UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT

[redacted]

Travail de rédaction juridique

Soustraction de données et accès indu à un système informatique (art. 143 et 143bis CP)

Sous la direction de la Professeure Katia VILLARD, assistée par Madame Joanna BAUMANN, dans le cadre du cours « Droit pénal spécial I – Infractions contre le patrimoine »

Date de dépôt : 11 décembre 2023

Année académique 2023-2024

Table des matières

Bibliographie

Doctrine

ACKERMANN Jürg-Beat/VOGLER Patrick/BAUMANN Laura/EGLI Samuel, Strafrecht – Individualinteressen : Gesetz, System und Lehre im Lichte der Rechtsprechung, Berne (Stämpfli) 2019.

CORBOZ Bernard, Les infractions en droit suisse, Volume I, 3e éd., Berne (Stämpfli) 2010.

DÉVAUD Blaise, Entre la protection de la correspondance et la protection de l'information : étude comparative de la protection pénale du secret de la correspondance en droits suisse, polonais et allemand, thèse Fribourg, Berne (Weblaw) 2017.

DUPUIS Michel/MOREILLON Laurent/PIGUET Christophe/BERGER Séverine/MAZOU Miriam/RODIGARI Virginie (édit.), Petit commentaire du Code pénal, 2e éd., Bâle (Helbing Lichtenhahn) 2017 (cité : PC CP).

HURTADO POZO José, Droit pénal : partie spéciale, nouvelle édition refondue et augmentée, Genève, Zurich, Bâle (Schulthess) 2009.

MACALUSO Alain/MOREILLON Laurent/QUELOZ Nicolas (édit.), Commentaire romand, Code pénal II, Art. 111-392 CP, Bâle (Helbing Lichtenhahn) 2017 (cité : CR CP II-AUTEUR).

MÉTILLE Sylvain/AESCHLIMANN Joanna, Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ?, *in* Revue Pénale Suisse (RPS/ZStrR) 2017, p. 283 ss.

MONNIER Gilles, Le piratage informatique en droit pénal, *in* sic! 2009, p. 141 ss.

MÜLLER Jérémie, La cybercriminalité économique au sens étroit : analyse approfondie du droit suisse et de quelques droits étrangers, thèse Lausanne, Genève, Zurich, Bâle (Schulthess) 2012.

NIGGLI Marcel Alexander/WIPRÄCHTIGER Hans (édit.), Basler Kommentar, Strafrecht II, Art. 111-392 StGB, 4e éd., Bâle (Helbing Lichtenhahn) 2018 (cité : BSK StGB II-AUTEUR).

TEICHMANN Fabian/GERBER Léonard, Les cyberattaques par spyware - Poursuite et qualification en droit pénal suisse, *in* Sécurité & Droit (S&D/S&R) 2021 III, p. 118 ss.

TRECHSEL Stefan/PIETH Mark (édit.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4e éd., Zürich (Dike) 2021 (cité : Praxiskommentar).

Autres sources

CONSEIL FÉDÉRAL, Message 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 p. 933 ss (cité : Message modification du Code pénal 1991).

CONSEIL FÉDÉRAL, Message relatif à l'approbation et à la mise en œuvre de la Convention du conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 II p. 4275 ss (cité : Message approbation de la Convention 2010).

I. Introduction

Le développement de l'informatique à la fin du 19ème siècle a entraîné la naissance d'une nouvelle forme de délinquance : la cybercriminalité. L'informatique constituait un formidable outil pour commettre des actes déjà répréhensibles par la loi, mais a aussi engendré de nouvelles infractions qui n'étaient pas couvertes par le droit pénal. Afin de combler ces lacunes, le législateur a profité de la révision partielle du Code pénal et du Code pénal militaire de 1994, pour introduire de nouvelles dispositions, parmi lesquelles figuraient les articles 143 et 143bis CP, respectivement intitulés « soustraction de données » et « accès indu à un système informatique »[1].

Ce travail consiste principalement en une analyse des conditions des infractions décrites aux art. 143 et 143bis CP, notamment afin d'évaluer la portée de ces dispositions, de comprendre comment elles s'articulent et d'identifier certains comportements qui y échappent.

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

La soustraction de données, ou « *cracking* »[2], est un délit formel et un délit de lésion[3]. Elle est régie par l'art. 143 CP, dont l'alinéa 1 punit celui qui, « dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui sont pas destinées et qui sont spécialement protégées contre tout accès indu de sa part ». Cet article protège le droit du bénéficiaire légitime de disposer de ses données et de ses logiciels[4].

