autre plateforme permettant aux auteurs de les récupérer. Et une fois les informations de carte de crédit obtenues, nos jeunes auteurs les utilisaient pour effectuer des achats à leur propre profit, pour des connaissances ou pour en tirer un bénéfice en revendant ultérieurement les marchandises acquises frauduleusement. Là encore, certaines connaissances astucieuses étaient nécessaires pour arriver à leurs fins dans des commerces locaux, notamment. En raison de leurs liens avec les cybercriminels étrangers qui leur fournissaient les prestations qui étaient nécessaires, ils n'avaient pas besoin d'autres complices géographiquement situés dans notre région. Nos auteurs locaux pouvaient donc agir de manière autonome et sont restés trop longtemps sous le radar.

Dans la seconde affaire qui a été jugée fin 2023, les auteurs qui ont pu être arrêtés dans notre canton appartenaient à un réseau international. Comme le rapporte un article du quotidien 24Heures qui relate le procès, « *les deux hommes renvoyés devant les juges veveysans ont été pincés comme les maillons d'un de ces réseaux agissant entre la Riviera et le Maghreb.* »[25]. Les auteurs présents en Suisse avaient pour mission d'envoyer les SMS frauduleux à l'aide de matériel de communication spécifique. Il est à ce sujet précisé dans l'article de presse : « *Quelques chiffres illustrent l'ampleur de la fraude : en une année, quelque 774'800 faux SMS de La Poste sont partis, via environ 90 numéros de téléphone différents.* » Lorsque les futures victimes mordaient à l'hameçon, les auteurs avaient ensuite pour tâche de valoriser les données volées. « *Car à peine les données bancaires renseignées, des hackers arrimés à leur ordinateur pass*[ai]*ent commande d'objets divers, en l'occurrence du matériel informatique ou de télécommunication, des cartes cadeaux et des bons d'achat.* […] *Par ailleurs, des dénonciations aux quatre coins de la Suisse n'ont pas pu être rattachées à ce réseau, apparemment piloté du Maroc par des comparses camouflés sous des pseudos. Les enquêteurs ont tout de même pu lister une quinzaine de victimes et estimé le préjudice minimal à 83'000 francs. Trente-deux adresses et noms différents dans l'Est vaudois ont été utilisés pour l'envoi des*

[25] Flavienne WAHLI DI MATTEO, Des milliers de SMS frauduleux sont partis de la Riviera, disponible sous : <https://www.24heures.ch/proces-pour-cybercriminalite-a-vevey-des-milliers-de-sms-frauduleux-sont-partis-de-la-riviera-889713161921> (*consulté le 10.1.2024*).

colis, qu'un des prévenus se chargeait de récupérer. Le fruit de la revente du matériel et le transfert de bons cadeaux au Maghreb ont constitué le butin. »[26].

En finalité, « *les juges ont suivi les réquisitions du Ministère public : 24 mois de prison, dont la moitié ferme pour le premier, 30 mois ferme pour le second en raison de ses antécédents, peines assorties d'expulsions de territoire de respectivement 5 et 20 ans.* »[27].

Ces deux affaires montrent que pour un même phénomène pour lequel les *modus* et les conséquences visibles ne changent que peu, on peut se retrouver face à plusieurs séries distinctes, celle-ci pouvant être le fait d'auteurs ou de groupes d'auteurs différents. Cette constatation n'est pas nouvelle et s'applique également à la criminalité sérielle traditionnelle qui évolue dans le monde physique. Les méthodologies de renseignement criminel sont alors justement utilisées pour pouvoir détecter les séries et enquêter plus efficacement.

B. Extorsions

Dans les affaires qui seront relatées ici, la problématique que je souhaite illustrer est de l'ordre de la localisation géographique des auteurs et de la tactique judiciaire pour la poursuite des auteurs. En effet dans l'une d'entre elles, les auteurs ont pu être interpellés en Suisse, alors que dans la deuxième, les suspects ont été poursuivis et auditionnés par voie de commission rogatoire dans leur pays de résidence et dans la dernière, un mandat d'arrêt international a permis l'extradition du suspect dans notre pays. Nous présenterons ici les considérations qui entrent en compte pour déterminer les choix devant permettre de mener les auteurs devant les tribunaux.

1. Signaux locaux – agir sur notre territoire

Cette première affaire remonte à janvier 2021. Comme le relatait la presse, « *La police cantonale vaudoise a mis la main sur deux individus*

[26] Flavienne WAHLI DI MATTEO, Des milliers de SMS frauduleux sont partis de la Riviera, disponible sous : <https://www.24heures.ch/proces-pour-cybercriminalite-a-vevey-des-milliers-de-sms-frauduleux-sont-partis-de-la-riviera-889713161921> (*consulté le 10.1.2024*).

[27] Flavienne WAHLI DI MATTEO, Des milliers de SMS frauduleux sont partis de la Riviera, disponible sous : <https://www.24heures.ch/proces-pour-cybercriminalite-a-vevey-des-milliers-de-sms-frauduleux-sont-partis-de-la-riviera-889713161921> (*consulté le 10.1.2024*).

suspectés d'une escroquerie sur internet. Leur victime a subi un préjudice dépassant les 250'000 euros (265'000 francs). »[28].

La victime avait été contactée par les réseaux sociaux et avait fini par aider financièrement une femme qui n'existait que virtuellement, selon un *modus operandi* bien rôdé. Les transferts d'argent ont été réalisés par des virements bancaires ou des coupons permettant des achats en ligne. Mais également par porteur de main à main et c'est lors d'une de ces transactions que deux auteurs ont été interpellés. Comme le rapporte 24Heures, il s'agissait de « *deux hommes de nationalité guinéenne et béninoise, vivant en France et âgés respectivement de 20 et 50 ans. Tous deux ont été interpellés le 21 janvier* [2021, ndlr] *à Lausanne, avant d'être placés en détention provisoire.* ».[29].

Il faut immédiatement reconnaître que ce cas de figure où les auteurs de ce type de délits résidant dans des pays étrangers se déplacent dans notre pays pour commettre leurs délits est plutôt rare. Mais, dans ce cas il nous incombe d'être en mesure d'identifier ces quelques occurrences et d'en tirer profit. Dans le cas d'espèce, l'enquête a permis de démontrer que les deux personnes interpellées étaient les réels auteurs de l'escroquerie sentimentale et pas de simples coursiers. Ils ont pu être poursuivis et condamnés à ce titre.

2. Remonter à la source – poursuivre à l'étranger

Dans cette deuxième affaire, les investigations ont permis d'identifier des suspects d'une autre escroquerie sentimentale qui avait très probablement affecté sa victime et contribué à ce qu'elle mette fin à ses jours. Ce cas n'a pas été médiatisé, mais la police et la justice n'ont pas ménagés leurs efforts dans le but d'identifier les escrocs et de les poursuivre. En raison de la gravité de l'issue de cette cyberescroquerie, une commission rogatoire internationale a été exécutée avec un déplacement d'enquêteurs suisses à l'étranger dans le pays de résidence du principal suspect, en Côte d'Ivoire. Elle a permis de l'identifier formellement et de poursuivre les actes d'investigation dans le but de le faire condamner en Suisse ou dans son pays d'origine en fonction des possibilités propres à la situation.

Cet exemple illustre le fait que l'identification formelle et le déplacement d'enquêteurs suisses dans des pays d'Afrique de l'Ouest notamment à l'origine de

---

[28] Site 24Heures, Arnaque aux sentiments : 265'000 fr. envolés, <https://www.24heures.ch/arnaque-aux-sentiments-265-000-fr-envoles-285850600451> (*consulté le 10.1.2024*).

[29] Site 24Heures, Arnaque aux sentiments : 265'000 fr. envolés, <https://www.24heures.ch/arnaque-aux-sentiments-265-000-fr-envoles-285850600451> (*consulté le 10.1.2024*).

très nombreuses escroqueries comme les arnaques aux petites annonces, sextorsions ou escroqueries sentimentales, soit la Côté d'Ivoire ou le Bénin et parfois le Nigéria, est coûteuse et difficile. En effet, les services de police de ces pays ne disposent souvent que de ressources limitées et de moyens d'identifier et localiser des suspects, sur la base des informations issues du cyberespace en notre possession, d'autant plus limités. On ne peut donc que trop rarement consentir à ces efforts, qui sont souvent réservés à des cas particuliers ou d'une gravité qui les justifient.

3. Poser un filet – mandat d'arrêt international

La troisième affaire d'extorsion décrite ici concerne une escroquerie décrite par le nouvel Office fédéral de la cybersécurité en ces termes : « *La 'pseudo-extorsion' est une escroquerie qui consiste à envoyer des courriels de menace émanant prétendument des autorités, lesquels accusent une personne d'un acte pénalement répressible pour lui faire croire que les poursuites ne seront abandonnées qu'en échange d'une certaine somme.* »[30]. Ce phénomène a connu une forte augmentation depuis 2021, mais heureusement il est en diminution en 2023, tout en restant une proportion importante des signalements à l'office fédéral de la cybersécurité (OFCS).

Les faits qui nous concernent remontent à début 2022 par le dépôt de plainte d'un citoyen vaudois qui s'est laissé prendre et a payé une somme importante. Le courriel à l'origine des versements était libellé à l'en-tête de fedpol et d'Europol, leurs logos étant facilement récupérables sur Internet. Plusieurs démarches d'investigation, dont des demandes d'informations basiques relatives à des adresses électroniques par voie de demande de remise spontanée à l'étranger ont permis de remonter petit à petit la piste et d'identifier certains profils sur les réseaux sociaux utilisant les éléments recueillis. Ces recherches en sources ouvertes (OSINF) aboutissant à l'aide des bribes d'information et des demandes à nos partenaires policiers au travers des organisations de coopération internationale à identifier un potentiel suspect. Etant donné que son style de vie exposé publiquement sur Internet mettait en évidence plusieurs voyages intercontinentaux, en Europe notamment, ce suspect a été placé sous mandat d'arrêt international par le procureur chargé de l'enquête au début du mois de décembre 2022. L'interpellation du suspect nous était communiquée peu de temps après puisqu'il avait été arrêté à Paris, le jour de Noël, à sa descente de l'avion en provenance de Côte d'Ivoire. Depuis, il a été extradé vers la Suisse et a ainsi pu être poursuivi. Ses déclarations ont été riches d'enseignements, non seulement sur le cas en question, mais également sur son parcours de vie

30 OFCS, Cybermenaces.

qui l'a amené à 30 ans à bien en vivre de ses activités criminelles, après avoir évolué et s'être perfectionné. Cela confirme les dires d'un collègue béninois que nous avons rencontré à fin 2021 et qui nous expliquait que la jeunesse béninoise était majoritairement attirée par des activités cybercriminelles à l'issue de la scolarité obligatoire plutôt que des formations professionnelles ou des études et que cela constituait un risque structurel pour le pays et motivait les autorités politiques à renforcer les forces de police devant lutter contre la cybercriminalité[31].

En prenant un peu de recul, on constate que pour les trois cas d'extorsion évoqués, il a été possible de mettre en œuvre des stratégies policières et judiciaires qui conduisent à des interpellations et *in fine* à des condamnations, ceci en se donnant les moyens d'agir lorsque des cybercriminels sont physiquement présents en Suisse et *a fortiori* dans notre juridiction, de remonter jusqu'à eux dans leur pays d'origine ou de séjour lorsque le cas le justifie, ou de déployer nos filets si on peut penser que les suspects se déplacent, rendant leur interpellation et leur extradition possibles. Ce sont des tactiques appartenant au cadre juridique traditionnel, contraignant et parfois peu adapté aux cyberinfractions, mais il permet malgré tout des succès.

C. Remonter aux gros poissons

Le dernier cas que je souhaite présenter ici constitue une des contributions les plus importantes de la police vaudoise dans de domaine cybercriminel.

L'enquête a été médiatisée en mai 2020 après les interpellations d'un réseau de cybercriminels d'importance mondiale. Les éléments rapportés par les médias indiquaient que « *l'enquête, qui a été lancée début 2019 dans le canton de Vaud, a permis de remonter jusqu'en Pologne pour démasquer un groupe de pirates informatiques dénommé '*InfinityBlack*'. Cinq membres présumés de ce groupe y ont été arrêtés le 29 avril, tandis que cinq personnes ont été interpellées sur sol vaudois entre le 30 avril et le 2 mai 2019* […]. *Ce sont ces premières arrestations en Suisse qui ont permis de mener l'enquête et de comprendre le fonctionnement de cette cyberattaque de bons de fidélité. La*

[31] Alexandre BISENZ, Cybercrime : La police cantonale développe un lien fort avec le Bénin, POLCANT INFO, N°124, mars 2022, p. 12, disponible sous : <https://www.vd.ch/fileadmin/user_upload/organisation/dse/polcant/fichiers_pdf/2022/PolCant_Info_124_Mars_2022_web.pdf> (*consulté le 10.1.2024*).

Brigade d'analyse des traces technologiques (BATT) de la police vaudoise a ensuite collaboré avec fedpol, la police polonaise et Europol. »[32].

Comme il était communiqué aux médias, « *tout est parti de plaintes de clients, surtout vaudois, ayant remarqué que leurs bons Cumulus de Migros avaient été utilisés à leur insu. Une dizaine de plaintes vers la fin 2018 puis plusieurs dizaines les mois suivants* […]. *En quelques mois d'enquête, cinq jeunes pirates sont arrêtés dans le canton. Ils avaient profité de mesures de sécurité 'peu optimales' sur la plateforme en ligne des points Cumulus Migros pour récupérer des identifiants et mots de passe de comptes-clients. Ils ont ensuite revendu les données et bons vers d'autres réseaux illégaux de distribution. Et de fil en aiguille, ce 'début d'entreprise criminelle' en Suisse a rebondi en Pologne vers le groupe de pirates informatiques 'très professionnel et important' 'InfinityBlack'.* »[33].

Sans entrer dans le détail des dizaines de mois d'investigation, tant dans le canton de Vaud, afin d'identifier les jeunes auteurs locaux qui, à l'instar des auteurs de *smishing* du même âge évoqués au chapitre précédent, ont profité de moyens mis à disposition par des groupes de cybercriminels professionnels disposant de données, connaissances ou moyens inaccessibles à leur niveau. Ce qui a été remarquable dans cette affaire est le rôle qu'a joué Europol et ses spécialistes de la lutte contre la cybercriminalité qui passent en revue et analysent le contenu des annonces des entités nationales. Autant dire que celle que nous avons produite et qui contenait des informations récupérées dans le cadre de nos propres investigations sur les auteurs suisses fraudant les comptes CUMULUS et pouvant potentiellement identifier les membres du groupe *InfinityBlack* n'est pas passée inaperçue. Il faut dire que *InfinityBlack* et notamment son leader *AZATEJ*, avec son complice *SANIX*, étaient à l'origine de la publication de *Collection #1*, soit, en son temps, la plus grande compilation mondiale de combinaisons d'identifiants (nom d'utilisateur – mot de passe). *SANIX* était lui arrêté en Ukraine peu de temps après *AZATEJ*, comme le rapporte un média en ligne[34].

Europol a permis une coopération étroite entre les unités cyber en Pologne et en Suisse grâce au réseau dédié d'officiers de liaison cyber (*Joint Cybercrime Action Taskforce* – J-CAT) hébergé en son siège de La Haye. Cette organi-

32 Site RTS, Une vaste arnaque internationale aux bons Cumulus a été démantelée, disponible sous : <https://www.rts.ch/info/suisse/11301900-une-vaste-arnaque-internationale-aux-bons-cumulus-a-ete-demantelee.html> (*consulté le 10.1.2024*).

33 Site RTS, Une vaste arnaque internationale aux bons Cumulus a été démantelée, disponible sous : <https://www.rts.ch/info/suisse/11301900-une-vaste-arnaque-internationale-aux-bons-cumulus-a-ete-demantelee.html> (*consulté le 10.1.2024).*

34 Catalin CIMPANU, Le hacker Sanix arrêté en Ukraine, ZNET, 20 mai 2020, disponible sous :<https://www.zdnet.fr/actualites/le-hacker-sanix-arrete-en-ukraine-39903965.htm> (*consulté le 10.1.2024*).

sation a également soutenu l'opération en facilitant l'échange d'informations et en fournissant un soutien technique et analytique. *Eurojust* a de son côté facilité la transmission d'informations entre les parquets de Suisse et de Pologne[35].

Les cyberenquêteurs vaudois sont très fiers et garderont longtemps leur motivation intacte sur la base d'un tel succès qui démontre que la lutte n'est pas vaine.

V. Conclusion

En guise de conclusion, nous souhaitons rester positif. Il serait facile de pointer ce qui ne va pas plutôt que ce qui va, malgré tout, pas trop mal. La poursuite des cybercriminels au quotidien est passionnante. On ne s'ennuie pas, d'une part en raison de l'évolution des technologies et leur détournement systématique par les cybercriminels et d'autre part grâce à l'évolution des pratiques et des procédures auxquelles il faut constamment s'adapter. Il y a ainsi encore beaucoup à faire afin de ne pas régresser, mais chercher à progresser sur les plans méthodologiques et techniques en informant les pouvoirs politiques, afin de faire évoluer le cadre général.

Si nous devions pouvoir faire un vœu aujourd'hui, ce serait que la prise de conscience politique, qui ne peut pas prétendre ne pas être au courant de la réalité en matière d'évolution quasi exponentielle des cyberinfractions, conduise à une planification des ressources à long terme. En effet, depuis plusieurs années, des moyens supplémentaires sont octroyés dans le canton de Vaud en respectant les procédures ordinaires. Or, ces augmentations au compte-goutte qui permettent d'obtenir des ressources pour l'année suivante et se basant sur les statistiques de l'année précédente ne permettront jamais de répondre à une évolution aussi disruptive. Il est donc désormais nécessaire de se projeter à long terme, soit de se fixer un objectif à 10 ans et d'argumenter dans ce sens auprès de nos autorités politiques. Dix ans, c'est également le temps qui sera sans aucun doute nécessaire pour simplement trouver, former, spécialiser les policiers du monde cybernétique, ce monde qui est nouveau comme nous le disions en introduction et qui nécessite de nouvelles forces en nombre absolu et répondant à un profil de compétence adapté à cette nouvelle réalité.

35 Europol, Communiqué de presse du 5 mai 2020.

VI. Bibliographie

Littérature/doctrine

Giulia MARGAGLIOTTI/Betina BORISOVA/Ahmed AJIL/Quentin ROSSY, Mon canton, ma sécurité : sentiment de sécurité physique et numérique et opinions sur la police neuchâteloise, 2019, Ecole des Sciences Criminelles, Lausanne (<https://serval.unil.ch/resource/serval:BIB_5ADBB3E74AB1.P001/REF.pdf> *consulté le 10.1.2024*) (cité : MARGAGLIOTTI *et al.*) ; **Nora MARKWALDER/Lorenz BIBERSTEIN/Dirk Baier**, Cybercrime gegen Privatpersonen in der Schweiz: Ergebnisse des Crime Survey 2022, ZHAW 2023 (cité : MARKWALDER *et al.*).

Documents officiels

CLDJP, Communiqué de presse de la CLDJP du 9 avril 2019, Les polices romandes se dotent d'un Centre de Compétence Cyber, <https://www.ge.ch/actualite/communique-presse-polices-romandes-se-dotent-centre-competence-cyber-9-04-2019> (*consulté le 10.1.2024*) ; **Conseil Fédéral**, SNPC 2018-2022, Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) (<https://www.ncsc.admin.ch/ncsc/fr/home/strategie/ strategie-ncss-2018-2022.html>, *consulté le 10.1.2024*) (cité : Conseil fédéral, SNCP 2018-2022) ; **Conseil fédéral,** Loi fédérale sur la sécurité de l'information au sein de la Confédération, FF 2023 2296 (<https://www.fedlex.admin.ch/eli/fga/2023/2296/fr#art_74_b>, *consulté le 10.1.2024*) ; **Conseil fédéral,** Stratégie nationale de protection des infrastructures critiques, Approche globale pour garantir l'approvisionnement en biens et prestations essentiels, FF 2023 1659 (<https://www.fedlex.admin.ch/eli/fga/2023/1659/fr>, *consulté le 10.1.2024*) (cité : Conseil fédéral, Stratégie) ; **Département fédéral de la défense, de la protection et des sports**, Obligation de signaler les cyberattaques contre les infrastructures critiques – autre calendrier, communiqué (<https://www.vbs.admin.ch/fr/obligation-de-signaler-les-cyberattaques-contre-les-infrastructures-critiques-autre-calendrier>, *consulté le 10.1.2024*) ; **Europol**, communiqué de presse du 5 mai 2020, Hacker group selling databases with millions of user credentials busted in Poland and Switzerland (<https://www.europol.europa.eu/media-press/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland>, *consulté le 10.1.2024*) (cité : Europol, communiqué de presse du 5 mai 2020) ; **Grand Conseil vaudois**, Rapport de la commission chargée d'examiner l'exposé des motifs et projet de décret autorisant le Conseil d'État à adhérer au Concordat du 3 avril 2014 réglant la coopération en matière de police en Suisse romande (<https://www.vd.ch/fileadmin/user_upload/organisation/gc/fichiers_pdf/2012-2017/196_RC.PDF>, *consulté le 10.1.2024*) ; **Ministère Public vaudois**, Communiqué de presse du 14 juillet 2023, Cybercriminalité : sept suspects identifiés pour du « phishing/hameçonnage » (<https://www.vd.ch/toutes-les-actualites/actualite/news/i-cybercriminalite-sept-suspects-identifies-pour-du-phishing-hameconnage>, *consulté le 10.1.2024*) (cité : Ministère public vaudois, Communiqué de presse du 14 juillet 2023) ; **Office fédéral de la cybersécurité (OFCS)**, Cybermenaces, Prétendus courriels de menace émanant des autorités (<https://www.ncsc.admin.ch/ncsc/fr/ home/cyberbedrohungen/fake-extortion.html>, *consulté le 10.1.2024*) (cité : OFCS, Cybermenaces) ; **Office fédéral de la statistique**, Schéma statistique policière de la criminalité (SPC), Schéma des modes opératoires en criminalité numérique (<https://www.bfs.admin.ch/bfs/fr/ home/statistiques/criminalite-droit-penal/police/criminalite-numerique.assetdetail. 28645898.html>, *consulté le 10.1.2024*).

Transformations numériques et changements d'échelles.

L'exponentielle et ses conséquences pour les pratiques pénales

OLIVIER RIBAUX/THOMAS SOUVIGNET
Professeurs, École des sciences criminelles
Faculté de droit, des sciences criminelles et d'administration publique,
Université de Lausanne

Table des matières

I. Introduction[1]

N'entendons-nous pas que des procureurs se sentent en « mode survie » en réalisant la hauteur de la pile et la diversité des dossiers qui attendent impatiemment un traitement, une décision ou une réponse ? Ne ressentons-nous pas, dans l'accomplissement de certaines tâches tout au moins, que le système est « au bout » et qu'« on ne peut plus pratiquer correctement son métier » ? Sous l'allure de politiques criminelles, est-ce que les priorités définies ne veulent pas plutôt sauver un système en apnée ? Ou de se questionner plus fondamentalement : « est-ce que je peux encore donner du sens à ce que je fais » dans des systèmes où la division du travail nous confine dans des contributions élémentaires spécialisées dont nous ne percevons plus l'impact dans un tout ? Enfin, ne ressentons-nous pas un sentiment d'impuissance, une impossibilité de « faire changer les choses » ?

Ces plaintes pourraient exprimer la frustration de personnes insatisfaites au travail. Cependant, en fonction de leur fréquence et de leur persistance, nous pensons plutôt qu'elles signalent des changements importants à la fois dans la structure de la criminalité et dans les dispositifs pénaux pratiques prévus pour y répondre.

Ces bouleversements sont variés et nombreux[2]. Nous croyons que l'essor du numérique constitue un des éléments centraux sous-jacents à beaucoup de ces transformations. Malgré les réorganisations et les nouveaux engagements occasionnels qui ont accompagné l'émergence de nouvelles spécialisations au cours des deux dernières décennies, les approches et la perception des orientations à prendre sur les questions numériques n'ont pourtant pas vraiment évolué. Il ne suffit toutefois pas de faire « plus de la même chose » pour répondre à l'évolution des flux. Il est probablement temps de se demander s'il ne convient pas de changer quelque chose de plus fondamental dans les cadres de pensée.

