Published in Criminalité économique et cybercriminalité: mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli, Helbing Lichtenhahn, 2021, pp. 203-216, which should be cited to refer to this work.

Accès indu à un système informatique, soustraction et détérioration de données : contribution à la résolution de quelques questions interprétatives

Bertrand Perrin*/Romain Roubaty**

* Professeur de droit pénal à l'Université de Fribourg.
** Responsable du Centre d'investigation numérique et de cryptologie (CINC), Neuchâtel (HES-SO // Haute école de Suisse Occidentale, Switzerland).

Bibliographie spéciale

Corboz Bernard, Les infractions en droit suisse, vol. I, 3e éd., Berne 2010 ; Donatsch Andreas, Strafrecht III – Delikte gegen den Einzelnen, 11e éd., Zurich/Genève/Bâle 2018 ; Dupuis Michel/Moreillon Laurent/Piguet Christophe/Berger Séverine/Mazou Miriam/Rodigari Virginie (éd.), Petit Commentaire – Code pénal, 2e éd., Bâle 2017 (PC CP) ; Ghernaouti Solange, Cybersécurité – Analyser les risques – Mettre en œuvre les solutions, 6e éd., Malakoff 2019 ; Hurtado Pozo José, Droit pénal – Partie spéciale – Nouvelle édition refondue et augmentée, Genève/Zurich/Bâle 2009 ; Macaluso Alain/Moreillon Laurent/Queloz Nicolas (éd.), Commentaire romand – Code pénal II (Art. 111-392 CP), Bâle 2017 (CR CP II-Auteur) ; Message du Conseil fédéral 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) du 24 avril 1991, FF 1991 II 933 ; Métille Sylvain/Aeschlimann Joanna, Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ?, RPS 132 (2014) ; Monnier Gilles, art. 143, 143bis, 144bis, *in* Macaluso Alain/Moreillon Laurent/Queloz Nicolas (éd.), Commentaire romand – Code pénal II (Art. 111-392 CP), Bâle 2017 ; Niggli Marcel Alexander/Wiprächtiger Hans, Basler Kommentar – Strafrecht II (Art. 137-392 StGB), 4e éd., Bâle 2018 (BSK StGB II-Auteur) ; Stratenwerth Günter/Jenny Guido/Bommer Felix, Schweizerisches Strafrecht – Besonderer Teil I : Straftaten gegen Individualinteressen, Berne 2010 ; Trechsel Stefan/Crameri Dean, art. 143, *in* Trechsel Stefan/Pieth Mark (éd.), Schweizerisches Strafgesetzbuch – Praxiskommentar, 3e éd., Zurich/St-Gall 2018 ; Trechsel Stefan/Pieth Mark, Schweizerisches Strafgesetzbuch – Praxiskommentar, 3e éd., Zurich/St-Gall 2018 (PK StGB-Auteur) ; Weissenberger Philippe, art. 143, 143bis, 144bis, *in* Niggli Marcel Alexander/Wiprächtiger Hans (éd.), Basler Kommentar – Strafrecht II (Art. 137-392 StGB), 4e éd., Bâle 2018.

I. Introduction

Affirmer que l'informatique occupe aujourd'hui une place centrale dans la vie quotidienne et les échanges économiques est presque devenu un lieu commun. La pandémie, liée à un coronavirus très perturbateur de nos usages sociaux, frappe actuellement le monde. Les communications à distance s'avèrent plus que jamais indispensables pour assurer l'équilibre d'un système fragilisé, ce qui accentue notre dépendance aux instruments numériques.

Comme pour tout outil, l'utilisation de l'ordinateur peut viser des fins constructives ou, au contraire, satisfaire les desseins malveillants des criminels. Les virus, qu'ils soient biologiques ou informatiques, constituent deux fléaux majeurs du XXIe siècle !

Les infractions informatiques au sens strict, c'est-à-dire celles qui impliquent par définition l'utilisation de l'informatique, sont principalement concentrées dans le Titre 2 des dispositions spéciales du Code pénal suisse (CP) qui réprime les infractions contre le patrimoine. Les articles relatifs à la soustraction de données (art. 143 CP), à l'accès indu à un système informatique (art. 143bis CP) et à la détérioration de données (art. 144bis CP) sont entrés en vigueur le 1er janvier 1995 (avec une modification de l'art. 143bis CP datant du 1er janvier 2012). Plus de 25 ans se sont écoulés et diverses questions d'interprétation demeurent. Nous nous proposons de contribuer au débat doctrinal en exposant des solu-

tions qui, selon nous, répondent le mieux à la fois aux exigences de l'interprétation juridique et à la réalité technico-informatique.

