Collection lausannoise
CEDIDAC

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

Lutter contre la cybercriminalité en Suisse

Stämpfli
Éditions

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 1

II. Explications théoriques 2
A. La théorie des brèches 2
B. La théorie des activités routinières 3
C. Approche situationnelle et prévention 3

III. La cybercriminalité en chiffres 4
A. Comment mesurer la criminalité numérique 4
B. Les statistiques officielles 5
1. La définition de la criminalité numérique dans les statistiques officielles 5
2. Le développement et la proportion des délits numériques 6
C. Les sondages de victimisation 8
1. Les sondages sur les cyberdélits en Suisse 8
2. Les résultats du Crime Survey 2022 9

IV. Conclusion 11

V. Bibliographie 12

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.

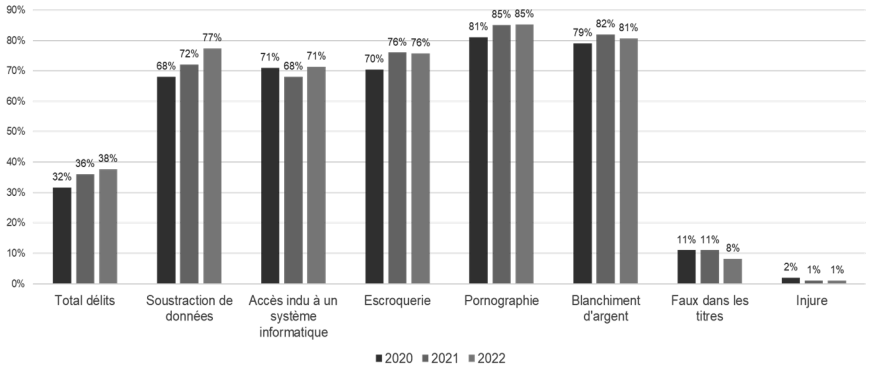
de télécommunication, en particulier Internet »[18]. Un délit est donc classé comme « numérique » si l'auteur a utilisé un *modus operandi* numérique pour agir. L'OFS distingue cinq catégories de délits numériques : (a) la cybercriminalité économique, (b) les cyberdélits sexuels, (c) les cyberatteintes 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

---

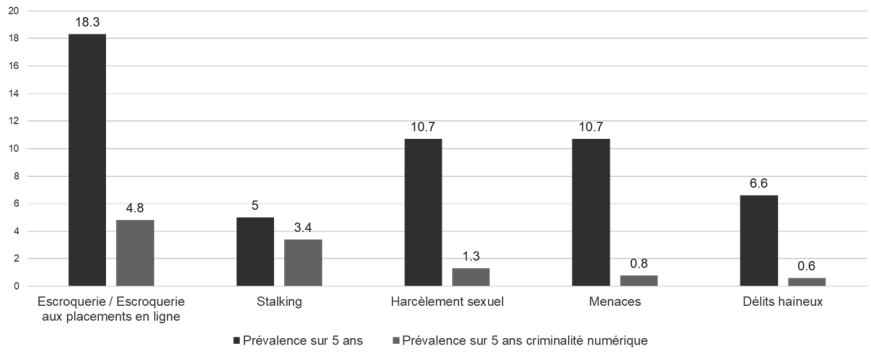
24 MILANI *et al*.
25 Pour plus d'informations sur la méthodologie du *Crime Survey* 2022, voir MARKWALDER *et al.*, Opfererfahrungen, p. 10 ss.
26 MARKWALDER *et al.*, Cybercrime, p. 4 ss.
27 MARKWALDER *et al.*, Cybercrime, p. 7 s.
28 BIBERSTEIN *et al.*, p. 18 s.
29 MARKWALDER *et al.*, Cybercrime,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