ZStrR Schweizerische Zeitschrift für Strafrecht

Band/Tome 132

RPS Revue Pénale Suisse

3

RPS Rivista Penale Svizzera

www.zstrr.recht.ch

Stämpfli Verlag

ZStrR Schweizerische Zeitschrift für Strafrecht
RPS Revue Pénale Suisse
RPS Rivista Penale Svizzera

Gegründet von/Fondée par/Fondata da *C. Stooss 1888*

www.ZStrR.Recht.ch

Die Zeitschrift erscheint jährlich in vier Heften, in der Regel im März, Juni, September und Dezember. Sie befasst sich mit Fragen aus dem Gebiet des Strafrechts und des Strafprozessrechts, des Vollzugs der Strafen und Massnahmen sowie der Kriminologie. Sie veröffentlicht nur bisher noch nicht im Druck erschienene Originalbeiträge. Die Aufnahme von Beiträgen erfolgt unter der Bedingung, dass das ausschliessliche Recht zur Vervielfältigung und Verbreitung an den Stämpfli Verlag AG übergeht. Der Verlag behält sich alle Rechte am Inhalt der ZStrR vor. Insbesondere die Vervielfältigung auf dem Weg der Fotokopie, der Mikrokopie, der Übernahme auf elektronische Datenträger und andere Verwertungen jedes Teils dieser Zeitschrift bedürfen der Zustimmung des Verlags.

La Revue paraît quatre fois par an, ordinairement en mars, juin, septembre et décembre. Elle traite des problèmes de droit pénal, de procédure pénale, d'exécution des peines ou mesures et de criminologie. Elle ne publie que des articles encore inédits. L'acceptation des contributions se produit à la condition que le droit exclusif de reproduction et de diffusion passe à la maison d'édition Stämpfli SA. La maison d'édition se réserve tous les droits sur le contenu du journal ZStrR. En particulier, la reproduction par voie de photocopie, de microcopie, de reprise de supports électroniques de données, et toute autre utilisation de l'ensemble ou de partie de ce journal nécessitent l'accord de la maison d'édition.

Abonnementspreis jährlich (inkl. Onlinearchiv): Schweiz Fr. 171.– Ausland Fr. 181.–
inkl. Versandkosten und 2,5% resp. für Onlineangebote 8,0% MWSt.
Abopreis reine Onlineausgabe: Fr. 132.–

Inserate Stämpfli AG, Postfach 8326, 3001 Bern
Annonces Tel. 031 300 63 82, Fax 031 300 63 90, E-Mail: inserate@staempfli.com

Rezensionsexemplare sind an den Stämpfli Verlag AG, Postfach 5662, 3001 Bern, zu senden.
Les ouvrages pour compte rendu doivent être adressés à la Maison Stämpfli Editions SA, case postale 5662, 3001 Berne.

Abonnements-Marketing Stämpfli AG, Postfach 8326, 3001 Bern
Marketing abonnements Tel. 031 300 63 43, Fax 031 300 63 90, E-Mail: abonnemente@staempfli.com

ISSN 0036-7893

Inhalt – Sommaire

Mitarbeiter dieses Heftes – Ont collaboré à ce fascicule:

Joanna Aeschlimann, BCCC Avocats Sàrl, Avenue des Toises 12, Case postale 5410, 1002 Lausanne
Prof. Dr. Peter Albrecht, Äussere Baselstrasse 212, 4125 Riehen
Prof. Dr. Felix Bommer, Universität Luzern, Rechtswissenschaftliche Fakultät, Frohburgstrasse 3, Postfach 4466, 6002 Luzern
Dr. Sylvain Métille, BCCC Avocats Sàrl, Avenue des Toises 12, Case postale 5410, 1002 Lausanne
Prof. Dr. Mark Pieth, Juristische Fakultät der Universität Basel, Peter Merian-Weg 8, 4002 Basel
Prof. Dr. Franz Riklin, Route du Roule 6, 1723 Marly
Nora Scheidegger, Universität Bern, Institut für Strafrecht und Kriminologie, Schanzeneckstrasse 1, Postfach 8573, 3001 Bern

Sylvain Métille et Joanna Aeschlimann, Lausanne

Infrastructures et données informatiques: quelle protection au regard du code pénal suisse?

Sommaire

I. Introduction

Si l'informatique ne cesse de se développer, les premiers ordinateurs datent déjà du milieu du XXe siècle. Au début des années nonante, le Conseil fédéral constatait des lacunes dans la punissabilité de la criminalité économique et de la criminalité informatique, et proposait d'introduire des dispositions légales pour viser en particulier quatre types d'infractions dont la prise en compte dans le droit pé-

nal présentait des difficultés: le vol de données, l'escroquerie à l'informatique, la détérioration de données et le sabotage informatique, ainsi que le vol de temps-machine[1]. Les données informatiques ne sont en effet pas considérées comme des choses mobilières ou des valeurs patrimoniales, ce qui exclut donc l'application des dispositions comme le vol ou la soustraction d'une chose mobilière, ou encore l'abus de confiance.

Ces dispositions ont encore été complétées au 1er janvier 2012 à la suite de l'entrée en vigueur en Suisse de la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2011 (STCE 185)[2].

Le droit pénal informatique est une notion large qui est utilisée pour désigner toutes les infractions pénales susceptibles d'être commises en lien avec les outils informatiques:

- Les infractions informatiques typiques, soit celles dirigées contre un ordinateur ou des données informatiques (droit pénal informatique au sens strict). Ces infractions sont recensées en droit suisse dans le Titre 2 de la partie spéciale du code pénal suisse[3] (CP), regroupant les infractions contre le patrimoine, telles que la soustraction de données, l'accès indu à un système informatique, la détérioration de données, ou l'utilisation frauduleuse d'un ordinateur.
- Les infractions informatiques «atypiques», soit des infractions existant indépendamment des technologies de l'information, mais qui peuvent être réalisées en recourant à un ordinateur ou des données informatiques. Ces infractions sont contenues dans divers titres du CP ou du droit pénal accessoire. Il s'agit, par exemple, de l'atteinte à l'honneur, de la pornographie, de l'incitation au terrorisme ou à la haine raciale, de l'escroquerie, ou de la violation de droits d'auteur.

Entre 2004 et 2012, on compte en moyenne une vingtaine de condamnations d'adultes par année pour soustraction de données, une dizaine pour détériorations de données et autant pour accès indu à un système informatique, contre plus de 7000 pour vol et environ 4500 pour dommages à la propriété[4]. En 2012, on a toutefois dénombré 1872 infractions de soustraction de données dont 149 seulement ont été élucidées et 264 cas d'accès indu à un système informatique (63 élucidés)[5]. Le rôle du lésé ou de toute cible potentielle est à cet égard primordiale.

1 FF 1991 II 948.
2 FF 2010 4275.
3 RS 311.0.
4 Source: OFS, http://www.bfs.admin.ch/bfs/portal/fr/index/themen/19/03/03/key/straftaten/gesetze.html.
5 Source: OFS, http://www.bfs.admin.ch/bfs/portal/fr/index/themen/19/03/02/key/02/01.html.

L'exploitant d'un système informatique a principalement des obligations de sécurité découlant de la Loi sur la protection des données[6] (art. 7 LPD) ou de normes particulières applicables à son secteur d'activité[7]. Son rôle est primordial pour éviter que des infractions ne soient commises ou d'en limiter le nombre et les conséquences[8], mais également pour transmettre les informations utiles aux autorités de poursuite pénales si une infraction a été commise. Il peut protéger ses droits, sur le plan juridique, en particulier à l'aide des dispositions pénales que nous allons examiner.

Plusieurs organismes sont susceptibles également de l'assister et fournissent des informations pratiques, en particulier le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI)[9] et la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)[10], ainsi que dans une moindre mesure la Prévention Suisse de la Criminalité (PSC)[11] et le Préposé fédéral à la protection des données et à la transparence (PFPDT)[12].

En ayant une meilleure compréhension du fonctionnement et des conditions d'application des instruments fournis par la législation pénale, la personne responsable de l'infrastructure informatique sera ainsi en mesure d'anticiper les problèmes liés à la poursuite, par exemple en s'assurant d'avoir mis en place une mesure de protection suffisante au sens de l'art. 143 CP au lieu de se contenter d'une interdiction morale[13].

Dans cette perspective, nous aborderons brièvement la question du droit applicable et du rattachement au droit suisse, puis nous centrerons notre contribution non pas sur les personnes lésées par la cybercriminalité ou sur le comportement des auteurs, mais sur la protection offerte par le CP à l'infrastructure informatique et notamment les art. 143 ss CP. Pour chaque infraction, les éléments constitutifs objectifs et subjectifs de l'infraction seront exposés de manière claire et précise, de même que les peines qui peuvent être prononcées et les problèmes particuliers qui peuvent se poser dans l'application de la partie générale.

Huit infractions typiques protègent les infrastructures informatiques et leur bonne utilisation: la soustraction de données (art. 143 CP), la soustraction de données personnelles (art. 179^{novies} CP), l'accès indu à un système informatique

6 RS 235.1.
7 Par exemple pour le domaine bancaire, art. 47 LB; voir également la décision de la FINMA in Bulletin 4/2013, 68 ss.
8 Des mesures de sécurité simples et le bon sens permettent de rendre la vie des criminels informatiques beaucoup plus difficile.
9 http://www.cybercrime.admin.ch.
10 http://www.melani.admin.ch.
11 http://www.prevention-criminalite.ch.
12 http://www.edoeb.admin.ch/?lang=fr.
13 Voir *infra* III.1.bb).

(art. 143bis al. 1 CP), la mise à disposition d'informations permettant l'accès indu à un système informatique (art. 143bis al. 2 CP), la détérioration de données (art. 144bis ch. 1 CP), la mise à disposition d'informations permettant la détérioration de données (art. 144bis ch. 2 CP), l'utilisation frauduleuse d'un ordinateur (art. 147 CP) et l'obtention frauduleuse d'une prestation (art. 150 CP).

II. Le droit applicable

Les délits informatiques posent plusieurs problèmes juridiques, notamment et en premier lieu s'agissant de la définition du droit applicable. L'art. 3 CP fait reposer l'application du droit pénal suisse sur le principe de la territorialité. L'art. 8 al. 1 CP précise qu'une infraction est réputée commise tant au lieu où l'auteur a agi, qu'au lieu où le résultat est survenu (principe de l'ubiquité). L'art. 31 du Code de procédure pénale suisse[14] (CPP) prévoit quant à lui un for au lieu où l'acte a été commis ou à l'endroit où le résultat s'est produit si le lieu de commission n'est pas situé en Suisse.