L'Institut de lutte contre la criminalité économique, ainsi que sa doyenne depuis les origines, Isabelle Augsburger-Bucheli, à laquelle nous rendons hommage dans ces Mélanges, ont toujours eu pour credo la défense de la pluri- et de l'interdisciplinarité. La criminalité économique et la délinquance informatique, pour être comprises et donc combattues efficacement, impliquent résolument la mise en œuvre de compétences complémentaires issues de plusieurs domaines de connaissance, comme le droit, la criminologie, les sciences économiques ou encore l'informatique. C'est dans cet esprit que nous analyserons quelques éléments constitutifs des trois infractions que nous avons citées, en tentant de conjuguer nos expériences respectives de pénaliste et d'informaticien.

Dans un premier temps, nous procéderons à une synthèse de la typicité des infractions sanctionnées par les art. 143, 143bis et 144bis CP. Puis, nous examinerons quatre notions qui, dans ce contexte, requièrent, selon nous, quelques éclaircissements interprétatifs : la « soustraction » (de données), l'« accès indu » (à un système informatique), l'exigence de protection spéciale (des données ou du système informatique) et le concept de « détérioration » (de données). En guise de conclusion, nous esquisserons une réflexion plus globale sur les enjeux de la lutte contre la cybercriminalité.

II. Les énoncés de fait légaux des trois infractions

A. La soustraction de données (art. 143 CP)

L'art. 143 al. 1 CP prévoit que « celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire ». L'alinéa 2 consacre un cas privilégié lorsque l'infraction est commise contre des « proches » ou des « familiers »[1].

Dans le monde « virtuel » ou « dématérialisé », la soustraction de données se rapproche du vol dans l'univers « physique » ou « matériel ». L'expression « vol de données » est d'ailleurs fréquemment utilisée dans le langage courant. Elle

1 « Les *proches* d'une personne sont son conjoint, son partenaire enregistré, ses parents en ligne directe, ses frères et sœurs germains, consanguins ou utérins ainsi que ses parents, frères et sœurs et enfants adoptifs » (art. 110 al. 1 CP). « Les *familiers* d'une personne sont ceux qui font ménage commun avec elle » (art. 110 al. 2 CP).

est toutefois incorrecte en droit pénal. D'une part, le vol, sanctionné par l'art. 139 CP, ne concerne que les choses mobilières, ce que les données de l'art. 143 CP ne sont pas. D'autre part, la personne lésée par un vol est dépossédée de sa chose, alors que dans la soustraction de données elle n'en perd pas nécessairement la maîtrise.

« Au sens large, le terme de *données* englobe toutes les informations relatives à un état de fait […] qui sont transmises, traitées ou conservées en vue d'une utilisation ultérieure. […] Mais, dans le contexte qui nous intéresse, seules sont considérées comme des données les informations qui sont traitées, mémorisées et transmises au moyen d'un *ordinateur*. Il s'agit donc d'informations qui sont recueillies, traitées, puis retransmises automatiquement, sous une forme généralement codée et non directement perceptible à l'œil, au moyen des logiciels qui assurent le fonctionnement d'une telle installation »[2]. La donnée correspond à « toute information qui peut faire l'objet d'une communication humaine. Elle sera qualifiée d'informatique si elle est traitée, mémorisée ou transmise au moyen d'un ordinateur »[3]. Même s'ils ne constituent pas des informations en tant que telles, les logiciels sont également concernés par l'art. 143 CP[4].

Les données doivent être « spécialement protégées ». La protection peut être informatique ou physique[5]. En d'autres termes, elle peut être mécanique ou consister en une sécurité intégrée dans le *software* ou le *hardware*[6]. Une barrière contractuelle ou morale n'est pas suffisante[7].

Les données doivent ne pas être « destinées » à l'auteur de l'infraction. Il se les procure sans y être autorisé[8]. Plus précisément, tel est le cas lorsqu'il ne peut pas en disposer, ou déterminer leur utilisation, en vertu du droit civil ou du droit public[9]. « Les données doivent appartenir à une personne autre que l'auteur. Il peut s'agir soit de la personne qui crée et stocke les données, soit de celle pour qui les données sont créées ou conservées. La maîtrise se situe au niveau du contenu des données ; peu importe de savoir qui est le propriétaire de l'ordinateur ou du porteur »[10]. Il s'agit, pour l'ayant droit, d'en disposer librement dans les limites de la loi[11]. Comme l'art. 143 CP protège la paix informatique, c'est-à-dire « la liberté d'utiliser l'outil et l'espace informatique sans

2 FF 1991 II 933, 952.
3 Métille/Aeschlimann, 290.
4 CR CP II-Monnier, art. 143 N 4.
5 CR CP II-Monnier, art. 143 N 6.
6 BSK StGB II-Weissenberger, art. 143 N 20.
7 PC CP, art. 143 N 14.
8 FF 1991 II 933, 978; BSK StGB II-Weissenberger, art. 143 N 14.
9 Donatsch, § 13 201.
10 Hurtado, 314 N 1039.
11 Stratenwerth/Jenny/Bommer, § 14 N 28.

avoir à craindre tel ou tel trouble »[12], les données sont « destinées » au titulaire de ce droit de disposition.