---

1 Plusieurs idées présentées ici sont reprises de RIBAUX, Traçologie, chapitre 3, et de David-Olivier JAQUET-CHIFFELLE/Olivier RIBAUX, Transformations forensiques, criminologiques et juridiques dans une société numérique, journée de lancement des pôles numériques facultaires, Université de Lausanne, FDCA, 25 novembre 2022.

2 NOLAN/CRISPINO/PARSONS.

Pour aborder la question, nous partons d'une hypothèse pessimiste, formulée avant même l'avènement du numérique, dans un contexte de mondialisation, de centralisation et de concentration croissante des activités humaines au sein de structures toujours plus vastes. REY cite KOHR (1909-1994) :

> *« (…) les problèmes sociaux ont la tendance malheureuse à croître exponentiellement avec la taille de l'organisme qui les porte, tandis que la capacité des hommes à y faire face, si tant est qu'elle puisse augmenter, croît seulement linéairement. »*[3].

L'exponentielle renvoie à une fonction mathématique dont la croissance s'accélère et devient rapidement impossible à interpréter dans une seule échelle. Elle rend parfois compte de changements de taille de certaines grandeurs et/ou d'une complexité grandissante dans des systèmes de différentes natures (vivants, économiques, administratifs, technologiques ou sociaux). Des bouleversements dans les proportions des organismes se produisent alors, mettant en péril des équilibres dans les écosystèmes qui les hébergent.

Par conséquent, l'écart entre les évolutions linéaires (c.-à-d. une croissance constante) et exponentielles conduirait immanquablement à des réponses décalées face à ces mutations numériques des problèmes. REY développe l'argument :

> *« Les analyses de Kohr montrent à quel point la dynamique actuelle est mortifère et réclamerait une révision complète de nos manières de penser. Mais plutôt que d'en tirer les conclusions qui s'imposent, nous préférons par paresse d'esprit et par paresse tout court, détourner le regard »*[4].

Pouvons-nous percevoir des signes de l'exponentielle de KOHR dans les problèmes engendrés par l'ensemble des systèmes de délinquance à connotation numérique ? Si oui, les capacités de réponses pénales qui se sont organisées sont-elles en phase avec ces changements, tant dans leur nature que dans leur ampleur et leurs bonnes proportions ? Si ce n'est pas le cas, révisons-nous nos manières de penser ou détournons-nous le regard ?

Considérer la dynamique des adaptations apportées au Code pénal par le législateur en fonction des transformations numériques de la criminalité constituerait une première mise à l'épreuve de l'hypothèse de KOHR. De même, le projet *Justitia 4.0* de numérisation en Suisse de la justice répond-il d'une manière appropriée à ces évolutions ? Nous n'en sommes pas sûrs. Nous admettons toutefois que nous ne sommes pas les mieux placés pour considérer par exemple l'influence des données massives (*big data*) sur le fonctionnement des systèmes

3 REY, p. 112.
4 REY, p. 110.

pénaux et de la police judiciaire. Cette question est traitée toujours plus offensivement en droit et nous n'avons pas la prétention d'apporter de la nouveauté dans ce débat déjà bien informé[5], d'autant plus que le système pénal fait lui-même partie d'un fonctionnement judiciaire beaucoup plus vaste et est influencé notamment par des préoccupations sécuritaires en évolution.

Nous nous limitons à examiner de manière plus approfondie quelques situations où une accélération exponentielle semble se manifester, entraînant des changements d'état encore disparates, mais ayant des effets qualitatifs globalement perceptibles sur les systèmes pénaux et la police judiciaire. Par exemple, la visibilité soudaine de l'intelligence artificielle et les inquiétudes qu'elle engendre en milieu policier et pénal signalent ce genre de mutations en cours.

Pour exprimer les mécanismes en jeu, nous nous concentrons d'abord sur deux exemples historiques qui ont exigé autrefois des réformes sécuritaires et judiciaires profondes. Ils sont *a priori* très différents, mais ils renferment tous les deux des mécanismes d'évolution semblables, qui renvoient à l'exponentielle, à la complexité et aux questions de taille : (1) la croissance des villes du XVI^{e} au XVIII^{e} siècle[6] et (2) l'émergence de l'automobile et des formes d'insécurité qui en ont découlé.

Nous soutenons que ce schéma de croissance se reproduit dans les transformations numériques de certaines formes de délinquance, ainsi que dans la nature et l'intensité de la réponse des autorités pénales. La vitesse des changements est toutefois radicalement différente entraînant une décroissance brusque de la temporalité qui amplifie les effets de ces mutations.

Nous continuons en exprimant quelques caractéristiques d'une fonction exponentielle, ainsi que sa relation à la complexité et à la taille des systèmes examinés. Nous remettons ensuite en question la commensurabilité et l'adéquation entre des problèmes sélectionnés et les solutions apportées, tout en notant que la croissance de certains dispositifs chargés de répondre aux problèmes engendre elle-même de nouvelles difficultés. En conclusion, nous suggérons l'emploi de concepts centraux pour essayer d'ajuster les échelles et modifier les perspectives, afin d'aider à repenser le fonctionnement de nos systèmes dans des environnements transformés par le numérique.

Nous suggérons plus précisément d'articuler un débat qui traverse la science, la justice et la sécurité en donnant davantage d'importance à des notions telles que : (1) la *sérialité,* les *répétitions* et les *concentrations criminelles* dans des

5 Voir par exemple l'ensemble des réflexions qui ont été menées, en Suisse, dans le cadre des programmes nationaux de recherche PNR 75 ou PNR 77 sur les transformations numériques qui comprennent une composante sur les défis juridiques imposés par le courant des données massives.

6 CUSSON, Sécurité.

modèles d'une action de sécurité plus *proactive* qui se fondent sur une connaissance dynamique des problèmes et (2) la *trace* sous toutes ses formes dans un contexte où la traçabilité des activités humaines change radicalement et doit devenir un enjeu de société mieux reconnu. Quelques considérations sur le redimensionnement et la transformation des institutions compatibles avec l'intégration de ces perspectives termineront ce chapitre.

II. Illustrations historiques

A. Les changements de taille des villes et la police moderne

La concentration de populations dans des villes comme Paris a atteint de nouvelles dimensions entre le XVI^e^ siècle et le XVIII^e^ siècle. Dans des endroits où un nombre inhabituellement élevé de personnes se sont rassemblées, et dans un contexte de développements scientifiques et technologiques rapides, divers problèmes ont nécessairement émergé sous des formes jusqu'alors inconnues[7]. Ainsi, les conflits sur les marchés, les incendies, les difficultés de circulation, l'insalubrité et les odeurs, les difficultés d'approvisionnement ou les pandémies ont posé des problèmes amplifiés par le nombre d'entités (p. ex. des personnes, des maisons, des matières, des véhicules, des munitions, des armes) qui entretenaient de nouvelles sortes de relations dans un environnement limité. La combinaison de ces éléments dans une ville d'une taille nouvelle a nécessité la création de dispositifs de sécurité publique qui ne pouvaient plus se fonder exclusivement sur les mécanismes de justice existants, sur un engagement communautaire ou de l'armée.

Pour stabiliser la situation, il fallait structurer, professionnaliser, diviser le travail dans des spécialités organisées dans des architectures dont les proportions étaient incertaines. C'est dans ce contexte qu'une police dite moderne a émergé et s'est autonomisée progressivement d'une justice pénale dépassée. C'est aussi une police très « scientifique » qui prend forme. Elle a assisté les autorités dans l'élaboration de réponses, car d'importants problèmes étaient liés à la chimie, à la physique ou à la médecine (p. ex. incendies, odeurs, pandémies). Elle a pris forme durant le siècle des Lumières en France, dans un ensemble varié de changements engendrés dans un certain contexte par de nombreux acteurs aux idéologies, positions et connaissances variées. Des historiens[8] ou des criminologues[9] ont démêlé l'écheveau selon leurs perspectives et leurs méthodes, mais les mécanismes de ces transformations et la complexité du nouveau

7 MILLIOT *et al.*
8 MILLIOT *et al.*
9 Voir une synthèse dans CUSSON, Sécurité.

système qui en a résulté sont fondamentalement insaisissables dans leur totalité. Dans une telle situation, les effets des transformations n'ont pas tous été prévisibles ou contrôlables. Par exemple, la police se dispersait tant la variété et la complexité des problèmes à contenir était grande[10]. Elle est aussi devenue très intrusive, car elle a grandi en abusant de la surveillance en tant qu'instrument du pouvoir.

Il n'y avait bien sûr pas qu'une seule manière d'élaborer un dispositif structuré pour faire face à des problèmes si complexes. Alors que l'idée de la police est devenue universelle, l'émergence de dispositifs policiers spécifiques a suivi diverses voies dans d'autres régions et pays en fonction de leur culture et de leur histoire. Adoptant une vision communautaire conciliante, en contraste avec la vision parisienne, la police de la ville de Londres (Scotland Yard) attendra jusqu'en 1829 pour se constituer, répondant ainsi à une situation qui devenait intenable avec les dispositifs en place[11]. Les polices en Suisse suivront aussi leurs cheminements cantonaux propres dès le début du XIX^{e} siècle[12]. Elles ont gardé une petite taille, dans un dispositif très décentralisé. Cependant, elles partagent toutes la caractéristique commune d'avoir été inspirée par le modèle de la gendarmerie française, suite à l'incursion de Napoléon à cette époque. Dans cette diversité, des tendances générales apparaissent. Les polices se centralisent, donnant ainsi progressivement naissance à des organismes plus grands confrontés à de nouveaux types de problèmes. Les fonctions de sécurité publique et de maintien de l'ordre des polices sont désormais distinctes d'un volet d'enquête étroitement lié, mais d'une manière très variée en fonction des systèmes, à la magistrature pénale[13]. Par ailleurs, l'enquête prend aussi de nombreuses formes en suivant d'autres voies traversant les droits, les procédures et les institutions. Ce n'est pas dans le champ du droit pénal qu'on enquête le plus. Une étude empirique, au Québec, montre que les fonctions d'investigation de tous types intégrées dans des organisations publiques et privées concernent aujourd'hui jusqu'à dix fois plus de professionnels que dans l'ensemble des polices judiciaires couvrant la province[14].

L'évolution de cette diversité de configurations avec les transformations numériques et ses nouvelles échelles informationnelles n'est pas prévisible tant la nouvelle situation est rendue complexe. Les solutions possibles sont nombreuses, mais incertaines, et les dispositifs en place ont grandi et se sont rigidifiés.

10 CUSSON, Sécurité.
11 CUSSON, Sécurité.
12 HEBEISEN ; RIBAUX, Fédéralisme.
13 BARLATIER.
14 CUSSON/LOUIS, p. 13.

B. L'évolution des technologies de l'automobile[15]

Grâce à l'automobile, nos déplacements se font désormais à une vitesse au moins dix fois supérieure à celle de nos déplacements à pied dans le passé. L'avènement des technologies automobiles a provoqué un changement radical dans l'échelle de nos vitesses de déplacement. L'accroissement du parc de véhicules motorisés, quant à lui, semble plus régulier au moins depuis 1980[16]. Cette progression aux allures de linéarité trompe toutefois notre perception, car les véhicules entrent en interaction avec leur environnement et d'autres entités (réseau routier, villes, piétons, cyclistes, faune, autres automobiles, autres moyens de transport). On peut envisager l'exponentielle en considérant chaque automobile supplémentaire comme un nœud à ajouter dans un graphe, avec tous les liens qu'elle crée avec d'autres entités (nœuds). L'accroissement des nœuds est linéaire, mais la complexité engendrée par les connexions est exponentielle (voir section III). La croissance de ces relations, une fois des seuils dépassés, engendre alors des inconvénients d'une nouvelle envergure, tels que la résonance du bruit des moteurs le long des routes, une utilisation répandue du klaxon, la pollution et les accidents.

Ces derniers semblent relever d'une certaine fatalité statistique, malgré tous les efforts mis en œuvre pour en réduire le nombre et la gravité depuis plus de cent ans. Il n'est pas étonnant que cela se produise : notre constitution physique n'est pas adaptée pour nous déplacer et réagir à l'imprévu à plus de 20 kilomètres à l'heure. Les causes de ces accidents sont donc diverses et étroitement liées, allant du facteur humain à la configuration des environnements routiers, en passant par des défauts techniques des véhicules et la dynamique du trafic. La réponse visant à atténuer ce problème d'intégration des technologies automobiles dans la société est complexe, avec une envergure et une nature que l'on espère appropriées compte tenu de ces changements majeurs. Dans un système aussi complexe, agir sur un composant peut avoir des effets secondaires difficiles à prévoir sur d'autres parties. Il faut donc garder une vue d'ensemble par une attitude systémique, respectueuse de la complexité.

Les solutions sont habituellement envisagées d'une manière conventionnelle, en adoptant une approche basée sur la division du travail qui fragmente le système en différentes parties. Ces composants spécialisés appartiennent à divers secteurs et professions *a priori* très éloignés les uns des autres, incluant les écoles, les constructeurs automobiles, les services d'entretien des

---

15 Nous reprenons cette analogie esquissée dans le cadre du Campus cybersécurité, Cercle de Cadenabbia, Réseau national de sécurité et Team Consult, 26-27 août 2021, Appenberg.

16 Disponible sous : <https://www.bfs.admin.ch/bfs/fr/home/statistiques/mobilite-transports/infrastructures-transport-vehicules/vehicules/vehicules-routiers-parc-taux-motorisation.html> (*consulté le 18 septembre 2023*).

infrastructures et de la signalétique, les garagistes, les entités de secours d'urgence post-accident, ainsi que les hôpitaux qui assurent un suivi médical particulièrement précis des traumatismes les plus couramment provoqués. La réduction des risques peut engager encore d'autres expertises variées et imposer des contraintes pour les conducteurs comme le permis de conduire, les examens médicaux à partir d'un certain âge ou les inspections techniques des véhicules. Dans les structures académiques traditionnelles, certains départements s'intéressent particulièrement à des domaines aussi variés que la psychologie des conducteurs ou la physique liée aux accidents. Enfin, la législation qualifie des comportements accidentogènes comme délictueux. Son application implique l'intervention de policiers spécialisés équipés d'une variété de technologies modernes de détection, telles que des radars, des caméras, des instruments de dépistage d'alcoolémie et de produits stupéfiants, et diverses banques de données. La circulation routière est devenue un pilier des organisations policières et occupe substantiellement les tribunaux depuis très longtemps. Le tout évolue continûment en quête d'une configuration et de proportions considérées comme « raisonnables » pour un système que l'on reconnaît de toute façon incapable d'éradiquer le problème. Il vise à assurer un équilibre sécuritaire convenant à une société prise, selon DUPUY, dans un « effet boule de neige », une « spirale de dépendance à l'automobile » qui indique un développement d'une nature exponentielle[17].

Nous constatons ainsi que face à une complexité croissante, nous élaborons un système qu'on espère proportionné, dérivé d'une décomposition du problème global. Une telle division n'est pas immédiate, étant donné l'interconnexion des éléments du problème : il existe toujours de multiples façons, plus ou moins adéquates, de procéder et des effets secondaires auxquels il faut s'attendre chaque fois que nous agissons à un point du système. Ces approches sont fortement influencées par nos préjugés portant sur une division historique des disciplines académiques, réparties dans les sciences humaines et sociales ou les sciences de la nature et de l'information. La mise en œuvre a été réalisée de manière répartie, avec un certain succès, au sein d'un ensemble d'institutions abritant des professions déjà bien établies (par exemple, la police, les hôpitaux, les constructeurs automobiles, les services sociaux). Toutefois, une fois morcelée dans les disciplines, les métiers et les institutions aux priorités propres, une telle perspective a tendance à évoluer au profit des spécialités, de leurs ressources et de leurs technologies, au risque de perdre la vue d'ensemble[18]. Il faut parfois réétudier l'ensemble hors des cadres institutionnels. Par exemple, les « coups de pouce » (*nudges*) introduits dans l'environnement incitant subtilement à des comportements adéquats sans qu'on s'en aperçoive font partie d'approches novatrices (p. ex. signes et obstacles sur la route, diverses

17 GALLEY.
18 GOLDSTEIN ; ROUX *et al.*

incitations à une conduite prudente dans les véhicules modernes, ou boîtiers proposés par les assureurs)[19]. Ces « coups de pouce » peuvent être utiles, notamment pour atténuer les tendances naturelles à une conduite agressive sur les routes, identifiée comme l'une des principales causes d'accidents[20]. Plus généralement, l'accidentologie routière adopte une perspective transversale, en évitant l'accumulation traditionnelle d'expertises cloisonnées, se développant de manière autonome et selon leurs propres intérêts.

Les deux questions fondamentales se manifestent clairement dans cet exemple. (1) La commensurabilité. C'est-à-dire, est-on capable de mettre en rapport des problèmes et des solutions adéquates dans des échelles comparables dans des systèmes en croissance ? Et (2) est-ce que les cadres de pensée sont compatibles avec les nouveaux problèmes résultants des changements d'échelles ? Nous pouvons admettre que des efforts considérables ont été déployés selon ces deux aspects. Cependant, il est nécessaire de prévoir que les problématiques continueront à évoluer, avec des éléments tels que le niveau de saturation des routes, une nouvelle perspective écologique, l'émergence de véhicules plus autonomes, la disponibilité restreinte d'énergie et de matières premières, ainsi que d'autres transformations dans l'environnement physique, social, économique et juridique. Les structures actuelles sont à nouveau remises en cause à des échelles qui méritent une attention particulière. Face à ces mutations, les systèmes montrent des degrés variés de résilience. Néanmoins, la complexité croissante et les disproportions de plus en plus handicapantes de leur structure ne garantissent plus les capacités d'un bon fonctionnement homéostatique (c'est-à-dire une autorégulation permettant un retour à la stabilité) face à des changements d'une telle envergure. La viabilité de l'ensemble est alors en jeu[21]. La rupture peut devenir inévitable.

Quoi qu'il en soit, l'intégration des technologies de l'automobile dans la société nous a forcés à concevoir la mobilité dans de nouvelles échelles. Elle a exigé une réponse multidimensionnelle d'une grande ampleur apportant ses propres dysfonctionnements.

C. Une nouvelle rupture

Dans l'histoire, beaucoup d'autres exemples remontant à une époque bien plus ancienne illustrent des systèmes ayant subi des mutations qualitatives provoquées par des changements de taille[22]. Les défis actuels des trans-

19 FLÜCKIGER.
20 BERDOULAT.
21 CATELIN.
22 REY.

formations numériques présentent des similitudes, voire sont plus préoccupants, notamment car tout va beaucoup plus vite[23]. La nature de nos interactions sociales a subi des transformations radicales, en transitant par des identités numériques qui ajoutent une quantité monumentale d'entités à prendre en compte. Cela entraîne une expansion soudaine des nouveaux risques auxquels nous sommes exposés. La quantité des infractions à forte connotation numérique dépasse maintenant l'addition de toutes les autres formes de criminalité confondues[24].

Ce n'est pas la première fois que les manières de traiter, stocker, émettre et recevoir de l'information ont désorganisé la société : successivement, la parole, l'écriture et l'imprimerie avaient déjà tout bouleversé. S'il a fallu beaucoup de temps pour que les choses se remettent en place, il est aujourd'hui nécessaire de reconnaître que les conséquences des transformations numériques, accentuées par la visibilité récente des performances inattendues de l'intelligence artificielle, nous déconcertent[25]. De la même manière que pour l'automobile, nous ne sommes pas constitués pour vivre immergés dans ces espaces informationnels. Nous sommes vulnérables en raison de nos difficultés à maîtriser l'utilisation des nombreux outils et désorientés par l'abondance et la diversité des données qui nous submergent. Inévitablement, nous créons des vulnérabilités supplémentaires en raison des *bugs* devenus inhérents à la réalisation de systèmes informatisés complexes[26].

Ce constat nous encourage donc à postuler une rupture semblable à celle constatée dans nos exemples historiques, bien que d'une soudaineté et d'une envergure sans précédent. En prendre conscience est particulièrement difficile, car nous sommes profondément immergés dans ces changements. Pour étayer cette position, nous devons préciser la nature des grandeurs en jeu et de leur combinatoire.

---

23 HILBERT.

24 Voir par exemple les statistiques intégrées (sondage, données provenant du secteur privé et de la police) en Angleterre et Pays de Galles qui classifient les infractions numériques depuis 2016 et sur lesquelles beaucoup d'autres études ont été basées subséquemment, disponible sous : <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice> (*consulté le 29.12.2023*).

25 Voir par exemple Michel SERRES, Les nouvelles technologies : révolution culturelle et cognitive, conférence, Institut national de recherche en sciences et technologies du numérique (INRIA), 2007, disponible sous : <https://interstices.info/les-nouvelles-technologies-revolution-culturelle-et-cognitive> (*consulté le 13.12.2023*).

26 BOULLIER, Sociologie, p. 41.

III. L'exponentielle et l'hypothèse de KOHR

L'exponentielle est une fonction mathématique dont la croissance s'accélère (voir fig. 1). En tant que modèle d'un phénomène, elle est fréquemment utilisée pour rendre compte de la complexité, notamment dans l'analyse des ressources requises pour l'exécution d'algorithmes, la mesure de l'expansion de la structure d'un graphe par l'ajout de nœuds et d'arcs, la représentation des changements progressifs de grandeurs et de proportions dans des organismes et des systèmes ou encore la modélisation de phénomènes de propagation[27]. L'évolution exponentielle conduit à des changements de taille qui, une fois un seuil critique atteint, peuvent engendrer des transformations qualitatives : le phénomène en jeu grossit, au moins selon certaines dimensions, et subit une métamorphose.

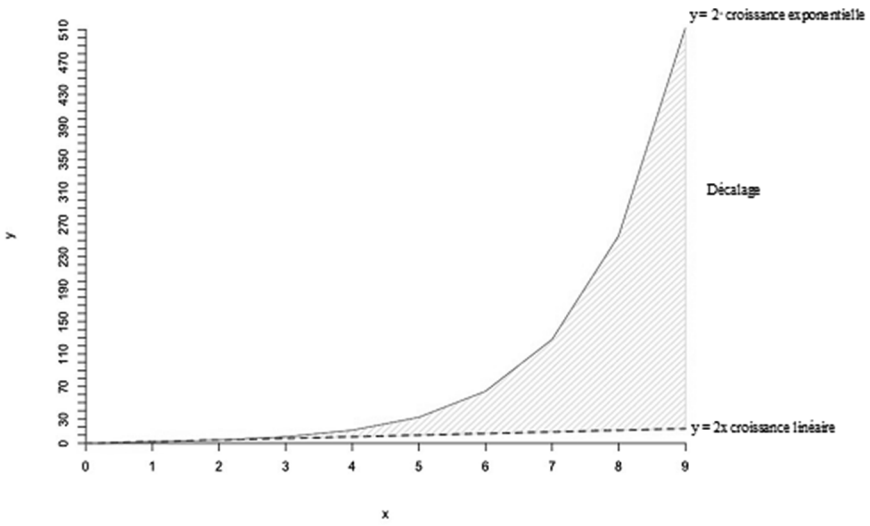


Fig.1. Pour aider à visualiser l'hypothèse de KOHR, représentation de l'accroissement du décalage entre une fonction exponentielle de base 2 et une fonction linéaire (y = 2x)

L'utilisation systématique de cette fonction durant la crise du COVID-19 pour imager la propagation du virus a contribué à ancrer encore davantage cette notion dans la conscience collective, tout en réduisant considérablement sa signification. Les courbes en général, l'exponentielle en particulier, influencent en effet nos croyances :

27 BOULLIER, Propagations.

> *« Elles gomment les imperfections de nos perceptions et celles des mesures dans une forme de réduction plaisante d'un réel complexe »*[28].