Le lieu où l'auteur a agi pose généralement peu de problèmes. Pour les infractions commises via des réseaux informatiques, on retient le lieu où se trouve l'auteur lorsqu'il transmet les ordres au système informatique[15] et non pas les lieux de situation des différents serveurs par lesquels les données transitent.

La détermination de la notion de résultat a suscité beaucoup plus de controverses pour les délits formels et divise la doctrine depuis des décennies, en particulier parce que les délits formels n'ont en principe pas de résultat[16]. On distingue en effet traditionnellement les délits entre les délits matériels (ou délits de résultat) et les délits formels (ou délits de comportement). Les premiers se composent d'un comportement incriminé et d'un résultat distinct modifiant matériellement l'état des choses, alors que les seconds sont réalisés par la seule violation de la disposition légale[17]. C'est l'adoption du comportement incriminé qui réalise le délit: la violation de domicile est consommée par l'introduction dans une maison à l'insu de son propriétaire, sans qu'il soit nécessaire que l'état de la maison en soit modifié.

14 RS 312.0.

15 Ou le lieu où les données sont chargées: arrêt du TF 8G.43/1999 du 11. 8. 2009, consid. 2a et b.

16 Pour un résumé, voir par exemple la décision de la cour des plaintes du Tribunal pénal fédéral du 24 janvier 2013 (BG.2012.37) et les références citées.

17 *P. Graven,* L'infraction pénale punissable, 2e éd., Berne 1995, 87 ss.

Alors que la doctrine majoritaire[18] estime que seuls les délits matériels, à l'exception des délits formels et de mise en danger abstraite, peuvent produire un résultat identifiable au sens technique, une autre partie de la doctrine considère que tous les types de délits produisent un résultat visible du monde extérieur[19]. Ce résultat au sens de l'art. 8 CP serait alors différent de la notion de résultat qui vaut dans la distinction entre délits formels et matériels. Un délit formel, soit un délit qui n'a pas de résultat matériel, pourrait néanmoins avoir un résultat au sens de l'art. 8 CP.

Ces interprétations divergentes de la notion de résultat ont des conséquences pratiques très différentes, puisque, selon la doctrine majoritaire, une infraction commise par le biais d'Internet ne pourra être poursuivie en Suisse que si l'auteur a agi en Suisse ou s'il s'agit d'un délit matériel produisant un résultat identifiable en Suisse[20]. Une telle interprétation conduit à réduire drastiquement la portée du droit suisse et de la protection qu'il apporte contre des actes dont la nature même fait qu'ils sont le plus souvent commis depuis l'étranger, voire d'un lieu inconnu.

A l'inverse, l'avis de la doctrine minoritaire conduit à admettre la compétence des autorités suisses et l'application du droit suisse dès lors qu'une infraction est commise contre une infrastructure suisse, sans qu'il soit nécessaire de connaître le lieu où se trouve l'auteur. Cette solution doit être retenue, d'autant qu'il ne s'agit pas d'une compétence universelle qui permettrait d'appliquer le droit suisse lorsqu'il n'y a qu'un vague rattachement.

Le Tribunal fédéral s'est rallié à la doctrine minoritaire et il convient désormais de retenir que la notion de résultat au sens de l'art. 8 CP ne correspond pas à son homonyme au sens technique utilisé en droit suisse dans la distinction entre les délits matériels et formels[21]. Le Tribunal fédéral a en effet considéré qu'un résultat au sens de l'art. 8 al. 1 CP peut se produire en Suisse pour certains délits for-

18 *A. Donatsch/B. Tag,* Strafrecht I, 8e éd, Zurich, 2006, 98; *S. Heimgartner,* Die Internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: C. Schwarzenegger/O. Arter/F. Joerg (éd.), Internet-Recht und Strafrecht, 4e éd., Berne 2005, 117 ss, 123; *H. Schultz,* Le lieu de commission, FJS 1960, 1, 3; *H. Schultz,* Neue Probleme des internationalen Strafrechts und des Auslieferungsrechtes, SJZ 1964, 84, 85; *C. Schwarzenegger,* Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Oesterreich, ZStrR 2000, 109, 120; *S. Trechsel,* Schweizerisches Strafrecht, Allgemeiner Teil I, 6e éd. Zurich 2004, 78; *E. Vögeli,* Strafrechtliche Verantwortlichkeit im Internet – einige Aspekte aus der Sicht der Praxis, in: C. Schwarzenegger/O. Arter/F. Joerg (éd.), Internet-Recht und Strafrecht, 4e éd., Berne 2005, 55, 66.

19 *G. Arzt,* Erfolgsdelikte und Tätigkeitsdelikte, ZStR1990, 168 ss; *Schwarzenegger* (n. 18), 109 ss; *F. Riklin,* Information Highway und Strafrecht, in: R. M. Hilty (éd.), Information Highway, Berne/Munich 1996, 579 ss.

20 *Schwarzenegger* (n. 18), 121.

21 ATF 133 IV 171, consid. 6.3; 128 IV 145, consid. 2.

mels commis à distance tels que la diffamation et l'abus de confiance[22]. Pour déterminer si le droit suisse s'applique, il faut donc se demander si le résultat pris en considération se trouve dans un rapport de connexité immédiate avec le comportement typique[23]. Si la réponse est positive, on admettra alors que ce résultat permet de fonder la compétence des autorités et l'application du droit suisses.

Ainsi dans le cas où un pirate informatique accède sans droit au site Internet d'une entreprise, on retiendra comme lieu de résultat au sens des art. 8 al. 1 CP et 31 CPP le lieu où se situent les serveurs. L'accès indu est en effet l'élément qui se trouve dans un rapport de connexité immédiate avec le comportement réprimé par l'art. 143bis CP[24]. A noter que le siège de l'entreprise ou le domicile de l'administrateur de la société ne pourront pas être retenus comme lieu de résultat. Celui qui veut profiter de la protection offerte par le droit suisse a donc tout intérêt à héberger ses données en Suisse.

III. Les infractions informatiques du code pénal suisse

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

Aux termes de l'art. 143 CP, «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'art. 143 al. 2 CP précise que la soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.

Si l'on veut faire une comparaison avec des données patrimoniales, la soustraction de données correspond à la notion de vol. On parle parfois également de «cracking».

L'infraction de soustraction de données implique donc la réalisation de cinq conditions, soit la soustraction (1.a.cc) intentionnelle (1.b.aa) et dans un dessein d'enrichissement illégitime (1.b.bb) d'une donnée informatique (1.a.aa) spécialement protégée (1.a.bb).

22 ATF 125 IV 177, consid. 3 pour la diffamation; 128 IV 145, consid. 2^{e}, et 124 IV 241, consid. 4d pour l'abus de confiance.

23 ATF 128 IV 145, consid. 2.

24 Décision de la Cour des plaintes du TPF BG.2012.37 du 24. 1. 2013, consid 2.1 et 2.2.2.

a) Les éléments constitutifs objectifs

aa) Une donnée informatique

Le code pénal ne définit pas la notion de données informatiques. Dans son Message, le Conseil fédéral faisait référence à des «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[25].»

Selon la STCE 185, les données informatiques constituent «toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction»[26], soit toute information qui peut faire l'objet d'une communication humaine par le biais de texte, image, musique, logiciel, etc.[27]

Les programmes ou les logiciels, soit les procédés permettant de traiter les données, ne constituent rien d'autre que des ensembles de données et doivent également être traités comme des données[28]. Les images et les sons enregistrés sous forme de données électroniques sont aussi des données au sens des art. 143 ss[29].

Une donnée est donc 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[30].

bb) Une donnée spécialement protégée contre tout accès indu

Une donnée informatique est d'abord spécialement protégée lorsqu'elle n'est pas destinée à la personne qui la soustrait ou l'intercepte[31]. Elle l'est ensuite surtout parce que certaines mesures ont été prises en faveur de sa protection. L'art. 143 CP

25 FF 1991 II 952.

26 Art. 1 de la Convention 185 sur la cybercriminalité du Conseil de l'Europe.

27 *J. Müller,* La cybercriminalité économique au sens étroit – Analyse approfondie du droit suisse et aperçu de quelques droits étrangers, RJL 2012, 32.

28 FF 1991 II 954; *G. Stratenwerth/G. Jenny/F. Bommer,* Schweizerisches Strafrecht, Besonderer Teil Band I, 7e éd., Berne 2010, § 14 N 24; *A. Donatsch,* Strafrecht III, 10e éd., Zurich 2013, 194; *S. Trechsel/D. Crameri,* in Praxiskommentar Strafgesetzbuch, Praxiskommentar, S. Trechsel/M. Pieth (éd.), 2e éd., Zurich/Saint-Gall 2013, art. 143 N 3.

29 Cf. notamment *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N. 57; *P. Weissenberger,* in: Basler Kommentar, Strafrecht II, M. A. Niggli/A. Wiprächtiger (édit.), 3e éd., Bâle 2013, art. 144bis N 7 et 8 *contra* Message du Conseil fédéral, in FF 1991 986 ss, 993, plus restrictif.

30 La notion d'ordinateur, comme celle de système informatique, doit être comprise dans un sens très large.

31 *B. Corboz,* Les infractions en droit suisse, vol. I, 3e éd., Berne 2010, art. 143 N 6; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 26; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143 N 5.

ne s'applique donc pas si la donnée en question est accessible à tous[32]. L'art. 143 CP ne vise pas à protéger les données de manière globale, mais seulement les données que le propriétaire ne veut pas laisser accessibles à l'auteur. Il ne doit pas être légitimé à disposer des données et il doit pouvoir reconnaître clairement que le titulaire des données ne veut pas qu'on y accède. Des mesures suffisantes de sécurité doivent notamment avoir été prises pour empêcher l'accès par un tiers aux données[33].

On n'exige en revanche pas que le propriétaire des données possède de meilleures compétences informatiques que l'auteur[34] (ce qui exclurait de fait toute application de l'art. 143 CP) et que la protection ait une efficacité particulière. La loi ne demande pas que le propriétaire des données soit un expert en sécurité informatique, mais simplement que l'auteur puisse reconnaître que les données sont protégées. Un code d'accès, un mot de passe, le codage des données ou bien encore le placement de celles-ci derrière un pare-feu est une protection suffisante[35]. Si l'auteur passe outre une barrière physique (une porte fermée à clé), la condition sera remplie[36].

Les instructions, les interdictions orales ou écrites, ou encore les mesures d'organisation visant à séparer les fonctions au sein du personnel ne constituent en revanche pas des mesures de sécurité suffisantes au sens de cette disposition[37]. Il n'y a ainsi pas de mesures suffisantes dans le cas d'un employé qui ne rencontre aucune mesure de sécurité spécifique lui entravant l'accès aux données détenues par son employeur, si ce n'est une barrière morale[38].

cc) Une soustraction

L'art. 143 CP exige que l'auteur soustraie une donnée informatique qui ne lui est pas destinée et qui est spécialement protégée.