Le comportement punissable consiste à soustraire une donnée. Nous reviendrons plus en détail sur cet élément constitutif.

L'art 143 CP sanctionne une infraction de lésion[13]. Le crime est consommé lorsque la paix informatique est affectée, c'est-à-dire touchée.

Selon Monnier, « il faut constater que les termes ‹ spécialement protégés contre tout accès indu de sa part › recouvrent entièrement la notion de données ‹ qui ne lui étaient pas destinées › »[14]. Des données ne sont pas destinées à quelqu'un lorsqu'il n'a pas le droit d'y accéder. S'il y accède malgré tout, cet accès doit être qualifié d'« indu », c'est-à-dire d'illicite. Dans cette mesure, les deux formulations se recouvrent effectivement.

Celui qui utilise des données informatiques, de manière contraire à ce que le rapport juridique qui lui a permis d'y accéder prévoit, n'est pas punissable pour soustraction de données. L'abus de confiance portant sur des données ne tombe en effet pas sous le coup de l'art. 143 CP[15]. Une initiative parlementaire visant à « améliorer la lutte contre l'espionnage économique » avait proposé d'ajouter un alinéa 3 à cette disposition pour incriminer ce type de comportement[16]. Le projet a malheureusement été classé par le Conseil des États en 2012[17]. L'informaticien indélicat qui est légalement chargé de traiter les données d'une entreprise ou d'une institution et qui les utilise de manière illégitime à son profit, ou celui d'un tiers, ne peut donc pas être sanctionné pour soustraction de données. Il en va de même pour tout employé de l'entreprise qui a légalement accès aux données. Même si d'autres dispositions pénales peuvent certes s'appliquer, par exemple, selon les circonstances, l'art. 162 CP (« violation du secret de fabrication ou du secret commercial ») ou l'art. 273 CP (« service de renseignements économiques »), nous ne pouvons que regretter cette lacune dans l'arsenal répressif.

L'infraction est intentionnelle. Le dol éventuel suffit[18]. De plus, l'auteur doit avoir agi dans le dessein de se procureur ou de procurer à un tiers un enrichissement illégitime.

12 CR CP II-Monnier, art. 143 N 5. En d'autres termes, « le droit du bénéficiaire légitime de disposer des données informatiques à sa guise » (PC CP, art. 143 N 2). « Computerfrieden » (BSK StGB II-Weissenberger, art. 143 N 3).

13 BSK StGB II-Weissenberger, art. 143 N 4 ; PC CP, art. 143 N 2; CR CP II-Monnier, art. 143 N 1.

14 CR CP II-Monnier, art. 143 N 10. Dans le même sens : PC CP, art. 143 N 20.

15 FF 1991 II 933, 978.

16 Initiative parlementaire n° 10.456.

17 BO 2012 E 540. L'initiative parlementaire n° 10.451, qui avait une teneur identique, a été retirée au Conseil national.

18 BSK StGB II-Weissenberger, art. 143 N 27 ; CR CP II-Monnier, art. 143 N 15.

B. L'accès indu à un système informatique (art. 143bis CP)

Selon l'art. 143bis al. 1 CP, « quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire ». L'alinéa 2 vise à sanctionner spécialement certains actes préparatoires au piratage[19], tels que la mise en circulation d'un mot de passe.

L'accès indu à un système informatique est conçu comme une forme de « violation de domicile informatique »[20]. L'infraction est le pendant, dans le monde « virtuel », de la violation de domicile (art. 186 CP) dans l'univers « physique ».

La notion de « système informatique » désigne tout particulièrement l'ordinateur, à l'exclusion des simples supports de données, comme une clé USB, et des équipements qui servent uniquement à la fourniture d'un bien ou d'un service donné ou à l'enregistrement de données déterminées, tels que les distributeurs automatiques de billets ou les téléphones, à moins que ces appareils ne soient reliés, directement ou non, à un ordinateur[21]. Le Tribunal fédéral précise que « font l'objet de l'attaque les systèmes ou installations de traitement de données et non pas – contrairement à l'art. 143 CP – les données qui y sont stockées »[22]. Comme le souligne pertinemment Monnier, si tout traitement s'appuie forcément sur une installation physique, la notion de « système informatique » ne se limite pas à cela, une même machine pouvant en effet renfermer plusieurs de ces systèmes, c'est-à-dire plusieurs sessions, chacune protégée contre les accès d'autrui, par exemple par un mot de passe[23]. Les systèmes d'exploitation actuels permettent d'ouvrir sur la même machine des sessions d'utilisateurs différentes. Celles-ci sont en général protégées par un mot de passe, une empreinte numérique ou une reconnaissance faciale. L'accès illégal à une session, même en disposant des droits pour une autre session, doit être considéré comme un accès indu. Rappelons aussi que l'accès indu à une machine se fait souvent par le biais de l'installation d'un *rootkit*[24], après une manœuvre d'hameçonnage *(phishing)*, donc en ayant réussi à tromper la vigilance de l'ayant droit.