La force symbolique de l'exponentielle est souvent instrumentalisée, car elle a tendance à susciter un sentiment d'urgence : il faut provoquer au plus vite une rupture, agir pour infléchir cette courbe infernale avant qu'elle ne bascule dans une phase d'accroissement irréversible aux conséquences désastreuses. Les grands débats de société actuels reposent largement sur l'anxiété générée par l'exponentielle : que va-t-il se passer si la disparition des espèces suit une telle courbe ? Qu'en est-il, à l'inverse, de la propagation du moustique tigre, du frelon asiatique, de la punaise de lit ou de la moule Quagga dans les eaux lémaniques ? Et de la fonte des glaciers ? De la croissance des populations ? Du phénomène bureaucratique dans les organisations ? Plus généralement, de l'amplitude des propagations de tous types[29] ? Qu'en est-il de certaines questions liées au crime à connotation numérique ? S'inscrivent-elles dans de telles formes d'accroissement ?

Si la fonction exponentielle demeure pertinente pour saisir des évolutions inquiétantes, son exploitation nécessite donc une approche prudente. D'autres manières plus nuancées de modéliser les problèmes et suggérer un futur sont parfois plus adéquates. Par exemple, l'évolution d'une grandeur peut être souvent représentée de manière non linéaire, subir des fluctuations, sans forcément suivre l'accroissement endiablé de l'exponentielle. Une progression linéaire peut aussi atteindre des seuils critiques en provoquant des changements qualitatifs. En outre, il existe parfois des limites physiques ou d'autres contraintes susceptibles d'infléchir l'allure d'une courbe[30]. Certains écosystèmes retrouvent souvent par eux-mêmes un nouvel équilibre en s'autorégulant. Les organismes, vivants ou non, sont aussi occasionnellement plus résilients qu'imaginés face à une évolution redoutée[31].

Au-delà, de nouveaux risques, souvent latents, accompagnent effectivement certaines croissances de type exponentiel. Ils restent souvent intangibles jusqu'à ce qu'ils s'actualisent dans des situations particulièrement spectaculaires (p. ex. par les rançongiciels)[32]. Il est justifié d'affirmer que la réponse pénale a tardé à s'adapter à l'évolution du problème. Pendant une période prolongée, elle est même demeurée pratiquement inexistante, malgré les efforts d'acteurs autodidactes qui ont alerté en vain au sein de leurs organisations respectives. Ce n'est que récemment qu'elle a commencé à s'organiser sérieusement.

---

28 CLAVERIE, p. 189.
29 BOULLIER, Propagations.
30 CLAVERIE.
31 DE ROSNAY.
32 BECK ; BRODEUR, p. 42.

Afin d'explorer d'une manière plus approfondie la nature exponentielle ou non des transformations liées aux milieux pénaux, nous suggérons initialement de recueillir des indicateurs plus précis de certaines évolutions en cours qui pourraient être exponentielles.

A. Les transformations numériques exponentielles

Il y a de bonnes raisons de penser les transformations numériques dans leur globalité par l'exponentielle. La célèbre loi de MOORE[33] en donne les bases physiques : elle stipule approximativement un doublement du nombre de transistors, les composants élémentaires des microprocesseurs, tous les deux ans. Ils sont répartis sur des puces de silicium qui consomment toujours moins d'énergie. Il faut penser la loi ainsi : le terme de « transistor » désigne une entité électronique capable de réaliser des opérations (calculs) élémentaires. Cette évolution du nombre de transistors interconnectés aux autres représente ainsi un indicateur de la croissance de la puissance de calcul qui devient finalement immense. Celle-ci est maintenant accessible aux développeurs et utilisateurs de systèmes informatisés avec toutes les conséquences sur un plan sociologique, juridique, économique ou éthique[34]. Énoncée initialement en 1965, cette loi a été empiriquement confirmée au fil du temps [35]. Récemment, cependant, elle a rencontré des limites physiques. Néanmoins, elle se prolonge grâce à de nouvelles architectures de calcul, à la mise en réseau des microprocesseurs et au déploiement des objets connectés [36]. Cette loi est bien exponentielle. Au bout de quatre ans, c'est quatre fois plus de transistors, au bout de six ans, c'est huit fois plus (et non six fois plus), au bout de huit ans, c'est seize fois plus, et ainsi de suite (voir Fig. 1). Cet accroissement de la puissance de calcul se prolonge dans une croissance légèrement moins rapide, mais également exponentielle, des volumes numérisés d'information. À l'échelle d'un ordinateur individuel, le Megaoctet (10^6 octets) était considéré comme une grandeur colossale il n'y a pas si longtemps, alors qu'un disque dur d'un Téraoctet (10^{13} octets) est aujourd'hui un peu « juste » pour stocker nos images et vidéos privées. Sans compter qu'il faut parler d'Exaoctets (10^{18} octets) pour représenter la quantité quotidienne d'informations créée et échangée sur Internet. Selon HILBERT, la création de données numérisées suit elle-même une loi exponentielle qui résulte de l'essor de l'informatique[37]. D'autres solutions sont déjà étudiées pour

33 Gordon MOORE est un des fondateurs et ancien président-directeur général du concepteur et fabricant de microprocesseurs *Intel*. Il est décédé en 2023.
34 BOULLIER, Sociologie.
35 BOULLIER, Sociologie.
36 LUNDSTROM/ALAM.
37 HILBERT.

augmenter les capacités de stockages, lorsque les moyens traditionnels ne suffiront plus pour mémoriser cette production phénoménale.

La combinaison entre une puissance de calcul et une disponibilité des données amplifiées toutes les deux exponentiellement a rendu possible la mise en œuvre concrète des méthodes d'apprentissage automatiques basées sur le modèle des réseaux de neurones (apprentissage profond, ou *deep learning*). Au cours du siècle dernier, les versions prototypes de ces réseaux comportaient quelques dizaines ou centaines de paramètres intégrés dans leur structure, ajustables via un mécanisme d'apprentissage. La quantité de ces paramètres élémentaires dépasse largement le milliard aujourd'hui dans des structures de réseaux bien plus élaborées. L'exponentielle s'est ainsi propagée dans les réseaux en changeant leur taille, avec des bouleversements qualitatifs devenant particulièrement apparents depuis que les fonctions de génération de texte sont accessibles au grand public[38]. L'omniprésence de l'intelligence artificielle nous prend de court. Il n'est pas exclu que les ordinateurs quantiques, une fois que la technologie sera maîtrisée, ouvrent la voie à une nouvelle croissance exponentielle, nous propulsant vers le prochain palier. Une approche différente de la conception des algorithmes est déjà envisagée sur le papier, voire mise en œuvre sur des prototypes[39].

Dans notre cheminement, l'idée que nos sociétés ont été perturbées par les exponentielles de la loi de MOORE, de la production des données, ou de la capacité des réseaux de neurones est fondamentale, mais elle devient un lieu commun. Cette notion demeure beaucoup trop générale pour être véritablement utile dans notre contexte. Nous devons progresser en examinant de manière plus détaillée ces évolutions.

B. Le modèle des 5 V

Une décomposition simple peut nous aider. Dès que la loi de MOORE a produit ses effets dans le développement de logiciels et la gestion des informations, l'émergence du concept de données massives a exprimé le ressenti de changements significatifs en ordre de grandeur. Ces évolutions ont été rapidement perçues dans les entreprises comme des enjeux cruciaux, les incitant à repenser profondément leur approche de la gestion et de l'exploitation de leurs informations. LANEY a proposé un cadre d'interprétation dans trois grandeurs dépendantes, appelées les 3V : le *Volume*, la *Variété* et la *Vitesse*[40]. Ce modèle

38 Voir <https://openai.com/chatgpt> (*consulté le 27.12.2023*).

39 S'intéresser par exemple à l'algorithme de SHOR qui ouvre la perspective de casser des cryptosystèmes à clé publique dans des temps aux ordres de grandeur réduits.

40 LANEY.

s'est vite étendu à 5V, en ajoutant la *Valeur* et la *Véracité*. Ces dimensions restent intimement liées : lorsque de vastes quantités d'informations diverses doivent être absorbées dans des temps limités, on parle d'un flux combinant *Volume, Variété* et *Vitesse*. En examinant des situations particulières, nous constaterons alors un changement d'échelle sur chacune de ces dimensions (les V).

Le repère des 5V aide ainsi à concevoir le nouvel espace dans lequel nous sommes propulsés par une croissance exponentielle sous-jacente de certains problèmes de criminalité à connotation numérique, ainsi que par plusieurs réponses apportées par les systèmes pénaux. C'est désormais dans cet espace largement inconnu que nous devons nous resituer et essayer d'évoluer.

C. Les transformations numériques de la criminalité

Nous ressentons évidemment que l'automatisation de certaines activités nuisibles, parfois relevant de l'infraction, engendre des changements significatifs d'ordre de grandeur. Par exemple, des envois massifs (*Volumes*), car largement automatisés, de messages électroniques s'inscrivent dans une grande *Variété* de scénarios malveillants. Ils altèrent l'ampleur de la répétition des incidents. La mutation qualitative peut être simplement exprimée : le cas individuel insignifiant, généralement négligé par le système pénal, se reproduit à une échelle inédite et à de nouvelles temporalités (*Vitesse*), causant inévitablement d'importants dommages globaux.

Par exemple, selon le suivi quotidien des responsables, l'ensemble des comptes de messagerie affiliés à l'Université de Lausanne reçoit actuellement entre 500'000 et 1 million de courriels quotidiennement dont moins de 5 % traversent les filtres prévus pour empêcher des intrusions de différentes sortes. Les messages bloqués (soit le 95 % des courriels entrants) par cette digue sont au mieux inutiles (p. ex. publicités non sollicitées).

FELSON et ECKERT expliquent que les évolutions numériques, observées à travers les transformations de nos activités quotidiennes, nous projettent dans une ère où l'exposition au crime atteint des proportions sans précédent (*The age of exposure*)[41]. La question des ordres de grandeur s'étend à la nature planétaire des espaces de rencontres, multipliant ainsi les opportunités criminelles (*Variété*) dans des environnements transformés dans lesquels les médias synthétiques sont capables de générer de grandes quantités (*Volumes*) de mensonges et rumeurs (*Véracité*) divers (*Variété*) persuasifs et déstabilisants. L'utilisation de la traduction automatique permet maintenant de persuader (*Véracité*) en temps réel (*Vitesse*) un interlocuteur ciblé de réaliser des opérations sur ses comptes bancaires virtualisés (*Valeur*) dans une multitude de langues (*Variété*).

41 FELSON/ECKERT, Chapitre 10.

Le tout en ajoutant une indirection redoutable entre l'auteur et une identité numérique construite ou usurpée, constituant une sorte de masque permettant de choisir le meilleur moyen de duper sa victime (*Véracité*). Le fonctionnement entièrement numérisé des entreprises fait prendre conscience de la *Valeur* des données, tant économique (p. ex. des idées à protéger, de l'argent virtualisé, des données dont elles sont responsables et entièrement dépendantes) que lorsqu'elles relèvent de la sphère privée (p. ex. la menace de rendre des données médicales volées librement accessibles sur le *Darkweb*). Des données qui ont de la valeur constituent alors obligatoirement un bien convoité par des voleurs qui sont désinhibés par l'environnement confortable et sécurisant d'où ils opèrent généralement. L'indirection de leur relation au lésé par les identités virtuelles leur évite un contact direct avec leur cible pour perpétrer leurs délits[42]. Les médias synthétiques nous ouvrent à une nouvelle *Variété* de formes criminelles dans des interactions en temps réel (*Vitesse*) qui se manifestent déjà, mais dont nous n'avons pas encore une idée très claire. Les exemples d'usage de l'intelligence artificielle dans des modes opératoires fondés sur la persuasion prolifèrent depuis peu.

Ces illustrations, mises ensemble, montrent que les échelles dans lesquelles nous devons considérer les 5V en combinaison changent significativement.

Dans ces bouleversements, il arrive fréquemment que les créateurs des systèmes de délinquance les plus techniquement avancés laissent involontairement des traces aisées à collecter et à interpréter. Même lorsqu'ils prennent des précautions, il leur devient impossible de maîtriser tous les aspects de leur comportement dans la complexité croissante des environnements numériques.

IV. Les réponses dans les pratiques de l'enquête

Qu'est-ce que les pratiques essentiellement réactives des autorités de poursuite pénale opposent-elles à ces changements d'échelles dans leurs fonctions traditionnelles ?

A. Des réponses non monopolistiques

Il faut admettre que le problème très particulier des courriels indésirables mettant sous pression les systèmes de messagerie d'une organisation ne reçoit que peu de réponses du point de vue du droit pénal et de l'enquête. Peut-être que quelques messages particuliers seront, dans le cadre de rares

42 Voir par exemple WALL.

situations reportées, qualifiés d'infractions et leurs auteurs poursuivis. Leur nombre sera toutefois insignifiant et sans effet sur un problème d'ensemble loin d'être socialement, économiquement voire psychologiquement anodin. De manière plus large, le domaine de la cybersécurité s'empare de ce genre de situations, ainsi que bien d'autres, à travers des méthodologies qui se désintéressent essentiellement d'un traitement potentiel par des poursuites. Cette prise en charge par des acteurs variés de la cybersécurité se généralise, reléguant largement le système pénal à un rôle secondaire.

Plus précisément, jusqu'à récemment, la poursuite des escroqueries qui relèvent de l'arnaque en série n'était de loin pas une priorité dans les pratiques courantes. Le lésé a également une responsabilité de vigilance face aux astuces éventuelles. La perception semble évoluer avec la numérisation du phénomène. Les fraudes en ligne constituent un problème de criminalité fréquent, persistant, varié, en constante évolution et rendu visible par son impact parfois dévastateur sur les individus. Elles remettent en question la réponse pénale conventionnelle qui se concentre principalement sur le traitement des cas individuels, et qui est déconnectée de la dimension sérielle de ces problèmes. Le système pénal semble désormais y accorder un peu plus d'attention, bien qu'il rencontre déjà beaucoup de difficultés à recueillir d'une manière structurée les plaintes[43]. L'hypothèse de KOHR ne doit sûrement pas craindre ici la réfutation, bien que des communications récentes d'Interpol[44] et d'Europol[45] aient indiqué une attitude plus proactive de ces institutions internationales en matière de coordination et de soutien aux enquêtes sur ces questions. Il faut toutefois admettre que, malgré ces opérations certes à grande échelle, mais encore ponctuelles, la mondialisation de ce genre de délinquance peut rapidement dissuader les magistrats locaux de s'engager dans des poursuites à l'échelle internationale.

Une autre préoccupation a une portée méthodologique et se généralise à un large éventail de problèmes. Elle réside, dans notre exemple des courriels, dans un renversement logique de la réponse par la construction automatisée en temps réel de modèles filtrant les messages indésirables et suspects entrants. Ce retournement est beaucoup plus fondamental qu'il n'y paraît[46], puisqu'il indique que la découverte de schémas ou patterns à la base des modèles-filtres, devenus indispensables pour protéger le fonctionnement du système de courriels, est essentiellement inductive. Cette construction s'appuie sur des données parfois

43 ROSSY/RIBAUX.

44 Voir par exemple, opération HAECHI IV, disponible sous : <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation> (*consulté le 28.12.2023*).

45 Voir par exemple Europol, Online fraud schemes : a Web of deceit, IOCTA, 2023, disponible sous : <https://www.europol.europa.eu/media-press/newsroom/news/europol-publishes-iocta-spotlight-report-online-fraud-schemes> (*consulté le 28.12.2023*).

46 ANDERSON.

identifiantes, collectées, suivies et explorées à large échelle. Dans une telle approche, les données elles-mêmes suggèrent des régularités sur le déroulement d'activités inquiétantes, avec le moins d'*a priori* possible, plutôt que l'inverse, comme nous raisonnions essentiellement jusqu'ici. Ce genre de méthode d'apprentissage automatique moderne fondé sur les réseaux de neurones n'est pas transparente. Dans ces schémas de pensée, on s'inquiète du *quoi* (le phénomène des courriels), plutôt que du *comment* (les relations causales, les mécanismes particuliers des fraudes et autres *spams*). Comment alors accommoder ce genre d'approches conduites par les données, avec les principes élémentaires de transparence, de finalité bien définie et exclusive, de pertinence et de mesure dans la détection des infractions et la conduite des enquêtes ? La méthodologie s'avère intrinsèquement problématique à mettre en œuvre pour les autorités de poursuite pénale. L'importance de ce bouleversement logique peut être moins immédiatement évidente pour les responsables de la cybersécurité d'une entreprise, en l'absence de régulation, dont la priorité est de garantir le bon fonctionnement de l'organisation ou une récupération rapide en cas de problèmes. Dans ce contexte, certaines recherches explorent des pistes mieux adaptées au domaine pénal, visant à rendre l'intelligence artificielle plus évaluable et plus transparente[47]. Cependant, le problème de fond persiste.

B. Des réponses d'intensité en croissance exponentielle

Des changements d'échelles impactent aussi les méthodes d'enquête. Pour commencer, nous présentons deux illustrations de la délégation de tâches à la machine et ses implications. Dans le paragraphe suivant, notre attention se porte sur l'évolution phénoménale du contrôle de l'identité s'appuyant sur des technologies biométriques. Ensuite, nous montrons que la diversité des technologies élaborées et engagées dans les enquêtes judiciaires perturbe l'approche traditionnelle de l'enquête. Enfin, nous observons que l'incorporation de ces changements passe par de nouvelles distributions du travail que nous estimons encore largement inabouties.

1. La délégation à la machine

L'idée fondamentale est souvent trop simpliste, et ses effets sont moins réjouissants qu'espérés. Dans ce contexte de numérisation, il suffirait de répondre à ces changements d'échelles en numérisant et automatisant les processus d'enquête. L'hypothèse de KOHR serait alors réfutée puisque l'ampleur de la réponse serait proportionnelle à la grandeur des problèmes transformés

47 Voir par exemple MESKEA *et al.*

numériquement, tout en récupérant, par ces moyens, des ressources pour le travail décisionnel qualifié de « véritable ».

Il y a évidemment beaucoup de débats en droit sur le bien-fondé de la délégation d'opérations judiciaires aux ordinateurs, que nous laissons aux experts mieux équipés que nous. Un postulat peut toutefois nous mettre en garde. Les autorités de poursuite pénale agissent en tant qu'intruses chaque fois qu'elles interviennent, même dans les espaces virtuels, car normalement, elles ne sont pas censées être présentes dans ces environnements. Leurs interventions ne sont jamais insignifiantes : l'effet amplificateur de l'automatisation entraîne inévitablement des répercussions sur l'ampleur et la nature de cette intrusion. Un second postulat vient renforcer le premier : lorsque des tâches sont automatisées, leur organisation préétablie est perturbée, voire altère la nature même du processus.

Le contexte de la circulation routière nous offre à nouveau un exemple. L'usage de technologies capables de reconnaître en temps réel et dans des conditions variées les numéros de plaques de véhicules, que ces derniers soient garés ou circulant à une certaine vitesse, devient de plus en plus répandue. Le traditionnel mode de contrôle des parkings, où un agent habilité distribue des contraventions en plaçant un fichet sur le pare-brise des véhicules en infraction, semble être dépassé par la possibilité d'utiliser de tels dispositifs. Une voiture, équipée d'une caméra intelligente, est reliée à la banque de données des horodateurs (*scancar*). Elle circule dans la rue, captant systématiquement les plaques d'immatriculation des véhicules, tout en vérifiant la validité du stationnement. Ce dispositif nous rapproche, sur ce problème spécifique, de « l'idéal » d'un système complet et automatisé d'application de la loi. Il présente aussi l'avantage de pouvoir produire lui-même la sanction par une facture (amende) automatiquement envoyée au propriétaire de la voiture ainsi sanctionné. La décision de justice est alors, selon le processus, plus ou moins validée par des opérateurs, c'est-à-dire plus ou moins accompagnée ou déléguée à la machine. D'un point de vue technique, la fiabilité de ces systèmes est excellente. De faux résultats positifs (c'est-à-dire des numéros de plaques d'immatriculation de véhicules en infraction lus avec des erreurs ou des autorisations exceptionnelles qui ne peuvent pas être anticipées) sont toutefois inévitables et difficiles à détecter par les éventuels opérateurs. Si l'erreur humaine se manifestait déjà dans la version manuelle de ces opérations, la quantité de personnes faussement amendées qui doit alors se confronter à une administration pas forcément complaisante pour contester la sanction change totalement. Les prémices d'un renversement systématique de la charge de la preuve par l'automatisation se manifestent ainsi.

Un autre exemple se situe dans un champ forensique a priori éloigné du processus précédent. Depuis 1986, l'exploitation des profils d'ADN a amplifié les

capacités d'identification de personnes à partir de traces relevées sur les lieux d'une infraction. Des banques de données ont été constituées progressivement, puis mises en réseau en Europe, par le biais des accords dits de Prüm[48]. La Suisse doit s'arrimer à ce système, bien que des retards techniques considérables soient annoncés[49]. En termes d'échelles, cela veut dire que de vastes banques de données de profils d'ADN correspondant à des traces ou à des personnes déjà connues sont exploitées dans des flux toujours plus importants dont la taille a changé. Dans ces conditions, l'assimilation de la quantité croissante des correspondances (apparentes) trouvées devient un sérieux problème. Afin d'améliorer l'efficience de la gestion de ces flux, des structures de management, en Angleterre, ont proposé le concept de *Streamlined forensic reporting.* Cette idée, appliquée aux délits courants (en anglais : *high volume crimes*), renverse l'idée d'une enquête à déclencher au moment où une correspondance entre une trace et une personne est détectée au moyen d'une banque de données. Il préconise d'immédiatement informer la personne d'intérêt afin de chercher un arrangement judiciaire avec elle, sans autres évaluations préalables. L'économie des moyens d'enquête ainsi réalisée se combine avec une régulation des flux de dossiers générés par ces moyens d'identification, destinés aux tribunaux. Bien sûr, un tel principe de gestion engendre des controverses[50]. Il illustre le sentiment que la simple intensification des solutions élémentaires pratiquées auparavant ne suffit pas. Elles doivent être reconsidérées profondément en regard des changements d'échelles.

2. La quantité et la qualité des contrôles de l'identité

Un autre exemple d'automatisation intensive vient ici *a priori* mettre en danger l'hypothèse de KOHR appliquée à notre contexte : les systèmes puissants de gestion des identités semblent en effet s'adapter, en ordre de grandeur. L'intensité de la réponse n'est ainsi pas linéaire, mais relève davantage de l'exponentielle.

En matière de police scientifique, les systématiques de gestion des identités renvoient essentiellement à BERTILLON, à la fin du XIX^{e} siècle. Ce dernier voulait initialement confondre les récidivistes en regroupant sur des fiches centralisées à une large échelle un ensemble de grandeurs physiques mesurées sur un

48 Décisions 2008/615/JAI et 2008/616/JAI du Conseil de l'Union européenne du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

49 Disponible sous : <https://www.eda.admin.ch/europa/fr/home/bilateraler-weg/bilaterale-abkommen-nach-2004/pruem.html> (*consulté le 20.9.2023*).

50 MCCARTNEY.

individu (anthropométrie) ainsi que d'autres données[51]. Au-delà de cette fonction policière élémentaire, BERTILLON provoque une rupture dans l'idée de suivre beaucoup plus précisément et systématiquement la mobilité d'abord de groupes de personnes considérées à risques, jusqu'à envisager une extension des possibilités civiles de contrôler l'identité de tous les individus de la population. Un premier palier dans la mise en œuvre de moyens de contrôle et de surveillance est ainsi atteint. Il se heurte toutefois à une vive réaction de la population qui, déjà à son époque, ralentit certains développements. Cependant, ces projets ont progressé avec les technologies biométriques tout en préfigurant des développements européens contemporains qui changent encore une fois de taille.