La question est discutée en doctrine de savoir à quel moment la soustraction est consommée. Certains considèrent que l'auteur doit s'approprier les données dans le sens de pouvoir les modifier, les consulter à tout moment ou les imprimer[39]. D'autres considèrent que le simple fait d'accéder à une donnée de manière à

32 *Corboz,* I (n. 31), art. 143 N 6; *Müller* (n. 27), 32.
33 *Corboz,* I (n. 31), art. 143 N 7.
34 *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 28.
35 *Müller* (n. 27), 32.
36 Contrairement à l'art. 143bis CP, l'art. 143 CP ne fait pas mention d'un «dispositif de transmission de données», ce qui implique que la barrière peut s'opposer à n'importe quel moyen d'accès. Voir également *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143 N 6; *Corboz,* I (n. 31), art. 143 N 7.
37 *N. Schmid,* Computer- sowie Check- und Kreditkarten-Kriminalität, Schulthess, Zurich 1994, § 4 N 39.
38 TC VS RVJ 2006, 222.
39 *N. Schmid* (n. 37), § 4 N 47 ss; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143 N 7; *Donatsch* (n. 28), 197.

pouvoir ensuite l'utiliser suffit à réaliser l'infraction, par exemple en prenant connaissance de la donnée par une simple lecture à l'écran[40]. Cela nous paraît suffisant car le but de l'infraction est de punir la possibilité pour l'auteur d'exploiter la donnée en tant que telle plutôt que de priver le propriétaire de son utilisation. Dès lors que l'auteur de l'infraction a en sa maîtrise une copie de la donnée soustraite qu'il peut ensuite utiliser à sa guise, l'infraction est consommée[41]. Il nous paraît inopportun d'avoir des exigences sévères sur la forme de la copie. Celui qui affiche des données sur un écran pour les mémoriser et les reproduire ensuite les soustrait et réalise l'infraction. Les données soustraites seront ainsi téléchargées dans la mémoire vive, éventuellement la mémoire-cache du système informatique de l'auteur, ce qui réalise également l'infraction.

Certains auteurs considèrent que celui qui intercepte des données cryptées (entre deux ordinateurs par exemple) consomme l'infraction car il peut les décrypter ou les faire décrypter ultérieurement, et être ainsi en mesure de les utiliser[42]. On peut partager ce point de vue dans la mesure où la disposition légale ne pose pas d'exigence quant au format des données et que les données, même encryptées, restent des données[43].

Si l'auteur copie les données et les détruit de leur support original, il se rend coupable de soustraction de données et de détérioration de données au sens de l'art. 144bis CP (qui prend le pas sur l'art. 143 CP).

b) Les éléments constitutifs subjectifs

aa) L'intention

L'acte doit être commis intentionnellement[44], mais le dol éventuel suffit[45].

bb) Le dessein d'enrichissement illégitime

L'auteur doit en outre avoir agi avec un dessein d'enrichissement illégitime, c'est-à-dire avec la volonté de s'enrichir ou d'enrichir un tiers. L'enrichissement doit être compris au sens large et recouvre l'augmentation d'actif, la diminution de pas-

40 *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 30; *Corboz,* I (n. 31), art. 143 N 9.

41 *Müller* (n. 27), 33.

42 *Weissenberger,* in: BSK StGB II (n. 29), art. 143 N 25 et 26.

43 A tout le moins au sens des art. 143 ss CP. Il pourrait en aller différemment si la disposition légale protégeait des données personnelles au sens de la LPD car il faudra déterminer s'il s'agit toujours de données relatives à une personne identifiable.

44 *Corboz,* I (n. 31), art. 143 N 10; *Donatsch* (n. 28), 198; *N. Schmid* (n. 37), §4 N 65; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 n. 31; *G. Stratenwerth/W. Wohlers,* Schweizerisches Strafgesetzbuch, Handkommentar, 3^{e} éd., Berne 2013, art. 143 N 4; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143 N 8; *Weissenberger,* in: BSK StGB II (n. 29), art. 143 N 27.

45 *Corboz,* I (n. 31), art. 138 N 15 et les références citées.

sif, la non-diminution de l'actif et la non-augmentation du passif[46]. La notion englobe tous les avantages économiques perçus par l'auteur ou un tiers[47].

Si ce dessein d'enrichissement illégitime est absent, l'art. 143 CP n'est pas applicable, et l'art. 143bis CP pourrait alors trouver application à titre subsidiaire[48]. Dans le cas où les données volées sont des données personnelles ou des profils de la personnalité, l'acte pourrait être poursuivi au sens de l'art. 179novies CP, qui réprime la soustraction de données personnelles sensibles ou de profils de la personnalité au sens de la Loi sur la protection des données[49].

c) L'application de la partie générale

L'infraction est poursuivie d'office, sauf si elle est commise au préjudice des proches ou des familiers[50], auxquels cas une plainte sera nécessaire (art. 143 al. 2 CP). Dans ces cas, le législateur a considéré avec raison que la justice ne devait intervenir que si cela était souhaité par la victime.

L'infraction est passible d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

Un concours parfait peut en outre être retenu entre l'art. 143 CP et l'art. 179novies CP, car les biens juridiques diffèrent en ce que la première disposition protège le patrimoine, tandis que la seconde est relative à la protection du domaine secret. Celui qui soustrait des données informatiques contenant des données personnelles peut ainsi se rendre coupable tant de l'infraction de 143 CP que de 179novies CP[51].

On rappellera encore que les données informatiques ne sont pas des choses mobilières ou des valeurs patrimoniales, et sont donc exclues du champ d'application de l'art. 139 CP réprimant le vol[52] au profit de l'art. 143 CP. A l'inverse, un sup-

46 *Müller* (n. 27), 33.

47 *Corboz,* I (n. 31), art. 138 N 14; *Donatsch* (n. 28), 198; *Weissenberger,* in: BSK StGB II (n. 29), art. 137 ss N 78; *Stratenwerth/Jenny/Bommer* (n. 28), § 13 N 34; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 137 ss N 12 et 13.

48 *Corboz,* I (n. 31), art. 143 N 11.

49 RS 235.1, art. 3 lit. c et d; *Corboz,* I (n. 31), art. 179novies N 1; *Donatsch* (n. 28), 420; *Stratenwerth/Jenny/Bommer* (n. 28), § 12 N 73; *Stratenwerth/Wohlers* (n. 44), art. 179novies N 1; *Müller* (n. 27), 34.

50 Conformément à l'art. 110 al. 1 et 2 CP, le 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 sont considérés comme les proches d'une personne, tandis que les familiers d'une personne sont ceux qui font ménage commun avec elle.

51 *Müller* (n. 27), 34; *Corboz*, I (n. 31), art. 179novies N 13; *Donatsch* (n. 28), 421; *J. Hurtado Pozo,* Droit pénal, Partie spéciale, Bâle 2009, N 2365; *G. Monnier,* Le piratage informatique en droit pénal, sic! 2009, 141, 153; *Stratenwerth/Wohlers* (n. 44), art. 179novies N 4; *Weissenberger,* in: BSK StGB II (n. 29), art. 143 N 39, et *Wyder/von Ins,* in: BSK StGB II (n. 29), art. 179novies N 33.

52 *Corboz,* I (n. 31), art. 143 N 1.

port de données, tel qu'un CD-ROM ou un disque dur externe, est une chose mobilière, de sorte que celui qui, intentionnellement et dans un dessein d'enrichissement illégitime, soustrait un tel objet appartenant à autrui pour se l'approprier, que ce soit en vue de le conserver ou de l'aliéner[53], commet un vol[54]. On peut se demander si sa soustraction peut éventuellement aussi tomber sous le coup de l'art. 143 CP, applicable en concours.

La question n'a toutefois pas été tranchée par le Tribunal fédéral et fait l'objet d'une division au sein de la doctrine[55]. Certains auteurs considèrent en effet qu'il y a concours réel, dès lors que les biens juridiques protégés, soit respectivement le patrimoine et le droit du bénéficiaire légitime des données d'en disposer librement et conformément à sa volonté, sont différents[56]. D'autres voient un concours idéal entre les art. 139 et 143 CP lorsque le propriétaire du support et le propriétaire des données sont des personnes différentes[57], alors que d'autres encore pensent au contraire que lorsque la soustraction porte sur des supports matériels comportant des données, seul l'article 139 CP devrait trouver application[58].

Si l'on exclut le concours, cela signifie en quelque sorte que l'on fait abstraction du contenu du support informatique. Une clé USB ou un CD-ROM vaut tout au plus quelques francs, ce qui en ferait un vol de peu d'importance, alors que les données contenues peuvent avoir une valeur inestimable. Il nous paraît choquant que cela puisse exclure toute poursuite à l'échéance du délai de plainte ou qu'une simple amende puisse être prononcée. Un concours doit être retenu à notre avis, d'autant que celui qui vole un support de données le fera le plus souvent avec l'intention d'accéder au contenu, bien plus intéressant que le contenant.

Enfin, un concours est également envisageable avec l'art. 144 CP dans l'hypothèse où une porte a été fracturée[59] et avec l'art. 150 CP si l'auteur soustrait des données et lèse l'exploitant du montant à payer[60].

2. La soustraction de données personnelles (art. 179novies)

L'entrée en vigueur de la Loi fédérale du 19 juin 1992 sur la protection des données («LPD»)[61] a donné l'impulsion au législateur pour introduire une nouvelle

53 ATF 85 IV 17, consid. 1 p. 19.
54 ATF 128 IV 11; 111 IV 74, consid. 1 p. 75.
55 ATF 128 IV 11, consid. 2b.
56 *Corboz,* I (n. 31), art. 143 N 14; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 34.
57 *N. Schmid,* Das neue Computerstrafrecht, RPS 1995, 22, 29.
58 *Donatsch* (n. 28), 198–199; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143 N 10.
59 *Corboz,* I (n. 31), art. 143 N 14.
60 *Corboz,* I (n. 31), art. 150 N 41. Opinion contraire: *Hurtado Pozo,* Partie spéciale (n. 51), N 1333.
61 RS 235.1.

infraction dans le CP visant à réprimer la soustraction de données personnelles[62]. L'art. 179novies CP érige ainsi en infraction le comportement de «celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la personnalité qui ne sont pas librement accessibles» et implique donc la réalisation de quatre conditions.

a) Les éléments constitutifs objectifs

aa) Des données personnelles sensibles ou des profils de la personnalité

En premier lieu, l'art. 179novies CP suppose l'existence de données personnelles sensibles ou de profils de la personnalité au sens de l'art. 3 lit. c et d LPD.