A. Les éléments constitutifs de l'infraction

1. Éléments constitutifs objectifs

La soustraction de données se caractérise par plusieurs éléments constitutifs objectifs : des données enregistrées ou transmises, une protection spéciale et une soustraction en contournant cette protection.

a. Les données enregistrées ou transmises

Afin de permettre une adaptation aux progrès technologiques, le législateur a choisi une formulation ouverte de l'art. 143 CP et a délibérément évité d'introduire une définition de la notion de donnée dans le Code pénal[5]. Cependant, d'après le Message du Conseil fédéral, il apparaît que les données constituent « toutes les informations relatives à un état de faits, représentées sous forme de lettres, de nombres, de signes, de dessins, etc., qui sont transmises, traitées ou conservées en vue d'une utilisation ultérieure », mais que, dans le cadre de l'art. 143 CP, sont exclusivement qualifiées de données les informations traitées, mémorisées et transmises par le biais d'un ordinateur[6]. Cela concerne donc les informations « recueillies,

[1] HURTADO POZO, N 1032.
[2] MÉTILLE/AESCHLIMANN, p. 289.
[3] CR CP II-MONNIER, CP 143 N 1 ; BSK StGB II-WEISSENBERGER, CP 143 N 4.
[4] Arrêt du Tribunal pénal fédéral SK.2014.46 du 27 novembre 2015, consid. 2.1.
[5] Message modification du Code pénal 1991, p. 951 s.
[6] Message modification du Code pénal 1991, p. 952.

traitées, puis retransmises automatiquement, sous une forme généralement codée et non directement perceptible à l'œil », par le biais de logiciels assurant le fonctionnement d'une telle installation[7]. La doctrine admet qu'une donnée informatique est une information enregistrée ou traitée par un système informatique, susceptible de faire l'objet d'une communication humaine[8]. Les logiciels entrent aussi dans cette définition, bien qu'ils ne renferment pas d'informations en tant que telles, mais plutôt des commandes permettant de les traiter[9].

L'art. 143 CP couvre les données enregistrées ou transmises électroniquement ou selon un mode similaire. Cela comprend aussi les enregistrements qui ne peuvent pas être mis sous une forme lisible, comme les enregistrements sonores, les sons en direct, les photos et films enregistrés et transmis électroniquement[10]. Il faut encore préciser que, même si les supports de stockage magnétique et optique (exemples : disque dur, CD-ROM) ne constituent pas des mémoires électroniques, les données se trouvant sur ces supports peuvent toutefois être considérées comme enregistrées selon un mode similaire et sont donc sujettes à la protection pénale de l'art. 143 CP[11]. Cette norme s'applique aussi si des données sont transférées vers un système informatique au moyen d'un équipement conventionnel, tel qu'un téléphone portable[12]. Par ailleurs la protection pénale couvre également la phase de la transmission des données ; l'interception de données est par conséquent couverte par l'art. 143 CP, et cet article s'appliquerait si, par exemple, des données étaient interceptées durant leur transfert depuis un ordinateur vers une unité de stockage[13].

b. La protection spéciale

Précisons d'abord que l'art. 143 CP ne vise pas toutes les données, mais uniquement celles que le propriétaire ne souhaite pas laisser accessibles à l'auteur de l'infraction (ci-après « auteur »), soit, les données dont l'auteur n'est pas autorisé à disposer et dont il doit pouvoir reconnaitre clairement que leur titulaire ne veuille pas qu'il y accède[14]. À titre d'exemple, celui qui a obtenu, par l'ayant droit, le mot de passe d'un système informatique ne tombe pas sous le coup de l'art. 143 CP[15]. Cette norme ne trouve pas non plus d'application lorsque la donnée en question est accessible à l'ensemble du public[16].

Ensuite, les données doivent être spécialement protégées. Pour cela, il faut que la protection soit habituellement suffisante pour prévenir un accès illégal ; il n'est donc pas requis de mettre en place une protection qui dépasse les normes usuelles du marché contre les virus et les actes

[7] Message modification du Code pénal 1991, p. 952.
[8] MÜLLER, p. 14 ; CORBOZ, CP 143 N 2 s ; Arrêt du Tribunal pénal fédéral SK.2020.35 du 22 janvier 2021, consid.3.3.2a ; ACKERMANN/VOGLER/BAUMANN/EGLI p. 156.
[9] TEICHMANN/GERBER, p. 125 ; BSK StGB II-WEISSENBERGER, CP 143 N 2 ; CR CP II-MONNIER, CP 143 N 4.
[10] BSK StGB II-WEISSENBERGER, CP 143 N 9 ; TRECHSEL/CRAMERI, Praxiskommentar, CP 143 N 3.
[11] TPF, SK.2020.35, 22 janvier 2021, consid. 3.3.2b ; ACKERMANN/VOGLER/BAUMANN/EGLI, p. 157.
[12] CR CP II-MONNIER, CP 143 N 5.
[13] Message modification du Code pénal 1991, p. 952 et 978 ; MONNIER, p. 149.
[14] TPF, SK.2014.46, 27 novembre 2015, consid. 2.1.
[15] Arrêt du Tribunal pénal fédéral BB.2019.248 du 26 janvier 2021, consid. 4.5.3.
[16] MÉTILLE/AESCHLIMANN, p. 290 s ; CORBOZ, CP 143 N 31 ; MÜLLER, p. 32.