Le contrôle de l'identité et d'objets visant toute une variété de formes de détection s'étend notamment par le Système d'Information de Schengen (SIS II). La recherche de personnes et d'objets signalés en grand nombre prend ainsi une dimension inédite par l'exploitation de nouvelles technologies d'identification automatisables (p. ex. la reconnaissance automatique des plaques de véhicules). La traçabilité des entrées et sorties d'Europe est également bouleversée par une nouvelle gestion des visas (*Visa Identification System*) et la perspective des développements du système numérisé à large échelle *Entry/Exit* qui doit intégrer la reconnaissance de visages. La gestion de l'immigration s'appuie aussi sur sa banque de données EURODAC constituée d'empreintes papillaires (*EUROpean DACtylographic system*). Les statistiques d'exploitation de SIS II uniquement illustrent la tendance[52] :

– en 2022, 85 millions « d'alertes » étaient stockées. Une alerte représente par exemple une personne, une arme à feu, une plaque de véhicule ou un document d'identité qui sont signalés pour une raison particulière (*e.g.* personne disparue, statut d'asile, visas, personnes recherchées pour des raisons judiciaires, objet dérobé). Ce nombre était de 50 millions en 2014, dans une progression perturbée par le COVID et le retrait du Royaume-Uni.
– Chaque jour, en 2022, en moyenne, environ 35 millions de requêtes étaient réalisées dans ce système par les pays partenaires. Le total de requêtes réalisées en 2022 était de 12,7 milliards, soit 80 % de plus qu'en 2021. Elles n'étaient « que » de 6 millions pour l'année 2014.
– Environ 263'000 correspondances étaient détectées par des contrôles en 2022, soit environ 720 par jour en moyenne, soit 18 % de plus qu'en 2021 et moins de 50 % de plus qu'en 2014.

Beaucoup d'aspects relatifs aux ordres de grandeur frappent dans ces statistiques. Ces développements pourraient constituer *a priori* une bonne nouvelle,

51 BERTILLON.

52 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security And Justice, SISII-2022, Annual statistics.

car, dans une conception d'application systématique de la loi, ils visent à dévoiler des comportements illicites avec une intensité commensurable à l'ampleur du problème. La réalité pratique nous renvoie toutefois quelques questions. Une vue des usages décomposée par pays partenaires montre une disparité inquiétante. Aucune stratégie d'ensemble n'est perceptible, au-delà de l'idée d'intensifier l'usage d'une opération de contrôle élémentaire. Nous observons aussi que la proportion des correspondances trouvées dans l'ensemble des requêtes est très faible (environ 0,02 ‰ des contrôles). L'augmentation des requêtes semble par ailleurs résulter de mécanismes d'automatisation liés surtout à la détection automatisée des numéros de plaques de véhicules opérée par certains pays et, dans une moindre mesure, à l'usage beaucoup plus systématique des empreintes papillaires intégré maintenant au système.

Les changements d'ordre de grandeur sont ici flagrants. Ils sont engendrés par des infrastructures et des processus grossissants apportant leurs propres problèmes notamment sur la manière d'organiser les développements informatiques ou de saisir les données à cette échelle, de coordonner les usages ou de gérer des flux. Les opérations élémentaires restent toutefois essentiellement les mêmes qu'auparavant, sans véritable questionnement sur des changements qualitatifs éventuellement engendrés par des contrôles transformés numériquement[53].

3. L'empilement des systèmes de détection et leurs conséquences sur les pratiques pénales

Les effets secondaires non anticipés sont effectivement multiples. Notamment, certaines questions fondamentales apparaissent sous une nouvelle forme, comme l'impact d'un contrôle et d'une surveillance beaucoup plus systématique, les risques pour les libertés individuelles et la capacité des dispositifs de garantir la sécurité des données et de leur usage dans des processus bien définis et agréés. Dans ce sens, l'absence patente d'une stratégie d'ensemble, le contexte de fuites de données informatisées en tout genre, et la qualité limitée des données qui sont enregistrées[54] inquiètent en fonction des échelles. La nature du SIS II, par rapport aux objectifs initiaux mesurés d'accompagner la mise en œuvre des accords de Schengen, est en train de changer avec la taille du dispositif qui tend à assimiler des problématiques liées au terrorisme, au crime organisé et à l'immigration[55].

53 PIAZZA.
54 BELLANOVA/GLOUFTSIOS.
55 PIAZZA.

Le SIS II a aussi évidemment des conséquences pragmatiques sur les pratiques pénales. Il produit des correspondances dont il faut s'occuper. Elles ne sont, par ailleurs, pas toujours pertinentes (faux résultats positifs). Elles peuvent demander, en bout de chaîne, de générer une action inutile des ministères publics tout en imposant des conséquences désagréables aux intéressés. Bien sûr, perçu à une échelle cantonale ou fédérale, le flux d'opérations à effectuer n'est pas encore très important et se compte en quelques dizaines actuellement. Il se combine toutefois avec d'autres mécanismes de détection qui exigent, eux aussi, sur des bases analogues, d'effectuer des opérations et de prendre des décisions. On n'a pas le choix, il faut y répondre. Cette obligation réduit inévitablement la capacité proactive des organes pénaux. Rien ne semble analysé quant aux avantages de cette détection par rapport à son coût. Des illustrations saillantes suffisent pour convaincre. Quant à la surcharge engendrée, elle semble pour l'instant s'absorber par un travail quotidien dans lequel on se sent débordé d'une manière persistante, sans véritable questionnement stratégique.

Le SIS II n'est qu'un exemple parmi les systèmes de détection de toutes sortes qui se multiplient dans nos environnements numériques :

– les infrastructures sont complétées aux frontières par des accès aux banques de données d'Interpol, démultipliant encore la quantité de requêtes réalisées systématiquement (p. ex. la banque de données de documents de voyage et d'identité SLTD[56] avec 1,7 milliard de requêtes en 2021 pour 146'000 signalements positifs[57]) ;
– le mécanisme prévu d'annonce par les intermédiaires financiers de transactions douteuses génère de nouvelles affaires sur les bureaux des ministères publics déjà débordés par les cas, souvent de grandes dimensions, à traiter[58] ;
– les signalements NCMEC[59] de contenus illicites détectés sur Internet, qui proviennent des mécanismes d'annonces aux États-Unis, produisent pour les ministères publics des dizaines de dossiers, de pertinence variable, accompagnés d'abondantes données, dont il faut s'occuper nécessairement[60] ;
– le perfectionnement des banques de données de traces et empreintes papillaires (banques de données appelées AFIS, *Automatic Fingerprint Identification Systems*) change la nature des relations entre l'homme et la

56 Stolen and Lost Travel Document database.

57 Disponible sous : <https://www.interpol.int/fr/Notre-action/Bases-de-donnees/Base-de-donnees-SLTD-documents-de-voyage-et-d-identite> (*consulté le 10.10.2023*).

58 CHAUDIEU.

59 National Center for Missing & Exploited Children, disponible sous : <https://www.missingkids.org> (*consulté le 18 septembre 2023*).

60 En 2020, après un filtrage opéré par fedpol, c'est 1166 signalements qui ont été transmis aux autorités de poursuite cantonale. Voir : Interpellation de Mme la conseillère nationale FERI, n°21.3263, *« Pédopornographie sur Internet. Nombre et pertinence pénale des signalements à Fedpol »* du 18 mars 2021.

machine dans les processus (p. ex. utiliser des banques de données sans aucune intervention humaine de validation. On appelle ce genre d'utilisation *light off*) ;
– la mise en réseau à l'échelle internationale de ces banques de données (p. ex. ADN et AFIS) augmente le nombre de correspondances dont il faut ensuite s'occuper ;
– toute une panoplie d'autres moyens de détection se déploie partout ; elle porte sur la reconnaissance automatique de substances illicites[61], des plaques d'automobiles et d'autres moyens de contrôler des objets, des véhicules, des endroits ou des personnes, par des caméras installées dans des espaces publics et privés ;
– ces fonctions se projettent dans les espaces virtuels ouverts d'Internet, par toute une variété de moyens d'y détecter et suivre des activités illicites.

La démultiplication de ces sentinelles conduit à changer les échelles de contrôle et de détection. Nous semblons ainsi une fois encore mettre en danger l'hypothèse de KOHR, car la réponse croît en intensité d'une manière clairement non linéaire, peut-être exponentielle.

Ces effets se concrétisent dans les embouteillages produits par le traitement combiné, même parfois (semi-)automatisé, de l'ensemble des dossiers qui s'ensuivent nécessairement : le système pénal, en bout de chaîne, n'est pas dimensionné pour traiter autant de comportements susceptibles d'être qualifiés d'infractions. Par exemple, une étude aux Pays-Bas a montré que la grande majorité des correspondances ADN détectées à l'échelle internationale avec ce pays n'est simplement pas suivie d'opérations judiciaires[62]. Les raisons sont multiples, mais la surcharge chronique des magistrats les encourage certainement, selon leurs prérogatives et leurs critères définis largement individuellement, à élargir les mailles du filtrage. En l'absence de stratégie d'ensemble prenant en compte ces changements d'amplitude, c'est le système qui est acculé à produire des mécanismes de survie toujours plus défensifs. Des pratiques de contournement sont alors inévitables[63]. Une augmentation des ressources allouées sans modifier les modèles traditionnels n'aura sans doute pas d'impact sur ces évolutions, car la réponse en termes de moyens peut difficilement aller au-delà d'une évolution linéaire. L'hypothèse de KOHR n'est donc pas définitivement réfutée par la croissance de ces dispositifs de détection.

61 COPPEY *et al*.
62 TOOM.
63 Voir par exemple CHAUDIEU qui décrit précisément de telles stratégies dans les systèmes de renseignement financiers.

4. La démultiplication des nouvelles traces et des nouveaux moyens d'investigation

Selon un rapport stratégique portant sur Angleterre et le Pays de Galles, environ 90 % de tous les crimes contiendraient maintenant un élément numérique[64]. Mener des investigations comprenant un volet numérique souvent substantiel est devenu un défi majeur pour les autorités de poursuite qui revoient actuellement l'ensemble de leur dispositif. Dans les modalités actuelles, et malgré les investissements réalisés jusqu'ici, il n'est pas possible de collecter et traiter les *Volumes* et la *Variété* des traces pertinentes accessibles enregistrées par une grande diversité d'applications (*Variété*) sur des supports différents, dans des procédures pénales et processus forensiques bien établis et dans une temporalité compatible avec l'évolution des enquêtes (*Vitesse*)[65] . Dans le champ en grande croissance de la science forensique numérique, GARFINKEL[66] avait déjà en 2010 annoncé la crise qui est effective maintenant. Il avait appelé la communauté à porter un regard plus stratégique et proactif.

Face à l'ampleur de ces défis, de gros consortiums financés par l'Union européenne, regroupant des acteurs publics et privés, s'allient pour évaluer toutes les possibilités de développer de nouvelles technologies d'investigation fondées sur l'intelligence artificielle[67]. Il s'agit aussi d'informer les décideurs et de prévoir leur intégration maîtrisée par les autorités de poursuite[68]. L'ampleur frappe à nouveau. Ce sont des consortiums de plus de 50 partenaires qui sont parfois réunis, évaluant un large éventail des potentialités. Cette puissance de développement tend à donner l'idée d'une réponse enfin adaptée, en ordre de grandeur, à la taille de la menace. Toutefois, derrière cette démarche qui relève de la recherche, la question de l'intégration dans des systèmes policiers très traditionnels de ces développements semble très loin d'être résolue : quel doit être le profil de ces enquêteurs ou procureurs d'un nouveau genre qui seront chargés de mettre en œuvre cette variété de technologies ? Comment les processus d'enquête seront-ils transformés ? Quelle doit être l'ampleur du dispositif ? Comment les considérer en regard des droits fondamentaux et de la procédure pénale ?

---

64 National Police Chief Council, Digital Forensic Science Strategy, Rapport, 2020, disponible. sous : <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf> (*consulté le 26.12.2023*).

65 GIBBS VAN BRUNSCHOT *et al.* et WILSON-KOVACS/WILCOX.

66 GARFINKEL.

67 Disponible sous : <https://grace-fct.eu> (*consulté le 10.10.2023*) ; <https://starlight-h2020.eu> (*consulté le 10.10.2023)*.

68 Disponible sous : <https://ap4ai.eu/about> (*consulté le 10.10.2023*).

Ces questions se posent déjà lors de la collecte des traces numériques de toute sorte sur les scènes de crime traditionnellement orientées vers la découverte de traces physiques. Téléphones intelligents (*smartphones)*, caméras et autres objets connectés s'ajoutent à la liste des générateurs de traces potentiellement enregistrées à distance, par exemple dans l'informatique en nuage. Les opportunités d'expliquer ce qui s'est passé par les traces se démultiplient, mais l'approche de la scène de crime se complexifie.

Ces technologies amplifient donc encore l'importance des nouvelles questions relatives à l'encadrement de la collecte et de l'accès à des données personnelles, notamment dans des sources dites ouvertes, ainsi qu'à l'analyse de la menace, à la détection et au suivi d'activités délictueuses par une surveillance qui change encore une fois d'échelles et remettent en cause des équilibres fondamentaux[69] et les perceptions du public, confuses et parfois contradictoires, vis-à-vis des utilisations policières de l'intelligence artificielle[70]. Rechercher sur Internet l'identité d'une personne à partir d'une photographie d'un individu prise sur le vif est devenu techniquement tout à fait possible. Si ce genre de recherches est effectué dans le cadre d'une opération d'observation validée par un tribunal des mesures de contrainte, on pourrait l'admettre comme suffisamment circonscrit et clair dans sa finalité. La délimitation des objectifs et la proportionnalité sont beaucoup moins claires pour d'autres utilisations possibles dans le cadre de systématiques de détection et de surveillance des espaces virtuels de l'Internet[71]. La régulation de l'usage de ces outils doit distinguer ces nouveaux genres de situations réalistes techniquement, afin de trouver les équilibres acceptables. Le manque de formalisation chronique des raisonnements dans l'enquête judiciaire et de respect de la complexité sous-jacente peut alors conduire à des visions trop simplistes qui ratent des distinctions essentielles.

Cela ne s'applique pas seulement à l'administration publique, mais aussi aux structures privées chargées de la cybersécurité et leurs composants de renseignement (*Cyber Threat Intelligence*), de réponses aux incidents (*Incident Response*) ou de détection dans un équilibre nouveau à trouver avec l'État et les autorités de poursuite pénale[72]. Ici, les transformations d'échelles renvoient à nouveau à des approches beaucoup plus inductives qu'auparavant, produisant ainsi des changements qualitatifs profonds (voir section III.B.). Le même genre

69 DUBOIS.

70 EZZEDDINE *et al.*

71 Voir sur l'usage de la reconnaissance de visages par les autorités de poursuite pénale, le cadre proposé par l'*European Data Protection Board*, <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf> *(consulté le 09.03.2024).*

72 KNIEPS *et al*.

d'effet boomerang que le déploiement des technologies d'identification se manifeste ainsi, exigeant de considérer ces questions d'une nouvelle manière.

5. La division du travail

Face à cette situation, une réaction consiste à augmenter timidement les effectifs et redimensionner ainsi les ministères publics ou la police judiciaire. Si cette solution n'est pas sans pertinence et peut soulager à court terme le système, elle ne réfute pas l'hypothèse de la linéarité de KOHR.

L'impasse ne se situe pas uniquement dans la quantité de ressources, mais aussi de leur utilisation. Il faut admettre qu'une attitude très répandue consiste ainsi à tenter de se « débarrasser » du problème par une nouvelle division du travail fondée sur des questions techniques : des unités d'appui centralisées « spécialisées en informatique » feront l'affaire.

Un récent sondage sur l'évolution des métiers policiers en Suisse, adressé aux organisations concernées, confirme ce point de vue, en mettant l'accent sur la spécialisation pour répondre à la complexité croissante des problèmes. Elles ambitionnent, par exemple, d'améliorer le « savoir-faire » informatique[73]. Cette approche qui situe la question sur un plan technique uniquement ne dit pas grand-chose sur les voies à suivre[74]. Il ne suffira pas de dispenser de la formation continue en informatique ou d'engager des techniciens pour répondre aux défis de l'exponentielle. Par ailleurs, de quels genres de techniciens a-t-on besoin ? Parle-t-on de conception d'architectures, de modélisation, de réseaux, de programmation, de composants matériels, d'objets connectés spécifiques, de banques de données, d'applications de téléphones mobiles, de traitement de données de masse, de visualisation, d'intelligence artificielle ? Probablement un peu de tout ça, mais il n'existe pas encore de vision d'ensemble sur les transformations numériques qui aiderait à élaborer des orientations réalistes et stratégiquement pertinentes.

Dans ce flou et cette division préconçue des tâches, les laboratoires ou les unités spécialisées dans une « chose » qui relève de l'informatique deviennent sources de malentendus[75]. Ces structures opérationnelles n'apportent pas ce qui est souvent implicitement attendu : même dans les cas d'homicides, l'accessibilité à l'expertise est rendue souvent impossible. En effet, les structures d'enquête doivent renoncer à tout un pan d'informations numériques, trop volumineuses, prenant trop de temps à être traitées, trop difficiles à

---

73 <https://www.institut-police.ch/fr/bulletins/themen/rapport-danalyse-forte-representativite-du-sondage-sur-lavenir-b1012> (*consulté le 28.12.2023*).

74 LOVEDAY.

75 WILSON-KOVACS/WILCOX.

comprendre, ou trop centralisées dans des structures peu accessibles constituées de spécialistes en informatique éloignés des besoins et contraintes des investigations. Ces organisations sont embouteillées et devenues très bureaucratiques, chères, et prennent peu en considération le cas singulier qui se perd dans des flux de demandes[76]. La solution réside dans les traces existantes, mais elle est rendue inatteignable par les *Volumes* de traces, leur *Variété* et la temporalité pragmatique et codifiée des enquêtes en décalage avec les capacités de traitement des structures où sont regroupés les experts (*Vitesse*). Ce qui frappe dans la gestion de l'accessibilité à la trace numérique est une structuration exagérée des processus fondée sur des modèles compliqués donnant une illusion de maîtrise des flux[77]. La logique ne tient plus : il faudrait savoir ce qu'on cherche *a priori* dans des niveaux de détail fins pour demander le service alors que souvent dans les investigations, les raisonnements basés sur l'information véhiculée par les traces sont beaucoup plus exploratoires : les affaires évoluent avec les connaissances progressivement acquises sur le problème ou dans une logique de découverte abductive et par sérendipité[78]. Face à une complexité pourtant nouvelle, tout semble fait pour sauver les manières de faire antérieures, sans véritable changement de cadres de pensée. Les facteurs de simplification *a priori* choisis pour traiter les flux d'une taille inédite sont réducteurs et empêchent de percevoir les éléments qu'un cas singulier inhabituel apporte à la connaissance de l'évolution de certains phénomènes sériels aux conséquences indirectes ou futures importantes.

Confrontés à ces problèmes d'accessibilité, les praticien.ne.s de la poursuite pénale s'illusionnent alors de pouvoir s'approprier son ou sa spécialiste ou de partager un groupe d'auxiliaires de proximité qui vont leur permettre de continuer de « faire leur travail » en déléguant des questions faussement considérées en tant que détails techniques. La vérité est qu'un tel couplage imaginé par certaines organisations, s'il apporte dans des cas particuliers un confort à certains acteurs, ne fonctionne globalement pas, ni dans une police judiciaire ni dans les ministères publics. Il demanderait une démultiplication irréaliste des moyens sans résoudre le problème plus fondamental de la manière d'intégrer la trace numérique dans la grande majorité des enquêtes.

Cette faiblesse est encore plus visible sur les lieux. Il n'est pas rare, encore aujourd'hui, que des traces numériques assez immédiates (p. ex. même des images) ne soient simplement pas recherchées lors d'interventions. Dans la distribution du travail pensée en silos par spécialités, tout le monde croit que c'est à l'autre de le faire, dans un malentendu persistant, alors que ce mode de pensée devrait être complètement transversal.

76 GIBBS VAN BRUNSCHOT *et al*.
77 WILSON-KOVACS/WILCOX.
78 CATELIN ; BAECHLER *et al*.

De plus, en l'absence de modèles d'organisation justement exprimés, l'intégration de nouveaux personnels pose des problèmes culturels dans les organisations policières[79] et crée des décalages entre leur contribution réelle et celle imaginée par les structures. Par leurs connaissances, certains spécialistes conduisent *de facto* certaines enquêtes numériques, avec une participation souvent passive des personnels habilités. Un décalage entre les rôles attribués par l'organisation et la réalité opérationnelle conduisent inévitablement à de nouveaux problèmes : perte de sens, surcharges, frustrations, tensions hiérarchiques, voire démissions. La concurrence dans le secteur privé finit par décourager les plus engagés. De nouveaux cadres de pensée, des formations innovantes et des modes d'interactions plus équilibrés entre les partenaires dans la résolution collective des problèmes restent à inventer et à exprimer dans nos structures où les professions protégées pourraient se questionner sur les freins éventuels qu'elles imposent aux changements.

V. Les concepts structurants et la transformation des institutions

Les manières de penser traditionnelles ne fonctionnent donc plus dans des univers transformés, une fois que certains seuils ont été dépassés. Comment pouvons-nous aborder ces situations ? Il existe de nombreuses approches, dont certaines émergent de la pratique, c'est-à-dire des solutions *ad hoc* élaborées au fur et à mesure que les problèmes se présentent. L'importance de l'apprentissage par le retour d'expériences est démultipliée dans ce nouveau contexte d'incertitude et de complexité. Malheureusement, trop souvent, la pression pour passer rapidement à la prochaine affaire empêche de prendre du recul. Au-delà, il s'agit de tenter la conception d'un nouveau cadre fondé sur quelques notions clés qui changent la perspective, sachant que sa validité et sa résilience seront déterminées par l'expérimentation et la confrontation à la réalité. Nous proposons deux perspectives, sans ambition d'exhaustivité. La manière dont les institutions se transforment et se redimensionnent donne finalement l'espoir de changements favorables au développement d'approches plus adaptées incorporant les idées avancées.

1. Du modèle d'application de la loi aux méthodes proactives

Nous avons constaté que les systèmes de sécurité ont déjà bien antérieurement dû s'adapter aux ruptures provoquées par des changements

79 WHELAN/HARKIN.

d'échelles. Des solutions ont été pensées et appliquées à des degrés variables dans des contextes d'une mobilité croissante de délinquants sériels. Ces idées ont véritablement émergé dans les pratiques des années 1990 sous des formes variées, par exemple, par la police communautaire, la résolution de problèmes, la détection et l'analyse des points chauds concentrant les désordres dans les villes, ou l'action de sécurité guidée par le renseignement. La mise en œuvre de ces modèles est maintenant relativement étendue[80]. Si leurs origines et objectifs spécifiques sont distincts, ils renferment néanmoins plusieurs points essentiels communs[81]. Ils se distancient notamment tous explicitement du modèle d'application de la loi, entièrement guidé par le droit pénal, fondé sur la réaction à des situations singulières. Face à une criminalité toujours plus sérielle et mobile, il s'agit d'abord de mettre en œuvre les moyens de détecter et de sérier les activités en question afin d'être en mesure d'élaborer des plans d'action qui privilégient la prévention. RATCLIFFE rappelle que la détection de régularités (*patterns*) est indispensable à toute approche proactive : sans connaissance, il est impossible d'aller au-devant des problèmes. Le modèle d'application de la loi est purement réactif, car il n'intervient que lorsqu'un événement relève potentiellement d'une infraction. RATCLIFFE synthétise une bonne partie de ces idées dans sa définition de l'action de sécurité fondée sur le renseignement criminel:

> *« La police fondée sur le renseignement criminel met l'accent sur l'analyse et le renseignement en tant qu'éléments fondamentaux d'un cadre décisionnel objectif qui s'appuie essentiellement sur les points chauds du crime, les victimes répétées, les délinquants prolifiques et les groupes criminels. Elle facilite la réduction de la criminalité et des dommages causés, la perturbation et la prévention par le biais d'une gestion stratégique et tactique du déploiement des moyens et de l'application de la loi. »*[82].

L'idée est donc d'obtenir des leviers de décision plus objectifs par une étude approfondie des répétitions criminelles sous toutes leurs formes (sérialité, concentrations, victimisation répétée) qui fait émerger des schémas sur lesquels une action proactive, préventive ou plus répressive, peut s'appuyer[83]. L'utilisation du terme de renseignement renvoie à ses connotations sulfureuses provenant de ses origines militaires, aux espions de la guerre froide ou à des mécanismes plus contemporains de surveillance intrusive. La rationalité du renseignement criminel dont nous parlons ici est beaucoup plus neutre, car elle consiste pour l'essentiel à comparer des traces ou des modes opératoires (p. ex.

80 WEISBURD/MAJUMUNDAR.
81 KHALFA/HARDYNS.
82 RATCLIFFE, p. 5 ; traduction libre, appuyée par deepl (<https://www.deepl.com>).
83 CUSSON, Répétitions.

comment fonctionne une fraude en ligne ? Peut-on détecter des analogies ou des différences sur des manières de procéder pour la même fraude ? Quelle est l'ampleur de la répétition ?).