Par «donnée personnelle», l'art. 3 lit. a LPD entend toutes les informations qui se rapportent à une personne (physique ou morale) identifiée ou identifiable. Les données personnelles ne sont protégées que si elles sont sensibles au sens de la LPD. Sont ainsi visées les données définies par l'art. 3 lit. c LPD portant sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'appartenance à une race, ou encore les données sur des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives. Le terme «profils de la personnalité» vise quant à lui un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique[63].

Les données personnelles peuvent dans certains cas également être des données informatiques (ce sera d'ailleurs le plus souvent le cas) ou alors être inscrites sur une chose mobilière (fichier papier, impression, etc.).

bb) Non destinées à l'auteur et spécialement protégées

Il s'agit de la même exigence que celle prévue à l'art. 143 CP[64].

cc) Une soustraction

Le comportement réprimé est une soustraction de données. La soustraction est réalisée dès que la donnée est à disposition de l'auteur et qu'il peut en prendre connaissance[65].

62 FF 1988 II 421, 496.

63 *Corboz,* I (n. 31), art. 179novies N 3 à 5.

64 Voir *supra* III. 1.a.bb.

65 *Donatsch* (n. 28), 419–420; *Stratenwerth/Jenny/Bommer* (n. 28), § 12 N 75; *Trechsel/Lieber,* in Praxiskommentar StGB (n. 28), art. 179novies N 6.

b) Les éléments constitutifs subjectifs

L'infraction suppose que l'auteur ait agi intentionnellement; le dol éventuel suffit.

c) L'application de la partie générale

L'infraction est poursuivie sur plainte de la personne dont les données personnelles sont atteintes et est punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire[66]. La question de savoir si l'exploitant du système, soit le maître du fichier, est également légitimé à déposer plainte est controversée en doctrine et n'a pas été tranchée par la jurisprudence[67]. Il faut à notre avis répondre par l'affirmative. Premièrement, le droit suisse ne connaît pas d'obligation d'annoncer les failles de sécurité, et le maître du fichier est souvent le seul à connaître l'existence de la soustraction. Si le législateur n'avait pas voulu permettre au maître du fichier de pouvoir également déposer plainte, il en aurait fait un délit poursuivi d'office. Deuxièmement, le maître du fichier est tenu d'assurer la protection des données (art. 7 LPD) par des mesures techniques et organisationnelles. En ce sens, l'art. 179^{novies} CP le protège dans son droit (et son obligation) de traiter des données personnelles conformément à la LPD et à prendre toutes les mesures pour protéger la personnalité des personnes dont il traite des données[68]. L'art. 179^{novies} CP peut être appliqué en concours avec l'art. 143 CP au vu des biens juridiquement protégés différents visés par ces deux dispositions. L'art. 143 CP protège en effet l'intérêt patrimonial de l'exploitant d'un ordinateur, alors que ce sont les droits fondamentaux des personnes visées par les informations contenues dans un fichier qui bénéficient de la protection de l'art. 179^{novies} CP[69].

3. L'accès indu à un système informatique (art. 143bis al. 1 CP)

L'accès indu à un système informatique peut être considéré comme l'équivalent informatique de la violation de domicile[70]. L'accès indu à un système informatique proprement dit (art. 143bis al. 1 CP) a été complété le 1er janvier 2012 par

66 *Stratenwerth/Jenny/Bommer* (n. 28), § 12 N 78; *Donatsch* (n. 28), 420; *Trechsel/Lieber,* in Praxiskommentar StGB (n. 28), art. 179^{novies} N 7.

67 *Corboz,* I (n. 31), art. 179^{novies} N 11; *Trechsel/Lieber,* in Praxiskommentar StGB (n. 28), art. 179novies N 7; *Donatsch* (n. 28), 420; *Stratenwerth/Jenny/Bommer* (n. 28), § 12 N 78.

68 *D. Rosenthal/Y. Jöhri,* Handkommentar zum Datenschutzgesetz, Zurich 2008, 794–795.

69 *Donatsch* (n. 28), 421

70 FF 1991 II 979.

l'introduction d'un alinéa 2 [71] qui vise la mise à disposition d'informations qui permettent l'accès indu.

On parle parfois aussi de «hacking» ou piratage informatique. Contrairement à la soustraction de données, le but de l'auteur n'est pas d'obtenir des informations, mais seulement d'être présent dans le système, d'avoir réussi à passer outre les interdits et se trouver au cœur de la forteresse. Ce comportement n'en est pas moins dangereux pour autant, car en agissant de la sorte, le pirate informatique peut ouvrir la voie à d'autres pirates et déjà créer des dommages conséquents[72]. Il viole également la limite posée par le propriétaire du système.

L'art. 143bis al. 1 CP punit d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire le comportement de 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.

Pour que l'accès indu à un système informatique soit réalisé, il faut être en présence de trois conditions, soit un accès indu (3.a.bb) et intentionnel (3.b) à un système informatique appartenant à autrui et spécialement protégé (3.a.aa). Un dessein d'enrichissement illégitime n'est pas nécessaire car il ne correspondrait que rarement aux motivations du pirate informatique[73].

a) Les éléments constitutifs objectifs

aa) Un système informatique appartenant à autrui et spécialement protégé

On entend par système informatique tous les types d'ordinateurs[74]. Il s'agit ainsi d'une installation technique traitant automatiquement des données, généralement sous forme de code[75] par opposition à un simple support de données[76]. L'art. 1 de la STCE 185 définit l'expression «système informatique» comme «tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données»[77]. C'est une notion large.

71 RO 2011 6293; FF 2010 4275.

72 En termes de réputation également, même si les entreprises ne sont (actuellement) en principe pas obligées d'annonce les failles de sécurité (*security breaches*).

73 Jusqu'au 31 décembre 2011, le texte de 143bis CP exigeait une absence de dessein d'enrichissement illégitime. Depuis l'entrée en vigueur de l'art. 2 de l'Arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité et la modification du Code pénal qui s'en est suivie (FF 2010 4321), une telle condition n'est plus nécessaire, et l'art. 143bis al. 1 CP s'applique dorénavant avec ou sans dessein d'enrichissement.

74 *Corboz,* I (n. 31), art. 143bis N 1.

75 FF 1991 II 951 ss; *N. Schmid* (n. 37), § 2 N 9 ss; *Weissenberger,* in: BSK StGB II (n. 29), art. 143bis N 9.

76 *Monnier* (n. 51), 142.

77 RS 0.311.43.

L'accès indu ne doit pas être confondu avec l'infraction de l'art. 143 CP, qui réprime la soustraction spécifique des données informatiques[78]. Une partie de la doctrine considère par exemple que celui qui pirate une disquette, un CD-ROM ou un DVD ne tombe pas sous le coup de l'art. 143bis CP, mais se rend uniquement coupable de soustraction de données au sens de l'art. 143 CP[79]. Cet avis peut être partagé uniquement si le support de données ne peut pas être qualifié de système informatique et que l'intention attribuée à l'auteur le permet. Finalement, une transmission de données interceptée ne fait pas l'objet de l'art. 143bis CP mais bien de l'art. 143 CP[80].

Le Tribunal fédéral a d'ailleurs retenu qu'une boîte aux lettres électronique devait être considérée comme un sous-système informatique composé d'un ensemble de données, dont la violation tombe donc sous le coup de l'art. 143bis CP[81]. Le mot de passe donne au titulaire non seulement le droit d'accéder à ses données contenues dans ses courriels, mais aussi à la partie du système informatique de traitement de données qui le concerne et lui permet de les administrer (sa boîte électronique et le système d'envoi/réception des messages, d'archivage, etc.). On pourrait donc dire d'une certaine manière que le compte e-mail n'est pas protégé pour lui-même, mais parce que celui qui le pénètre s'introduit également dans l'installation de traitement. Cette solution a été critiquée par une partie de la doctrine[82]. Elle a cependant l'avantage de permettre l'application de l'art. 143bis al. 1 CP qui n'exige pas de dessein d'enrichissement illégitime, contrairement à l'art. 143 CP qui pourrait être appliqué aux données des courriels.

Le système informatique doit appartenir à autrui. Il convient donc de déterminer qui a le droit d'accéder au système et d'en disposer[83]. La personne qui loue ou utilise un ordinateur qui lui a été prêté sera considérée comme l'ayant droit temporaire et bénéficiera de la protection de l'art. 143bis CP[84]. A moins que des droits d'accès particuliers n'aient été convenus, le propriétaire qui accède sans droit au contenu de l'ordinateur qu'il a donné en location se rend coupable de violation de l'art. 143bis CP. Il n'aurait pas non plus la qualité de lésé pour déposer une plainte pénale en cas d'accès par un tiers.

Le système informatique doit enfin être spécialement protégé contre tout accès grâce à une barrière informatique qui peut se concrétiser par la mise sur pied d'un codage, un chiffrement ou encore un code d'accès[85]. La protection est la même

78 Voir *supra* III.1.a.
79 *Monnier* (n. 51), 143–144.
80 FF 1991 II 952 et 978.
81 Arrêt du TF 6B_456/2007 du 18. 3. 2008.
82 Voir notamment *Monnier* (n. 51), 144.
83 *Monnier* (n. 51), 143; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 39.
84 *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 39.
85 *Monnier* (n. 51), 145.

que celle de l'art. 143 CP, sous une réserve. Les barrières physiques, telle qu'une porte (même fermée à clé), ne sont pas suffisantes au sens de l'art. 143bis CP[86]. Cet article exige en effet que l'accès se fasse au moyen d'un dispositif de transmission de données, ce qui implique que la protection doit empêcher un accès par ce moyen. Sont visées ainsi dans le cadre de l'art. 143bis CP des barrières informatiques mises en place spécifiquement pour contrer des attaques externes du même type[87].

L'efficacité de la barrière n'a en revanche que peu d'importance, au vu des prouesses techniques sans cesse développées par les pirates informatiques, sauf à conclure que le dispositif mis en place est de si peu d'efficacité qu'elle s'apparente à une absence pure de protection[88].

La doctrine est divisée sur la question de savoir si l'ingénierie sociale peut réaliser l'infraction de l'art. 143bis CP. On entend par ingénierie sociale l'utilisation de procédés tels que l'envoi de courriels de «phishing» ou hameçonnage, visant à tromper une personne, notamment en se faisant passer pour quelqu'un d'autre, afin d'obtenir des informations utiles pour s'introduire ensuite dans les systèmes informatiques dont celle-ci est l'ayant droit[89]. Une partie de la doctrine est d'avis que l'infraction n'est pas réalisée par l'adoption d'un tel comportement, car la transmission volontaire des données par la victime, même due à une erreur sur le destinataire, ne fait tomber aucune barrière technique et ne résulte pas d'un procédé informatique[90].