Un système appartient à celui qui a le droit d'y accéder et d'en disposer[25] et donc « à autrui » si l'auteur ne jouit pas juridiquement de cette faculté. Comme

19 CR CP II-Monnier, art. 143bis N 15.
20 FF 1991 II 933, 979; CR CP II-Monnier, art. 143bis N 5.
21 CR CP II-Monnier, art. 143bis N 3.
22 ATF 145 IV 185, c. 2.1, JdT 2019 IV 312.
23 CR CP II-Monnier, art. 143bis N 4.
24 Outil de dissimulation d'activité. C'est un « logiciel dont l'objet est de masquer l'exécution de codes malveillants afin de les rendre indétectables et de contourner les mesures de sécurité pour réaliser des cyberattaques » (Ghernaouti, 380). Installé à l'insu de l'ayant droit, il permet en général de manipuler un ordinateur à distance.
25 CR CP II-Monnier, art. 143bis N 6 ; PC CP, art. 143bis N 9.

pour l'art. 143 CP, le bien protégé est ici la paix informatique[26]. Pour le Tribunal fédéral, « c'est la liberté qu'a l'ayant droit de décider qui peut accéder à une installation informatique sécurisée et aux données qui y sont stockées qui est protégée »[27]. L'ayant droit est celui qui a légalement la possibilité de maîtriser l'accès au système informatique et de le contrôler.

Selon Monnier, l'accès indu à un système informatique représente une infraction de lésion[28]. Weissenberger, plus nuancé, note que, d'un côté, le délit revêt effectivement cette caractéristique. Mais, de l'autre, les ayants droit du système informatique doivent également être protégés contre de possibles dommages (par exemple des pertes de données), violations de secrets contenus dans les données, « vols » de données, atteintes à la réputation, arrêts du système en raison d'un contrôle de sécurité requis après une attaque, etc., résultant d'un accès indu au système. En ce sens, il s'agit d'une infraction de mise en danger concret[29]. Il est vrai que la paix informatique peut être concrètement menacée par un accès indu, sans toutefois être (encore) troublée. Une mise en danger abstraite ne suffit en tous les cas pas.

L'auteur doit accéder au système « sans droit ». L'infraction suppose qu'il « ne soit pas autorisé à utiliser le système comme il l'a fait, que ce soit en vertu de la loi ou d'un accord »[30]. Plus précisément, l'accès « n'a pas été autorisé par la loi, le consentement de la victime ou par un autre motif justificatif »[31].

Le système doit être « spécialement protégé ». Contrairement à la règle applicable à l'art. 143 CP, la protection ne peut être ici qu'informatique[32]. Enfermer un ordinateur dans un coffre, sans autre protection, ne suffit donc pas.

Le comportement typique consiste à s'introduire, au moyen d'un dispositif de transmission de données, dans le système informatique. La question de savoir si l'accès doit forcément se faire à distance est controversée[33]. Comme les auteurs du Petit Commentaire, nous sommes d'avis qu'il convient de répondre négativement. L'auteur peut aussi commettre le délit en utilisant le clavier de l'ordinateur visé[34]. Nous rejoignons Monnier qui écrit : « Nous nous interrogeons sur la pertinence de ces distinctions à l'aune de CP 143bis I, et serions enclins à penser que la situation ne fonde pas un traitement pénal différent si l'auteur utilise pour agir l'ordinateur de l'ayant droit, lequel constitue alors l'installation au moyen de laquelle l'auteur s'est indûment introduit. En

26 BSK StGB II-Weissenberger, art. 143bis N 5 ; CR CP II-Monnier, art. 143bis N 1.
27 ATF 145 IV 185, c. 2.1, JdT 2019 IV 312.
28 CR CP II-Monnier, art. 143bis N 1.
29 BSK StGB II-Weissenberger, art. 143bis N 6.
30 Corboz, 291 N 9.
31 Métille/Aeschlimann, 301.
32 CR CP II-Monnier, art. 143bis N 7 ; PC CP, art. 143bis N 11.
33 PC CP, art. 143bis N 17 et les références doctrinales citées.
34 PC CP, art. 143bis N 17.

résumé, le texte légal définit à notre sens un comportement informatique, pas obligatoirement un comportement à distance »[35]. Nous souscrivons pleinement à cette argumentation. La distinction entre les deux modes opératoires s'avérerait très artificielle. L'accès peut avoir lieu aussi bien à distance que directement sur la machine, le but de la loi étant d'empêcher tout accès indu au système informatique.

L'infraction est intentionnelle. Le dol éventuel suffit[36].