Parmi les mesures possibles, les poursuites dans un modèle d'application de la loi n'ont néanmoins pas disparu. Les clés de leur usage approprié ne sont toutefois ni dans des décisions individuelles de triage de dossiers au cas par cas basées sur la gravité pénale ou la charge ressentie du décideur ni par des traitements de flux qui éliminent toute considération du cas particulier. Il s'agit plutôt de développer une capacité de prioriser les voies à suivre d'un point de vue plus stratégique, à partir d'une connaissance approfondie des phénomènes de criminalité en jeu, c'est-à-dire par le renseignement criminel. La structure très concentrée des formes de délinquances numériques indique alors l'importance démultipliée de réaliser des regroupements et ainsi d'approcher des problèmes répétitifs et persistants, davantage que de considérer les situations au niveau atomique du cas individuel. Le procureur ne peut par ailleurs pas contester que, plus ou moins implicitement, l'ampleur d'un phénomène ou la sérialité influence ses décisions. Lorsqu'il est rendu conscient de l'actualité d'une fraude sérielle d'une grande ampleur, il sera prêt à donner davantage de priorité aux affaires concernées. Dans cette utilisation, le renseignement veut ainsi, dans une certaine mesure, expliciter des choix laissés jusqu'ici et dans un contexte transformé, trop implicites, discrétionnaires, et fluctuants entre les acteurs.

La méthodologie PICSEL[84] développée en Suisse romande à l'intention des polices judiciaires a justement la capacité de produire une vision d'ensemble sur ces nouveaux phénomènes numériques de criminalité en suivant directement ce principe de regroupement systématique et d'organisation des répétitions criminelles fondé sur les traces recueillies.

Il est parfois possible de déclencher des enquêtes à partir de ces analyses, surtout lorsque le phénomène détecté reste dans une dimension spatiale limitée, mais ce n'est plus l'objectif principal. La résolution des traces n'est souvent pas visée directement, laissant le traitement sous une forme ainsi pseudonymisée. Les mécanismes judiciaires s'enclenchent parfois dans des situations particulières. C'est dans ce contexte que l'origine de la trace est recherchée. Il est préférentiellement fait appel à une autre notion structurante qui apparaît dans la définition de RATCLIFFE. La « perturbation » (*disruption*) du crime revient à définir des opérations actives visant à désorganiser les systèmes de délinquances en les empêchant de déployer leurs activités, en les rendant plus difficiles et moins intéressantes. Par exemple, le blocage des noms de domaines,

84 Cette méthodologie a été développée dans les polices suisses romandes, en collaboration avec l'École des sciences criminelles de la Faculté de droit, des sciences criminelles et d'administration publique de l'Université de Lausanne. Voir aussi CARTIER (dans cet ouvrage) ou ROSSY.

sans nécessairement déclencher des poursuites pénales, est un mécanisme de perturbation parmi bien d'autres possibles[85].

Bien sûr, ces approches ne sont pas sans défaut. Le renseignement peut être biaisé, comme cela a été relevé notamment lorsque des méthodes dites prédictives (*predictive policing*) ont été frénétiquement implantées[86]. Cette remarque est d'autant plus importante lorsque le renseignement porte directement sur des personnes, par exemple dans les analyses sur les groupes criminels. La détection peut aussi produire des effets de bords indésirables : le retrait de petites annonces, le filtrage de courriels ou toute autre forme de détection peut engendrer des faux positifs aux conséquences plus ou moins désagréables pour les personnes concernées.

La plupart des environnements informatiques sont toutefois protégés selon des principes très semblables. L'identification de la menace, parfois même automatisée, fait partie des standards de la cybersécurité[87]. Elle permet d'orienter un monitoring constant qui est aujourd'hui indispensable pour assurer le simple fonctionnement des installations (voir III.C.). Les poursuites pénales et la police dans ses fonctions judiciaires et de sécurité publique recherchent ainsi des points de connexion à ces approches pour s'adapter à ces évolutions.

2. La trace et la traçologie

Faire « plus de la même chose » ne fonctionne donc plus. Cette attitude met en évidence une faiblesse reconnue de l'enquête judiciaire. Elle est mal exprimée dans des univers opérationnels policiers qui se sont chargés de construire leurs méthodologies d'une manière *ad hoc*, en fonction des situations rencontrées, sans véritable appui académique, voire, selon BRODEUR, comme le reste de la police, en se « dérobant à la recherche »[88]. Les changements d'échelles mettent à jour l'insuffisance théorique qui restait discrète jusque-là. Le positionnement de la trace change radicalement, en exigeant la transparence des logiques relatives à son traitement. La notion de trace change également la focale en permettant une meilleure visibilité dans des espaces aux échelles transformées. La traçologie, ou la science qui étudie la trace[89], donne

85 Ordonnance sur les noms de domaines du 5 novembre 2014 (ODI), RS 784.104.2.
86 SIMMLER *et al.*
87 Voir par exemple <https://www.nist.gov/cyberframework > (*consulté le 9.3.2024*).
88 BRODEUR.
89 RIBAUX, Traçologie. La traçologie est considérée ici comme une évolution de la science forensique. Elle veut donner une unité autour de la notion de trace, à une discipline fragmentée par la prolifération de technologies disparates. Ainsi, au-delà de ses relations au droit pénal, elle s'inscrit dans les enjeux sociétaux plus généraux liés à la traçabilité des activités humaines.

ainsi des pistes pour exprimer l'articulation entre les technologies, les sciences, l'enquête, le renseignement et le droit[90]. Cette qualité de pivot permet par exemple de discuter transversalement le basculement progressif vers une logique plus inductive relative aux données massives.

Une telle rencontre interdisciplinaire autour de la trace est caractérisée par de multiples difficultés pratiques : il n'est pas évident de dialoguer avec des scientifiques concentrés sur leurs méthodes et leurs technologies. L'interdisciplinarité ne se décrète pas. L'échange ne fonctionne souvent pas, car il est fondé sur une tension récurrente, qu'on pourrait même appeler le « malentendu de l'interdisciplinarité ». En effet, lorsque les professions judiciaires s'associent directement à des milieux informatiques, les points de vue respectifs des interlocuteurs se présentent trop souvent tête-bêche : les uns voient la solution technique à leurs problèmes (professions judiciaires), alors que les autres perçoivent un domaine d'application de leurs modèles (informatique). Pour assurer les conditions nécessaires à une collaboration équilibrée fondée sur la confiance et la réciprocité, il s'agit de se pencher sur des objets et problèmes communs, puis de puiser et filtrer dans les connaissances offertes selon chaque point de vue les éléments essentiels, pour les combiner et faire émerger une nouvelle approche ou une solution.

La traçologie et la science forensique veulent donner de la structure à cet espace de traduction[91]. En tant que résultat d'une activité qui a eu lieu dans le passé, la trace présente une multitude de caractéristiques fondamentales pour penser les strates dans lesquelles elle est à rechercher et à interpréter en fonction d'un problème particulier. Ces strates s'empilent à partir d'un niveau physique (p. ex. le disque dur endommagé), jusqu'au message électronique enregistré sur ce même support qui contient des informations sur des entités pertinentes et leurs relations dans les circonstances d'une affaire. La recherche de la trace et la recomposition de l'information demandent alors de prendre une multitude de décisions laissées trop souvent implicites, puis un immense travail de traduction et d'interprétation en traversant les échelles et les niveaux qui n'appartiennent *a priori* totalement ni aux divers champs de l'informatique ni aux autorités de poursuite pénale. Il existe bien un champ forensique et traçologique intermédiaire partagé, fondé sur une compréhension de la trace, de l'information qu'elle véhicule et de son potentiel à devenir une preuve lorsqu'un verdict doit être prononcé par les acteurs habilités. Ce champ devient toujours plus vaste et se situe au centre de ces enjeux, car la trace renvoie également aux méthodes proactives en reflétant et reliant les activités criminelles à considérer. Elle sert ainsi de socle au renseignement criminel et à l'étude du crime en général. Plus fondamentalement, elle s'associe à la fameuse abduction de PEIRCE (la

90 RIBAUX, Traçologie.
91 RIBAUX, Traçologie.

recherche de l'explication à la trace), avec ses liens à la sérendipité. Il s'agit du couple entre la détection de quelque chose d'anormal et la sagacité nécessaire à son interprétation, à la source de la découverte scientifique[92]. La trace devient ainsi un véritable enjeu de société.

3. L'évolution des institutions

Les cadres scientifiques et méthodologiques, ainsi que les solutions technologiques sont exploitables pour répondre aux défis soulevés par le développement exponentiel du numérique. Il reste à ce que les institutions, notamment judiciaires et policières, soient en mesure de les mettre en œuvre.

Des changements sont substantiels dans quelques réformes d'envergure. Nous considérons ici celles qui portent sur les systèmes de sécurité et qui concernent la police judiciaire. Les développements articulés autour des questions numériques sont par exemple conséquents à l'échelle d'organisations comme Interpol et Europol. En France, la capacité de formation pour alimenter le réseau de spécialistes de la gendarmerie nationale[93] a déjà doublé en très peu de temps, dans des perspectives d'élargissement. En Suisse, les polices cantonales disposent maintenant de structures judiciaires spécialisées de taille semblable à celles de la police scientifique, alors qu'elles n'existaient que dans des formes très embryonnaires il y a moins de quinze ans.

Bien qu'*a priori* spectaculaire, ce genre de transformations n'est pas en relation avec la taille des problèmes. Créer des unités ou engager du personnel spécialisé dans la magistrature ou la police ne suffit pas. Il devient impératif de bousculer courageusement les cadres prédéfinis, souvent rigidifiés par leur histoire et par l'attitude défensive des métiers protégés. Dans ces conditions, il est intéressant de constater à l'inverse une certaine force de réaction internationale et dans certains pays. En France, la gendarmerie a créé en 2021 une entité de commandement destinée au cyberespace[94]. Cette structure transversale vise à accompagner les citoyens dans leur vie numérique, en traitant tant de sécurité publique et de prévention que de questions judiciaires. Elle dépasse donc les divisions séculaires des rôles de la police traditionnelle. Elle s'inscrit également dans la réarticulation de la police et des structures pénales avec les acteurs de la cybersécurité. Cette entité fait partie du « Campus Cyber » français inauguré en février 2023, situé à la Défense (Paris), décidé à un niveau politique élevé[95]. Ce projet concentre sur un seul site les principaux acteurs de la

92 CATELIN.
93 Cybergend, structure créée dans les années 90.
94 ComCyberGend.
95 Disponible sous : <https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/inauguration-du-campus-cyber-a-la-defense> (*consulté le 4.1.2023*).

cybersécurité, privés, associatifs, académiques et publics, afin de créer des synergies tant opérationnelles qu'en matière de recherche ou de formation. En Suisse, le terreau vaudois semble également suffisamment fertile pour de tels développements, à l'image de plusieurs structures en matière de cybersécurité qui se coordonnent entre l'industrie et les Hautes Écoles. Parmi d'autres, le nouvel office central de la cybersécurité fait aussi partie des nouvelles structures, porteuses de transversalité et d'une reconfiguration des connexions entre les institutions publiques et privées concernées, ainsi que le public. Comme souvent, la vision en cybersécurité peine à intégrer directement les questions judiciaires et pénales. Quoi qu'il en soit, ces modifications de structures doivent s'accompagner d'une reconstruction des méthodologies. Cette étape manque souvent, car elle est masquée par le foisonnement de technologies qui émergent et attirent toute l'attention. Les structures académiques devraient ainsi aider prioritairement à donner de la substance et une certaine durabilité à ces nouvelles structures en aidant à exprimer les notions clés et les principes fondamentaux stables liés à la trace, à l'expertise scientifique, aux investigations numériques, au renseignement criminel et aux liens à tisser avec les approches de la cybersécurité. À part pour quelques exceptions notables[96], ces changements de cadre de pensée n'ont pas encore eu lieu.

Au-delà des nouvelles structures alimentées jusqu'ici souvent par des formations techniques spécialisées, la construction d'une culture numérique transversale à la police et dans la justice reste indispensable. Elle relève par exemple de l'école des aspirants de police qui opère ses propres transformations numériques. Elle se prolonge dans les formations de base aux métiers policiers. Dans cette perspective, l'ampleur du redimensionnement impressionne aussi en France. Le temps accordé au numérique dans la formation initiale de l'ensemble des recrues sera démultiplié en gendarmerie. L'objectif, à terme, serait de multiplier par cinq le temps consacré aux outils et problématiques numériques, pour atteindre 25 % du temps total de formations[97]. Cet objectif est très supérieur, en ordre de grandeur, à ce qui est prévu en Suisse dans ses écoles d'aspirants de police[98]. L'intégration du personnel civil dans les polices est une autre évolution patente. La police nationale en Suède a modifié profondément la structure de ses engagements. Un peu moins d'un tiers de ses effectifs en

96 Voir à ce titre les recherches et formations de maîtrise à l'École des sciences criminelles de l'Université de Lausanne articulées autour de ces questions, disponible sous : <https://www.unil.ch/esc> (*consulté le 4.1.2024*).

97 Disponible sous : <https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/clap-de-fin-pour-les-eleves-de-la-toute-premiere-e-promotion-de-l-ecole-de-gendarmerie-de-chaumont> (*consulté le 4.1.2024*).

98 Voir le plan de formation policière suisse, disponible sous : <https://www.edupolice.ch/fr/formation-policiere/PLAN-DE-FORMATION-POLICIÈRE-(PFP)> (*consulté le 4.1.2024*).

police judiciaire a maintenant un statut d'employé civil aux habilitations quasi identique à celles des policiers engagés dans les mêmes tâches[99].

VI. Conclusion

Les transformations numériques exponentielles de toute sorte ont provoqué des changements d'état de nos systèmes. Nous avons remarqué que lorsque l'échelle de la réponse évolue sans que les cadres de pensée suivent, des seuils critiques sont aussi franchis. Cela entraîne des effets secondaires indésirables largement imprévisibles, souvent liés aux droits fondamentaux et à la nécessité de trouver de nouveaux équilibres. Les organisations habilitées apportent également de nouveaux dysfonctionnements en grossissant (p. ex. bureaucratie, vision en silos concentrée sur les moyens plus que sur les fins, perte de sens).

L'hypothèse de KOHR a le mérite de poser une question pertinente et d'interpeller frontalement nos dispositifs. Elle doit toutefois être interprétée à différents niveaux, selon la variété des organismes examinés, de leurs relations et de leur capacité d'autorégulation. Nous oublions parfois que la criminalité n'a aucune raison de se conformer à la bonne conceptualisation de nos organisations. Nous avons plutôt des systèmes en interaction qui doivent se réguler dans des environnements évolutifs complexes. Vus ainsi, nous nous apercevons que les systèmes de délinquance, bien que souvent flexibles et robustes, font également face à une expansion générant de nombreuses erreurs que les autorités doivent être en mesure de détecter.

Quelques notions clés ont été proposées pour réadapter les perspectives et la focale. L'idée de l'exponentielle et le repère des 5 V clarifient le diagnostic. Les modèles proactifs aident à penser l'enquête comme un moyen dans une finalité sécuritaire mieux exprimée. La traçologie fonctionne comme une charnière entre la science et la justice, en identifiant les enjeux et exprimant les logiques de l'enquête judiciaire laissées trop longtemps implicites.

La vision de KOHR nous incite finalement à nous intéresser à une autre de ses affirmations, assez ancienne :

> *« Il n'y a pas de diplôme ou de formation, d'études universitaires ou d'organisation qui soient à même de combler l'écart croissant entre les problèmes de taille et nos efforts pour nous mettre à niveau. »*[100]

[99] RANTATALO/LINDBERG/HAAKE.
[100] KOHR, cité par REY, p. 113.

Les formations en matière de cybersécurité prolifèrent, mais délaissent largement les droits fondamentaux des citoyens, les dimensions pénales, d'expertise, d'investigation, et plus criminologiques. Si les polices judiciaires et les ministères publics évoluent, ils restent encore assez timides en fonction de l'ampleur des évolutions. Les efforts numériques qui se déploient dans toutes les facultés de droit en milieux académiques sont aussi considérables. Toutefois, ces développements sont insuffisants, car ils restent eux aussi d'une linéarité décalée. Ils sont restés trop longtemps confinés dans des « spécialités », alors que les changements sont totalement transversaux. L'Université de Lausanne dispose d'un petit avantage par sa configuration regroupant le droit, l'administration publique et les sciences criminelles. Un master conjoint spécifique[101], organisé avec le département des systèmes d'information de la Faculté des HEC, et des projets croisés y sont développés depuis passablement d'années avec succès, mais toujours avec les réticences des cercles disciplinaires tout puissants et de leurs agendas spécifiques. Quitte à dépasser nos compétences selon les disciplines indétrônables, nous avons l'impression qu'un droit plus général qu'on l'imagine réside dans les questions numériques que nous avons abordées. Nous assumons cette ingérence, car tout reste à faire pour que les acteurs prennent humblement, mais sans arrière-pensée le risque d'une sincère interdisciplinarité, seule attitude sensée pour faire face aux effets redoutables de l'exponentielle.

VII. Bibliographie

Chris ANDERSON, The end of theory: The data deluge makes the scientific method obsolete, Wired Magazine, 23 juin 2008 (<https://www.wired.com/2008/06/pb-theory>, *consulté le 5.12.2023*) ; **Simon BAECHLER/Marie MORELATO/Claude ROUX/Pierre MARGOT/Olivier RIBAUX**, Un modèle continu, non linéaire et collaboratif de l'enquête, Criminologie, 53, 2020, p. 43 ss (cité : BAECHLER *et al.*) ; **Jérôme BARLATIER**, Management de l'enquête et ingénierie judiciaire, thèse Lausanne, Lausanne 2017 ; **Ulrich BECK**, La société du risque, Paris 2008 ; **Rocco BELLANOVA/Georgios GLOUFTSIOS**, Controlling the Schengen Information System (SIS II): The infrastructural politics of fragility and maintenance, Geopolitics, vol. 27, 2022, p. 160 ss ; **Émilie BERDOULAT**, La prise de risque dans l'espace routier : l'exemple de la conduite agressive, Le Journal des psychologues, n°360, 2018, p. 30 ss ; **Alphonse BERTILLON**, De l'identification par les signalements anthropométriques, Archives d'anthropologie criminelle et des sciences pénales, 1889, p. 193 ss ; **Dominique BOULLIER**, La sociologie du numérique, 2e éd., Paris 2019 (cité : BOULLIER, Sociologie) ; **Dominique BOULLIER**, Propagations, Un nouveau paradigme pour les sciences sociales, Malakoff 2023 (cité : BOULLIER, Propagations) ; **Jean-Paul BRODEUR**, Les visages de la police, Presses de l'Université de Montréal, Montréal 2003 ; **Sylvie CATELIN**, Sérendipité, Du conte au concept, Paris 2014 ; **Killian CHAUDIEU**, À quoi sert le renseignement financier ? De la trace financière à la « fabrique de la criminalité » en Suisse et au Canada, thèse

[101] <https://www.unil.ch/dcs> (*consulté le 6.1.2024*).

Lausanne/Montréal 2022 ; **Bernard CLAVERIE**, Dynamique exponentielle et naturalité de l'intelligence artificielle, Hermès, La Revue, n°85, 2019, p. 187 ss ; **Florentin COPPEY/Andy BÉCUE/Pierre-Yves SACRÉ/Eric M. ZIEMONS/Philippe HUBERT/Pierre ESSEIVA**, Providing illicit drugs results in five seconds using ultra-portable NIR technology: An opportunity for forensic laboratories to cope with the trend toward the decentralization of forensic capabilities, Forensic Science International, vol. 317, 2020 (cité : COPPEY *et al.*) ; **Maurice CUSSON**, Répétitions criminelles, renseignements et opérations coup-de-poing, Problèmes actuels de science criminelle, n°21, 2008, p. 37 ss (cité : CUSSON, Répétitions) ; **Maurice CUSSON**, L'art de la sécurité, Montréal 2011 (cité : CUSSON, Sécurité) ; **Maurice CUSSON/Guillaume LOUIS**, L'art de l'enquête criminelle, Québec 2019 ; **Joël DE ROSNAY**, Le macroscope, **Jean-Pierre DUBOIS**, Nos droits face aux « big data » : quels enjeux, quels risques, quelles garanties ?, Après-demain, 2016/1, p. 6 ss ; **Yasmine EZZEDDINE/Petra S. BAYERL/Helen GIBSON**, Safety, privacy, or both: evaluating citizens' perspectives around artificial intelligence use by police forces, Policing and Society, 33, 2023, p. 861 ss (cité : EZZEDDINE *et al.*) ; **Markus FELSON/Mary A. ECKERT**, Crime and Everyday life, 6e éd., Thousand Oaks 2018 ; **Alexandre FLÜCKIGER**, Gouverner par des « coups de pouce » (nudges) : instrumentaliser nos biais cognitifs au lieu de légiférer ?, Les cahiers de droit, vol. 59, 2018, p. 199 ss ; **Caroline GALLEY**, La dépendance automobile. Retour sur la genèse du concept et ses enjeux politiques. Entretien avec Gabriel DUPUY, Flux, n°111-112, 2018, p. 104 ss ; **Simson L. GARFINKEL**, Digital forensics research: The next 10 years, Digital Investigation, vol. 7, 2010, p. S64 ss ; **Erin GIBBS VAN BRUNSCHOT/Graham ABELA/Christina WITT/Jonathan W. HAK**, « Poisoned chalice? »: The challenges of forensic science and technology for homicide investigations, Police Practice and Research, 2023, p. 1 ss (cité : GIBBS VAN BRUNSCHOT *et al.*) ; **Herman GOLDSTEIN**, Problem oriented policing, Temple University Press, Philadelphia 1990 ; **Philippe HEBEISEN**, La naissance et la mise en place de la gendarmerie neuchâteloise : d'un corps civil original à l'institution militaire (1809-1850), Crime, Histoire & Société, vol. 14, 2010 ; **Martin HILBERT**, Digital technology and social change: the digital transformation of society from a historical perspective, Dialogues in Clinical Neuroscience, vol. 22, 2020, p. 189 ss ; **Robin KHALFA/Wim HARDYNS**, « Led by Intelligence »: A Scoping Review on the Experimental Evaluation of Intelligence-Led Policing, 2024 ; **Mélanie KNIEPS/Pauline MEYER/Sylvain MÉTILLE/Markus CHRISTEN**, La cybersécurité entre autonomie et soutien étatique, Plaidoyer, 4, 2023, p. 22 ss (cité : KNIEPS *et al.*) ; **Douglas LANEY**, 3D Data Management: Controlling data volume, velocity, and variety, Meta Group Research Note, Rapport technique n°949, 6 février 2001 ; **Barry LOVEDAY**, The shape of things to come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the police service of England and Wales. Policing : A Journal of Policy and Practice, vol. 12, 2018, p. 398 ss ; **Markus S. LUNDSTROM/Muhammad M. ALAM,** Moore's law: The journey ahead, Science, vol. 378, 2022, p. 722 ss **; Carole MCCARTNEY**, Streamlined forensic reporting: Rhetoric and reality, Forensic science international : Synergy, 1, 2019, p. 83 ss ; **Christian MESKEA/Enrico BUNDE/Johannes SCHNEIDER/Martin GERSCH**, Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities, Information Systems Management, vol. 39, 2022, p. 53 ss (cité : MESKEA *et al.*) ; **Vincent MILLIOT/Emanuel BLANCHARD/Vincent DENIS/Arnaud-Dominique HOUTE**, Histoire des polices en France, Des guerres de religion à nos jours, Paris 2020 (cité : MILLIOT *et al.*) ; **James J. NOLAN/Frank CRISPINO/Timothy PARSONS**, Policing in an age of reform. An agenda for research and practice, Cham 2020 ; **Pierre PIAZZA**, Du bertillonnage à l'Europe biométrique, *in :* Identification et surveillance des individus : Quels enjeux pour nos démocraties ?, [en ligne]. Paris 2010 (<https://books.openedition.org/bibpompidou/1217>, *consulté le*

5.12.2023) ; **Oscar RANTATALO/Ola LINDBERG/Ulrike HAAKE,** The Enactment of Professional Boundary Work: A Case Study of Crime Investigation, Professions & Professionalism, vol. 14, 2024, p. e5345 ss ; **Jerry RATCLIFFE**, Intelligence-led policing, Willan, Cullompton 2016 ; **Olivier REY**, Une question de taille, 2e éd., Monaco 2022 ; **Olivier RIBAUX**, Fédéralism and Swiss police reforms, Cahiers Politiestudies, 51, 2019, p. 247 ss (cité : Ribaux, Fédéralisme) ; **Olivier RIBAUX**, De la police scientifique à la traçologie, Le renseignement par la trace, Lausanne 2023 (cité : RIBAUX, Traçologie) ; **Quentin ROSSY/ Olivier RIBAUX**, Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms, European Journal on Criminal Policy and Research 26, 2020, p. 335 ss ; **Claude ROUX/Sheila WILLIS/Céline WEYERMANN**, Shifting forensic science focus from means to purpose: A path forward for the discipline ?, Science & Justice, vol. 61, 2021, p. 678 ss (cité : ROUX *et al.*) ; **Monika SIMMLER/Simone BRUNNER/Kuno SCHEDLER**, Smart criminal justice. – Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege, Université de St-Gall, St-Gall 2020 (cité : SIMMLER *et al.*) ; **Victor TOOM**, Cross-border exchanges and comparison of forensic DNA data in the context of the Prüm decision, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, Rapport, Bruxelles 2008 (<https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604971>, *consulté le 28.12.2023*) ; **David S. WALL**, The internet as a conduit for criminal activity, *in* April PATTAVINA (éd.), Information Technology and the Criminal Justice System, Sage, Thousand Oaks 2005, Chapitre révisé en 2015 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626>, *consulté le 28.12.2023*) ; **David WEISBURD/Maley K. MAJMUNDAR**, Proactive policing. Effects on crime and communities, National Academies of Sciences, USA, 2018 ; **Chad WHELAN/Diarmaid HARKIN**, Civilianising specialist units: Reflections on the policing of cyber-crime, Criminology & Criminal Justice, 21, 2019, p. 529 ss ; **Dana WILSON-KOVACS/Jen WILCOX**, Managing Policing Demand for Digital Forensics through Risk Assessment and Prioritization in England and Wales, Policing: A Journal of Policy and Practice, vol. 17.