Toutefois, l'exclusion systématique de l'ingénierie sociale au profit de la seule ingénierie technique peut aboutir à des résultats choquants[91]. A notre avis, l'ingénierie sociale réalise l'infraction dans le cas où elle vise à faire tomber une barrière technique ou lorsque son résultat permet de faire tomber une barrière. Ainsi, l'ensemble des démarches visant à obtenir les informations qui permettront ensuite de contourner les mesures de protection ou d'obtenir par une voie détournée le mot de passe (par exemple la réponse à une question secrète qui permet de récupérer le

86 Elles peuvent l'être au sens de l'art. 143CP.

87 *Monnier* (n. 51), 144.

88 Dans ce sens, voir *Monnier* (n. 51), 145.

89 *M. Amman,* Sind Phishing-Mails strafbar?, PJA 2006, 195, 198; *Weissenberger,* in: BSK StGB II (n. 29), art. 143bis N 19; *Monnier* (n. 51), 147; *Müller* (n. 27), 84 ss.

90 *Monnier* (n. 51), 147.

91 Voir le cas «Hacker Croll», du surnom d'un pirate informatique français qui s'est introduit depuis la France dans des comptes d'employés de Twitter, dont celui d'Evan Williams, l'un de ses fondateurs. Ce cas de figure serait théoriquement resté impuni en Suisse si l'on retient que l'art. 143bis CP ne réprime que l'ingénierie technique. En effet, Hacker Croll a eu accès aux comptes Paypal, Amazon, Apple, AT&T, MobileMe et Gmail de certains employés par recoupements d'informations privées récoltées sur Internet (le nom sur tel site, la date de naissance sur tel autre, etc.) et la constitution de profils, dont il finissait par déduire un login et un mot de passe, notamment en utilisant le mécanisme de la question secrète. Cf. *G. Monnier,* Le hacking: enjeux actuels à la lumière du cas «Hacker-Croll», Medialex 2010, 130.

mot de passe) remplissent la condition de l'accès sans droit à un système informatique. En revanche, si le détenteur du mot de passe l'a volontairement transmis, y compris à une personne qu'il pensait être une autre, on doit malheureusement admettre qu'aucune barrière n'est tombée et qu'il faudra considérer l'application d'autres dispositions légales, par exemple l'escroquerie (art. 146 CP).

bb) L'accès sans droit

Le comportement punissable consiste à pénétrer un système informatique en détournant les sécurités et barrières informatiques prévues par l'ayant droit[92]. Il va de soi que la violation d'un local dans lequel se trouve un système informatique ne suffit pas encore à réaliser l'infraction de l'art. 143bis CP. La notion d'accès sans droit s'entend ainsi uniquement d'un accès informatique à un système et non un accès réel, comme l'accès à une salle de serveurs[93].

Le texte de l'art. 143bis CP parle de «s'introduire», tandis que la note marginale utilise le terme d'«accéder»[94]. 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. Comme il s'agit d'un accès à distance, il est aussi difficile de délimiter ce qui serait à l'intérieur et à l'extérieur. Le terme d'«accès» est ainsi à préférer, mais il faut alors préciser à partir de quel moment celui-ci intervient, ce qui est moins évident à définir que le moment d'une introduction physique en un lieu. On peut retenir qu'il y a accès dès que les données du système informatique sont «visibles» et utilisables par l'auteur[95]. Il ne s'agira évidemment pas des données «externes» que constituent la barrière, mais tout ce qui se trouve protégé, autrement dit ce qui est «derrière» ou au-delà de cette protection.

Le texte légal exige pour le surplus que l'accès intervienne par le biais d'un dispositif de transmission de données. La notion est large et doit être interprétée comme telle, le législateur ayant voulu mettre en exergue le caractère informatique du délit, soit le fait d'accéder à un système via un procédé informatique. Les systèmes de communication, avec ou sans fil[96], tels que le réseau Internet par exemple, sont considérés comme de tels dispositifs.

Le comportement visé par l'accès indu à un système informatique protège l'installation technique du système informatique mais également le traitement et la transmission des données. Ce qui est déterminant est donc le droit d'accéder au

92 *Hurtado Pozo,* Partie spéciale (n. 51), N. 1062, p. 319; *Corboz,* I (n. 31), art. 143bis N 4; *Donatsch* (n. 28), p. 201; *Weissenberger,* in: BSK StGB II (n. 29), art. 143bis N 4.

93 *Monnier* (n. 51), 145.

94 FF 1991 II 979.

95 Dans ce sens, *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 40.

96 *Monnier* (n. 51), 146.

système informatique, pas le droit de disposer des données[97]. L'accès doit avoir été effectué sans droit, c'est-à-dire qu'il n'a pas été autorisé par la loi, par le consentement de la victime ou par un autre motif justificatif[98]. Le consentement de la victime autorise donc le hacking éthique. Il faut néanmoins rester prudent sur la portée du consentement et l'étendue des systèmes pour lesquels la «victime» à la capacité de consentir[99].

Finalement, on relèvera encore qu'en cas d'utilisation de «Government Software», soit d'un système de surveillance de type «cheval de Troie» placé dans un téléphone ou un ordinateur relié à un réseau de communication (Internet par exemple), le futur art. 269bis CPP servira de fait justificatif[100].

b) L'élément constitutif subjectif

L'acte doit être intentionnel, mais le dol éventuel suffit[101].

Une partie de la doctrine considère que celui qui entre dans un système à la suite d'une erreur de manipulation de sa part et qui décide ensuite d'y rester et d'explorer n'y a pas accédé intentionnellement[102]. L'intention manquerait en effet de passer outre la barrière, à moins que l'infraction ne soit commise par dol éventuel. Il nous semble cependant que celui qui continue d'explorer et d'accéder à différentes parties du système réalise l'infraction, car il sait qu'il accède à des parties du système qui lui sont défendues.

c) L'application de la partie générale

L'accès indu à un système informatique proprement dit est poursuivi sur plainte. Il est passible d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

L'art. 143bis CP est une disposition subsidiaire par rapport aux autres infractions qui nécessitent une introduction dans le système, tels que les art. 143, 144bis et 147 CP. En outre, il convient de garder à l'esprit que l'art. 143bis CP protège les systèmes informatiques, alors que l'art. 143 CP protège les données. La limite entre ces deux dispositions est parfois ténue et elle s'effectuera souvent en déterminant

97 Arrêt du Tribunal fédéral 6B_456/2007 du 18 mars 2008.

98 *Corboz,* I (n. 31), art. 143bis N 9 et 10.

99 Il y aura souvent plusieurs systèmes et sous-systèmes, ce qui imposerait le consentement de multiples personnes et pourrait enlever tout intérêt à la démarche de hacking éthique.

100 Même si cela est à notre avis déjà couvert par l'art. 280 CPP (cf. *O. Jotterand/J. Müller/J. Treccani,* L'utilisation du cheval de Troie comme mesure de surveillance secrète, Jusletter 21, mai 2012, *contra: T. Hansjakob,* Einsatz von GovWare zulässig oder nicht?: zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie, Jusletter. – 1er novembre 2011).

101 *Corboz,* I (n. 31), art. 143bis N 11.

102 *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 143bis N 9.

quelle intention poursuivait l'auteur. Si sa motivation résulte d'un précepte tel que «*hackito ergo sum*»[103], l'auteur est mu par le seul désir de défier les limites technologiques et de montrer ses compétences. Il ne s'agira donc pas d'une soustraction de données au sens de l'art. 143 CP, mais son action tombera plutôt sous le coup de l'art. 143bis CP. Si c'est l'obtention de données qui le motive, accompagnée d'un dessein d'enrichissement illégitime, alors on tombera dans le champ d'application de l'art. 143 CP.

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

a) Les éléments constitutifs objectifs

L'art. 143bis al. 2 CP punit d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire quiconque 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'art. 143 al. 1 CP. Dès lors que la commission de l'infraction de l'art. 143bis CP nécessite d'avoir les outils de piratage pour accéder indûment à des systèmes informatiques, cela crée inévitablement un marché noir de la production et de la distribution de tels outils. Pour contrer efficacement ce risque à la source, l'art. 143bis al. 2 CP interdit certains actes spécifiques préalables à la commission de l'infraction visée à l'art. 143bis al. 1 CP[104].

L'art. 143bis al. 2 CP suppose donc la réalisation de trois conditions, soit rendre intentionnellement (4.b) accessibles des informations (4.a.aa et 4.a.bb) qui permettent l'accès indu (4.a.cc).

aa) Un mot de passe, un programme ou toute autre donnée

L'élément visé par l'art. 143bis al. 2 CP est un mot de passe, un programme ou toute autre donnée propre et destinée à être utilisée dans le but de commettre une infraction visée à l'al. 1.

Cette définition correspond à celle de l'art. 6 de la STCE 185, qui réprime la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition (i) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 de la STCE 85, ou (ii)

103 «*Je hacke donc je suis*».

104 Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité ad art. 6.

d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique.

Sont visés par cette définition, en plus des listes de mots de passe, des programmes qui sont objectivement conçus dans le but d'altérer ou détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques.

bb) La mise à disposition

Sont punis les actes visant à mettre en circulation ou rendre accessibles les données décrites ci-dessus. Cela implique à notre sens le fait de produire, vendre, obtenir pour utilisation, importer ou diffuser sous toutes ses formes les données concernées.

L'infraction est réalisée dès que les informations sont rendues accessibles. Il s'agit donc d'une infraction de mise en danger abstrait.

cc) Les actes punissables de l'al. 1

Les informations mises à disposition doivent pouvoir être utilisées pour commettre les actes réprimés par l'al. 1. Que l'infraction de l'art. 143bis al.1 CP soit effectivement commise ou non ne joue aucun rôle. Il suffit que les informations soient propres à commettre l'infraction de l'al. 1.

b) L'élément constitutif subjectif

L'infraction est intentionnelle, mais le dol éventuel suffit[105]. L'auteur doit vouloir ou accepter le fait que les informations seront ou pourront être utilisées dans le but de commettre une infraction visée à l'art. 143bis al. 1 CP.

c) L'application de la partie générale

Comme il s'agit d'un délit de mise en danger abstrait, la mise à disposition d'informations permettant de commettre l'infraction de l'art. 143bis al. 1 est poursuivie d'office, contrairement à l'accès indu à un système informatique proprement dit qui est poursuivi sur plainte.

L'accès indu et la mise à disposition d'informations permettant l'accès indu sont passibles de la même peine, soit une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

105 *Corboz,* I (n. 31), art. 143bis N 11.