C. La détérioration de données (art. 144bis CP)

L'art. 144bis ch. 1 CP dispose que « celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office ». Le chiffre 2 de la disposition réprime la fabrication et la mise en circulation (intentionnelle) de programmes de détérioration.

L'art. 144bis ch. 1 CP est basé sur l'art. 144 CP, qui sanctionne les dommages à la propriété. Comme pour l'art. 143 CP, ce sont des « données enregistrées ou transmises électroniquement ou selon un mode similaire » qui sont concernées, alors que dans l'art. 144 CP l'objet de l'infraction est une chose. Ces données n'ont pas besoin d'être spécialement protégées.

Le comportement typique consiste à modifier, effacer ou mettre hors d'usage des données informatiques. L'auteur doit agir « sans droit ».

L'infraction est intentionnelle. Le dol éventuel suffit[37]. La négligence n'est pas punissable.

III. Interprétation de quelques éléments constitutifs

A. La soustraction

La soustraction signifie que l'auteur acquiert la maîtrise de la donnée ; il doit être en mesure de l'utiliser pour lui-même[38]. Il obtient un pouvoir de disposition *(Verfügungsmacht)* sur celle-ci[39]. En d'autres termes, la soustraction correspond à tout comportement par lequel l'auteur acquiert le contrôle des données *(Verfügungsgewalt)*, pour lui-même ou autrui[40].

35 CR CP II-Monnier, art. 143bis N 9.
36 BSK StGB II-Weissenberger, art. 143bis N 25 ; CR CP II-Monnier, art. 143bis N 12.
37 BSK StGB II-Weissenberger, art. 144bis N 38 ; CR CP II-Monnier, art. 144bis N 7.
38 CR CP II-Monnier, art. 143 N 13 ; PC CP art. 143 N 22.
39 BSK StGB II-Weissenberger, art. 143 N 25.
40 Donatsch, § 13 202.

La question à résoudre est de savoir quand, précisément, il est possible de considérer que l'auteur a acquis la maîtrise sur la donnée. Monnier estime qu'il suffit qu'il ait pu la lire, c'est-à-dire en prendre connaissance[41]. Les auteurs du Petit Commentaire partagent cet avis, en écrivant qu'il suffit « que l'auteur ait pu accéder à la donnée »[42]. Selon Weissenberger, l'auteur établit son pouvoir de disposition sur les données, par exemple, lorsqu'il se les envoie à lui-même par voie électronique, les transfère sur un autre support de stockage, les imprime ou encore s'empare du support de données (un vol pouvant aussi, en principe, être retenu dans ce dernier cas)[43]. Pour Stratenwerth/Jenny/Bommer, l'auteur soustrait une donnée lorsqu'il peut l'utiliser pour lui-même, après avoir déjoué les dispositifs de sécurité. Ils donnent aussi comme exemple le fait de subtiliser le support de données – ce comportement pouvant aussi être typique d'un vol selon les circonstances – ou de transférer les données sur un autre support, à condition, ajoutent-ils, que les données ne soient pas cryptées ou qu'elles soient déchiffrables pour l'auteur[44]. Par contre, pour Weissenberger, peu importe que les données soient chiffrées ou non et que l'auteur puisse surmonter l'encryptage. Le seul élément décisif est de savoir s'il peut ou pourrait utiliser des données cryptées, par exemple en les vendant ou en demandant à des tiers de les déchiffrer[45].

Hurtado souligne que « la soustraction signifie partage du bien. Un rapprochement avec l'art. 139 [CP] concernant le vol (donc le dessein de s'approprier) est possible, en cela que l'auteur envisage de créer un pouvoir de disposition durable sur l'objet de l'infraction. Le simple fait d'accéder aux données et d'en prendre connaissance ne suffit pas »[46]. Pour Corboz, « le comportement punissable consiste dans le fait que l'auteur, par n'importe quel moyen, accède à la donnée informatique […]. L'analogie avec le vol n'est pas complète, puisque la victime ne perd pas nécessairement la donnée qui lui est soustraite […]. Peu importe que l'auteur prenne ou non connaissance de la donnée qu'il a soustraite. Il est également sans importance qu'il n'ait pas agi pour acquérir lui-même la donnée, mais seulement pour la transmettre à un tiers »[47].

Donatsch précise que si l'auteur peut disposer physiquement des données, l'infraction est consommée. En général, il les obtient en les copiant depuis un ordinateur ou un support de données ou en les lisant dans son propre système de traitement de données[48]. Donatsch ajoute que l'infraction n'est pas unique-

41 CR CP II-Monnier, art. 143 N 13.
42 PC CP, art. 143 N 22.
43 BSK StGB II-Weissenberger, art. 143 N 25.
44 Stratenwerth/Jenny/Bommer, § 14 N 31.
45 BSK StGB II-Weissenberger, art. 143 N 25.
46 Hurtado, 315 N 1042.
47 Corboz, 286 N 8.
48 Donatsch, § 13 202.

ment réalisée lorsque l'auteur obtient le contrôle sur les données, mais également lorsqu'il prend simplement connaissance des informations qu'elles contiennent et qu'il peut ainsi les utiliser. En effet, les données sont des biens immatériels et, contrairement à ce qui prévaut pour les choses en cas de vol, elles peuvent être utilisées même si aucun pouvoir de disposition n'est établi[49].