illicites[17]. Par contre, les exigences de protection varient en fonction du domaine ou du type de données et sont, entre autres, plus rigoureuses pour les données sensibles liées à la vie économique, comme les données concernant les clients d'une banque, du fait de la nécessité pour le titulaire de considérer des potentiels auteurs professionnels[18]. Les mesures de protection peuvent être informatiques ou physiques. Une protection physique se manifeste, par exemple, par une porte fermée à clé, alors qu'une protection informatique peut consister, notamment, en un code d'accès, mais pas en une fragmentation, un cryptage ou une anonymisation des données[19]. Finalement, il y a lieu de préciser qu'une interdiction morale ou contractuelle ne suffit pas et qu'un « abus de confiance informatique » n'est donc pas punissable[20].

c. La soustraction en contournant la protection

Avant tout, un commentaire à propos de la différence dans la description du comportement incriminé dans les versions allemande, italienne et française s'impose. La version allemande emploie le mot « *beschaffen* », correspondant au verbe « se procurer ». Le texte italien reprend le verbe « *procurarsi* », signifiant également « se procurer », alors que le texte en français utilise le mot « soustraire ». Cette différence a été soulignée par la doctrine, qui relève que le verbe « se procurer » suggère que l'auteur fasse entrer l'objet de l'infraction dans sa sphère d'influence, alors que le verbe « soustraire » suppose en outre la suppression du pouvoir de disposition de l'ayant droit sur cet objet[21]. Il convient d'interpréter la notion de soustraction à l'aune des versions allemande et italienne, et de comprendre ce terme comme l'acquisition de la maîtrise de la donnée, impliquant la possibilité pour l'auteur d'utiliser la donnée pour lui-même[22]. Par exemple, rediriger le contenu d'un courriel vers sa propre adresse relève d'une soustraction au sens de l'art. 143 CP[23]. Il est aussi important de noter que l'art. 143 CP ne nécessite pas la perte de la maîtrise de l'ayant droit sur les données, ni même la survenance d'un dommage[24]. Néanmoins, une perte de maîtrise de l'ayant droit peut entraîner l'application de l'art. 144bis CP, portant sur la détérioration des données[25].

Par ailleurs, la doctrine est partagée quant au moment auquel la soustraction est consommée. Certains auteurs de doctrine, auxquels nous nous rattachons, estiment que le fait pour l'auteur d'accéder aux données et d'en prendre connaissance suffise, sans qu'il ne soit requis qu'il utilise effectivement les données[26]. WEISSENBERGER ajoute que l'acte est déjà accompli lorsque les données protégées apparaissent à l'écran ; que le fait que l'auteur en prenne des notes, qu'il les photographie, qu'il mémorise les informations etc., ou même qu'il les comprenne n'est pas déterminant[27]. Une autre partie de la doctrine considère que l'auteur doit, entre autres, être en

[17] TPF, SK.2014.46, 27 novembre 2015, consid. 2.1.
[18] TPF, SK.2014.46, 27 novembre 2015, consid. 2.1 ; BSK StGB II-WEISSENBERGER, CP 143 N 19.
[19] TRECHSEL/CRAMERI, Praxiskommentar, CP 143 N 6 ; TPF, SK.2014.46, 27 novembre 2015, consid. 2.2 ss.
[20] PC CP, art. 143 N 14 ; MÉTILLE/AESCHLIMANN, p. 291.
[21] DÉVAUD, p. 344 s ; HURTADO POZO, N 901.
[22] CR CP II-MONNIER, CP 143 N 13.
[23] ATF 130 III 28, consid. 4.2 s, JdT 2004 I 63 ; PC CP, art. 143 N 22.
[24] CR CP II-MONNIER, CP 143 N 12 ; BSK StGB II-WEISSENBERGER, CP 143 N 2.
[25] CR CP II-MONNIER, CP 143 N 12.
[26] TEICHMANN/GERBER, p. 126 ; PC CP, art. 143 N 22 ; BSK StGB II-WEISSENBERGER, CP 143 N 26.
[27] BSK StGB II-WEISSENBERGER, CP 143 N 26.

mesure de travailler avec les données, de les consulter à tout moment, mais qu'il ne suffit pas de simplement accéder aux données et d'en prendre connaissance[28]. Le Tribunal fédéral n'a pas encore tranché. Notons encore que, bien que cela ne ressorte pas du texte de l'art. 143 CP, pour satisfaire aux conditions de cette norme, l'auteur doit contourner la protection spéciale et il doit y avoir un lien causal entre ce contournement et la soustraction des données[29].