Accès transfrontière aux preuves électroniques : l'avenir de l'entraide internationale en matière de cybercriminalité ?

MARIA LUDWICZAK GLASSEY
Dr iur., Professeure
Facultés de droit, Universités de Genève et Neuchâtel

Table des matières

I. Introduction

Si l'on définit la cybercriminalité en fonction non pas du type d'infraction commise (par exemple l'accès indu à un système informatique, art. 143bis CP) ni selon le mode opératoire choisi par l'auteur (par exemple l'utilisation d'un site de rencontres en ligne afin de contacter le potentiel lésé d'une « arnaque aux sentiments » ou *romance scam*[1]), mais en fonction de la nature des preuves qu'il faut/faudra administrer afin d'établir les faits, l'on

[1] À ce propos, voir notamment la page dédiée de l'Office fédéral de la cybersécurité (OFSC), disponible sous : <https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/romance-scam.html> (*consulté le 15.03.2024*).

s'aperçoit que la quasi-totalité de la criminalité actuelle, y compris les infractions du droit pénal classique comme le meurtre ou le vol peut être qualifiée de « cyber ». En effet, qu'il s'agisse de messages, de courriels ou de fichiers, notamment de photographies, d'enregistrements audio ou de vidéos[2], force est de constater qu'il s'agit de moyens de preuve essentiels dans un monde numérique et interconnecté. Ces données numériques sont parfois enregistrées sur des supports locaux, comme un disque dur d'ordinateur. Plus souvent, elles sont (aussi) stockées dans des centres de données, éventuellement sur un *Cloud* (informatique en nuage). Elles se caractérisent alors par une accessibilité en tout temps et à distance, sans l'accord de, ni l'information à, la personne concernée. Par ailleurs, cette accessibilité peut les rendre éphémères : elles peuvent être créées, consultées, modifiées, voire supprimées.

Se pose la question de l'accès à ces preuves électroniques pour les besoins d'une procédure pénale. En l'absence d'élément d'extranéité, cette question relève du droit de la procédure pénale classique. Il n'est toutefois pas rare que le lieu de stockage se trouve dans un État autre que celui qui conduit la procédure pénale. Dans ce cas, l'on doit se demander si la voie de l'entraide judiciaire internationale en matière pénale, traditionnellement suivie s'agissant de preuves « classiques », doit être suivie ou s'il se justifie, au vu de la nature particulière des preuves électroniques, de prévoir une voie plus efficiente parce que, notamment, moins chronophage (*infra* II). Afin de répondre à cette question, l'on s'intéressera dans cette contribution aux modèles mis en place unilatéralement par les États-Unis d'Amérique, d'une part, et entre les États membres de l'Union européenne, d'autre part (*infra* III) avant de s'interroger sur la situation en Suisse et les perspectives qui s'offrent à notre État (*infra* IV).

II. Preuves électroniques et entraide internationale : une inadéquation manifeste

A. Preuves électroniques : de quoi parle-t-on ?

Par les termes « preuves électroniques », nous entendons les données sauvegardées sur un support à distance, donc une donnée présentant un format numérique. Ces données peuvent être de trois sortes : on parlera de données relatives aux abonnés, de données relatives au trafic ou de données de contenu. Les données relatives aux abonnés permettent d'identifier une personne. Il peut s'agir par exemple d'un nom, d'un numéro de téléphone ou d'une adresse de l'abonné au service informatique. En d'autres termes, l'obtention de ces

[2] Sont en revanche exclues de la présente contribution les données bancaires, qui font l'objet de réglementations spécifiques. À ce propos, voir LASSALLE, p. 191 ss.

données permet de répondre à la question « qui » est concerné par les données en cause, qu'il s'agisse de l'auteur de l'infraction ou d'une personne autrement impliquée dans les faits commis. Les données relatives au trafic sont des données caractérisant le contenu : elles permettent de comprendre « comment » les données ont été générées. En particulier, il s'agira de déterminer quelle est la nature de la connexion utilisée, combien de temps celle-ci a duré, avec qui l'abonné a communiqué. On parle à ce titre également de données accessoires ou secondaires, ou de métadonnées. Finalement, les données de contenu sont l'information elle-même (« quoi ») : le texte du message ou de l'*email*, la vidéo, l'enregistrement audio, la photographie.

Les données peuvent être interceptées au moment où elles sont générées ; nous avons toutefois exclu volontairement cette forme d'interception de la présente contribution[3]. Elles peuvent aussi, et c'est plus fréquemment le cas, être obtenues *a posteriori* auprès des fournisseurs informatiques alors qu'elles sont déjà stockées.

B. Procédure d'entraide *vs* preuves électroniques

Encadrée par des règles strictes, l'entraide judiciaire internationale en matière pénale dans sa forme classique implique l'interaction de deux États, requérant et requis : les autorités du second exécutent la demande qui leur est adressée par le premier pour les besoins d'une procédure pénale. Toutefois, présenter une demande d'entraide présuppose de savoir à quel État l'adresser, donc de savoir dans quel État se trouvent les éléments nécessaires. Or le lieu d'enregistrement des données électronique est aléatoire et dépend uniquement d'exigences logistiques liées au stockage. Par ailleurs, il n'est pas rare que les données soient fragmentées. Ainsi, l'*email* peut être stocké dans un *data center* localisé dans un État, pendant que la pièce jointe, par exemple le fichier vidéo, sera stockée dans un autre État. Moyennant d'identifier au préalable de quels États il s'agit, il n'est pas exclu de leur adresser des demandes d'entraide en sollicitant une mesure de contrainte, qu'il s'agisse de la perquisition des locaux où se trouvent les *data center* ou l'obtention des données de la part de la personne habilitée à les gérer, vraisemblablement un fournisseur de services les contrôlant, pour autant que le droit de ces États le permette.

[3] Elle est couverte par U.S. CLOUD Act, H.R. 4943, voir notamment Sec. 104 ; en revanche, le système *e-Evidence* exclut expressément l'interception des données de son champ d'application, par. 19 Règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales, JO L 191 du 28 juillet 2023, p. 118-180) (ci-après : Règlement (UE) 2023/1543). En droit suisse, elle se fonde sur les art. 269 ss CPP, voir *infra*.

Cela étant dit, il ne nous semble pas utile, tant cela est évident, de rappeler combien la procédure d'entraide internationale est chronophage. Les mois voire années nécessaires pour obtenir une information s'accordent mal avec le caractère éphémère, déjà mentionné, des données en cause, en particulier le risque que les données de contenu soient modifiées ou supprimées.

L'entraide internationale dans sa forme classique, attachée à la souveraineté des États, ne constituant pas une solution efficace à la problématique posée par les preuves électroniques, se pose la question pour les autorités pénales de la possibilité d'un accès simplifié, à distance, n'impliquant pas les autorités de l'État de localisation des données, voire n'impliquant pas la détermination de ce lieu. Doit alors être envisagée l'opportunité de renoncer au critère de la localisation physique des données au profit d'autres critères plus pertinents.

III. État des lieux à l'étranger

Deux systèmes vont être présentés ci-après, à savoir la solution adoptée unilatéralement par les États-Unis d'Amérique véhiculée par le *U.S. Clarifying Lawful Overseas Use of Data* (abrégé *CLOUD*) *Act* de 2018 (*infra* A) ainsi que le système *e-Evidence* mis en place en juillet 2023 entre les États membres de l'Union européenne (*infra* B). Ces exposés ne se veulent pas exhaustifs, mais visent à donner au lecteur un aperçu des solutions en vigueur à l'étranger, dans le but de poser les bases des réflexions menées en fin de la présente contribution (*infra* IV)[4].

A. Aux États-Unis d'Amérique : *U.S. CLOUD Act*

La communication des données par les fournisseurs informatiques aux autorités pénales des États-Unis d'Amérique se fondait jusqu'à récemment sur le *Stored Communications Act*[5] adopté dans les années 80 du siècle passé. En adéquation avec les besoins au moment de son adoption, cette loi ne traitait pas de la question des données électroniques stockées physiquement à l'étranger. Les autorités pénales américaines obtenaient lesdites données de la part des fournisseurs informatiques américains sans qu'ils ne manifestent de réticences.

Ce n'est qu'en 2016 que *Microsoft* a refusé pour la première fois de fournir des données numériques, en l'occurrence des *emails*, à une autorité de poursuite

4 Pour approfondir, voir (en général) BIASIOTTI *et al.*, p. 13 ss ; GIACOMETTI, p. 459 ss ; LUDWICZAK GLASSEY ; PFEFFER ; (pour des rapports nationaux) SIEBER/VON ZUR MÜHLEN/TROPINA, Vol. I, p. 127 ss et Vol. II.

5 18 U.S.C., § 2701 ss.

américaine qui les sollicitait dans le cadre d'une procédure pénale conduite en matière de stupéfiants. Le motif invoqué pour motiver le refus résidait dans la localisation géographique des données, stockées dans un *data center* en Irlande. *Microsoft* a indiqué ne pas pouvoir fournir lesdites données sans porter atteinte à la souveraineté de cet État et a préconisé à l'autorité requérante de passer par la voie de l'entraide internationale. En 2018, avant que la Cour suprême américaine statue sur la question – le litige ayant occupé diverses instances au préalable, avec des réponses variées[6] – une loi venant compléter le *Stored Communications Act* a été adoptée : le *U.S. CLOUD Act*[7].

Le système mis en place repose sur deux principes essentiels. D'une part, la localisation physique des données électroniques, *i.e.* leur lieu de stockage – qu'il soit aux États-Unis ou à l'étranger, n'est pas pertinent (*U.S. CLOUD Act*, Sec. 103). D'autre part, tout fournisseur présent sur sol américain a l'obligation de fournir les données dont il dispose lorsqu'elles sont requises par une autorité de poursuite pénale américaine (*U.S. CLOUD Act*, Sec. 103). En d'autres termes, le critère de rattachement de la localisation physique des données est remplacé par celui, volontairement vague et large, de la présence du fournisseur de services sur sol américain. Par la notion de présence, l'on entend le siège, une filiale mais aussi toute autre forme de présence aux États-Unis. Sont visés les services fournis sur sol américain, l'activité économique qui y est déployée[8]. Les données concernées ne doivent pas nécessairement être contrôlées par le fournisseur de services lui-même : il peut en particulier s'agir d'une filiale sise à l'étranger. Tel est le cas indépendamment du fait de savoir si la maison-mère a ou non accès aux données[9].

L'obligation de remise des données n'est pas limitée à un certain degré de gravité des faits (en particulier la notion de *serious crime*, mentionnée en préambule du *CLOUD Act* [*U.S. CLOUD Act*, Sec. 101] ne semble pas être pertinente dans ce cas de figure[10]), ni à la nature des données (*i.e.* qu'elles soient relatives aux abonnés ou au trafic ou encore de contenu). Les données doivent être remises sur présentation, par l'autorité de poursuite, d'un *warrant*, délivré par

---

6 District Court for the Southern District of New York, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) ; Second Circuit Court of Appeals, 829 F.3d 197 (2d Cir. 2016).

7 18 U.S.C., § 2701 ss. Contrairement à ce que pourrait impliquer son intitulé, cette loi ne s'applique pas exclusivement aux données stockées sur un *Cloud*.

8 À ce propos, voir U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 8 et 17. Voir aussi notamment MIGNON, p. 111 et 113.

9 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 16-17.

10 Cette notion n'est toutefois pas définie dans le *U.S. CLOUD Act* ; le critère trouve application uniquement en lien avec un *Executive Agreement*. *U.S. CLOUD Act*, Sec. 105. *Contra* FISCHER/PITTET.

une autorité judiciaire américaine, qui se fonde sur la *probable cause*, *i.e.* en substance le fait que les données sont la preuve de la commission d'un crime[11]. Le fournisseur ne peut contester l'ordre de transmettre les données que dans un seul cas de figure, lié à l'existence d'un *Executive Agreement* et pour autant que la personne concernée par les données ne soit pas une *U.S. person*[12] ni ne réside sur le territoire des États-Unis (*U.S. CLOUD Act*, Sec. 103). L'exception a ainsi une portée très limitée. Cette exception ne vise pas à protéger la personne concernée par les données à remettre, mais éviter au fournisseur de service de se voir imposer des exigences contradictoires, *i.e.* l'obligation de remettre les données imposée par le *U.S. CLOUD Act* d'une part et, d'autre part, la potentielle interdiction de le faire, imposée par le droit de l'État où se trouvent les données, notamment en raison de normes applicables à la protection des données personnelles, tel par exemple le Règlement général sur la protection des données (RGPD[13]) au sein de l'Espace économique européen.

En tant que de très nombreux fournisseurs de services informatiques, en particulier les géants du *web*, ont leur siège aux États-Unis et que, pour le surplus, la notion de présence sur sol américain comprise généreusement[14] est susceptible d'englober les cas de figure restants, les autorités pénales américaines sont désormais assurées de pouvoir obtenir les données électroniques sans avoir recours à l'entraide internationale. Afin d'éviter aux fournisseurs de services d'être astreints à des obligations contradictoires, le processus de conclusion d'*Executive Agreements* est en cours. Les premiers, conclus avec le Royaume-Uni[15] et

11 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 8 et 15.

12 Une *U.S. person* est « *a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States* », *U.S. CLOUD Act,,* Sec. 2523. Sur cette notion, voir MIGNON, p. 109.

13 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119 du 4 mai 2016, p. 1-88. Sur la compatibilité entre les obligations découlant du *U.S. CLOUD Act* et du RGPD, voir notamment Office fédéral de la justice, Rapport sur le US CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 23 ss. Voir aussi EDPB-EDPS, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 juillet 2019.

14 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 17.

15 *Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime*, 3 octobre 2019.

l'Australie[16], sont déjà en vigueur, pendant que d'autres discussions sont en cours, notamment avec le Canada et l'Union européenne[17].

B. Entre les États de l'Union européenne : système *e-Evidence*

En parallèle au système permettant aux autorités américaines d'accéder aux données stockées dans des États étrangers, les États membres de l'Union européenne ont, eux aussi, mis en place une solution venant remplacer les formes préexistantes d'accès transnational aux données électroniques. Celles-ci, variant fortement entre les États membres, rendaient la problématique d'autant plus complexe et urgente à régler. Cette nécessité concernait non seulement les autorités pénales et le besoin d'une administration efficace des preuves afin de faciliter la lutte contre la criminalité, mais aussi les fournisseurs de services qui, bien qu'actifs au sein d'un espace caractérisé avant tout par un marché unique européen, étaient confrontés à des exigences potentiellement divergentes, voire contradictoires dans les différents États membres.

Ainsi, la question de l'accès transfrontière aux preuves électroniques a été réglée dans un Règlement et une Directive *e-Evidence* du 12 juillet 2023[18], dont l'entrée en vigueur est agendée au 18 août 2026. Ce que nous appellerons le « système *e-Evidence* » dans les lignes qui suivent s'articule en deux volets. Le premier volet consiste en la mise en place d'un critère de rattachement uniformisé. Tout comme aux États-Unis, la localisation physique du stockage des données n'a plus d'importance (art. 1 par. 1 Règlement *e-Evidence*), mais le critère choisi est différent : bien qu'il concerne le fournisseur de service, il porte non pas sur sa « nationalité » mais sur la question de savoir si le fournisseur propose des services dans l'espace européen (art. 2 par. 1 Règlement *e-Evidence*). Si tel est le cas, et il s'agit du deuxième volet de la solution mise en place, le fournisseur de services a l'obligation d'indiquer un établissement désigné ou annoncer un représentant légal dans un des États membres de l'Union européenne (art. 3 Directive *e-Evidence*). Ce représentant est l'unique interlocuteur des autorités pénales : il est chargé de répondre aux demandes des autorités pénales de tous les États membres portant sur l'intégralité des preuves

16 *Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime*, 15 décembre 2021.

17 À ce propos, voir BISMUTH, p. 689 ss ; BRIÈRE, p. 502 ss ; MIGNON, p. 115-116.

18 Règlement (UE) 2023/1543 ; Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, JO L 191 du 28 juillet 2023, p. 181-190).

électroniques qu'il stocke ou qui sont stockées pour son compte (art. 3 par. 8 Règlement *e-Evidence*), indépendamment du lieu de stockage.

La fourniture de services dans l'Union européenne consiste dans le fait de permettre aux personnes physiques ou morales dans un État membre d'utiliser les services et avoir un lien substantiel, fondé sur des critères factuels spécifiques, avec cet État membre (art. 3 par. 4 Règlement *e-Evidence)*. Un lien substantiel est réputé exister lorsque le fournisseur de services dispose d'un établissement dans un État membre ou lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou encore lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (art. 3 par. 4 Règlement *e-Evidence*). La notion se définit ainsi de manière large et nombreux seront les fournisseurs de services astreints au système *e-Evidence*, voire rares seront ceux qui ne le seront pas.

Les demandes doivent être adressées directement par l'autorité pénale de l'État membre dit d'émission au représentant du fournisseur de services (art. 7 Règlement *e-Evidence*), au moyen d'un formulaire standardisé, appelé certificat d'injonction européenne de production (*European Production Order Certificate*, EPOC, art. 9 et Annexe I Règlement *e-Evidence*)[19].

Le fournisseur a l'obligation de transmettre toutes les données dont il dispose, les motifs de refus pouvant être invoqués par les autorités de l'État chargé de la mise en œuvre étant très limités (art. 10 Règlement *e-Evidence*). L'obligation porte sur les données relatives aux abonnés et au trafic ainsi que les données de contenu. Toutefois, en tant que les deux derniers types de données sont plus intrusifs, une autorité judiciaire de l'État d'émission doit valider la demande (art. 4 Règlement *e-Evidence*). Le EPOC est alors, en principe, transmis en parallèle à une autorité de l'État de mise en œuvre (art. 8 par. 1 Règlement *e-Evidence*)[20]. De plus, dans ce cas, l'application du mécanisme est limitée à un certain degré de gravité des faits (art. 5 par. 4 Règlement *e-Evidence*).

Le système *e-Evidence* supprime ainsi la nécessité de recourir à l'entraide internationale entre les États membres de l'Union européenne pour obtenir des preuves électroniques et pose des règles de procédure pénale communes[21]. Par ailleurs, au vu de la portée large du critère de rattachement choisi, rares seront les fournisseurs qui ne seront pas soumis au système et donc de fournir directement les données électroniques aux autorités pénales des États membres, y compris s'agissant de données hébergées hors du territoire de l'UE. Dans les (vraisemblablement rares) cas dans lesquels les conditions du système

19 Pour une critique de l'opportunité de procéder par le biais d'un formulaire standardisé, voir CASEY *et al*., p. 43 ss.

20 Voir toutefois les exceptions prévues à l'art. 8 par. 2 Règlement *e-Evidence*.

21 Pour une appréciation critique, voir CHRISTODOULOU *et al.*, p. 423 ss.

e-Evidence ne seraient pas réunies, les autorités pénales des États membres devront (continuer à) procéder par la voie classique de l'entraide internationale.

IV. État des lieux en Suisse

A. Les règles de la procédure pénale et la Convention cybercriminalité

L'accès par les autorités de poursuite pénale suisses aux fournisseurs de services électroniques est régi par le droit de procédure pénale[22]. Le système en place ne prévoit pas d'accès direct, mais désigne le Service Surveillance de la correspondance par poste et télécommunication (Service SCPT, art. 3 al. 1 LSCPT) comme intermédiaire compétent. Sur demande, le Service SCPT est chargé de recueillir les données auprès des fournisseurs puis de les transmettre à l'autorité de poursuite (art. 15 al. 1 LSCPT). Chaque fournisseur est tenu de désigner un service responsable de la surveillance et de la fourniture de renseignements auquel le Service SCPT adressera les demandes (art. 5 al. 1 *cum* 4 al. 1 OME-SCPT)[23]. En principe[24], toute surveillance de la correspondance par télécommunication, qu'elle porte sur des données relatives aux abonnés, au trafic ou au contenu, doit être validée par une autorité judiciaire, à savoir le Tribunal des mesures de contrainte (TMC ; art. 272 al. 1 et 273 al. 2 CPP). La procédure se fait en deux temps : l'autorité de poursuite ordonne la mesure et l'adresse au Service SCPT, puis dispose de 24 heures pour transmettre sa demande au TMC (art. 274 al. 1 CPP), qui statue dans les cinq jours (art. 274 al. 2 CPP) et communique sa décision tant à l'autorité de poursuite qu'au Service SCPT (art. 274 al. 3 CPP). Le fournisseur a l'obligation de transmettre les données requises au Service SCPT (art. 21 ss LSCPT) qui, lui-même, les transmet à l'autorité pénale requérante (art. 17 let. d LSCPT).

S'est posée la question de savoir quelle est la portée (extraterritoriale) des règles suisses de procédure pénale *i.e.,* d'une part, quel fournisseur est astreint à l'obligation de fournir et, d'autre part, quelles sont les données sur lesquelles porte ladite obligation, en particulier lorsqu'elles sont stockées à l'étranger. La jurisprudence a répondu à cette question en ce sens que l'obligation vise le seul fournisseur de services « soumis au droit suisse » et qui « contrôle » les données requises[25]. Le fait d'être soumis au droit suisse concerne notamment les

22 Sur cette notion, voir CR CPP-MÉTILLE, Intro. art. 269-281, N 26 ss.

23 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017 (OME-SCPT), RS 780.117.

24 Par exemple, l'identification des auteurs (22 LSCPT) n'y est pas soumise.

25 ATF 143 IV 21, consid. 3.4 ; TF, arrêt 1B_142/2016 du 16 novembre 2016, consid. 3.6. À ce propos, voir BENHAMOU/OETTLI, p. 214 ss.

sociétés dont le siège se trouve en Suisse et les filiales suisses d'un fournisseur de services étranger[26]. Les données doivent être contrôlées par cette entité, et non par exemple la maison mère (étrangère) de la filiale suisse[27], par quoi il y a lieu d'entendre que l'entité doit disposer d'« *un pouvoir de disposition, en fait et en droit, sur ces données* »[28]. À défaut, l'autorité de poursuite pénale suisse doit procéder par le biais de l'entraide judiciaire internationale en matière pénale. Les possibilités qui s'offrent aux autorités de poursuite suisses en vertu du droit de procédure pénale ne s'écartent ainsi pas, sur le principe, de celles dont disposent les autorités américaines et celles des États membres de l'Union européenne. Toutefois, le critère choisi en droit suisse a pour conséquence pratique que rares sont les fournisseurs qui sont astreints à l'obligation de transmettre les données. En effet, il n'existe que peu de fournisseurs suisses, respectivement peu d'entités soumises au droit suisse contrôlent les données stockées à l'étranger.