5. La détérioration de données proprement dite (art. 144bis ch. 1 CP)

L'art. 144bis CP regroupe deux infractions: la détérioration proprement dite (ch. 1) et la production ou la mise en circulation de programmes de détérioration (ch. 2). Cette disposition vise de manière large tous les actes de sabotage informatique qui peuvent être commis dans le cyberespace. Elle correspond aux dommages à la propriété pour les choses mobilières.

a) Les éléments constitutifs objectifs

Aux termes de l'art. 144bis ch. 1 CP, «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.

Cette disposition suppose la réalisation de trois éléments constitutifs objectifs, soit la détérioration (5.a.bb) intentionnelle (5.b) et sans droit (5.a.cc) d'une donnée informatique (5.a.aa).

aa) Une donnée informatique

La notion de donnée informatique est identique à celle visée à l'art. 143 CP[106].

L'auteur de l'infraction doit porter atteinte à des données stockées sur des supports informatiques ou transférées par le biais d'un mode informatique, y compris les données enregistrées sur des supports externes, tels que par exemple des clés USB, des disques durs externes. Toutes les données électroniques sont protégées par l'art. 144bis CP, y compris les images et les sons enregistrés sous forme de données électroniques[107]. En revanche, les documents imprimés, même s'ils sont issus de données informatiques, ne sont plus sur un support informatique et ne sont donc plus protégés par l'art. 144bis ch. 1 CP[108]. Le fait qu'elles aient été imprimées n'empêche évidemment pas l'application de l'art. 144bis ch. 1 CP aux données qui sont toujours sur le support électronique. Les documents imprimés ne figurant plus sur des supports informatiques peuvent en revanche tomber sous le coup des art. 139 ou 144 CP.

106 Voir *supra* III.1. a. aa).

107 *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 3; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 57; *Weissenberger,* in: BSK StGB II (n. 29), art. 144bis N 8. Avis contraire: *Corboz,* I (n. 31), art. 144 bis N 3, qui est plus restrictif.

108 *Corboz,* I (n. 31), art. 144bis N 3.

L'art. 144bis CP n'exige aucune mesure de protection[109]. Dans ce sens, il a un champ d'application plus large que l'art. 143 CP. Cela se justifie car le Code pénal criminalise l'accès à des données protégées (dont l'auteur ne veut pas qu'elles puissent être consultées) et la détérioration de toutes les données (protégées ou non), de la même manière que la violation de domicile exige un élément de protection, alors que l'atteinte à la propriété a lieu que le site soit clôturé ou non, même en l'absence d'une protection.

bb) La détérioration

En second lieu, l'art. 144bis ch. 1 CP exige que l'auteur ait modifié, effacé, ou mis hors d'usage les données informatiques[110]. Cela recouvre toutes les atteintes autres que la consultation.

Une modification peut intervenir de quelque manière que ce soit[111]. Une donnée est considérée comme effacée dès qu'elle a été supprimée et a disparu du support sur lequel elle se trouvait, indépendamment de la question de savoir si elle peut potentiellement être récupérée au moyen d'une intervention technique, si une copie existe sur un autre support, etc.[112] Quant à la mise hors d'usage, on entend par là l'inaccessibilité soudaine d'une donnée, même pour une durée limitée[113].

Dans le cas du défacement[114] d'un site web, les données présentes sur le serveur ne sont en principe pas supprimées. L'art. 144bis CP s'applique néanmoins car, même s'il n'y a pas de destruction des données sur le serveur, le code HTML de la page d'accueil est soit remplacé, soit modifié[115]. En parallèle, des atteintes à l'honneur et une violation de la Loi sur la concurrence déloyale (LCD)[116] sont envisageables.

109 *Corboz,* I (n. 31), art. 144bis N 2.

110 *Corboz,* I (n. 31), art. 144bis N 4; *Donatsch* (n. 28), 212; *Hurtado Pozo,* Partie spéciale (n. 54), N 1121; *N. Schmid* (n. 31), § 6 N 24; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 60; *Stratenwerth/Wohlers* (n. 44), art. 144bis N 1; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 4; *Weissenberger,* in: BSK StGB II (n. 29), art. 144bis N 17.

111 *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 5; *Corboz,* I (n. 31), art. 144bis N 5.

112 *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 6; *Corboz,* I (n. 31), N 5 ad art. 144bis.

113 *Corboz,* I (n. 31), art. 144bis N 5; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 7.

114 On parle de défacement d'un site web lorsque la page d'accueil d'un site web est remplacée par une autre en utilisant les failles présentes sur une page Web ou une faille du système d'exploitation du serveur. La plupart du temps, les sites défacés le sont uniquement sur la page d'accueil.

115 L'auteur ajoute la nouvelle page et «désactive» l'ancienne.

116 RS 241.

cc) L'illicéité

L'auteur doit pour le surplus agir sans droit, en général contre la volonté expresse ou présumée de l'ayant droit, ou sans autorisation légale, sur des données dont il ne pouvait disposer seul[117].

La condition de l'illicéité fait défaut dans certains cas. Ainsi, lorsque l'auteur est propriétaire ou locataire de la machine utilisée et qu'il peut librement utiliser les données qu'elle contient, lorsqu'il peut disposer librement de ses propres fichiers au sein d'une entreprise ou qu'il est autorisé à disposer de fichiers de tiers par le bénéfice de directives expresses ou tacites, de telles situations constituent des cas licites n'entrant pas dans le champ d'application de l'art. 144bis CP[118]. Il en va de même lorsque des supports de données sont saisis ou confisqués durant une instruction pénale ou une procédure judiciaire, ainsi que dans l'hypothèse où une donnée est modifiée par un préposé au registre officiel sur impulsion d'un jugement exécutoire[119].

b) L'élément constitutif subjectif

L'infraction est intentionnelle[120], mais le dol éventuel suffit.

Une simple erreur de manipulation ne réalisera donc pas l'infraction, puisque l'élément subjectif fait défaut.

Aucun dessein spécifique n'est en outre exigé par le législateur[121].

c) L'application de la partie générale

L'infraction de l'art. 144bis ch. 1 CP est poursuivie sur plainte uniquement et est passible d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Toutefois, la peine privative de liberté peut être plus élevée en cas de dommage considérable causé à la victime (art. 144bis ch. 1 al. 2 CP), soit lorsqu'un dommage excédant CHF 10 000.– est constaté[122]. Dans cette hypothèse, la poursuite s'effectuera d'office. Cette solution fait écho à celle prévue à l'art. 144 al. 3 CP, réprimant de manière plus sévère les «dommages considérables» causés à la propriété.

117 *Corboz,* I (n. 31), art. 144bis N 8.
118 *Corboz,* I (n. 31), art. 144bis N 9.
119 *Corboz,* I (n. 31), art. 144bis N 10.
120 *Corboz,* I (n. 31), art. 144bis N 11; *Donatsch* (n. 28), 213; *Hurtado Pozo,* Partie spéciale (n. 51), N 1129; *N. Schmid* (n. 37), § 6 N 40; *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 61; *Stratenwerth/Wohlers* (n. 44), art. 144bis N 2; *Trechsel/Crameri*, in Praxiskommentar StGB (n. 28), ad art. 144bis N 9; *Weissenberger,* in: BSK StGB II (n. 29), art. 144bis N 38.
121 *Müller* (n. 27), 38.
122 Arrêt du TF 6B_202/2010 du 31. 5. 2010, consid. 4.3.1.

L'art. 144bis CP peut être appliqué en concours avec l'art. 144 CP relatif aux dommages à la propriété lorsque le support de données est lui aussi endommagé par le comportement de l'auteur[123], ou avec l'art. 139 CP lorsque le support est volé.

Un concours est également possible selon nous entre l'art. 144bis CP et l'art. 143 CP réprimant la soustraction de données, car les biens protégés par ces deux dispositions sont différents, l'un étant l'intégrité des données, tandis que l'autre tend à éviter le pillage des données[124]. La doctrine est partagée et s'est pour l'instant contentée d'aborder la question de manière superficielle[125]. Une partie des auteurs estime qu'il y a concours imparfait en faveur de l'art. 143 CP, lorsque les données ne sont plus à disposition du bénéficiaire à la suite d'une destruction résultant de la soustraction de données[126]. D'autres auteurs[127], auxquels nous nous rallions, envisagent plutôt un concours parfait au vu des buts différents des art. 144bis et 143 CP. Un concours doit à notre sens être admis puisqu'une soustraction de données n'est pas accompagnée dans tous les cas d'une détérioration de données et inversement.

En revanche, dans la mesure où l'accès aux données est nécessaire à leur détérioration, l'art. 144bis CP absorbe l'infraction de l'art. 143bis CP, et aucun concours n'est possible[128].

6. La mise à disposition d'informations permettant la détérioration de données (art. 144bis ch. 2 CP)

a) Les éléments constitutifs objectifs

L'art. 144bis ch. 2 CP réprime les actes préparatoires à l'endommagement de données informatiques. Est visée ici la mise en danger abstraite des données informatiques par des logiciels de détérioration dits virus informatiques[129]. Le bien juridiquement protégé par cette disposition est l'intérêt de l'ayant droit à utiliser ses données sans perturbation[130].

123 *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 70; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 20; *Donatsch* (n. 28), 213–214; *Corboz,* I (n. 31), art. 144bis N 15.

124 *Corboz,* I (n. 31), art. 144bis; *Donatsch* (n. 28), 213.

125 *A. Baltisser,* Datenbeschädigung und Malware im Schweizer Strafrecht – Der Tatbestand des Art. 144bis StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, Zurich 2013, 129 et 130.

126 *N. Schmid* (n. 37), § 6 N 75.

127 *Donatsch* (n. 28), p. 213; *Weissenberger,* in: BSK StGB II (n. 29), art. 144bis N 79.

128 *Corboz,* I (n. 31), art. 144bis N 16; *Donatsch* (n. 28), 214.

129 *B. Perrin,* La protection pénale des données informatiques de l'entreprise, ECS 2011, 605, 607.

130 ATF 129 IV 231, consid. 2.1.1.

La loi prévoit ainsi que «celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des indications en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Cette disposition suppose la réalisation de trois conditions, soit la «mise à disposition» (6.a.bb) intentionnelle (6.b) d'un logiciel permettant de réaliser l'infraction de l'al. 1 de (6.a.aa).

aa) Un logiciel de détérioration

La loi exige en premier lieu que l'objet mis à disposition soit un logiciel propre et destiné à provoquer une détérioration de données informatiques au sens de l'art. 144bis ch. 1[131].

Il s'agit principalement d'un virus informatique. La notion de virus informatique doit être considérée de manière large, et il n'est pas nécessaire que le logiciel revête un effet reproductif, ni qu'il cible un programme particulier ou une personne déterminée. Un logiciel qui permet exclusivement de consulter des informations n'entre pas dans cette catégorie. En revanche, on peut admettre que ce sera le cas de celui qui permet de prendre le contrôle à distance d'une machine car la prise de contrôle induira la modification de données.

Il n'est pas pertinent à cet égard de savoir si l'infraction à l'art. 144bis ch. 1 CP a été commise ou non.

bb) Les actes punissables

Le comportement réprimé par l'art. 144bis ch. 2 CP est la fabrication, l'importation, la mise en circulation, la promotion, l'offre ou toute autre manière de rendre accessible un logiciel de détérioration.

L'incitation à la fabrication de logiciels aptes à détériorer des données est réalisée dès que les informations, les instructions et les moyens permettant la fabrication de virus informatiques exécutables respectivement opérationnels et aptes à détériorer des données sont fournis[132].

De telles instructions ne doivent pas nécessairement revêtir un caractère exhaustif: le potentiel de mise en danger est d'autant plus grand lorsque des connaissances techniques ne sont pas indispensables[133].

131 *Stratenwerth/Jenny/Bommer* (n. 28), § 14 N 63 ss; *Donatsch* (n. 28), 214; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 144bis N 13; *Corboz,* I (n. 31), art. 144bis N 18.

132 ATF 129 IV 233, consid. 3.1 et 4.1.

133 Jurisprudence dite «Hacker CD-Rom III»: arrêt rendu par l'OGer ZH le 3 octobre 2002, consid. V.B.a/1-4, 6.4, 8, publié in sic ! 2003, 239.

Celui qui fournit des indications permettant de fabriquer un virus informatique est également punissable. Le législateur a voulu inclure dans les comportements incriminés l'instigation ou la complicité, qui a donc été érigée en infraction distincte[134].

b) L'élément constitutif subjectif

L'infraction est intentionnelle, mais le dol éventuel suffit.

L'auteur doit ainsi vouloir ou à tout le moins accepter le fait que le programme puisse être utilisé à des fins de détérioration des données. Une jurisprudence cantonale de 2002 a confirmé que le dol éventuel doit en principe être admis lorsque des logiciels aptes à détériorer des données, fabriqués et distribués uniquement au sens de l'art. 144bis ch. 2 CP, sont divulgués sans que leur usage ne soit contrôlé [135].

c) L'application de la partie générale

Contrairement à l'art. 144bis ch. 1 CP, l'infraction au sens du ch. 2 est poursuivie d'office. La loi dispose que celui qui se rend coupable d'actes préparatoires à l'endommagement de données informatiques sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Lorsque la circonstance aggravante du métier s'applique, le juge peut prononcer une peine privative de liberté de un à cinq ans.

Les ch. 1 et 2 de l'art. 144bis CP peuvent s'appliquer en concours si l'auteur utilise un virus pour détruire des données et le met ensuite à disposition d'autrui. La doctrine dominante considère en outre que l'auteur qui importe ou fabrique un virus pour l'utiliser lui-même réalise également les deux infractions en concours[136].

7. L'utilisation frauduleuse d'un ordinateur (art. 147 CP)

Le législateur a entendu réprimer à l'art. 147 CP l'«escroquerie informatique» couvrant la manipulation frauduleuse de données dans le but de s'enrichir illégitimement en influençant le résultat d'un système informatique. L'infraction est consommée lorsque tous les éléments constitutifs objectifs et subjectifs sont remplis.

134 ATF 129 IV 231, consid. 2.1.1.

135 Jurisprudence dite «Hacker CD-Rom III»: arrêt rendu par l'OGer ZH le 3 octobre 2002, publié in sic! 2003, 239.

136 *Corboz,* I (n. 31), art. 144bis N 24 et références citées.

a) Eléments constitutifs objectifs

aa) Une utilisation incorrecte, incomplète ou indue des données

Contrairement aux cas d'escroquerie, où l'auteur est puni pour avoir trompé une personne, l'art. 147 CP vise les situations dans lesquelles une personne fausse les conditions déterminant la réaction normale d'une machine informatique en adoptant un comportement condamné par la loi. Les comportements réprimés peuvent se concrétiser de diverses manières, énumérées ci-après.

– L'utilisation des données de manière incorrecte

La première situation visée constitue l'introduction par l'auteur de fausses données dans un ordinateur ou un programme. On peut penser par exemple à l'insertion d'un faux numéro de code ou de compte[137].

– L'utilisation des données de manière incomplète

L'auteur commet également un des comportements réprimés par l'art. 147 CP lorsqu'il omet volontairement d'indiquer toutes ou certaines informations nécessaires[138].

– L'utilisation des données de manière indue

L'auteur utilise des données authentiques mais sans y être autorisé, par exemple en usurpant l'identité de sa victime pour tromper les systèmes de contrôle sur sa véritable identité, ou en utilisant le code d'accès d'autrui pour s'introduire dans un système[139]. La jurisprudence a ainsi retenu le mécanisme visant à faire une copie de bandes magnétiques de cartes de crédit originales lors d'une utilisation régulière de celles-ci par leurs détenteurs légitimes, pour procéder ensuite à des transactions[140].

– Un procédé analogue

Enfin, le législateur a entendu laisser un champ d'application évolutif pour punir les comportements résultant de «procédés analogues». Il s'agit d'une formule générale qui permettra d'englober le cas échéant l'utilisation frauduleuse issue de développements de la technique[141].

137 ATF 129 IV 315, consid. 2.1; *Corboz,* I (n. 31), art. 147 N 4; *Donatsch* (n. 28), 249; *Hurtado Pozo,* Partie spéciale (n. 51), N 1236; *Müller* (n. 27), 39.

138 *Corboz,* I (n. 31), art. 147 N 5; *Donatsch* (n. 28), 249; *Hurtado Pozo,* Partie spéciale (n. 51), N 1237; *N. Schmid* (n. 37), § 7 N 54 ss; *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 6; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 147 N 5; *Müller* (n. 27), 39.

139 Arrêt du TF 1P.454/2005 du 9. 11. 2005.

140 Arrêt du TF 1P.454/2005 du 9. 11. 2005.

141 *Müller* (n. 27), 39.

bb) Une influence sur le processus électronique

L'auteur doit ensuite avoir une influence sur le processus électronique. Cet élément constitue le pendant de l'erreur provoquée par la tromperie pour l'escroquerie, à la différence près qu'il n'est ici pas exigé d'astuce.

La doctrine relève de nombreuses cibles potentielles d'une utilisation indue de données informatiques et cite, outre les automates distributeurs d'argent et les systèmes de paiement sans espèces (comme par exemple EC-Direct et Postcard), les procédés permettant d'effectuer en particulier des transactions bancaires à distance, les systèmes de débit automatique, ainsi que tous ceux qui permettent l'accès, au moyen de codes, à des banques de données payantes[142], comme par exemple celles permettant d'accéder à des services de téléphonie[143].

L'art. 147 CP concerne en outre également des situations dans lesquelles l'auteur est un employé ou un organe de l'entreprise usant de mauvaise foi de données auxquelles il a accès au préjudice de sa propre entreprise, par exemple pour accéder à des services téléphoniques payants. L'auteur doit pour accéder à ce genre de services violer des codes de clearing ou des fichiers hébergés dans des serveurs de sociétés de télécommunication, ou encore avoir recours à des codes et numéros de cartes appartenant à autrui. Les comportements de ce type sont donc punissables[144].

cc) Un résultat inexact

La loi exige en troisième condition que le comportement de l'auteur aboutisse à un comportement inexact de la machine[145].

dd) Un transfert d'actifs ou sa dissimulation

La manipulation doit ensuite aboutir à un transfert d'actifs ou à sa dissimulation. Tel est le cas, par exemple, lorsque l'argent passe d'un compte bancaire à un autre ou que l'auteur arrive à retirer de l'argent à un bancomat d'un compte appartenant à autrui. L'emploi illégal d'une carte de bancomat par une personne non autorisée aboutissant à un traitement informatique ou à une transmission de données inexactes est en effet un cas d'application typique de l'art. 147 CP[146]. Dès lors, tombe sous le coup de l'art. 147 CP celui à qui la banque donne, à la suite d'un faux changement d'adresse, le numéro de compte d'un homonyme et qui, en s'appuyant sur

142 *N. Schmid* (n. 37), § 7 N 61 ss.
143 ATF 129 IV 315 = JdT 2005 IV p. 9.
144 *N. Schmid* (n. 37), § 7 N 61 ss.
145 *Corboz,* I (n. 31), art. 147 N 9; *N. Schmid* (n. 37), § 7 N 80; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 147 N 8; *Müller* (n. 27), 39.
146 Arrêt du TF 6S.247/2001 du 10. 5. 2001.

cet élément pour faire croire à la banque qu'il est le titulaire du compte, fait en sorte d'obtenir une carte valable lui permettant de retirer de l'argent[147].

On considère également qu'il y a dissimulation d'un transfert quand l'auteur obtient une valeur patrimoniale lui appartenant mais fait en sorte que celle-ci ne soit pas débitée de son compte par une manipulation de la machine.

ee) Un dommage

L'infraction suppose un dommage patrimonial[148], qui résulte en principe du transfert de fonds frauduleusement obtenu et porte par conséquent atteinte aux intérêts pécuniaires d'autrui, qu'il s'agisse du tiers à qui appartient le compte bancaire ou de la banque lésée par la manipulation de la machine.

ff) Un rapport de causalité entre tous les éléments

Un rapport de causalité entre les divers éléments doit être constaté. Ainsi, c'est précisément l'utilisation incorrecte, incomplète ou indue d'un système ou d'une machine informatique, influençant le processus électronique et conduisant à un résultat inexact, qui engendre un transfert d'actifs portant atteinte à autrui.

b) Les éléments constitutifs subjectifs

aa) L'intention

L'acte doit être commis intentionnellement, mais le dol éventuel suffit.

bb) Le dessein d'enrichissement illégitime

L'auteur doit agir dans le dessein de s'enrichir de manière illégitime. Cette notion doit être comprise au sens large et englobe tous les avantages économiques (augmentation d'actif, diminution de passif, non-diminution de l'actif et non-augmentation du passif) que l'auteur vise à retirer de son action.

c) L'application de la partie générale

Le comportement réprimé est poursuivi d'office, sauf lorsqu'il est commis au préjudice de proches ou de familiers, ce qui nécessite alors que la victime porte plainte.

La loi prévoit une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. Lorsque l'auteur agit par métier, il est passible d'une peine privative de

147 Arrêt du TF 6S.247/2001 du 10. 5. 2001.

148 *Corboz,* I (n. 31), art. 147 N 13; *Donatsch* (n. 28), 251; *N. Schmid* (n. 37), § 7 N 116; *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 12; *Trechsel/Crameri,* in Praxiskommentar StGB (n. 28), art. 147 N 10; *Müller* (n. 27), 39.

liberté aggravée de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins.

Si la manipulation de la machine ne suffit pas pour obtenir le résultat et qu'il faut encore qu'une personne soit trompée, c'est l'infraction d'escroquerie au sens de l'art. 146 CP qui trouvera application et primera l'art. 147 CP. De même, l'application de l'art. 147 CP s'efface devant celle de l'art. 148 CP dans les cas où l'auteur utilise sa propre carte à un distributeur automatique.

Lorsque le titulaire d'un compte remet à l'auteur une carte bancaire avec le mot de passe et que ce dernier viole les instructions du titulaire pour prélever de l'argent à ses propres fins, il y a abus de confiance (art. 138 CP) et non utilisation frauduleuse d'un ordinateur (art. 147 CP)[149].

Dans le cas d'une carte d'abord volée puis utilisée, les dispositions sur le vol (art. 139 CP) et utilisation frauduleuse d'un ordinateur (art. 147 CP) s'appliquent[150].

Enfin, l'extorsion prévue à l'art. 156 CP absorbe l'art. 147 lorsque la manipulation n'intervient qu'à l'appui de contrainte exercée sur une personne[151].

8. L'obtention frauduleuse d'une prestation (art. 150 CP)

L'art. 150 CP punit le parasitisme informatique, soit le vol de temps-machine. La loi dispose que «celui qui, sans bourse délier, aura frauduleusement obtenu une prestation qu'il savait ne devoir être fournie que contre paiement, notamment celui qui (…) se sera servi d'un ordinateur ou d'un appareil automatique, sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire».

Pour que cette infraction soit réalisée, l'auteur doit avoir obtenu une prestation à caractère onéreux (8.a.aa) sans la payer (8.a.bb) par le biais d'un comportement typique frauduleux (8.a.cc).

a) Les éléments constitutifs objectifs

aa) L'obtention d'une prestation qui exige un paiement

Cette notion vise n'importe quelle prestation à caractère onéreux, qu'elle soit destinée à l'auteur ou à un tiers[152]. Il faut toutefois qu'il s'agisse d'une prestation et non d'un objet, dans quel cas la soustraction serait caractéristique d'un vol au sens de l'art. 139 CP[153]. Dans le cas qui nous intéresse, il s'agit de l'utilisation

149 RSJ 103/2007, 281–282.
150 *G. Fiolka,* in: BSK StGB II (n. 29), art. 148 N 53.
151 ATF 129 IV, consid. 4.2 et 4.3.
152 *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 51.
153 *Corboz,* I (n. 31), art. 150 N 27.

d'un ordinateur ou d'un appareil automatique, ou encore de l'accès à une banque de données[154].

La prestation peut être fournie par le lésé à son propre insu et ne requiert donc pas d'acte spécifique de ce dernier[155]. Il est en outre admis qu'une prestation puisse être obtenue sans intervention humaine, par le biais d'un appareil comme par exemple l'utilisation d'une cabine téléphonique[156].

bb) L'absence de paiement

La prestation est obtenue par l'auteur sans que celui-ci ne s'acquitte, partiellement ou intégralement, de la contre-prestation due[157]. Le lésé est ainsi privé d'une part de revenu et subit un dommage patrimonial. Si l'on considère l'acte du point de vue du lésé, on peut dire que celui-ci est frustré d'un revenu[158].

Le paiement doit toutefois être exigible, ce qui n'est pas le cas si un délai pour s'acquitter de la contre-prestation a été accordé à l'auteur. Dans cette dernière situation, tant que le délai n'est pas échu, l'infraction n'est pas consommée[159].

cc) La fraude

Il ne suffit ainsi pas de ne pas payer, la loi exigeant une fraude, soit une attitude trompeuse qui revêt un caractère déloyal. L'auteur doit adopter un comportement typique pour que l'infraction soit réalisée. La doctrine dominante retient que l'auteur doit détourner des contrôles (humains ou techniques)[160], s'y soustraire en se cachant lors de leur survenance ou leur échapper par un comportement malhonnête[161]. L'auteur agit par exemple frauduleusement lorsqu'il se sert d'un code d'accès auquel il n'avait pas droit pour utiliser une machine ou accéder à une banque de données.

Si l'auteur peut accéder librement à une telle prestation onéreuse et décide volontairement de ne pas payer son dû sans toutefois s'en cacher, il n'y a pas de fraude[162].

154 *Corboz,* I (n. 31), art. 150 N 24.
155 *Hurtado Pozo,* Partie spéciale (n. 51), N 1316.
156 *Corboz,* I (n. 31), art. 150 N 6.
157 *Corboz,* I (n. 31), art. 150 N 8 et 9.
158 *Donatsch* (n. 28), 264; *Corboz,* I (n. 31), art. 150 N 10.
159 Aussi longtemps que l'auteur dispose d'un délai pour payer: cf. *Corboz,* I (n. 31), art. 150 N 11.
160 *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 51; *Hurtado Pozo,* Partie spéciale (n. 51), N 1320; ATF 117 IV 450, consid. b/aa et les références citées.
161 ATF 117 IV 451, consid. cc. Par exemple, s'il se cache dans un transport public ou présente un titre de transport inapproprié: cf. *Corboz,* I (n. 31), art. 150 N 15.
162 *M. Schubarth/P. Albrecht,* Kommentar zum schweizerischen Strafrecht. Strafgesetzbuch, Besonderer Teil. Zweiter Band: Art. 137–172 (Delikte gegen das Vermögen), Berne 1990, art. 151 N 6 ss; *Hurtado Pozo,* Partie spéciale (n. 51), N 1323.

b) L'élément subjectif

L'intention est requise pour réaliser l'infraction, mais le dol éventuel est suffisant[163].

Celui qui oublie simplement de payer est négligent et ne réalise pas l'infraction de l'art. 150 CP[164].

Le dessein d'enrichissement illégitime n'est pas requis, l'auteur pouvant donc notamment agir par simple défi[165].

c) L'application de la partie générale

L'obtention frauduleuse d'une prestation n'est poursuivie que sur plainte et est punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Si la prestation visée est de faible valeur, l'art. 172ter CP s'appliquera, et la peine sera alors une simple contravention[166].

L'art. 150 CP s'applique de manière subsidiaire si l'auteur réalise en même temps une escroquerie (art. 146 CP[167]) ou une utilisation frauduleuse d'un ordinateur (147 CP) dans le cas où l'auteur réussit, par une utilisation frauduleuse de l'ordinateur, à mettre à la charge d'un tiers la prestation qu'il obtient[168].

L'obtention frauduleuse d'une prestation peut en revanche entrer en concours avec une soustraction de données et être cumulée à l'art. 143 CP, lorsque l'auteur soustrait des données pour en tirer profit et prive en plus de cela l'exploitant du montant à payer[169].

IV. Conclusion

Après avoir passé en revue les différentes infractions informatiques contenues dans le code pénal suisse et analysé leurs éléments constitutifs (voir le tableau récapitulatif ci-dessous pour les principaux points de comparaison), nous pouvons confirmer que la législation pénale suisse offre de nombreux outils pour protéger l'infrastructure et les données informatiques.

163 *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 52; *Hurtado Pozo,* Partie spéciale (n. 51), N 1327; *Schubarth/Albrecht* (n. 162), art. 151 N 12.

164 *Donatsch* (n. 28), 267; *Hurtado Pozo,* Partie spéciale (n. 51), N 1327.

165 *Stratenwerth/Jenny/Bommer* (n. 28), § 16 N 52; *Donatsch* (n. 28), 267; *Hurtado Pozo,* Partie spéciale (n. 51), N 1328.

166 *Corboz,* I (n. 31), art. 150 N 37.

167 ATF 117 IV 450, consid. 6b.

168 *Donatsch* (n. 28), 268; *Hurtado Pozo,* Partie spéciale (n. 51), N 1333.

169 FF 1991 II 1000 et dans ce sens *Corboz,* I (n. 31), art. 150 N 41.

S'il existe évidemment toujours des possibilités d'amélioration de la part du législateur, par exemple sur la question du recel de données, le cadre juridique actuel n'est pas dépassé et devrait, pour l'essentiel, pouvoir continuer à s'appliquer sans difficultés majeures malgré les évolutions technologiques. Au besoin, la jurisprudence se chargera de préciser certaines notions techniques.

Il est toutefois essentiel que l'utilisateur d'infrastructures informatiques prenne conscience des instruments à sa disposition et des conditions à remplir pour qu'une infraction puisse être considérée comme réalisée. Cette compréhension des mécanismes de protection lui permettra en effet de se défendre en recourant à la justice en toute connaissance de cause. On ne peut donc que vivement recommander aux principaux intéressés de recourir à un serveur situé en Suisse et de mettre en place des mesures de protection suffisantes pour empêcher l'accès à leurs données.

V. Annexe: Tableau récapitulatif simplifié[170]

Infraction	**Objet de la protection**	**Comportement visé**	**Exigence de protection**	**Dessein**	**Concours**
143 CP Soustraction de données	Donnée informatique	Soustraction	Spécialement protégé (y c. barrière physique)	Dessein d'enrichissement illégitime	179novies 139 144 150
179novies CP Soustraction de données personnelles	Donnée personnelle sensible ou profil de la personnalité	Soustraction	Spécialement protégé (y c. barrière physique)	Aucun	143
143bis al. 1 CP Accès indu à un système informatique	Système informatique appartenant à autrui	Accès au moyen d'un dispositif de transmission de données	Spécialement protégé (barrière informatique)	Aucun	

170 Ce tableau n'est pas exhaustif et sert seulement à faciliter la lecture du texte.

Infraction	Objet de la protection	Comportement visé	Exigence de protection	Dessein	Concours
143bis al. 2 CP Mise à disposition d'informations en vue d'un accès indu	Mot de passe, un programme ou toute autre donnée	Mise à disposition	Aucune	Aucun	
144bis ch. 1 CP Détérioration de données	Donnée informatique	Modification, effacement ou mise hors d'usage	Aucune	Aucun	143 144bis ch. 2
144bis ch. 2 CP Détérioration de données	Donnée informatique	Fabrication, importation, mise en circulation, promotion, offre ou accès à un logiciel de détérioration	Aucune	Aucun	144bis ch. 1
147 CP Utilisation frauduleuse d'un ordinateur	Bon fonctionnement d'un processus électronique	Utilisation incorrecte, incomplète ou illicite	Aucune	Dessein d'enrichissement illégitime	139
150 CP Obtention frauduleuse d'une prestation	Temps-machine (ordinateur)	Absence de paiement et fraude	Aucune	Aucun	143