2. Les éléments constitutifs subjectifs

Ensuite, l'art. 143 CP suppose la réalisation de deux éléments subjectifs constitutifs.

a. L'intention

Premièrement, il faut que celui qui soustrait des données agisse intentionnellement ; le dol éventuel est suffisant, mais la négligence n'est pas punissable[30].

b. Le dessein d'enrichissement illégitime

Deuxièmement, l'auteur doit agir avec un dessein d'enrichissement illégitime, soit, avec l'intention de s'enrichir ou d'enrichir autrui de manière illicite[31]. La notion d'enrichissement couvre tous les avantages économiques perçus par l'auteur ou un tiers et doit être comprise de manière large, c'est-à-dire qu'elle englobe l'augmentation d'actif, la diminution du passif, la non-diminution de l'actif, ou la non-augmentation du passif[32]. Le dessein d'enrichissement est donné lorsque les données ont une valeur marchande, lorsque l'auteur est payé pour se procurer les données, lorsque les données n'ont qu'une valeur d'usage patrimoniale, par exemple quand elles ne sont pas disponibles dans le commerce et ne peuvent être développées qu'à grands frais, ou encore lorsqu'elles doivent être utilisées pour faire du chantage[33]. L'exigence d'un dessein d'enrichissement illégitime est critiquable. En effet, elle exclut du champ d'application de l'art. 143 CP toutes les soustractions de données accomplies pour des raisons non pécuniaires, par exemples lorsqu'elles sont accomplies pour des motifs politiques, pour nuire, ou encore pour s'entraîner[34]. Faute d'un dessein d'enrichissement illégitime, l'art. 143bis al. 1 CP pourrait s'appliquer à titre subsidiaire ; ou, si l'auteur a soustrait des données personnelles, alors son acte relève de l'art. 179^{novies} CP, qui traite de la soustraction de données personnelles sensibles et qui ne requiert pas de dessein d'enrichissement illégitime[35].

B. Peine et poursuite

La soustraction de données est passible d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. En principe, l'auteur est poursuivi d'office, mais l'art. 143 al. 2 CP ajoute que, la soustraction de données commise au préjudice des proches est poursuivie uniquement sur plainte.

---

[28] TRECHSEL/CRAMERI, CP 143 N 7 ; HURTADO POZO, N 1042.
[29] DÉVAUD, p. 349 ; BSK StGB II-WEISSENBERGER, CP 143 N 23.
[30] BSK StGB II-WEISSENBERGER, CP 143 N 27.
[31] *Ibid*.
[32] MÉTILLE/AESCHLIMANN, p. 292.
[33] BSK StGB II-WEISSENBERGER, CP 143 N 29 ; ATF 111 IV 74, consid. 1, JdT 1985 IV 100, SJ 1986 65.
[34] DÉVAUD, p. 362.
[35] CORBOZ, CP 143 N 11 ; MÉTILLE/AESCHLIMANN, p. 292 ; CORBOZ, CP 179novies N 1.

C. Le projet pour un 3ème alinéa

Un projet pour ajouter un 3ème alinéa à l'art. 143 CP, qui devait réprimander : « celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement, s'approprie des données auxquelles il a accès dans le cadre de ses tâches ou utilise de manière illégitime de telles données à son profit ou au profit d'un tiers», avait fait l'objet d'une proposition aux Chambres fédérales en 2010[36]. Cet alinéa aurait sanctionné une sorte d'abus de confiance en matière informatique, mais a finalement été classé par le Conseil des Etats, au motif que la violation des secrets commerciaux est déjà punissable à l'art. 162 CP[37]. Cette justification est discutable, puisque le projet de l'art. 143 al. 3 CP visait des « données auxquelles [l'auteur] a accès dans le cadre de ses tâches », ce qui pourrait s'interpréter plus largement que les notions de « secret de fabrication » ou de « secret commercial » protégées par l'art. 162 CP.

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

L'art. 143bis CP regroupe deux infractions distinctes, qui seront examinées successivement : l'accès indu à un système informatique (art. 143bis al. 1 CP) et la mise à disposition d'informations en vue d'un accès indu (art. 143bis al. 2 CP).

A. L'accès indu au sens de l'art. 143bis al. 1 CP

L'accès indu à un système informatique, parfois appelé « *hacking* » ou « piratage informatique », est traité à l'art. 143bis al. 1 CP[38]. Cet article vise celui qui « 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 ». L'art. 143bis al. 1 CP vise davantage à sauvegarder la paix informatique, qu'à protéger le patrimoine, assurant ainsi au propriétaire du système informatique le droit d'en maîtriser l'accès et d'exercer un contrôle sur le système[39]. La doctrine convient que cette infraction contient les caractéristiques d'un délit matériel et de lésion ; toutefois, une partie de la doctrine estime qu'en plus de renfermer ces attributs, l'infraction contient aussi les caractéristiques d'un délit de mise en danger concrète[40].