Pour Trechsel/Crameri, l'auteur n'a pas soustrait les données lorsqu'il a surmonté les obstacles qui devaient l'empêcher d'y accéder, mais quand il est en mesure de les « travailler », de les consulter, de les modifier, de les imprimer, de les combiner, etc. L'enregistrement sur une disquette[50] ou un autre support de données en sa possession représente un cas clair. Il suffit qu'il ait eu la possibilité d'utiliser les données du système informatique de la personne autorisée à sa discrétion[51]. Toutefois, pour Trechsel/Crameri, une simple prise de connaissance ne suffit pas, celle-ci pouvant tomber tout au plus sous le coup de l'art. 143bis CP[52].

Selon nous, la soustraction doit être définie comme **tout processus permettant à l'auteur d'obtenir une copie de la donnée**. **L'auteur acquiert une maîtrise (un pouvoir de disposition) sur cette copie**. L'infraction est consommée dès que cette dernière est réalisée. Le mode opératoire peut consister à enregistrer la donnée sur un autre support, à l'imprimer ou à la transmettre. **Une simple prise de connaissance du contenu est suffisante**. En effet, le processus de mémorisation humaine correspond à une forme de transmission et d'enregistrement de l'information. En lisant le contenu de la donnée, l'auteur le transfère dans sa mémoire[53]. Aucune raison ne justifie de différencier l'enregistrement d'informations dans l'esprit humain de celui opéré sur un support informatique. Certes, des problèmes de preuve peuvent survenir. Mais ce n'est pas une question liée à la typicité de l'infraction.

L'infraction est réalisée dès que l'auteur obtient la copie de la donnée, qu'elle soit chiffrée ou non[54]. Une règle contraire aboutirait à un résultat incohérent : celui qui déroberait une donnée protégée uniquement par un chiffrement ne se rendrait pas coupable de soustraction (mais uniquement de tentative de soustraction[55]), alors que ce chiffrement représente pourtant une protection au sens de l'art. 143 CP. Par contre, si la donnée n'était pas chiffrée,

49 Donatsch, § 13 202-203.

50 Notons que les disquettes ne sont plus guère utilisées aujourd'hui et ne sont même plus prévues pour les ordinateurs les plus récents.

51 PK StGB-Trechsel/Crameri, art. 143 N 7.

52 PK StGB-Trechsel/Crameri, art. 143 N 7.

53 Cette lecture implique bien sûr que la donnée ait été déchiffrée si elle était préalablement encryptée.

54 Rappelons que la donnée doit en tous les cas être (spécialement) protégée. Elle peut l'être par un chiffrement ou un autre procédé.

55 L'infraction ne serait réalisée qu'au moment du déchiffrement.

mais avec un autre obstacle ayant été déjoué, l'infraction serait réalisée. Le chiffrement représenterait alors, paradoxalement, une barrière à la consommation de l'infraction. Or, les données doivent être spécialement protégées et elles le sont dans la plupart des cas par ce procédé. En général, l'auteur de la soustraction ne peut se rendre compte de la difficulté du décryptage des données que subséquemment. Le succès du « cassage » dépendra alors fortement de son savoir et surtout de la puissance de calcul à sa disposition. En conformité avec l'idée de protection de la paix informatique, le fait que les données aient pu ou non être déchiffrées ne doit pas entrer en ligne de compte pour délimiter les contours de l'infraction. Dans la mesure où elles sont à disposition de l'auteur, cette dernière est réalisée.

B. L'accès indu et sa délimitation avec la soustraction

L'accès indu est caractérisé par « une intrusion dans la sphère informatique d'autrui »[56]. « Le comportement punissable consiste à pénétrer dans un système informatique »[57]. Le Tribunal fédéral précise qu'« en tant qu'acte préparatoire à une soustraction de données au sens de l'art. 143 CP, l'infraction d'accès indu à un système informatique au sens de l'art. 143bis al. 1er CP suppose déjà – de manière d'ailleurs analogue à la violation de domicile (art. 186 CP) – une intrusion dans un système informatique appartenant à autrui »[58]. Comme le notent Métille/Aeschlimann, « le texte de l'art. 143bis CP parle de ‹ s'introduire ›, tandis que la note marginale utilise le terme d'‹ accéder ›. La notion de ‹ s'introduire › fait référence à la violation de domicile mais n'est pas très précise au niveau technique, puisqu'elle impliquerait que l'auteur entre dans un système informatique, ce qui n'est pas forcément visible. […] Le terme d'‹ accès › est ainsi à préférer […] »[59]. L'accès est réalisé « dès que les données du système informatique sont ‹ visibles › et utilisables par l'auteur »[60]. Dans le milieu informatique, l'expression « pénétration » nous semble la plus usitée. Toutefois, elle signifie clairement « accès indu ».

L'accès indu peut effectivement représenter un acte préparatoire à la soustraction de données. Il n'en est toutefois pas toujours ainsi. L'auteur peut notamment accéder à un système informatique pour procéder à des actes de sabotage (par exemple, couper l'alimentation électrique d'une ville) ou pour provoquer un déni de service. Dans ces cas, des données ne sont pas soustraites. Nous pouvons retenir comme règle que **l'auteur a accédé indûment au sys-**

56 CR CP II-Monnier, art. 143bis N 8.

57 Corboz, 290 N 4. Weissenberger précise aussi que l'auteur s'introduit *(« eindringt »)*, c'est-à-dire pénètre, dans le système (BSK StGB II-Weissenberger, art. 143bis N 17).

58 ATF 145 IV 185, c. 2.1, JdT 2019 IV 312.

59 Métille/Aeschlimann, 300.

60 Métille/Aeschlimann, 300.

tème informatique lorsqu'il a réussi à y installer un logiciel ou ouvrir une session informatique.

Du point de vue de la fixation de la peine, l'art. 143 CP absorbe l'art. 143bis al. 1 CP[61]. En d'autres termes, lorsque les éléments constitutifs de la soustraction de données sont réalisés, il n'y a plus de place pour une application de l'infraction d'accès indu à un système informatique. Il convient toutefois de rappeler que l'art. 143 CP exige que l'auteur ait agi avec un dessein d'enrichissement illégitime, ce qui n'est pas le cas pour l'art. 143bis CP. Si cet élément subjectif spécial fait défaut, seul l'accès indu à un système informatique peut être envisagé.

C. La protection spéciale

Les art. 143 et 143bis CP exigent tous deux une protection spéciale, respectivement des données et du système informatique. Monnier résume bien la problématique : « Que faut-il comprendre par ‹ protection spéciale › ? Faut-il une protection d'une **efficacité particulière** ? Deux approches sont concevables :

– Certains auteurs s'appuient sur la systématique de l'escroquerie (CP 146). Il s'agit donc de diriger l'analyse vers le lésé et d'exiger de celui-ci qu'il ait pris au préalable des mesures de protection suffisamment efficaces pour pouvoir se prévaloir de la protection pénale.
– Une autre opinion s'appuie, en référence aux travaux législatifs, sur la violation de domicile (CP 186). Il serait alors nécessaire et suffisant que la fermeture se manifeste de façon objectivement reconnaissable, soit que l'auteur se trouve devant une ‹ porte fermée à clé ›, sans plus ample exigence d'efficacité particulière »[62].

Le Tribunal pénal fédéral souligne que « la protection doit être *habituellement suffisante* pour empêcher un accès illégal. Il n'est pas nécessaire, par exemple, que des mesures de protection spécifiques, allant au-delà d'une protection habituelle sur le marché contre les virus et les accès illicites, aient été prises »[63].

Selon le Tribunal fédéral, tombe sous le coup de l'art. 143bis CP « la personne qui, généralement par défi, parvient à pénétrer dans un système informatique protégé contre tout accès indu. Il suffit qu'il n'y ait plus de barrières informatiques qui puissent sérieusement l'empêcher de prendre connaissance des données »[64]. Dans une affaire plus récente d'accès indu à un système informatique, il a souligné que « le délit d'intrusion désigne le fait de forcer les obstacles posés au traitement des données, tels que des codes ou des dispositifs de cryp-

61 BSK StGB II-Weissenberger, art. 143 N 41 ; CR CP II-Monnier, art. 143 N 30.
62 CR CP II-Monnier, art. 143 N 8 et les références citées.
63 TPF 2016 28, c. 2.1.
64 ATF 130 III 28, c. 4.2.

tage, via des chemins d'accès câblés ou des canaux de transmission de données à distance sans fil, qui sont censés empêcher l'auteur d'accéder aux données […]. L'utilisation d'un code d'accès ou d'un mot de passe constitue une protection suffisante au sens de la disposition pénale […]. Constitue une intrusion – de manière d'ailleurs analogue à la violation de domicile au sens de l'art. 186 CP […] – tout acte propre à rendre inopérante la protection mise en place, sans qu'un investissement particulier en temps ou en moyens techniques ne soit nécessaire »[65]. Dans le cas d'espèce, après s'être séparée de son mari, l'épouse avait accédé sans droit au compte Google (Gmail) de celui-ci. Elle n'en était pas titulaire et il était protégé par un mot de passe. Selon le Tribunal fédéral, le fait qu'elle « n'ait pas obtenu le mot de passe en adoptant un comportement actif visant à forcer les obstacles posés à l'accès au système informatique, mais l'ait simplement trouvé par hasard dans l'ancien bureau commun n'y change rien. La manière dont l'auteur se procure le mot de passe qui lui permet d'accéder indûment à une installation de traitement de données ne revêt aucune signification au moment de déterminer si l'on se trouve en présence d'un acte de piratage informatique. Ainsi, la disposition pénale vise également les cas dans lesquels l'auteur obtient le code d'accès d'une tierce personne […] »[66].

La jurisprudence du Tribunal fédéral plaide en faveur des tenants d'une approche fondée sur l'art. 186 CP. Il n'est pas nécessaire que les mesures de protection soient sophistiquées. **Il suffit que l'auteur ait été confronté à un élément montrant que l'accès était réservé à autrui**. **Il faut examiner si un obstacle avait été érigé, quelque petit qu'il soit, et s'il était reconnaissable pour l'auteur**. Par exemple, le mot de passe qui se résume à « 123 » suffit (même si, en termes préventifs, il est bien sûr vivement conseillé de choisir une combinaison plus complexe !). La seule présence d'un mot de passe démontre que quelqu'un a voulu placer une barrière à l'accès au système informatique ou aux données.

D. La détérioration

L'art. 144bis CP protège l'intérêt qu'a l'ayant droit à un usage exempt de perturbation[67], mais aussi l'intégrité des données informatiques[68]. Toute modification est en principe suffisante pour consommer l'infraction, « par exemple un changement dans l'ordre d'une énumération, un ajout apporté à un texte, faire en sorte que des données conçues pour être retravaillées ne puissent plus l'être ou encre le brouillage ou le cryptage d'une information transmise »[69]. Pour

65 ATF 145 IV 185, c. 2.2.2, JdT 2019 IV 312.
66 ATF 145 IV 185, c. 2.2.2, JdT 2019 IV 312.
67 ATF 129 IV 230, c. 2.1.1.
68 BSK StGB II-Weissenberger, art. 144bis N 6 ; CR CP II-Monnier, art. 144bis N 3.
69 CR CP II-Monnier, art. 144bis N 3.

qu'une donnée soit effacée, « il suffit que la donnée enregistrée ne se trouve plus sur son support électronique et que la donnée transmise soit retirée de la communication »[70]. La disposition envisage aussi le cas de celui qui aura « mis hors d'usage » des données. Il suffit qu'elles ne puissent plus être utilisées, par exemple en raison de la transformation indue d'un mot de passe ou d'une attaque DDoS *(Distributed Denial of Service)*, sans qu'il soit nécessaire qu'elles aient perdu de la valeur[71].

Le critère de la **perturbation dans l'usage des données** est déterminant. Par exemple, celui qui mélange les répertoires d'un serveur de fichiers est déjà punissable. Il n'efface rien, mais il crée un désordre qui peut s'avérer très perturbateur. La **protection de l'intégrité des données** est le second aspect décisif. L'ayant droit doit pouvoir les conserver intactes. Toute modification intentionnelle est suffisante pour consommer l'infraction.

IV. Conclusion

Nous avons donné quelques exemples de mise en commun de connaissances issues du droit et de l'informatique pour mieux cerner le sens de quelques notions juridiques dans le domaine de la cybercriminalité. Pour lutter efficacement contre cette forme de délinquance, réunir les savoirs constitue une condition *sine qua non* de la réussite. Comme tout le monde ne peut pas se prévaloir de plusieurs formations, il est essentiel d'apprendre à dialoguer entre spécialistes utilisant des langages différents. Le juriste doit savoir ouvrir son horizon conceptuel et l'expert informaticien se montrer capable d'une efficace vulgarisation.

La lutte contre la cybercriminalité ne se limite pas à l'analyse et à la compréhension des éléments constitutifs de certaines infractions, même si cet aspect est central. Aujourd'hui, de nombreux autres défis se posent. Les infractions d'accès indus à un système informatique ou de soustraction de données ne sont pas le fait uniquement d'individus isolés, mais aussi de groupes organisés et même d'États, ce qui rend la répression beaucoup plus complexe, voire, quelquefois, illusoire. Les auteurs ne se trouvent pas toujours en Suisse, ce qui implique de recourir à l'entraide internationale, avec des succès très divers, certains pays se montrant fort peu coopératifs. Il est pourtant essentiel de persévérer dans l'application du dispositif pénal, en s'efforçant de fédérer toutes les énergies, mais aussi d'insister sans cesse sur l'importance cruciale de la prévention ! Dans une société de plus en plus numérique, la sauvegarde de nos libertés fondamentales passe obligatoirement par un meilleur contrôle du « cyberespace ».

70 CR CP II-Monnier, art. 144bis N 4. Il suffit que la donnée ne se trouve plus à la place qui était la sienne.

71 CR CP II-Monnier, art. 144bis N 4-5.