Au-delà des règles posées par le CPP, la Suisse applique la Convention sur la cybercriminalité (CCC), à laquelle sont également parties les États-Unis d'Amérique et quasiment tous les États membres de l'Union européenne[29]. La Convention pose des règles de base en matière de procédure pénale (art. 18 ss CCC) et d'entraide internationale (art. 23 ss CCC), qui ne vont toutefois pas au-delà de ce que permet le droit suisse interne. L'exception est l'art. 32 let. b CCC qui permet aux États parties, sans l'autorisation de l'autre État partie, d'« *accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique* ». L'art. 32 let. b CCC prévoit ainsi une possibilité d'accès transfrontière supplémentaire par rapport au CPP : les autorités pénales suisses peuvent accéder à des données stockées situées dans un autre État partie à la CCC, données qui ne seraient par hypothèse pas contrôlées par un fournisseur soumis au droit suisse. Toutefois, le mécanisme repose sur une base volontaire : le fournisseur de service peut, librement, refuser de fournir les données aux

26 Voir l'état de fait de l'ATF 143 IV 21.

27 BENHAMOU/OETTLI, p. 215.

28 ATF 143 IV 21, consid. 3.4 ; TF, arrêt 1B_142/2016 du 16 novembre 2016, consid. 3.6. Pour une discussion relative au critère de la localisation des données vs le pouvoir de contrôle sur les données, voir Jan SPOENLE, *Cloud Computing and cybercrime investigations : Territoriality vs. The power of disposal?, Discussion Paper, Council of Europe, Economic Crime Division, Project on Cybercrime*, 21 août 2010.

29 Convention sur la cybercriminalité du 23 novembre 2001 (CCC), RS 0.311.43. Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques du 12 mai 2022 (STCE n°224), n'a, quant à lui, en l'état pas été ratifié par la Suisse.

autorités de l'État partie[30]. Les demandes adressées par les autorités suisses aux fournisseurs américains sont traitées de la sorte depuis plusieurs années déjà, ce afin de désengorger les autorités exécutant les demandes d'entraide internationale[31]. Pour le surplus, nous ne nous rallions pas à l'avis de GRAF, selon lequel la disposition prévoit un mécanisme violant la souveraineté étrangère. En effet, la solution est prévue par une convention internationale librement ratifiée par les États parties et ne s'applique qu'entre lesdits États[32].

S'agissant du système *e-Evidence*, il ne fait pas partie des acquis de Schengen, ne fait pas l'objet d'un accord bilatéral entre l'UE et la Suisse et ne pourra en l'état être appliqué par la Suisse. Ainsi, les autorités suisses ne pourront s'adresser directement à l'établissement désigné ou au représentant légal dans l'Union européenne. Le système *e-Evidence* ne permet pas non plus à un État non-membre, en l'occurrence la Suisse, d'adresser une demande d'entraide à un État membre qui fera usage de l'EPOC pour l'exécuter (par. 23 des considérants et art. 2 par. 4 Règlement *e-Evidence*). En d'autres termes, le système *e-Evidence* ne permet pas de remplacer les règles applicables en matière de coopération internationale en matière pénale avec les États non-membres de l'Union[33].

B. Perspectives

Face au constat selon lequel les États-Unis d'Amérique et les États de l'Union européenne ont connu des évolutions majeures ces dernières années et que les autorités pénales de ces États ont désormais les moyens d'accéder largement aux preuves électroniques situées à l'étranger, l'on peut se demander quelles sont les perspectives pour la Suisse, dont le droit est bien plus restrictif. Se pose en particulier la question de l'opportunité de la conclusion d'un *Executive Agreement* avec les États-Unis, d'une part, et de négociations avec l'Union européenne, d'autre part.

La première solution, bien qu'elle permettrait aux fournisseurs américains, en application du *U.S. CLOUD Act*, de pouvoir s'opposer à la remise de données aux autorités américaines s'ils venaient à être soumis à des obligations incompatibles découlant du droit suisse (*U.S. CLOUD Act*, Sec. 103), ne permettrait

30 À propos du consentement, en particulier la question de savoir qui est habilité à le donner, voir ATF 141 IV 108, consid. 5.9-5.12, JdT 2015 IV 207 (trad.).

31 *U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act, White Paper*, avril 2019, p. 5.

32 OK CCC-GRAF, art. 32, N 4.

33 Pour une analyse détaillée du droit de la coopération internationale en matière de surveillance des télécommunications, voir TOSZA, p. 270 ss ; WAHL, p. 11 ss.

vraisemblablement pas aux autorités suisses d'avoir un accès plus large aux données que ce qui est pratiqué actuellement[34]. Il faudrait pour cela que l'injonction suisse de produire ait un effet obligatoire pour les fournisseurs américains, ce qui dépendrait des négociations menées par les deux États[35]. De plus, l'*Executive Agreement* ne pourrait probablement concerner que des données relatives à des personnes soumises au droit suisse : là aussi la solution dépendrait des négociations entre les deux États[36]. Par ailleurs, seules des données ne concernant pas une *U.S. person* ou un résident américain pourraient être obtenues par cette voie (*U.S. CLOUD Act*, Sec. 103). Finalement, une telle solution ne serait pas sans poser de problème sous l'angle du droit de la protection des données personnelles.

Quant à l'adhésion de la Suisse au système *e-Evidence*, elle pourrait être très intéressante mais ne nous semble pas réaliste sans un certain nombre d'aménagements. À titre d'exemple, les motifs (résiduels) de refus prévus dans le Règlement *e-Evidence* renvoient à d'autres instruments du droit de l'Union européenne en matière de collecte des preuves notamment, dont le Règlement *e-Evidence* reprend les conditions et les mécanismes. La Suisse ne connait ni n'applique ces instruments, qui ne sont pas compatibles avec notre droit. Plus généralement, le système *e-Evidence* repose sur le principe de la confiance mutuelle, pierre angulaire des rapports entre les États membres de l'Union européenne dans le domaine pénal, principe qui ne s'applique pas dans les relations entre la Suisse et lesdits États[37]. Par ailleurs, l'on peut se demander quel pourrait être l'avantage de l'Union européenne à associer la Suisse à ce système. En tout état de cause, dans la mesure où des discussions sont en cours entre l'Union européenne et les États-Unis, il est, à ce stade, probablement plus judicieux d'attendre leur issue.

Cela étant, une solution pour la Suisse pourrait résider dans l'adaptation du droit de la procédure pénale et plus particulièrement des exigences fixées par la jurisprudence en la matière : si les critères choisis venaient à être adaptés aux réalités et besoins suisses, la voie de l'entraide internationale perdrait du terrain au profit de la procédure pénale et de l'accès unilatéral par les autorités pénales

---

34 En général sur la compatibilité du U.S. *CLOUD Act* avec le droit suisse et l'opportunité pour la Suisse de conclure un *Executive Agreement* avec les États-Unis d'Amérique, voir Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021.

35 Tel n'est par exemple pas le cas dans l'*Executive Agreement* conclu avec le Royaume-Uni. Voir à ce propos Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 24.

36 À propos de l'asymétrie existant dans l'accord avec le Royaume-Uni, voir Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 24.

37 En général sur ce principe, voir les très nombreuses contributions doctrinales, dont la récente thèse de RIZCALLAH.

suisses. Il en serait ainsi en cas de suppression de l'exigence du contrôle sur les données ou du remplacement de la condition de la soumission de l'entité au droit suisse par celle de l'activité déployée en Suisse. De tels modèles, calqués sur le *CLOUD Act* et le système *e-Evidence*, seraient plus intrusifs dans la souveraineté étrangère que celui, plus respectueux, en vigueur en Suisse. Ils auraient aussi pour conséquence d'exiger d'une entité des données qu'elle ne contrôle pas. Ils se profileraient néanmoins dans le sens d'une procédure pénale transnationale, constituant possiblement l'avenir – par l'abandon – de l'entraide internationale en matière pénale.

V. Bibliographie

Lorena BACHMAIER, Mutual Admissibility of Evidence and Electronic Evidence in the EU, A New Try for European Minimum Rules in Criminal Proceedings?, Eucrim 2023 ; **Yaniv BENHAMOU/Jean-René OETTLI**, Traitement des données par les autorités pénales : de l'accès aux données à la procédure de tri, RPS 2021, p. 209 ss ; **Maria Angela BIASIOTTI/Jeanne P. MIFSUD BONNICI/Joe CANNATACI/Frabrizio TURCHI** (éds), Handling and Exchanging Electronic Evidence Across Europe, Cham 2018 ; **Régis BISMUTH**, Le Cloud Act face au projet européen *e-evidence* : confrontation ou coopération ?, Revue critique de droit international privé 2019, p. 681 ss ; **Chloé BRIÈRE**, EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments, European Papers 2021, N°1, p. 493 ss ; **Eoghan CASEY *et al.***, The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form, *in* Maria Angela BIASIOTTI/Jeanne P. MIFSUD BONNICI/Joe CANNATACI/Frabrizio TURCHI (éds), Handling and Exchanging Electronic Evidence Across Europe, Cham 2018, p. 43 ss ; **Hélène CHRISTODOULOU/Laetitia GAURIER/Alice MORNET**, La proposition e-evidence : révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire ?, European Papers 2021, N°1, p. 423 ss (cité : CHRISTODOULOU *et al.*) ; **Philipp FISCHER/Sébastien PITTET**, US CLOUD Act – un aperçu, 8.11.2021 (<www.swissprivacy.law/101>, *consulté le 29.11.2023*) ; **Mona GIACOMETTI**, La récolte transfrontière de preuves électroniques dans le contexte européen, Bruxelles 2023 ; **Damian K. GRAF** (éd.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention), version du 26.10.2023 (<https://onlinekommentar.ch/de/kommentare/ccc32>, *consulté le 29.11.2023*) (cité : OK CCC-AUTEUR/E) ; **Maxime LASSALLE**, L'accès transnational aux données bancaires dans le cadre de l'enquête pénale, Bruxelles 2021 ; **Maria LUDWICZAK GLASSEY**, Preuves électroniques : état de la situation en Suisse face à l'avancée majeure du droit européen, Eucrim 2023, p. 204 ss ; **Yvan JEANNERET/André KUHN/Camille PERRIER DEPEURSINGE** (éds), Commentaire romand CPP, 2e éd., Bâle 2019 (cité : CR CPP-AUTEUR/E) ; **Emmanuelle MIGNON**, The CLOUD Act : Unveiling European Powerlessness, Revue européenne du droit 2020, N°1, p. 108 ss ; **Kristin PFEFFER**, Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln, Aktuelle nationale, europa- und völkerrechtliche Entwicklungen, Eucrim 2023, p. 170 ss ; **Cecilia RIZCALLAH**, The Principle of Mutual Trust in European Union Law, An Essential Principle Facing a Crisis of Values, Bruxelles 2022 ; **Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Thomas WAHL**, Rechtshilfe zur Telekommunikationsüberwachung, Berlin 2021 ; **Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Tatiana TROPINA** (éds), Access to Telecommunication Data in

Criminal Justice, A Comparative Legal Analysis, Vol. 1 et 2, 2e éd., Berlin 2021 ; **Stanislaw TOSZA**, Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies, *in* Vanessa FRANSSEN/Daniel FLORE (éds), Société numérique et droit pénal, Belgique, France, Europe, Bruxelles 2019, p. 269 ss ; **Thomas WAHL**, Grundlagen : Internationale Zusammenarbeit in der Telekommunikationsüberwachung, *in* Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Thomas WAHL (éds), Rechtshilfe zur Telekommunikationsüberwachung, Berlin 2021, p. 11 ss.

Plusieurs approches pour lutter contre la cybercriminalité

SYLVAIN MÉTILLE
Professeur associé, Faculté de droit, des sciences criminelles et d'administration publique, Université de Lausanne
Avocat associé, Étude HDC

PAULINE MEYER
Doctorante FNS, Faculté de droit, des sciences criminelles et d'administration publique, Université de Lausanne

Table des matières

I. Introduction

La cybercriminalité désigne les infractions pénales commises à l'encontre ou au moyen d'un système d'information et de communication. C'est donc le droit pénal qui sert à dissuader de commettre ces infractions et à

sanctionner celles qui ont été commises, dans la mesure où leurs auteurs sont identifiés et les conditions de leur poursuite réunies (II).

En pratique, cette approche unique ne suffit pas à appréhender l'ensemble des enjeux liés aux comportements délictuels dans le cyberespace. En effet, si l'effet dissuasif du droit pénal suffisait à empêcher la réalisation de tout comportement délictuel, aucune infraction n'aurait lieu. Ce serait évidemment très satisfaisant, mais cela ne correspond pas à la réalité du terrain.

Il est important de s'intéresser à l'ensemble des personnes concernées par la réalisation d'une infraction : celles susceptibles de passer à l'acte et les auteurs d'infractions, mais également les potentielles lésées d'actes de cybercriminalité. Ces dernières peuvent aussi agir pour rendre la commission d'infractions plus difficiles ou en réduire le caractère attrayant. Elles diminuent ainsi leur probabilité d'être lésées à titre individuel, mais participent en même temps à un effort collectif de lutte simple et efficace contre la cybercriminalité.

Ce n'est pas le droit pénal qui permet aux victimes de mieux s'armer contre la cybercriminalité, mais la cybersécurité. La cybersécurité contribue à une protection contre la cybercriminalité, en réduisant le risque de faire l'objet d'une attaque réussie (III.B). Comme nous le verrons, certaines lois poussent les organisations à augmenter leur cybersécurité. Les exigences de cybersécurité permettent de diminuer l'attrait que peuvent présenter les personnes physiques et morales pour des délinquants. La cybersécurité permet également de rendre plus difficile la réalisation d'actes de cybercriminalité.

Certains domaines du droit, plus transversaux encore, apportent des considérations de cybersécurité et participent à rendre plus difficile, ou moins intéressante, la commission d'infractions. C'est par exemple le cas de la protection des données personnelles, avec ses obligations de sécurité (III.C).

Finalement, le droit n'étant pas l'unique réponse face à la cybercriminalité, d'autres incitations doivent permettre une augmentation de la cybersécurité au sein de la société, parmi lesquelles en particulier l'éducation et la sensibilisation (III.D).

II. La répression et la prévention générale

Le droit pénal est un mode de contrôle social qui permet à l'État d'incriminer et de pénaliser certains comportements[1]. Il a une fonction réactive et sanctionnatrice, mais également préventive (dans une moindre mesure).

1 HURTADO POZO/GODEL, N 3.

En termes de dissuasion ou de prévention primaire, le droit pénal sert typiquement à la prévention des dangers collectifs, à l'intimidation d'auteurs potentiels et à l'encouragement à toute personne de veiller au respect des normes. Le droit pénal comporte également des dimensions de prévention secondaire et tertiaire, dont font partie la neutralisation des personnes à l'origine d'actes délictuels ou les mesures tendant à diminuer la probabilité de récidive[2].

Le droit pénal est prévu dans le CP[3] et le CPP[4], lois centrales consacrant les infractions applicables à une majorité des actes de cybercriminalité et les compétences des autorités de poursuite pénale[5]. Ce cadre légal produit un effet dissuasif sur la population comme sur les délinquants. La Cyberstratégie (CSN) publiée en 2023 par le Conseil fédéral compte par ailleurs parmi ses objectifs un renforcement des ressources pour la lutte contre la cybercriminalité. Le cadre légal et son application devraient donc encore être renforcés ces années à venir[6].

De nombreux éléments peuvent être utilisés pour expliquer pourquoi le droit pénal n'a pas un effet dissuasif suffisant en matière de cybercriminalité. Premièrement, les auteurs ont souvent un sentiment d'impunité, étant cachés derrière leur ordinateur. Cela est renforcé lorsqu'ils agissent depuis l'étranger, étant très loin de la victime et des autorités de poursuite pénale qui risquent en priorité de s'intéresser à eux[7]. Les difficultés pratiques auxquelles ces autorités font face dans les enquêtes internationales leur donnent également l'impression d'être à l'abri[8]. Même dans le cas d'auteurs présents en Suisse, les efforts mis dans la poursuite des infractions commises en ligne restent souvent inférieurs à ceux concernant des infractions commises dans la vie réelle[9].

Deuxièmement, le gain possible peut être très important. Dans le cas d'escroqueries ou de chantage, les montants demandés ne sont parfois pas très élevés pour les victimes en Suisse[10]. Ils peuvent néanmoins déjà constituer une motivation très intéressante selon le coût de la vie et les revenus possibles dans le pays où se trouve l'auteur[11]. À l'inverse, comme ces montants ne sont pas

2 QUELOZ, p. 7, 11, 13 et 15.
3 Code pénal suisse du 21 décembre 1937 (CP), RS 311.0.
4 Code de procédure pénale suisse du 1er janvier 2011 (CPP), RS 312.0.
5 HURTADO POZO/GODEL, N 10 s.
6 Conseil fédéral, SN, p. 28 à 31.
7 GHERNAOUTI, p. 20.
8 NICOLET/PEISSARD, p. 165 ss.
9 IRL (*in real life*), même si toutes les infractions commises en ligne un évidemment un impact sur la vie réelle des personnes concernées.
10 Cela ne signifie pas pour autant qu'il n'y a pas de cas où les montants demandés sont importants, l'un n'empêchant pas l'autre. Les montants moins importants appellent généralement moins de vigilance et peuvent être commis plus facilement.
11 De plus, la criminalité sérielle permet à ses auteurs de s'enrichir en commettant une série d'infractions portant sur des montants relativement faibles.

toujours très importants en Suisse, ils peuvent décourager les victimes à déposer plainte et à engager une procédure civile ou pénale. Ainsi tant la prévention que la répression s'en trouvent diminuées.

Troisièmement, l'automatisation et la reproductibilité de certaines infractions les rendent aussi très intéressantes. L'auteur peut valoriser beaucoup plus facilement son investissement dans le monde virtuel que dans le cas d'un cambriolage par exemple. Une fois qu'il a développé un logiciel malveillant, il lui suffit de le diffuser[12]. L'effort pour atteindre une ou plusieurs cibles est assez similaire.

Quatrièmement, les auteurs vont souvent s'appuyer sur des erreurs ou incompétences des victimes[13], les rendant parfois honteuses et peu enclines à engager des poursuites pénales. Les victimes ne disposent souvent pas des mesures appropriées pour prévenir des actes de cybercriminalité, alors qu'il est nécessaire qu'elles soient incitées à se prémunir contre des cyberattaques.

Tant que des infractions continuent d'être réalisées quotidiennement avec des conséquences importantes, il faut reconnaître que le droit pénal n'a pas un effet dissuasif suffisant. Il est donc nécessaire d'utiliser d'autres moyens tendant à rendre la commission d'infractions plus difficile, ainsi qu'à diminuer d'une part l'attrait des victimes potentielles et d'autre part la probabilité d'être la cible d'une attaque réussie. Pour ce faire, la cybersécurité doit permettre de renforcer les mesures de protection.

III. La diminution de l'intérêt à commettre des infractions

A. Le principe

Plusieurs moyens existent pour rendre la commission d'une infraction plus compliquée et pour en diminuer l'attrait. Plus le niveau de sécurité est élevé, moins les auteurs seront tentés de commettre des infractions[14]. Un effort plus important sera en effet attendu de leur part, ce qui rend le coût de l'opération plus élevée sans pour autant en augmenter le bénéfice. Les chances de succès de la cyberattaque sont aussi moindres.

Par exemple, plus les individus au sein d'une entreprise sont informés et sensibilisés sur des pratiques de cyberhygiène, moins ils sont susceptibles de tomber dans un piège tendu par un délinquant. De la même manière, la mise en place

12 NCSC, Rapport semestriel 2021/1, p. 15 ; TEICHMANN/GERBER, N 1.
13 NCSC, Rapport semestriel 2022/1, p. 35.
14 Sur la prévention situationnelle, voir MARKWALDER, Internet et facilitation du passage à l'acte, p. 3 .

de correctifs sur des vulnérabilités permet de limiter les risques que des personnes mal intentionnées exploitent ces dernières, pour compromettre des moyens informatiques et altérer les informations qui y sont traitées.

B. La cybersécurité

1. Les objectifs de la cybersécurité

La cybersécurité est étroitement liée à la poursuite pénale de la cybercriminalité. Elle comprend les mesures permettant de prévenir et de gérer les cyberincidents ainsi qu'à améliorer la résilience face aux cybermenaces[15]. Les cyberincidents sont des évènements « *survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement* » (art. 5 lit. d LSI2[16]). Les cyberattaques sont un type particulier de cyberincidents, soit des cyberincidents provoqués intentionnellement[17].

La cybersécurité vise à permettre aux personnes susceptibles de faire l'objet d'un cyberincident de prévenir, détecter et réagir à de tels incidents. Il s'agit de responsabiliser les personnes physiques et morales, pour qu'elles puissent diminuer la probabilité d'être victimes d'actes de cybercriminalité ou d'être utilisées comme vecteur par des délinquants afin de causer du tort à d'autres personnes. En cas d'attaques abouties, la cybersécurité permet aux lésées de rétablir au plus vite une situation sûre.

2. Un cadre légal disparate

Il n'existe pas en Suisse une loi générale sur la cybersécurité applicable à l'ensemble de la population, à l'image du Code pénal. Le cadre légal fonctionne d'une façon radicalement différente. Les bases légales en vigueur ne s'appliquent pas à tout individu, mais à des cercles limités d'assujettis. L'autoréglementation et la réglementation sectorielle sont privilégiées par l'État et le fédéralisme implique une certaine réserve de la Confédération, qui souhaite conserver un rôle partenarial et subsidiaire[18].

---

15 Conseil fédéral, CSN, p. 9.

16 Modification du 29 septembre 2023 de la Loi fédérale sur la sécurité de l'information au sein de la Confédération (FF 2023 2296, LSI2). Lorsque la loi n'est pas modifiée, nous continuons à utiliser l'abréviation LSI.

17 Voir art. 5 lit. e LSI2.

18 Conseil fédéral, CSN, p. 12 et 21.

Certains secteurs élaborent des réglementations (contraignantes et non contraignantes) de cybersécurité. Les actes législatifs adoptés dans ce contexte s'appliquent régulièrement à certaines « infrastructures critiques », soit des organisations essentielles à l'économie nationale, au bien-être de la population ou au fonctionnement de la société[19]. Les infrastructures critiques sont définies à l'art. 5 lit. c LSI[20] comme « *l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population* ». Cette définition très générale renvoie implicitement aux organisations actives dans les secteurs critiques reconnus en Suisse dont les secteurs des autorités, de l'approvisionnement en énergie, des transports ou encore de la santé[21].

Parmi les secteurs réglementés, les autorités et les organisations de la Confédération sont aujourd'hui soumises à la LSI. La LSI doit permettre aux autorités et organisations assujetties de se protéger de la cybercriminalité, de l'empêcher et de remédier à ses conséquences. La LSI adopte une approche globale des mesures techniques et organisationnelles permettant d'une part d'assurer la sécurité de l'information et d'autre part la sécurité des moyens informatiques[22]. Cette loi est en voie de révision pour introduire une obligation de signaler les cyberattaques visant les infrastructures critiques[23], à savoir à un cercle d'organisations plus étendu que celui des autorités et organisations de la Confédération[24].

19 Les sous-secteurs critiques regroupent « *tout système de services ou d'approvisionnement qui englobe l'ensemble d'un processus d'approvisionnement et couvre tous les domaines pertinents pour le fonctionnement du système en question* », voir FF 2023 1659, p. 7. Les secteurs critiques regroupent des domaines tels que la santé, les autorités, les finances ou encore les transports, voir FF 2023 1569, p. 6.