1. Le système informatique appartenant à autrui

Tout d'abord, l'accès indu a pour objet un « système informatique ». Ce terme n'a pas été défini par le Code pénal, mais peut être compris comme une installation technique qui, contrairement aux simples supports de données, traite de manière automatique des données, habituellement sous la forme d'un code[41]. Cela couvre notamment « les ordinateurs, les téléphones portables, les caméras digitales ainsi que toutes installations intégrant le traitement de données », mais aussi les sous-systèmes informatique[42]. Par exemple, le Tribunal fédéral a considéré que, même si elle ne constitue pas un système informatique en tant que tel, une boîte aux lettres électronique

[36] Initiative parlementaire 10.456.
[37] TPF, SK.2014.46, 27 novembre 2015, consid. 2.1 ; COMMISSION DU CONSEIL DES ETATS, BO 2012 E 540.
[38] MÉTILLE/AESCHLIMANN, p. 296.
[39] BSK StGB II-WEISSENBERGER, CP 143bis N 5 ; CR CP II-MONNIER, CP 143bis N 1.
[40] PC CP, art. 143bis N 2 ; MONNIER, p. 146 ; MÜLLER, p. 40 ; BSK StGB II-WEISSENBERGER, CP 143bis N 6.
[41] MÜLLER, p. 34 ; MÉTILLE/AESCHLIMANN, p. 297.
[42] TEICHMANN/GERBER, p. 125 ; BSK StGB II-WEISSENBERGER, CP 143bis N 5 ; PC CP, art. 143bis N 10.

devait être couverte par l'art. 143bis al. 1 CP[43]. Cette jurisprudence, depuis reconfirmée par le Tribunal fédéral, a été critiquée par la doctrine, notamment parce que le Tribunal fédéral semble reconnaître la protection de la boîte aux lettres électronique non pas pour elle-même, mais exclusivement au motif que celui qui y accède pénètre simultanément et illégalement dans l'installation de traitement[44]. D'autres auteurs de doctrine soulignent que cette jurisprudence a au moins le mérite de reconnaître une protection pénale des données des courriels par l'art. 143bis al. 1 CP, qui, contrairement à l'art. 143 CP, ne requiert pas de dessein d'enrichissement illégitime[45]. Ensuite, les supports de données (exemples : clé USB, CD, DVD) ne bénéficient de la protection que s'ils sont reliés à un système informatique protégé[46]. Par ailleurs, à moins qu'ils ne soient reliés directement ou indirectement à un ordinateur, l'exigence d'un traitement automatique a aussi pour effet d'exclure les appareils qui servent exclusivement à fournir des marchandises et des services, à enregistrer ou à envoyer des données, comme c'est régulièrement le cas des distributeurs automatiques de marchandises et de billets, des téléphones fixes ou encore des photocopieuses[47].

Selon le texte de la loi, le système informatique auquel l'auteur accède doit appartenir à autrui. Il est donc déterminant d'identifier qui a le droit d'accéder au système et d'en disposer[48]. Par exemple, celui à qui on a prêté un ordinateur est temporairement considéré comme l'ayant droit, et jouit donc de la protection de l'art. 143bis al. 1 CP[49]. De plus, même s'il lui appartient, le propriétaire qui a prêté cet ordinateur, et qui y accède sans droit, réalise les conditions d'un accès indu[50]. Qui plus est, selon une partie de la doctrine, avec laquelle nous nous alignons, celui qui se trouve légitimement dans un système informatique pourrait lui aussi se rendre coupable d'un accès indu au sein même de ce système, par exemple, s'il peut utiliser une session informatique d'un ordinateur, et qu'il accède sans droit à une autre session de ce même ordinateur[51]. Le Tribunal fédéral n'a pas encore pris position sur ce dernier point.

2. La protection spéciale

L'art. 143bis al. 1 CP exige aussi la présence d'une protection spéciale. Cette notion est la même que celle dans l'art. 143 CP, toutefois, une réserve s'impose. Étant donné que l'art. 143bis al. 1 CP requiert un accès « au moyen d'un dispositif de transmission de données », une barrière physique n'est par conséquent pas suffisante et la protection spéciale devra se manifester de manière informatique[52]. Pour le surplus, nous pouvons renvoyer à ce qui a été expliqué au sujet de la protection spéciale dans le cadre de l'art. 143 CP[53].

---

[43] MÉTILLE/AESCHLIMANN, p. 298 ; Arrêt du Tribunal fédéral 6B_456/2007 du 18 mars.2008, consid. 4.3.
[44] MONNIER, p. 143 s ; ATF 145 IV 185, consid. 2.1, JdT 2019 IV 312
[45] MÉTILLE/AESCHLIMANN, p. 298.
[46] *Ibid*.
[47] Message modification du Code pénal 1991, p. 953 ; BSK StGB II-WEISSENBERGER, CP 143bis N 10.
[48] MONNIER, p. 143.
[49] MÉTILLE/AESCHLIMANN, p. 298.
[50] *Ibid*.
[51] PC CP, art. 143bis N 10 ; BSK StGB II-WEISSENBERGER, CP 143bis N 13 ; TRECHSEL/CRAMERI, Praxiskommentar, CP 143bis N 4.
[52] CR CP II-MONNIER, CP 143bis N 7 ; MÉTILLE/AESCHLIMANN, p. 299.
[53] *Cf*. notion de protection spéciale *supra* p. 2 s.

3. L'accès indu en contournant la protection

Afin de décrire le comportement incriminé, le texte en français de l'art. 143bis al. 1 CP utilise le verbe « s'introduire », alors que la note marginale emploie le mot « accès ». Dans la version allemande, le texte de l'article et la note marginale utilisent le verbe « *eindringen* », signifiant « s'introduire ». La version italienne correspond à la version française, puisqu'elle utilise dans la note marginale le mot « *accesso* », soit « accès », et emploie dans le texte le verbe « *introdursi* », soit « s'introduire ». Le terme « s'introduire » n'est pas adéquat, étant donné qu'il évoque la violation de domicile en paraissant décrire une action impliquant le déplacement physique de l'auteur, entrant dans un espace ; le mot « accès » est donc préférable[54].

Dès lors que le législateur exige que l'accès se fasse au moyen d'un dispositif de transmission de données, la notion d'accès doit être comprise uniquement comme un accès informatique, et non comme un accès réel, tel que le fait d'entrer dans une salle de serveurs[55]. La notion de dispositif de transmission de données doit être interprétée largement et englobe les dispositifs de communication, avec ou sans fil, comme le réseau Internet[56]. En outre, bien que cela ne figure pas dans le texte de l'art. 143bis al. 1 CP, il est nécessaire que l'auteur ait agi en contournant la protection spéciale[57]. La manière dont la protection spéciale est contournée n'est pas déterminante, et peut se manifester, par exemple, par un déverrouillage d'un mot de passe[58].

Il y a controverse quant au moment de la consommation de l'infraction lorsque plusieurs barrières de protections ont été mises en place. Une partie de la doctrine, ainsi que le Tribunal fédéral, estiment qu'il faut que toutes les barrières susceptibles d'empêcher l'auteur de prendre connaissance des données aient été contournées[59]. Une autre partie de la doctrine juge que le contournement d'une seule barrière suffit pour être constitutif d'un accès[60]. Nous nous rattachons à cette seconde conception. En effet, même si la lettre de l'art. 143bis al. 1 CP exige que l'auteur accède effectivement au système informatique, il faut souligner que l'art. 143bis al. 1 CP vise aussi à punir l'auteur qui agit seulement par défi, soit celui qui souhaite simplement se mesurer aux barrières informatiques, et que cet article a davantage pour but de sauvegarder la paix informatique, que de protéger le patrimoine. Nous plaidons donc pour une interprétation téléologique de l'art. 143bis al. 1 CP, permettant d'élargir la portée de cet article aux cas où l'auteur contourne partiellement la protection spéciale.

L'art. 143bis al. 1 CP n'exige pas forcément un piratage à distance, et est aussi applicable, par exemple, si quelqu'un utilise le clavier d'un ordinateur pour y accéder[61]. Toutefois, si une personne initialement autorisée à accéder à un système informatique reste à l'intérieur de ce même système en dépit d'une injonction de le quitter, alors elle ne réalise pas d'accès indu[62].

---

[54] DÉVAUD, p. 351 ; MÉTILLE/AESCHLIMANN, p. 300 ; MÜLLER, p. 35.
[55] MÉTILLE/AESCHLIMANN, p. 300 ; MONNIER, p. 146.
[56] *Ibid*.
[57] DÉVAUD, p. 351 ; ATF 145 IV 185, consid. 2.1, JdT 2019 IV 312.
[58] ATF 145 IV 185, consid. 2.2.2, JdT 2019 IV 312.
[59] CORBOZ, CP 143bis N 7 ; HURTADO POZO, N 1065 ; MÜLLER, p. 35 ; ATF 130 III 28, consid. 4.2, JdT 2004 I 63.
[60] CR CP II-MONNIER, CP 143bis N 10 ; BSK StGB II-WEISSENBERGER, CP 143bis N 21.
[61] BSK StGB II-WEISSENBERGER, CP 143bis N 5 ; CR CP II-MONNIER, CP 143bis N 9 ; MONNIER, p. 146 s.
[62] PC CP, art. 143bis N 16 ; CR CP II-MONNIER, CP 143bis N 8.

Enfin, le caractère indu de l'accès se superpose avec l'exigence de l'appartenance à autrui du système informatique[63]. La notion d'accès indu a encore pour effet d'exclure les situations dans lesquelles l'accès est justifié par la loi, ou par le consentement de l'ayant droit[64].

4. L'intention

Subjectivement, l'intention est nécessaire, et le dol éventuel est suffisant[65]. En revanche, si l'auteur entre par négligence dans le système informatique, et qu'il en profite pour l'explorer, alors il n'est pas punissable[66]. Jusqu'au 31 décembre 2011, le texte de l'infraction exigeait que l'auteur agisse sans dessein d'enrichissement, ce qui avait fait l'objet de critiques de la part de la doctrine[67]. C'est dans le cadre de la ratification de la Convention du 23 novembre 2001 sur la cybercriminalité (CCC ; RS 0.311.43) que cette condition a été supprimée[68].

B. La mise à disposition d'informations en vue d'un accès indu (art. 143bis al. 2 CP)

La seconde infraction traitée à l'art. 143bis CP est la mise à disposition d'informations en vue d'un accès indu. L'art. 143bis al. 2 CP vise celui qui « met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 ». Cette infraction constitue un délit formel et un délit de mise en danger abstraite[69]. L'ajout de cet alinéa résulte aussi de la modification de l'art. 143bis CP dans le cadre de la ratification de la Convention sur la cybercriminalité. En effet, afin de se conformer aux exigences de l'art. 6 CCC, il était nécessaire de couvrir une lacune du droit pénal suisse en punissant certaines formes d'actes préparatoires au *hacking*[70]. Conformément à la possibilité offerte par l'art. 6 al. 3 CCC, le Conseil fédéral a choisi d'émettre une réserve ayant pour effet de dispenser le législateur de punir la possession, l'importation et la production de données destinées au piratage, à moins que ces actes ne puissent être qualifiés de complicité ou de tentative punissable d'une autre infraction, notamment dans le cadre des art. 143 et 143bis al. 1 CP[71]. Cette démarche, laissant subsister une lacune dans le droit pénal suisse, a été jugée difficilement compréhensible par la doctrine[72].

1. Un outil de piratage

Les objets de l'infraction sont des mots de passe, des programmes, ou d'autres données susceptibles de servir à commettre une infraction au sens de l'art. 143bis al. 1 CP. Les outils de piratage visés doivent pouvoir apporter une contribution essentielle et causale à un accès indu selon l'art. 143bis al. 1 CP[73]. Les programmes qui nécessitent une modification ou une adaptation en vue de servir à un accès indu sont aussi concernés, à moins qu'ils ne nécessitent

---

[63] PC CP, art. 143bis N 18 ; *cf.* condition d'appartenance à autrui *supra* p. 6.
[64] CR CP II-MONNIER, CP 143bis N 11 ; PC CP, art. 143bis N 18.
[65] BSK StGB II-WEISSENBERGER, CP 143bis N 42 ; PC CP, art. 143bis N 20.
[66] TRECHSEL/CRAMERI, Praxiskommentar, CP 143bis N 9 ; PC CP, art. 143bis N 20.
[67] CORBOZ, CP 143bis N 12 ; HURTADO POZO, N 1069 ss.
[68] Message approbation de la Convention 2010, p. 4281 s.
[69] BSK StGB II-WEISSENBERGER, CP 143bis N 7 ; MÜLLER, p. 40.
[70] Message approbation de la Convention 2010, p. 4285 s ; CR CP II-MONNIER, CP 143bis N 11.
[71] Message approbation de la Convention 2010, p. 4287.
[72] PC CP, art. 143bis N 27 ; BSK StGB II-WEISSENBERGER, CP 143bis N 35.
[73] BSK StGB II-WEISSENBERGER, CP 143bis N 36.

des modifications essentielles et que l'auteur n'ait pas orienté son offre dans le sens d'une mise à disposition d'informations en vue d'un accès indu[74].

2. La mise à disposition

L'acte incriminé consiste à mettre en circulation ou simplement à rendre disponible un outil de piratage. La mise à disposition peut être accomplie à l'aide d'Internet ou par des communications électroniques, mais aussi de manière plus traditionnelle, notamment par la communication orale ou écrite[75]. Commet par exemple une infraction au sens de l'art. 143bis al. 2 CP, celui qui communique oralement le code d'accès de l'ordinateur de quelqu'un d'autre à un tiers, ou celui qui vend sur Internet des logiciels permettant de cracker des mots de passe informatiques. L'infraction étant un délit de mise en danger abstraite, la mise à disposition de l'outil de piratage suffit, et il n'est pas nécessaire que l'outil en question soit effectivement utilisé en vue de commettre un accès indu au sens de l'art. 143bis al. 1 CP[76].

3. L'intention

La mise à disposition d'informations en vue d'un accès indu est une infraction intentionnelle ; toutefois, tel que le suggère la formule « sait ou doit présumer » utilisée dans le texte de l'article 143bis al. 2 CP, le dol éventuel est suffisant[77]. Il suffit donc que l'auteur soit « conscient de circonstances telles qu'il doit bien se douter que les données feront l'objet d'un usage illicite » ; la négligence n'est donc pas punissable[78].

C. Peine et poursuite

Les alinéas 1 et 2 de l'art. 143bis CP prévoient tous les deux une peine privative de liberté de trois ans au plus, ou une peine pécuniaire. En revanche, l'accès indu au sens de l'art. 143bis al. 1 CP est poursuivi sur plainte, alors que la mise à disposition d'informations en vue d'un accès indu selon l'art. 143bis al. 2 CP est poursuivie d'office[79].

IV. Délimitations et concours

La délimitation entre l'art. 143bis al. 2 CP ainsi que, respectivement, l'art. 143 CP et l'art. 143bis al. 1 CP ne nécessite pas d'explications, étant donné que l'acte incriminé de l'art.143bis al. 2 CP se distingue facilement des actes incriminés décrits dans les deux autres infractions. En revanche, la délimitation entre l'art. 143 CP et l'art. 143bis al. 1 CP est moins aisée, puisque les notions de soustraction et d'accès peuvent se rejoindre, notamment si, comme nous le préconisons, on admet que le simple fait d'accéder aux données soit constitutif d'une soustraction de données[80]. Dans cette hypothèse, ce sont les éléments constitutifs subjectifs qui permettent de distinguer les deux infractions ; si l'auteur agit simplement pour se mesurer à la

---

[74] BSK StGB II-WEISSENBERGER, CP 143bis N 36 ; MÉTILLE/AESCHLIMANN, p. 303.
[75] BSK StGB II-WEISSENBERGER, CP 143bis N 39.
[76] BSK StGB II-WEISSENBERGER, CP 143bis N 40.
[77] BSK StGB II-WEISSENBERGER, CP 143bis N 42.
[78] Message approbation de la Convention 2010, p. 4286 s.
[79] Message approbation de la Convention 2010, p. 4286.
[80] *Cf. supra* p. 3.

protection spéciale, il entre dans le champ d'application de l'art. 143bis al. 1 CP, alors que s'il agit dans le but d'obtenir des données, il tombe sous le coup de l'art. 143 CP[81].

Sur le plan du concours, l'art. 143bis al. 2 CP est subsidiaire à l'art. 143bisal. 1 CP, qui est lui-même en principe subsidiaire aux autres délits informatiques, notamment à l'art. 143 CP[82]. Celui qui accède de manière indue à un système informatique (143bis al. 1 CP) et qui en soustrait des données (143 CP) sera donc puni uniquement selon l'art. 143 CP[83].

Des cas de concours existent aussi avec d'autres articles. À titre d'exemples, des questions de concours se posent notamment à propos de l'art. 143 CP, en lien avec l'art. 179^{novies} CP (soustraction de données personnelles) et l'art. 139 CP (vol). Tout d'abord, étant donné que l'art. 143 CP et l'art. 179^{novies} CP protègent des biens juridiques différents, à savoir, le patrimoine et le domaine secret, un concours idéal entre ces deux dispositions peut entrer en ligne de compte lorsque l'auteur soustrait des données personnelles[84]. Ensuite, l'existence d'un concours entre l'art. 143 CP et l'art. 139 CP, en cas de soustraction d'un support de données, divise la doctrine et n'a pas encore été tranché par le Tribunal fédéral[85]. En l'occurrence, nous estimons qu'un concours devrait être retenu. En effet, comme l'ont fait remarquer certains auteurs de doctrine, exclure le concours et privilégier l'application de l'art. 139 CP reviendrait à faire abstraction du contenu du support de données, alors que c'est justement ce contenu qui intéresse le plus souvent le criminel[86].

V. Conclusion

En conclusion, en s'abstenant de définir les notions de « donnée » et de « système informatique » et en proposant une formulation ouverte pour les art. 143 et 143bis CP, le législateur a permis à ces dispositions de s'adapter aux progrès technologiques. En revanche, certains comportements échappent à ces articles, dont la portée peut paraître trop étroite, par exemple, lorsque le législateur exclut les « abus de confiance informatiques » du champ d'application de l'art. 143 CP, lorsqu'il exige un dessein d'enrichissement illégitime pour cette même disposition, ou encore lorsque le Conseil fédéral émet une réserve, dispensant le législateur de punir certaines formes d'actes préparatoires au *hacking*. Soulignons encore qu'il subsiste quelques conflits doctrinaux, notamment sur le moment auquel la soustraction de données est consommée, qui mériteraient d'être tranchés par le Tribunal fédéral.

Finalement, il faut se rappeler qu'une lutte efficace contre la cybercriminalité n'aboutira pas grâce à la seule force du droit pénal, et que le combat devra nécessairement passer par la prévention, ainsi que par la mise en place de mesures de protection par les différents acteurs de l'informatique.

---

[81] MÜLLER, p. 36 ; MÉTILLE/AESCHLIMANN, p. 301 s.
[82] TRECHSEL/CRAMERI, Praxiskommentar, CP 143bis N 12 ; BSK StGB II-WEISSENBERGER, CP 143bis N 30 et 47.
[83] HURTADO POZO, N 1074.
[84] MÜLLER, p. 33 s ; CORBOZ, CP 143 N 14.
[85] HURTADO POZO, N 1055 et références citées ; MÉTILLE/AESCHLIMANN, p. 293 s et références citées.
[86] MÉTILLE/AESCHLIMANN, p. 294.