20 Loi fédérale du 1er mai 2022 sur la sécurité de l'information au sein de la Confédération (LSI), RS 128.

21 Il existe neufs secteurs critiques en Suisse : les autorités, l'énergie, l'élimination, les finances, la santé, l'information et la communication, l'alimentation, la sécurité publique et les transports, voir FF 2023 1659, p. 6 s.

22 La LSI distingue la sécurité de l'information et la sécurité des moyens informatiques, HUSI-STÄMPFLI, N 21 ss et 30. Les notions de sécurité de l'information et de sécurité des moyens informatiques se recoupent avec la notion de cybersécurité ; elles impliquent souvent des mesures similaires.

23 Sur la notion d'infrastructure critique, voir FF 2023 1659, p. 7.

24 La révision a été acceptée par les deux chambres du Parlement.

D'autres réglementations sectorielles existent, par exemple pour l'approvisionnement en électricité ou pour d'autres secteurs liés à l'approvisionnement économique du pays[25].

3. La Loi fédérale sur la sécurité de l'information

a) La portée de la loi

La LSI actuellement en vigueur a été adoptée parce que la Confédération a estimé que le cadre légal helvétique pour la sécurité de l'information était lacunaire et manquait de coordination[26]. La LSI visait initialement à assurer une plus grande sécurité des informations traitées par la Confédération et des moyens informatiques exploités pour ce faire (art. 1 al. 1 LSI ; art. 1 al. 1 lit. a LSI2)[27]. Les autorités et organisations de la Confédération traitent en effet beaucoup d'informations, souvent sensibles.

La LSI a fait l'objet d'une révision en 2023 afin d'introduire une nouvelle obligation de signaler les cyberattaques visant les infrastructures critiques[28]. Cette révision, qui n'est pas encore entrée en vigueur, vient soutenir un autre objectif jusque-là sous-jacent de la loi qui est l'amélioration de la capacité de résilience de la Suisse face aux cybermenaces (art. 1 al. 1 lit. b LSI2), par le renforcement des compétences dans le domaine de la cybersécurité et l'introduction de l'obligation de signaler les cyberattaques ciblant les infrastructures critiques[29].

Pour atteindre ses objectifs, la LSI instaure deux approches différenciées entre différents cercles d'assujettis. La première, applicable principalement aux autorités et organisations de la Confédération, dresse un catalogue d'exigences pour garantir la sécurité de l'information et la sécurité des moyens informatiques. La seconde impose à un cercle plus étendu d'autorités et d'organisations une obligation de signaler certaines cyberattaques.

---

25 Voir par exemple *infra* III.B.4 pour l'approvisionnement en électricité. Pour d'autres exemples, voir les normes minimales des différents secteurs de l'approvisionnement économique du pays, disponible sous : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html> (*consulté le 24.2.2024*).

26 FF 2017 2765, p. 2777.

27 DZAMKO-LOCHER, p. 113 s. ; HARASGAMA *et al.*, p. 42 ; HUSI-STÄMPFLI, N 29.

28 FF 2023 2296.

29 FF 2023 84, p. 20 s. ; MEYER/MÉTILLE, N 2.

b) Les exigences de sécurité

Le premier volet d'exigences posé par la LSI date de la première version de la loi et n'a pas été substantiellement modifié lors de la révision. Il impose des obligations aux autorités et organisations de la Confédération pour garantir la sécurité de l'information et la sécurité des moyens informatiques.

Les exigences s'appliquent dans tous les cas à l'Assemblée fédérale, au Conseil fédéral, aux tribunaux de la Confédération, au Ministère public de la Confédération et à son autorité de surveillance ainsi qu'à la Banque Nationale Suisse[30]. Certaines mesures attendues par la loi doivent être mises en place également par des organisations telles que les Services du Parlement, l'administration fédérale, les services administratifs des tribunaux de la Confédération, l'armée et les organisations de l'art. 2 al. 4 LOGA[31] Les cantons sont susceptibles d'être soumis à quelques dispositions de la loi[32].

La LSI adopte une approche fondée sur les besoins de protection et sur les risques[33]. Les exigences figurent aux art. 6 ss LSI et sont concrétisées dans l'OSI[34]. L'approche suivie est majoritairement préventive. En d'autres termes, l'on peut voir que de nombreuses mesures de prévention sont attendues des assujettis, en comparaison avec le nombre de mesures détectives ou réactives prévues par la loi. La LSI et son ordonnance imposent l'implémentation de mesures techniques et organisationnelles à l'instar de l'analyse de risques[35], de la formation des collaborateurs[36], de l'établissement d'un plan pour faire face aux « *graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches indispensables de la Confédération* »[37] ou encore la réalisation d'entraînements en vue de tels incidents[38]. Elle impose également des obligations générales de détection et de réaction aux violations de la sécurité de l'information[39] ou encore la sécurité des moyens informatiques

30 Voir l'art. 2 al. 1 LSI.

31 Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA), RS 172.010. Le Conseil fédéral peut restreindre le champ d'application de la loi aux organisations de l'art. 2 al. 3 et 4 LOGA à celles exerçant des activités sensibles ou recourant et accédant aux moyens informatiques de la Confédération (art. 2 al. 3 LSI).

32 Art. 3 LSI ; FF 2017 2823 à 2825 ; HUSI-STÄMPFLI, N 26 à 28 ; MEYER/MÉTILLE, N 5 à 9.

33 Art. 6 à 8 LSI.

34 Ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI), RS 128.1.

35 Art. 8 al. 1 LSI, 8 al. 1 OSI.

36 Art. 11 OSI.

37 Art. 12 al. 2 LSI.

38 Voir art. 12 al. 2 LSI ; FF 2017 2765, p. 2828 ss ; SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif, p. 13 ss ; ECKERT/GLAUS, p. 12 ; HUSI-STÄMPFLI, N 33 ss ; MEYER/MÉTILLE, N 16 ss.

39 Art. 12 al. 1 LSI.

exploités[40]. Le respect de ces exigences permet aux autorités et organisations assujetties de diminuer la probabilité d'être la cible d'actes de cybercriminalité ou que des délinquants utilisent leurs moyens informatiques ou les informations qu'elles traitent pour porter préjudice à des tiers.

c) L'obligation de signaler les cyberattaques

La modification de la LSI a principalement permis l'introduction de l'obligation de signaler les cyberattaques visant les infrastructures critiques[41]. Cette obligation devrait participer à l'amélioration de la résilience de la Suisse contre les cyberattaques.

L'art. 74*b* LSI liste les exploitants d'infrastructures critiques soumis à l'obligation en limitant les assujettis aux exploitants d'infrastructures critiques les plus importantes sur le plan national[42]. Par exemple, l'approvisionnement en biens d'usage quotidien indispensables (notamment en denrées alimentaires) compte de nombreux opérateurs plus ou moins importants dans la chaîne d'approvisionnement. Seules les organisations dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement sont soumises à l'obligation de signaler les cyberattaques[43].

Les cyberattaques doivent être signalées lorsqu'elles mettent en péril le fonctionnement de l'infrastructure critique concernée, lorsqu'elles entraînent une manipulation ou une fuite d'informations, lorsqu'elles n'ont pas été détectées durant une période prolongée (particulièrement s'il y a des indices supposant qu'elles ont été exécutées en vue de préparer d'autres attaques) ou lorsqu'elles s'accompagnent d'actes de chantage, de menaces ou de contrainte[44].

Le signalement doit être effectué auprès de l'OFCS[45] dans les 24h suivant la détection de la cyberattaque. Il doit contenir des informations relatives

---

40 Art. 19 LSI ; voir notamment FF 2017 2831 ; MEYER/MÉTILLE, N 23 à 25.

41 Voir les art. 74*a* ss LSI2.

42 FF 2023 84, p. 34 ss ; ROESLE, p. 2 ; MEYER/MÉTILLE, N 49 s. Par ailleurs, pour éviter que les cyberattaques ayant un effet limité doivent être signalées, le Conseil fédéral peut exempter les assujetties à l'obligation lorsque les perturbations provoquées par les cyberattaques n'ont qu'un effet limité sur le fonctionnement de l'économie ou sur le bien-être de la population (art. 74*c* LSI2).

43 FF 2023 84, p. 39 s.

44 Voir art. 74*d* LSI2 ; FF 2023 84, p. 43.

45 Office fédéral de la cybersécurité, anciennement Centre national pour la cybersécurité (NCSC), voir SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications, p. 5 s.

notamment à l'entité ciblée, au mode opératoire de l'attaque ou encore aux effets et aux mesures envisagées et prises (art. 74*e* LSI2)[46].

Les signalements de cyberattaques effectués dans le cadre des art. 74*a* ss LSI2 permettent à l'OFCS de disposer d'une vue d'ensemble des cybermenaces[47]. Avec les informations que l'office obtient sur la base des signalements[48], il apporte un soutien technique à certaines autorités, dont celles chargées de la poursuite pénale. Les informations pouvant être transmises concernent l'identité ou le mode opératoire d'auteurs de cyberattaques en vertu de l'art. 76*a* LSI2[49]. L'accès à ces informations aide naturellement les autorités de poursuite pénale à exécuter leurs tâches.

L'obligation de signaler permet d'apporter une plus-value à la protection contre la cybercriminalité également dans la mesure où les exploitants d'infrastructures critiques ont droit au soutien de l'OFCS lorsqu'ils signalent une cyberattaque[50]. Il peut conseiller et soutenir les exploitants d'infrastructures critiques pour que ces derniers puissent limiter les dommages. L'on pourrait même se risquer à espérer que ce soutien passe par des recommandations en vue de prévenir de nouvelles cyberattaques, en tous cas similaires.

4. Les autres instruments réglementaires

La LSI n'est pas l'unique loi régissant des aspects de cybersécurité en Suisse. Certains secteurs se sont pourvus de bases légales pour imposer des exigences de cybersécurité à d'autres cercles de destinataires. À titre d'exemple, les fournisseurs de télécommunication sont maintenant soumis à certaines obligations de sécurité. Les art. 96*a* ss OST[51], concrétisant l'art. 48*a* LTC[52], imposent aux fournisseurs de télécommunication de prendre des mesures de sécurité pour lutter contre toute manipulation non autorisée d'installations de télécommunication. L'art. 96*a* al. 2 OST prévoit par exemple concrètement que les fournisseurs d'accès à Internet doivent lutter par des moyens techniques appropriés contre les attaques de déni de service distribué.

46 FF 2023 84, p. 44 s.
47 Art. 74*a* al. 4 LSI2 ; FF 2023 84, p. 33.
48 L'OFCS acquiert des informations sur la base des signalements obligatoires de cyberattaques comme sur la base des signalements d'autres cybermenaces (art. 73*b* LSI2).
49 FF 2023 84, p. 51.
50 Art. 74 al. 1, 74*a* al. 4 LSI2 ; FF 2023 84, p. 33.
51 Ordonnance du 1er avril 2007 sur les services de télécommunication (OST), RS 784.101.1.
52 Loi du 20 octobre 1997 sur les télécommunications (LTC), RS 784.10.

Un autre exemple est celui du sous-secteur critique de l'approvisionnement en électricité. Un nouvel art. 8*a* LApEl[53] est adopté dans le contexte de la nouvelle obligation de signaler les cyberattaques. Il imposera aux gestionnaires de réseau, aux producteurs et aux agents de stockage de prendre des mesures pour protéger adéquatement leurs installations contre les cybermenaces. Il en va particulièrement de mesures permettant de prévenir et de régler au plus vite les cyberincidents visant les installations concernées[54]. L'art. 8*a* LApEl sera concrétisé dans l'ordonnance, qui rendra contraignante la norme minimale pour la sécurité des TIC de l'OFAE[55].

C. La Loi fédérale sur la protection des données

Certaines réglementations n'ayant pas comme vocation « principale » à appréhender des considérations de cybersécurité présentes néanmoins un lien étroit avec ces dernières Il en va de la sorte pour les lois de protection des données personnelles, dont la LPD[56] au niveau fédéral.

La LPD consacre une importance particulière au principe de la sécurité des données[57]. C'est aussi une obligation pour le responsable du traitement et le sous-traitant de prendre des mesures techniques et organisationnelles pour assurer la sécurité des données (confidentialité, intégrité, disponibilité, traçabilité)[58]. Elles doivent être adaptées au risque pour la personne concernée et en tenant compte des possibilités et du coût des différentes mesures pouvant être mises en place[59].

Le but de la protection des données est d'assurer la protection de la personnalité en lien avec le traitement de ces données. La sécurité des données impose le cadre technique et organisationnel minimal dans lequel peuvent avoir lieu les traitements de données personnelles[60]. En évitant qu'elles ne soient accessibles à des personnes qui ne sont pas censées pouvoir les consulter, les lois de protection des données incitent les responsables du traitement et les sous-traitants

53 Loi du 15 juillet 2007 sur l'approvisionnement en électricité (LApEl), RS 734.7.
54 FF 2023 84, p. 56.
55 Rapport explicatif concernant l'avant-projet relatif à la révision de l'ordonnance sur l'approvisionnement en électricité, p. 1.
56 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), RS 235.1.
57 Voir art. 8 LPD.
58 Voir art. 2 Ordonnance du 31 août 2022 sur la protection des données (OPDo), RS 235.11 ; Ordonnance sur la protection des données (OPDo), Rapport explicatif, p. 23 ; CR LPD-FANTI/STAEGER, art. 8, N 11.
59 Ordonnance sur la protection des données (OPDo), Rapport explicatif, p. 21. Pour plus d'information à ce sujet, voir notamment CR LPD-FANTI/STAEGER, art. 8, N 87 ss ; MEYER/DAVIES, N 16 ss.
60 FF 2017 6565, p. 6650.

à protéger les données des individus. La mise en œuvre du principe de sécurité évite également que des tiers ne puissent les utiliser pour commettre des infractions, notamment des usurpations d'identité.

La LPD a introduit, lors de sa révision totale du 25 septembre 2020, l'obligation d'annoncer certaines violations de la sécurité des données à l'autorité nationale de surveillance (PFPDT) et aux personnes concernées[61]. Les personnes concernées doivent désormais être informées directement lorsque des données les concernant ont été exposées et qu'elles peuvent prendre des mesures utiles à leur protection. C'est notamment le cas si des identifiants et mots de passe ont par exemple été rendus accessibles. Dans une telle situation, les personnes concernées peuvent prendre des mesures pour se protéger en modifiant leurs mots de passe et leurs données d'accès[62]. Ainsi les personnes concernées peuvent prendre, conjointement aux responsables du traitement et aux sous-traitants, des mesures pour rendre la commission d'une infraction plus difficile[63].

La LPD contient également une obligation de protection des données dès la conception[64] et de protection des données par défaut[65]. Ces mesures techniques et organisationnelles ainsi que ces préréglages appropriés participent aussi à limiter les accès indus aux données, et sont donc une pierre à l'édifice de la cybersécurité.

D. L'éducation et la sensibilisation

En matière de cybersécurité, le point faible est tantôt l'infrastructure, tantôt l'être humain. Dans les cas d'attaques par rançongiciel par exemple, l'expérience a montré le plus souvent que soit l'infrastructure n'était pas suffisamment mise à jour (faille *zero day* par exemple) ou que des mesures élémentaires de protection manquaient (absence de double authentification ou mot de passe insuffisant par exemple), soit l'humain était le maillon faible et avait pu être piégé (en lui faisant par exemple croire qu'il était contacté par une autre personne que l'attaquant).

Pour anticiper les situations dans lesquelles l'être humain est exploitable par les délinquants, l'éducation et la sensibilisation sont cruciales. Elles doivent se faire à tous les échelons[66]. Des programmes doivent exister pour sensibiliser la

61 Art. 24 LPD.
62 FF 2017 6565, p. 6682.
63 Pour plus d'informations sur la nouvelle obligation d'annoncer les violations de la sécurité des données, voir CR LPD-MÉTILLE/MEYER, art. 24, N 28 ss.
64 Art. 7 al. 1 et 2 LPD.
65 Art. 7 al. 3 LPD.
66 Au sujet de l'objectif stratégique de la Suisse en la matière, voir Conseil fédéral, CSN, p. 15.

population en général quant aux mesures que tout individu peut mettre en place pour une utilisation sécurisée des moyens informatiques[67]. Les entreprises et les autorités doivent également sensibiliser leurs collaborateurs et peuvent par exemple mener des campagnes internes d'hameçonnage[68]. Il existe par ailleurs certaines exigences légales en rapport avec la formation des collaborateurs[69].

En améliorant la sensibilisation et l'éducation, il serait possible, avec des coûts assez limités, de rendre bien mieux informées les potentielles personnes lésées. Elles pourraient ensuite détecter plus efficacement les cas les plus évidents de cybercriminalité, et ainsi d'éviter de tomber dans un piège[70].

La sensibilisation et l'éducation sont susceptibles de couvrir une multitude de situations. Il ne faut effectivement pas se limiter aux risques financiers ou économiques liés aux cyberattaques pouvant être perpétrées sur les moyens informatiques d'une entreprise. L'éducation et la sensibilisation doivent aussi porter sur des sujets tels que les risques liés à la pornodivulgation, au surpartage parental (*sharenting)*, *etc*.

IV. Conclusion

Le droit pénal et la poursuite de la cybercriminalité sont indéniablement des instruments nécessaires pour la prévention générale de la cybercriminalité et pour la poursuite pénale des auteurs d'infraction. En revanche et comme nous avons pu le voir, le droit pénal ne suffit pas à lui seul pour empêcher la cybercriminalité. D'autres instruments légaux doivent être utilisés pour inciter les personnes susceptibles d'être lésées à mieux se protéger. Une meilleure protection permet de rendre la commission d'infractions plus difficile et moins attrayante pour les auteurs.

Le domaine juridique de la cybersécurité est récent en Suisse et est en plein développement. Certaines lois ont été adoptées ou révisées pour permettre d'inciter certaines organisations à mettre en place des mesures appropriées pour prévenir, détecter les cyberincidents (et donc les cyberattaques) ainsi qu'y réagir correctement. La LSI impose à ce titre un catalogue d'exigences à différents cercles d'assujettis. Alors que les autorités et organisations de la Confédération doivent mettre en place des mesures techniques et organisationnelles permettant d'assurer leur cyberrésilience, un cercle plus important d'infrastructures

67 Voir la campagne S-U-P-E-R du NCSC, disponible sous : <https://www.s-u-p-e-r.ch/fr/> (*consulté le 24.2.2024*).

68 NCSC, Rapport semestriel 2022/II, p. 7.

69 Voir art. 11 OSI qui impose aux unités administratives de la Confédération de former et de sensibiliser leurs collaborateurs à leur entrée en fonction et périodiquement.

70 NCSC, Rapport semestriel 2022/II, p. 7 s.

critiques est soumis à une obligation de signaler les cyberattaques. Des lois sectorielles se développent dans un esprit similaire à celui de la LSI, comme la LApEl qui imposera une obligation aux organisations actives dans l'approvisionnement en électricité d'assurer leur protection contre les cybermenaces.

D'autres lois prévoient des considérations connexes à la cybersécurité, comme la LPD. La sécurité des données personnelles est nécessaire pour qu'un responsable du traitement ou un sous-traitant garantissent la protection de la personnalité et des droits fondamentaux des personnes concernées. Par conséquent, elles doivent mettre en œuvre les mesures techniques et organisationnelles adaptées au besoin de protection de leurs traitements, aux risques et ainsi de suite.

Bien que certaines considérations de cybersécurité disposent d'un réel point d'ancrage dans la loi et que l'on assiste à des avancées législatives, la situation n'est pas totalement satisfaisante. La CSN de 2023 prévoit d'analyser en tout temps où des lacunes persistent et comment les combler, mais toujours selon une approche sectorielle[71]. On pourrait se demander si une autre approche, éventuellement avec des exigences minimales transversales, permettrait au moins aux organisations et infrastructures les plus importantes pour la Suisse d'être mieux protégées face à la cybercriminalité. Dans tous les cas, les efforts législatifs ne doivent pas se limiter au droit pénal.

Cela étant, le droit ne constitue qu'une partie de la réponse au besoin de cybersécurité. Parmi les mesures à prendre pour se protéger des cyberattaques, les infrastructures critiques, les entreprises, la population doivent être sensibilisées et formées. Comme cela, toutes les personnes potentiellement lésées par une infraction peuvent être plus amplement et clairement informées, ce qui leur permet d'éviter de tomber dans des pièges, de détecter des cybermenaces ainsi que de réagir en cas de cyberattaques de façon plus efficace.

V. Bibliographie

Doctrine

Daniel DZAMKO-LOCHER, Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung, L'informatique en nuage, Berne 2022 ; **Martin ECKERT/Noëlle GLAUS**, Das neue Informationssicherheitsgesetz (ISG), RR.COMP 3/2023, p. 12 ; **Rehana C. HARASGAMA/Jan KLEINER/Viviane BERGER**, Cyberangriffe beim Bund – Was gilt es aus rechtlicher Sicht zu beachten ?, Sécurité & Droit 1/2022, p. 40 ss (cité : HARASGAMA *et al.*) ; **José HURTADO POZO/Thierry GODEL**, Droit pénal général, 3e éd., Genève/Zurich/Bâle 2019 ; **Sandra HUSI-STÄMPFLI**, Informationssicherheits- und Datenschutzgesetz : Chance auf ein neues Zeitalter, Jusletter 25 septembre 2023 ; **Philippe MEIER/Sylvain MÉTILLE** (éds), Loi

[71] Conseil fédéral, CSN, p. 21.

fédérale sur la protection des données, Commentaire Romand, Bâle 2023 (cité : CR LPD-AUTEUR/E, art. X, N Y) ; **Pauline MEYER/Ryan DAVIES**, Portée pratique du caractère approprié des mesures de sécurité des données sous la LPD, Jusletter 25 septembre 2023 ; **Pauline MEYER/Sylvain MÉTILLE**, Loi fédérale sur la sécurité de l'information : version 2.0, Jusletter 5 septembre 2022 ; **Yves NICOLET/Jean-Philippe PEISSARD**, Cybercriminalité : difficultés et enjeux de la poursuite pénale, Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Ausburger-Bucheli, p. 103 ss ; **Nicolas QUELOZ**, Droit pénal suisse, partie générale, 2e éd., Genève/Zurich/Bâle 2016 ; **Eugen ROESLE**, Meldung von Data B-reaches, RRCOMP 2/2022, p. 2 ss ; **Fabian TEICHMANN/ Léonard GERBER**, La qualification des attaques DDoS en droit suisse, Jusletter 27 septembre 2021.

Documents officiels

Centre national pour la cybersécurité (NCSC), Rapport semestriel 2021/1 du 2 novembre 2021 (cité: NCSC, Rapport semestriel 2021/1) ; **Centre national pour la cybersécurité (NCSC)**, Rapport semestriel 2022/I du 3 novembre 2022 (cité : NCSC, Rapport semestriel 2022/I) ; **Centre national pour la cybersécurité (NCSC)**, Rapport semestriel 2022/II du 11 mai 2023 (cité : NCSC, Rapport semestriel 2022/II) ; **Conseil fédéral**, Cyberstratégie (CSN), avril 2023 (cité : Conseil fédéral, CSN) ; **Conseil fédéral**, Message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF 2023 84 (cité : FF 2023 84) ; **Conseil fédéral**, Stratégie nationale de protection des infrastructures critiques du 16 juin 2023, Approche globale pour garantir l'approvisionnement en biens et prestations essentiels, FF 2023 1659 ; **Département fédéral de l'environnement, des transports, de l'énergie et de la communication**, Rapport explicatif du 21 septembre 2023 concernant l'avant-projet relatif à la révision de mai 2004 de l'ordonnance sur l'approvisionnement en électricité (protection contre les cybermenaces) (cité : Rapport explicatif concernant l'avant-projet relatif à la révision de l'ordonnance sur l'approvisionnement en électricité) ; **Global Cyber Security Capacity Centre**, Cybersecurity Capacity Review, Switzerland, juin 2020 (cité : Cybersecurity Capacity Review) ; **Office fédéral de la justice**, Ordonnance sur la protection des données (OPDo), Rapport explicatif du 31 août 2022 (cité : Ordonnance sur la protection des données (OPDo), Rapport explicatif) ; **Secrétariat général du DDPS (SG-DDPS)**, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications du 8 novembre 2023 (cité : SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications) ; **Secrétariat général du DDPS**, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif du 24 août 2022 (cité : SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif).