www.jusletter-it.eu

Fabian Teichmann / Léonard Gerber

Cybercriminalité en Suisse – Le phishing

Le phishing regroupe les techniques informatiques employées par les malfaiteurs pour recueillir des données bancaires à travers la collaboration aveugle de leurs victimes. L'ingéniosité des techniques informatiques met potentiellement en danger le patrimoine des victimes et requiert ainsi une réponse adéquate en droit pénal suisse. Cette contribution offre une vue d'ensemble et concise des infractions du droit pénal informatique suisse et de la Convention du Conseil de l'Europe sur la cybercriminalité. Le droit pénal suisse est également étudié dans le but de qualifier pénalement les différentes formes de phishing et les infractions du Code pénal entrant ainsi en concours idéal.

Catégories d'articles : Beiträge
Region : Switzerland
Rechtsgebiete : Cybercrime

Proposition de citation : Fabian Teichmann / Léonard Gerber, Cybercriminalité en Suisse – Le phishing, in : Jusletter IT 27 mai 2021

Table des matières

I. Introduction

[1] En 2020, la numérisation transperce notre société et ouvre une voie vers une économie viable. Ce que le Forum économique mondial qualifie de 4ème révolution industrielle a également une influence sur la vie quotidienne des justiciables.[1] Concrètement, les gens communiquent par email ou message whatsapp, rencontrent leurs amis sur Facebook ou par zoom, publient leurs photos et vidéos sur instagram, commercent sur des plateformes internet et effectuent leurs paiements par e-banking.[2] Néanmoins, de nombreux comportements frauduleux ont émergé depuis le développement de l'informatique, certains tombant dans le champ du droit pénal informatique. La difficulté de la qualification juridique pénale de ces comportements réside dans la réalisation simultanée de plusieurs infractions sous la forme d'un concours idéal. Il en va ainsi des infractions se déroulant par le biais d'internet, par exemple les ransomwares, l'usurpation d'identité, l'hacking, la distribution de malwares, les attaques DDoS[3], la cyber-escroquerie, les infractions liées au cybersex, la cyber-concurrence déloyale ainsi que du phishing.

[2] La présente contribution traite brièvement la Convention du Conseil de l'Europe sur la cybercriminalité conclue le 23 novembre 2001 à Budapest apportant une première réponse juridique face aux comportements informatiques frauduleux (II). Parallèlement, le droit pénal suisse apporte une deuxième réponse juridique à la criminalité informatique au niveau national (III). Cette étude préliminaire permettra de présenter le phishing, ses différentes formes ainsi que sa qualification en droit pénal suisse qui seront également traités dans un chapitre à part (IV). Cette

1 Davos Manifesto 2020 : The Universal Purpose of a Company in the Fourth Industrial Revolution, disponible sous le lien suivant : https ://www.weforum.org/agenda/2019/12/davos-manifesto-2020-the-universal-purpose-of-a-company-in-the-fourth-industrial-revolution/ (consulté le 31 mars 2021).

2 Jérémie Müller, « Le droit matériel suisse est-il conforme aux exigences minimales posées par la Convention du Conseil de l'Europe sur la cybercriminalité ? », 2016, sic !, p. 332–339, p. 332.

3 Une attaque DDoS (en anglais Distributed Denial of Service) vise à bloquer un système informatique par une inondation de requêtes auprès du serveur d'un site web par exemple, pour en empêcher l'accès aux utilisateurs légitimes, voir par exemple, Daniel Stoll, « Le bitcoin et les aspects pénaux des monnaies virtuelles », forumpoenale 2/2015, p. 99–108, p. 104 ainsi que les références citées.

contribution conclue par une présentation des difficultés liées à la poursuite du phishing sur internet et des perspectives actuelles des autorités suisses (V).

II. Au niveau international – La Convention du Conseil de l'Europe sur la cybercriminalité

[3] Le Conseil de l'Europe a émi sa Convention de Budapest sur la cybercriminalité, conclue le 23 novembre 2001 qui constitue la première convention internationale à traiter de la cybercriminalité.[4] Intéressant à cet égard, les 65 État-adhérents en 2021 comprennent également des État non-membres du Conseil de l'Europe qui ont également ratifié la CCC à l'exemple des États-Unis d'Amérique, du Japon, de l'Australie ou du Canada.[5] La CCC et ses État-adhérents reconnaissent ainsi la nécessité de combattre et prévenir au niveau international la cybercriminalité pouvant s'exerçer à l'échelle mondiale et corollairement au-delà de la compétence délimitée d'une seule et unique juridiction.[6] La CCC a principalement pour but d'enjoindre les pays-adhérents à mener une politique criminelle commune destinée à protéger la société de la criminalité dans le cyberespace par l'adoption de mesures législatives et par un renforcement de la coopération internationale.[7]

[4] Concrètement, les État-adhérents sont requis de réprimer les infractions suivantes dans leur droit domestique, bien qu'ils puissent émettre des réserves individuellement :[8]

- Hacking ou accès illégal à l'ensemble ou à une partie d'un système informatique (art. 2 et 40 CCC)
- Interception illégale de données informatiques (art. 3 CCC)
- Atteinte à l'intégrité des données (art. 4 CCC)
- Atteinte à l'intégrité du système (art. 5 CCC)
- Abus de dispositifs, logiciels, codes d'accès ou mot de passes pour commettre une infraction aux art. 2 à 5 de la Convention (art. 6 CCC)
- Falsification informatique (art. 7 CCC)
- Fraude informatique (art. 8 CCC)
- Infractions se rapportant à la pornographie enfantine (art. 9 CCC)
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes (art. 10 CCC)
- Tentative et complicité (art. 11 CCC)

---

4 Convention sur la cybercriminalité du 23 novembre 2001, (RS 0.311.43), abrégée CCC ; voir également Message du Conseil fédéral daté du 18 juin 2010 relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, publié à la FF 2010 4275, 4278.

5 Voir la liste des États ayant ratifié la CCC sur le site du Conseil de l'Europe https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=6v8OvU1t (consulté le 31 mars 2021), voir également Müller (2016), p. 333 ainsi que les références citées

6 Stéphane Werly, « La transposition de la Convention du Conseil de l'Europe sur la cybercriminalité en droit suisse », 2010, Medialex, p. 121–123, p. 122, ainsi que Nicolas Bottinelli, « L'obtention par l'autorité pénale de données informatiques situées à l'étranger », PJA 2016, p. 1327–1333, p. 1328.

7 FF 2010 4275, 4279.

8 FF 2010 4275, 4281ss.

[5] Enfin un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de système informatique daté du 28 janvier 2003 a été signé par la Suisse le 9 octobre 2003 qu'elle n'a toutefois pas ratifié à ce jour.[9]

[6] En matière de coopération internationale, les principes généraux de la CCC requièrent des Etat-adhérents de supprimer les obstacles à la circulation rapide et sans problème de l'information et des preuves.[10] Plus concrètement en matière de cybercriminalité, un échange plus rapide des informations lors de procédures de coopération judiciaire internationale pénale devrait être assuré pour toutes les infractions pénales liées à des systèmes et données informatique ainsi qu'à la collecte des preuves sous forme électronique se rapportant à une infraction pénale.[11] Ainsi, l'introduction de l'art. 18b de la Loi fédérale sur l'entraide internationale en matière pénale[12] permet à la Suisse divulguer les données relatives au trafic informatique avant la clôture d'une procédure d'entraide, non pas toutefois du contenu des communications informatiques.[13] Le tribunal des mesures de contraintes cantonal ou fédéral compétent ainsi que l'Office fédéral de la Justice (OFJ) doivent préalablement contrôler la mesure de surveillance et les données transmises ne peuvent servir de moyens de preuve avant la clôture de la procédure.[14] Un service de piquet est assumé par l'OFJ afin d'assurer une assistance immédiate des investigations pénales nationales et internationales concernant la cybercriminalité ou pour recueillir des preuves sous forme électronique.[15]

III. Au niveau national – Le droit pénal informatique suisse

[7] Sur le plan matériel, le droit pénal suisse réprimait d'ores et déjà une grande partie des infractions comprises dans la CCC lors de sa ratification le 18 mars 2011.[16] Pour cause, les infractions dans le domaine informatique sont entrées en vigueur le 1er janvier 1995 par une adaptation du Code pénal suisse satisfaisant en grande partie aux dispositions pénales matérielles de la CCC.[17] La CCC est ainsi entrée en vigueur le 1er janvier 2012 pour la Suisse menant néanmoins à une révision partielle du CP ainsi que de la EIMP.[18] En l'état de 2021, les infractions spécifiques à la criminalité informatique suivantes sont réprimées par le droit pénal suisse.

- La soustraction de données (art. 143 CP)
- L'accès indu à un système informatique (art. 143bis CP)
- La détérioration de données (art. 144bis CP)
- L'utilisation frauduleuse d'un ordinateur (art. 147 CP)

9 Voir la liste des États ayant ratifié le Protocole additionnel sur le site du Conseil de l'Europe https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=a4xljJi1 (consulté le 17 mars 2021).

10 Voir l'art. 23 CCC, ainsi que FF 2010 4275, 4301.

11 Art. 14 II let. c et 23 CCC, voir également FF 2010 4275, 4301.

12 Loi fédérale sur l'entraide internationale en matière pénale du 20 mars 1981 (RS 351.1), ci-après EIMP.

13 FF 2010 4275, 4310.

14 Voir l'art. 18b EIMP, FF 2010 4275, 4310 ainsi que Werly, p. 121s.

15 Voir l'art. 35 CCC, FF 2010 5275, 4315 ainsi que Werly, p. 122.

16 FF 2010 4275, 4276.

17 FF 2010 4275, 4276.

18 FF 2010 4275, 4275.

- Mise en circulation et réclame en faveur d'appareils d'écoute, de prise de son et de prise de vues (art. 179^{sexies} CP)
- Violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vues (art. 179^{quater} CP)
- Pornographie (art. 197 CP)
- Violation du droit d'auteur (art. 67 LDA)
- Omission de la source (art. 68 LDA)
- Violation de droits voisins (69 LDA)
- Violation de la protection des mesures techniques ou de l'information sur le régime des droits (art. 69a LDA)

[8] La cybercriminalité peut faire l'objet d'une division en deux catégories.[19] La première catégorie regroupe la criminalité contre les infrastructures internet comme l'ordinateur, la connectivité, un programme ou plus généralement le support informatique des victimes.[20] Il en va ainsi par exemple du hacking, des attaques DDoS, le partage de malwares (virus, cheval de Troie, ou worm par exemple). La deuxième catégorie regroupe la criminalité commise au moyen d'internet (par exemple la discrimination raciale, la violation des droits d'auteur, la concurrence déloyale, ou le phishing).[21] Les infractions liées à internet ont également une portée transnationale car elles ne se limitent pas nécessairement à une unique juridiction.[22] Néanmoins, l'internet est le médium par lequel de nombreux comportements abusifs de la part de ses utilisateurs ne sont que ponctuellement réprimés par le droit pénal suisse. La partie spéciale du CP, complétée par les infractions du domaine informatique, offre une protection similaire à celle de la CCC.[23] Ces comportements abusifs peuvent entraîner la réalisation de plusieurs infractions du droit pénal sous la forme d'un concours idéal et à plus fortes raisons comme nous le verrons du phishing.[24]

IV. Le phishing

1. Définition

[9] Le phishing provient de la contraction de deux termes anglais, à savoir password (mot de passe), harvesting (récolte) et fishing (pêche), plus communément appelé hammeçonnage en français.[25] Le phishing regroupe les techniques employées pour soutirer des renseignements person-

19 Voir par exemple Sylvain Métille/Joana Aeschlimann, « Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ? », 2014, RPS 132/2014, p. 283 ainsi que Nikolaus Gyarmati, « Phänomen Cybercrime und seine Bekämpfung », RSC 1-2/2019, p. 86–97, p.87s.

20 Voir par exemple Bernhard Isenring/Roy Maybud/Laura Quiblier, « Phänomen Cybercrime – Herausforderungen und Grenzen des Straf – und Strafprozessrechts im Überblick », 2019, RSJ 115/2019, p. 439–447, p. 440s.

21 Voir par exemple Philipp Kronig/Eva Bollmann, dans : Schwarzenegger/Arter/Jörg (éd.), Internet-Recht und Strafrecht, 4ème édition, Berne 2005, p. 22

22 Métille/Aeschlimann, p. 287.

23 FF 2010 4275, 4276.

24 Voir par exemple Nadja Capus, *Droit pénal – Evolutions en 2018*, Neuchâtel 2018, p. 33.

25 Jérémie Müller, La cybercriminalité économique au sens étroit, dans : Hansjörg Peter (éd.), Recherches juridiques lausannoises N. 52, Lausanne 2012, p. 79.

nels de façon frauduleuse, le plus souvent de nature bancaire, en général dans le but de perpétrer des infractions contre le patrimoine et liées à l'usurpation d'identité.[26]

2. Modus operandi

[10] Les attaques classiques de phishing apparues autour de l'année 2003 reposaient principalement sur la collaboration « aveugle » des victimes avec les auteurs du phishing.[27] On parle alors de techniques classiques du phishing reposant principalement sur des techniques d'ingénierie sociale destinées à manipuler les victimes pour qu'elles collaborent activement avec les auteurs.[28] Concrètement, la victime reçoit un courrier par email ou par SMS de la part du ou des auteurs du phishing se faisant passer pour une banque ou une autorité officielle.[29] Les auteurs agissent le plus souvent en envoyant des courriels ou SMS en masse, souvent avec des adresses d'expédition falsifiée ou imitée, par exemple celle d'une banque (e-mail spoofing).[30] Les messages contiennent généralement une demande de renouvellement des données personnelles pour des raisons de sécurité ou de mises à jour, le remboursement d'une somme payée en trop ou un manco à couvrir, ainsi qu'un lien vers une page web imitée comprenant un formulaire à remplir de données personnelles, notamment bancaires.[31] Le courriel de phishing peut également ouvrir directement la page web ou le formulaire à remplir au lieu de contenir un lien vers une page web, ou bien il peut arriver que les sites webs authentiques aient été piratés pour héberger des pages de « phishing » (cybersquatting).[32]

[11] Dès l'année 2008, les techniques de phishing ont évolué.[33] Les cybercriminels emploient des mesures techniques permettant de s'introduire directement dans le support informatique de la victime, notamment par l'emploi de malware de type cheval de Troie par exemple.[34] Ce type de phishing nommé Man in the Middle (abrégé MitM) consiste concrètement à installer un programme malveillant dans le système informatique de la victime.[35] L'auteur du phishing peut ensuite décider soit prendre le contrôle du support informatique de ses victimes soit de surveiller leur activité sur leur support et d'intercepter les données qu'ils transmettront notamment à leur banque. Le grand danger des attaques MitM réside essentiellement dans le fait que les victimes

---

26 Rapport de janvier 2020 du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (ci-après GCBF) sur l'escroquerie et hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur en tant qu'infractions préalables au blanchiment d'argent, p. 27, voir également Mark Spas, « Phénomènes cybercriminels – Descriptions et réponses juridiques », Jusletter du 10 novembre 2014, p. 5.

27 Spas, p. 5.

28 Voir par exemple Sylvain Métille, *Internet et droit*, Lausanne 2017, p. 139s., Peter Reichart, « Betrugsversuche im Zahlungsverkehr im digitalen Zeitlater », RDSA 2019, p. 392–404, p. 392, Stefan Frei, « Cyber Crime als Dienstleistung – Die Entwicklung der Sicherheit im Internet – vom schlauen Hacker zur organisierten Kriminalität », digma 2008, p. 160–164, p. 161, ainsi que Müller (2012), p. 70.

29 Spas, p. 5 ; Rapport du GCBF, p. 27.

30 Rapport du GCBF, p. 27.

31 Rapport du GCBF, p. 27 ; Métille, p. 139s. ; Spas, p. 5.

32 Michel Jaccard/Hoang Lê-Binh, Internet, médias sociaux, applications : terrains propices à la déloyauté commerciale ?, dans : de Werra (éd.), Défis du droit de la concurrence déloyale/ Challenges of Unfair Competition Law, Genève 2014, PI, p. 131–157, p. 134s.

33 Müller (2012), p. 80.

34 Jaccard/Lê-Binh, p. 135 ; voir également Annina Baltisser, « Datenbeschädigung und Malware im Schweizer Strafrecht », 2013, ZStStr, p. 41–57, p. 42.

35 Müller (2012), p. 80 ; Reichart, p. 393,

ne se rendent pas compte des actions de l'auteur du phishing et ne collaborent pas consciemment avec l'auteur.

a. Les attaques classiques de phishing

[12] Les fraudes nécessitant la participation active de la victime se divisent principalement en deux types :

- Spear phishing : se focalise sur un utilisateur ou un groupe d'utilisateur en particulier par exemple avec un message fortement personnalisé avec un contenu cohérent, difficilement identifiable avec une attaque provenant d'un hacker.[36] Les victimes potentielles peuvent comprendre des directeurs d'entreprises ou de leurs collaborateurs proches, souvent en utilisant une adresse e-mail internet à l'entreprise.[37]
- Vishing : Utilisation de la technologie VoIP (voix sur IP ou voice over IP) par exemple par appel téléphonique dans le but de duper quelqu'un lui faisant divulguer des informations personnelles, financières ou des mots de passe, ou bien divulguer des absences de vacances.[38] L'équivalent du vishing par SMS constitue le smishing.[39]

b. Les attaques MitM

[13] Bien que les attaques classiques aient généré des profits, elles sont en pertes de vitesse au profit des MitM beaucoup plus efficaces et ne nécessitant pas nécessairement une active collaboration de la victime.[40] Essentiellement, deux types d'attaques MitM se distinguent :

- Le Pharming : cette technique consiste à rediriger la victime à son insu, vers un site web falsifié où elle saisira des informations que l'auteur pourra exploiter, par exemple les mots de passe et identifiants d'un compte d'e-banking.[41] Cette technique de piratage informatique exploite les vulnérabilités d'un nom de domaine DNS (en anglais pour Domain Name System, à savoir le protocole chargé de la résolution des noms de domaine en adresses IP) et consiste à ce que l'IP d'un site frauduleux soit donné suite à une requête DNS d'un nom de domaine légitime de la part de la victime.[42] L'auteur peut également employer un maliciel pour modifier les paramètres du nom de domaines d'un site web légitime.[43]
- In session phishing : Cette techniques consiste à faire croire à la cible que sa banque ou un autre organisme de confiance lui demande des informations confidentielles en envoyant

36 Sandro Germann/David Wicki-Birchler, « Hacking und Hacker im Schweizer Recht », PJA 2020, p. 83–94, p. 85s.

37 Idem.

38 Pascal Kocher, « Social Engineering – Risikofaktor Mensch », 2017, Revue de l'avocat, p. 431–434, p. 432.

39 Idem ; voir également Spas, p. 5.

40 Müller (2012), p. 80 ; Reichart, p. 393.

41 Aurélia Rappo/Branka Stojaniovic, « E-Banking et fraudes informatiques », 2018, Expert Focus 1-2/18, p. 60–63, p. 60, voir également Rolf H. Weber, *E-Commerce und Recht*, Zurich 2010, p. 540s.

42 Weber, p. 540s, ainsi que Spas, p. 6.

43 Rappo/Stojanovic, p. 60.

des courriers électroniques aux potentielles victimes.[44] Le courrier comprend en général un lien menant à un site sur lequel une fenêtre pop-up s'affichera automatiquement invitant l'internaute à réinscrire son identifiant et son mot de passe. Une fois les informations validées, l'instigateur de l'attaque peut les réutiliser pour ses propres affaires.[45] L'ouverture du site web peut également entraîner le téléchargement d'un programme malveillant à l'intérieur du système informatique de la victime (par exemple de type Cheval de Troie) qui s'exécutera au moment de l'ouverture du fichier.[46] Une fois téléchargé, le programme malveillant s'installe automatiquement et modifie les données qui composent le navigateur afin de ménager un accès au cybercriminel sans le consentement de l'utilisateur légitime.[47] À l'aide d'un programme de type Cheval de Troie par exemple, l'auteur pourra surveiller l'activité des utilisateurs du support informatique infecté par exemple lors de l'ouverture d'une session de e-banking et/ou en prendre directement le contrôle.[48]

3. Qualification en droit pénal suisse

[14] Le mode opératoire des auteurs de phishing consiste à envoyer un courriel au contenu fallacieux à la victime potentielle dans le but de récolter des données confidentielles.[49] Les diverses formes de phishing peuvent néanmoins entraîner une qualification juridique pénale différente. La création et l'expédition de courriels de phishing n'est pas en soi punissable.[50] Néanmoins, l'auteur entraîne la réalisation de plusieurs infractions en droit pénal suisse suivant les techniques informatiques qu'il emploi et du résultat obtenu par l'entremise de leurs victimes. Les infractions suivantes du droit pénal suisse entrent ainsi en compte[51] :

a. Accès indu à un système informatique (art. 143bis CP)

[15] L'art. 143bis CP est la norme de droit pénal suisse réprimant le hacking , à savoir l'accès indu à un système informatique.[52] Cette infraction comprend deux éléments constitutif objectifs ainsi qu'un élément constitutif subjectif.[53]

[16] Premièrement, cette norme protège les systèmes informatiques appartenant à autrui et spécialement protégés contre les intrusions sans droit d'autrui.[54] Les ordinateurs, les téléphones por-

44 Spas, p. 6.

45 Spas, p. 6.

46 Müller (2012), p. 98s.

47 Idem.

48 Voir par exemple, David Raedler, *Les enquêtes internes dans un contexte suisse et américain*, Lausanne 2018, CEDIDAC, p. 667s.

49 Müller (2012), p. 82.

50 Matthias Ammann, « Sind Phishing-Mails strafbar ? », AJP 2006, p. 195 ss.

51 En sis des infractions principales réalisables par l'auteur de phishing, d'autres infractions entrent naturellement en compte, comme la détérioration de données (art. 144bis CP) ainsi que le blanchiment d'argent (art. 305bis CP). Ces infractions nécessitent toutefois des actions supplémentaires de la part de l'auteur du phishing.

52 Voir Giles Monnier, « Le piratage informatique en droit pénal », 2009, sic !, p. 141–153, p. 14 ainsi que FF 2010 4275, 4281.

53 Michel Dupuis/Laurent Moreillon/christophe Piguet/Séverine Berger/Miriam Mazou/Virginie Rodigari, Petit Commentaire Code Pénal, 2ème éd., Bâle 2017, ad art. 143bis CP N 3.

54 FF 2010 4275, 4281.

tables, les caméras digitales ainsi que toutes installations de traitement de données incorporées se comprennent comme des systèmes informatiques.[55] Il n'en va pas ainsi de l'intrusion dans un support de données, par exemple les clés USB, les CD, DVD ou disquettes à moins qu'ils ne soient reliés à un système informatique protégé.[56] Les données en tant que telles ne sont pas protégées par l'art. 143bis CP mais par l'art. 143 CP réprimant quant à lui la soustraction de données.[57] Pour déterminer si un système informatique est spécialement protégé, il faut s'intéresser à la manifestation de volonté de la personne ayant légalement accès au système d'empêcher des tiers d'accéder à ses données ou de restreindre cet accès.[58] Ce critère est respecté si des barrières informatiques ont été installées par exemple en cas d'emploi d'un antivirus, d'un verrouillage par code d'accès ou mot de passe, d'un chiffrement ou d'une clé biométrique, toutefois pas s'il n'existe que des barrières physiques protégeant le système informatique par exemple à l'aide d'une pièce close, ou d'une armoire scellée.[59] Deuxièmement, la norme protège contre l'accès indu au moyen d'un dispositif de transmission de donnée.[60] L'infraction est consommée, à partir du moment où l'auteur pénètre la première barrière d'accès, par exemple le code, le mot de passe ou de la clé biométrique du système général du système informatique protégé.[61]

[17] Pour Müller, l'auteur n'est pas punissable d'un accès indu à un système informatique au sens de l'art. 143bis CP en se contentant d'envoyer un mail de phishing.[62] Pour cause, il manque à son action une intrusion dans un système informatique. Le phishing se déroulant principalement par email ou sms, l'auteur ne désactive ni ne surmonte aucune barrière technique d'accès, à défaut d'emploi d'un malware de type cheval de Troie par exemple.[63] C'est donc principalement le « in session phishing » qui remplit ce critère, par exemple lorsque l'auteur emploi un malware de type cheval de Troie lui permettant de prendre contrôle de la session de la victime à distance.[64] Parallèlement, s'agissant des autres types de phishing, il en va également de même lorsque l'auteur accède à la messagerie de la victime en se faisant passer pour elle en utilisant ses données volées, car il accède indument à un serveur web hébergeant la boîte aux lettres électroniques d'autrui.[65] Il accède donc à un système informatique spécialement protégé contre les intrusions d'autrui.[66] Enfin, au niveau subjectif, il faut uniquement pouvoir prouver que l'auteur ait agi intentionnellement, un dessein d'enrichissement n'est plus exigé par l'art. 143bis CP.[67]

55 Philippe Weissenberger, Basler Kommentar, Strafrecht (StGB, JStGB), 4ème éd., Bâle 2019 ad art. 143bis StGB N 9.

56 Weissenberger, BSK-StGB, art. 143bis N 9.

57 FF 2010 4275, 4281.

58 FF 2010 4275, 4283.

59 Weissenberger, BSK-StGB ad art. 143bis N 16 ; PC-CP ad art. 143bis N 11.

60 PC-CP ad art. 143bis N 2.

61 Spas, p. 6.

62 Idem.

63 Ammann, p. 195 ss.

64 Müller (2012), p. 85.

65 Idem.

66 Idem.

67 FF 2010 4275, 4282.

b. Soustraction de données (art. 143 CP)

[18] L'infraction de soustraction de données est une infraction formelle et de lésion protégeant le droit du bénéficiaire légitime de disposer des données informatiques à sa guise.[68] La soustraction de données comprend deux éléments constitutifs objectifs ainsi que deux éléments constitutifs subjectifs.[69]

[19] Premièrement, des données enregistrées ou transmises électroniquement ou selon un mode similaire, non destinées à l'auteur doivent être spécialement protégées contre tout accès indu.[70] Deuxièmement, le comportement typique réprimé est la soustraction.[71] Une fois les données obtenues, les auteurs du phishing peuvent en faire usage eux-mêmes ou les revendre sur le marché noir.[72] Pour réaliser l'infraction de soustraction de données, il suffit néanmoins que l'auteur puisse accéder aux données, c'est-à-dire en prendre connaissance, mais il n'est pas nécessaire qu'il en fasse effectivement usage une fois obtenues.[73] Du point de vue subjectif, la soustraction de donnée est une infraction intentionnelle dont le législateur exige également un dessein d'enrichissement illégitime.[74] L'enrichissement englobe tous les avantages économiques susceptible d'être estimée ou tout élément doté d'une valeur pécuniaire.[75]

[20] Selon Ammann, le premier élément n'est pas réalisé en cas de phishing, car bien que les mots de passes introduits dans le système informatique par la victime constituent des données au sens de l'art. 143 CP, l'auteur n'a pas nécessairement franchi de mesures de sécurité protégeant ses données.[76] L'auteur offre de son plein gré, les données confidentielles en question. D'autres auteurs, auxquels nous nous rallions, considèrent qu'il y a soustraction de données, à partir du moment où un antivirus ou un pare-feu a été installé par l'utilisateur légitime du support informatique créant ainsi une barrière à l'accès d'autrui aux données du support.[77] Contrairement à l'art. 143bis CP, un dispositif de transmission de données n'est pas exigée, la notion de « spécialement protégé contre les attaques extérieures » est donc plus large que celle de l'art. 143 CP et devrait donc comprendre les barrières physique de protection comme l'enfermement dans une armoire ou une pièce fermée à clé.[78] Le phishing est subjectivement constitutif de soustraction de données notamment lorsque l'auteur compte utiliser les identifiants d'une victime pour payer des biens et des services, y compris par dol éventuel.[79]

---

68 PC-CP ad art. 143 N 2.

69 PC-CP ad art. 143 N 3.

70 Bertrand Perrin, « La protection pénale des données informatiques de l'entreprise », 2011, ECS 8/11, p. 605–610, p. 606 ainsi que les références citées, ainsi que p. 32, ainsi que PC-CP ad art. 143 N 6ss.

71 Perrin, p. 606, ainsi que PC-CP ad art. 143 N 21ss.

72 Dans la deuxième situation, l'auteur peut se rendre également coupable de mise à disposition d'informations en vue d'un accès indu au sens de l'art. 143bis II CP, voir à cet égard Métille/Aeschlimann, p. 302s.

73 FF 2010 4275, 4282s et PC-CP ad art. 143 N 22 ainsi que les références citées.

74 Jérémie Müller, La cybercriminalité économique au sens étroit, Lausanne 2012, RJL, p. 33.

75 Stoll, p. 106 ainsi que les références citées.

76 Ammann, p. 197

77 Voir par exemple PC-CP ad art. 143 N 13 et Müller (2012), p. 83, ainsi que les références citées.

78 PC-CP ad art. 143 N 13.

79 Stoll, p. 104.

c. Soustraction de données personnelles (art. 179^novies CP)

[21] La soustraction de données personnelles introduite par la loi fédérale sur la protection des données du 19 juin 1992 protège les droits de la personnalité de l'individu auquel les données se rapportent.[80] Par rapport à l'art. 143 CP, seule l'objet de l'infraction change dans la qualification pénale car l'art. 179^novies CP protège spécifiquement les données personnelles sensibles et les profils de personnalité pas librement accessibles, de la soustraction.[81] Subjectivement, seule l'intention de l'auteur est requise.[82]

[22] Si l'auteur soustrait des données personnelles[83] sensibles[84] ou des profils de personnalité[85] non-librement accessibles, il pourra être également coupable de soustraction de données personnelles.[86] Pour Ammann, les données d'accès de compte ne sont pas des données personnelles sensibles ou des profils de personnalité, il faut donc que l'auteur du phishing prenne connaissance d'autres données pour entraîner l'art. 179^novies CP.[87] De plus, pour une partie de la doctrine, la notion de « pas librement accessible » de l'art. 179^novies CP est plus large que la notion de « protégé contre tout accès » de l'art. 143 CP et n'implique donc pas que les données personnelles sensibles ou que les profils de personnalités soient cachées.[88] Une barrière technique n'est donc pas nécessaire, et à ce niveau une barrière physique comme une porte fermée sans clé devrait répondre à ce critère.[89]

d. Escroquerie (art. 146 CP)

[23] L'infraction d'escroquerie protège le patrimoine de la victime, il s'agit d'une infraction de commission et suppose ainsi un comportement actif de l'auteur.[90] Les éléments constitutifs objectifs suivants doivent être réunis, lesquels doivent se trouver dans un rapport de causalité.

---

80 Loi fédérale sur la protection des données du 19 juin 1992 (235.1), ci-après LPD ; PC-CP ad art. 179^novies CP N 2.

81 Müller (2012), p. 86.

82 PC-CP ad art. 179^novies N 12 ainsi que les références citées.

83 Selon le TF, une donnée est considérée comme personnelle au sens de l'art. 3 let. a LPD, une personne est identifiée lorsque l'information permet d'affirmer qu'il s'agit exactement de la personne concernée. Elle est identifiable lorsqu'elle peut être identifiée au moyen d'informations complémentaires sans efforts disproportionnés. Ce n'est pas le cas si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre. Voir à cet égard, l'ATF 136 II 508, c. 3.2. (trad. JdT 2011 II 446 c. 3.2.) ainsi que Rudin Beat, *Kommentar DSG*, Berne 2015, ad art. 3 N 10.

84 Conformément à l'art. 3 let. c LPD, on entend par données sensibles, les données personnelles sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales administratives. Sur la notion voir par exemple Métille, p. 134s ainsi que les références citées

85 Conformément à l'art. 3 let. d LPD, on entend par profil de personnalité, un assemblage de donnöes qui permet d'apprécier les caractéristiques essentielles de la personnalità d'une personne physique. Sur la notion voir par exemple Métille, p. 134s ainsi que les références citées.

86 Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1), ci-après LPD ; PC-CP ad art. 179^novies N 2.

87 Ammann, p. 201, ainsi que Müller (2012), p. 86.

88 Pour des avis favorables voir notamment PC-CP ad art. 179^novies N 10, Monnier, p. 152, ainsi que Raffael Ramel/André Vogelsang, BSK-StGB ad art. 179^novies N 20–22 ainsi que les références citées. Pour un avis défavorable voir Métille/Aeschlimann, p. 295.

89 PC-CP ad art. 179^novies N 10 ainsi que Ramel/Vogelsang, BSK-StGB ad art. 179^novies N 20–22.

90 Voir par exemple l'arrêt du Tribunal fédéral du 8 janvier 2009, 6B_530/2008, c. 3.1. ainsi que l'arrêt du 5 novembre 2012, 6B_525/2012, c. 3.3.

[24] Premièrement, il faut une tromperie sous la forme d'une affirmation fallacieuse, la dissimulation de faits vrais ou le fait de conforter autrui dans son erreur.[91] Deuxièmement, cette tromperie doit être astucieuse, plus concrètement, l'auteur doit avoir agi avec un certain raffinement ou une rouerie particulière.[92] Selon la ligne constante du TF, ceci est le cas lorsque l'auteur recourt à un édifice de mensonges, à des manœuvres frauduleuses ou à des mises en scènes.[93] Toutefois, l'échec de la tromperie ne signifie pas nécessairement qu'elle n'était pas astucieuse.[94] Troisièmement, l'auteur doit avoir induit une personne en erreur soit l'avoir confortée dans une erreur préexistante, néanmoins la tromperie doit être la cause de l'erreur. Cette condition est également remplie lorsque l'auteur l'a déterminé à un ou plusieurs actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, il faut donc un acte de disposition du bien issus du patrimoine de la victime. Enfin, il faut un dommage, sous la forme d'une diminution de l'actif, une augmentation du passif, une non-augmentation de l'actif ou une non-diminution du passif de la victime. Le dommage peut également consister en une mise en danger du patrimoine, telle qu'elle a pour effet d'en diminuer la valeur d'un point de vue économique.[95] Sur le plan subjectif, l'auteur doit avoir agi intentionnellement avec le but de se procurer ou de procurer à un tiers un enrichissement illégitime.

[25] Le phishing consiste à tromper la victime par exemple par une affirmation fallacieuse que sa banque nécessite de mettre à jour leurs données clients. L'auteur du phishing et à plus fortes raisons de « spear phishing » mène astucieusement ses victimes en erreur non seulement sur l'expéditeur du courrier mais également sur le contenu faussement attribuable à la banque de la victime.[96] Cependant, les données obtenues de la victime n'ont pas de valeurs directes.[97] Il n'y a donc pas de dommage financier pour le patrimoine des victimes avant que l'auteur ne fasse utilisation des données obtenues par le phishing.[98] Même dans l'optique où l'auteur accède aux comptes bancaires de ses victimes et effectuent des transferts menant à une diminution de leur patrimoine pour réaliser une escroquerie, il manquera encore le lien de causalité entre l'erreur de la dupe et la disposition du patrimoine.[99] En d'autres termes, la dupe n'est pas menée en erreur par la tromperie astucieuse pour mener elle-même un acte de disposition.[100] La victime ne provoque donc pas elle-même l'acte de disposition mais cette dernière nécessite une action supplémentaire de la part de l'auteur.[101] L'auteur de phishing n'est donc pas passible d'escroquerie à défaut de causalité entre l'erreur et l'acte de disposition.

---

91 Voir par exemple l'ATF 135 IV 76, c. 5.1.

92 Voir par exemple l'ATF 135 IV 76, c. 5.2.

93 Le caractère astucieux est en principe réalisé en présence de titres falsifiés au sens de l'art. 251 CP, il s'agit alors d'une manœuvre frauduleuse. Voir par exemple l'ATF 128 IV 18, c. 3a.

94 Voir par exemple l'arrêt du TF du 27 juin 2013, 6B_423/2013, c. 3.2.

95 Voir par exemple l'arrêt du TF du 9 mars 2010, 6B_543/2009, c. 2, ainsi que l'arrêt du TF du 5 octobre 2007, 6B_371/2007, c. 6.5.

96 Ammann, 198s.

97 Voir par exemple, Müller (2012), p. 83.

98 Ammann, 198s.

99 Müller (2012), p. 83.

100 Daniel Jositsch/Aline Lüthi, Betagte Menschen – präsidentinierte Betrugsopfer ? – Auseinandersetzung über die Grenzen der arglistigen Täuschung, dans : Schwarzenegger/Nägeli, 6. Zürcher Päventionsforum – Ältere Menschen und ihre Erfahrungen mit der Kriminalität, Zürich 2013, p. 61s.

101 Idem.

e. Utilisation frauduleuse d'un ordinateur (art. 147 CP)

[26] Tout comme l'escroquerie, l'infraction d'utilisation frauduleuse d'un ordinateur est une infraction de commission et protège le patrimoine.[102] L'art. 147 CP comprend trois éléments objectifs constitutifs essentiels ainsi que deux éléments constitutifs essentiels.[103]

[27] Premièrement, il faut une manipulation frauduleuse des données, sous la forme d'une utilisation incorrecte, incomplète ou indue de données.[104] Deuxièmement, il faut prouver l'influence sur un processus électronique ou similaire de traitement ou transmission de données de tel sorte qu'un résultat inexact soit obtenu.[105] Troisièmement, il faut un transfert d'actif au préjudice d'autrui ou sa dissimulation, à savoir que la victime ait subie un dommage patrimonial.[106] Enfin, un rapport de causalité entre la manipulation frauduleuse, l'obtention du résultat inexact entraînant un transfert d'actifs puis un préjudice patrimonial.[107] Sur le plan subjectif, l'art. 147 CP au même titre que l'escroquerie requiert l'intention de l'auteur, ainsi qu'un dessein d'enrichissement illégitime.[108]

[28] Si l'auteur du phishing emploi indûment les données obtenues de la victime pour effectuer une transaction bancaire sous l'identité de ses victimes, les éléments constitutifs objectifs de l'art. 147 CP sont en principe réunis.[109] En effet, pour une partie de la doctrine, il y a utilisation indue de données lorsque l'auteur obtient des données par un système d'hameçonnage.[110] Néanmoins, une question plus controversée est de déterminer si les données récoltées par l'auteur ont une valeur directe dans le patrimoine de la victime et s'il faut donc conclure à un dommage patrimonial à défaut d'un acte de disposition contre le patrimoine de la victime.[111] À tout le moins, un dommage patrimonial doit être retenu lorsque l'auteur se sert des données bancaires de ses victimes pour disposer de leurs valeurs patrimoniales et effectuer des paiements.[112]

f. Faux dans les titres (art. 251 et 110 IV CP ainsi que l'ATF 116 IV 343)

[29] L'infraction de faux dans les titres est un délit formel de mise en danger abstraite protégeant la confiance qui, dans les relations juridiques, est placée dans un titre comme moyen de preuve.[113] L'art. 251 CP protège donc la confiance individuelle placée dans les titres au sens de l'art. 110 IV CP destinés à prouver un fait ayant une portée juridique et tous les signes destinés à prouver un tel fait.[114] Premièrement, il convient de déterminer si un E-mail ou un site web fasli-

102 Gerhard Fiolka, BSK-StGB, ad art. 147 N 7.

103 PC-CP ad art. 147 N 1s.

104 Fiolka, BSK-StGB, ad art. 147 N 9.

105 PC-CP ad art. 147 N 14s.

106 PC-CP ad art. 147 N 16.

107 Stéphane Grodecki Commentaire Romand Code Pénal II, ad art. 147 N 16.

108 PC-CP ad art. 147 N 2.

109 Ammann, p. 200s.

110 Voir par exemple Ammann, p. 195 ainsi que Grodecki, CR-CP II ad art. 147 N 9.

111 Sur cette question voir notamment Métille/Aeschlimann, p. 285s et 302s.

112 Stoll, p. 104 et Müller p. 234s.

113 ATF 129 IV 53, c. 3.2.

114 PC-CP ad art. 251 N 4 pour une étude détaillée voir également Lorenz Aenis/David Mühlemann, « Zur Qualifikation von E-Mails als Urkunde », digma 2013, p. 164–168, p. 164ss.

fié constitue un titre au sens de l'art. 110 IV CP.[115] Deuxièmement, l'acte typique considéré porte sur la création et l'usage du faux d'un document digital, sous la forme d'un titre conformément à la définition de l'art. 110 IV CP, et faisant constater faussement un fait ayant une portée juridique.[116] S'agissant des éléments constitutifs subjectifs, l'intention ainsi qu'un dessein de porter atteinte aux intérêts pécuniaires ou aux droits d'autrui, ou de se procurer ou de procurer à un tiers un avantage illicite doivent être réunis.[117]

[30] La question principale est de déterminer si les sites webs falsifiés ainsi que les courriers électroniques envoyés par les auteurs de phishing constituent des titres au sens des art. 110 IV et 251 ch. 1 CP.[118] Un titre consiste en un écrit destiné à prouver un fait ayant une portée juridique.[119] Selon, l'interprétation du Tribunal fédéral se ralliant au à la *Geistigkeitstheorie*, un courrier de phishing en tant que faux document digital remplit les fonctions de perpétuité, de preuves et de garantie de l'identité de l'auteur et doit être considérer comme un faux matériel car le véritable auteur du titre ne correspond pas à l'auteur apparent.[120] Il en va de même en cas de faux grossier, aisément reconnaissable.[121] Il n'est pas nécessaire à cet égard, que la dupe ait pris connaissance du courrier pour que l'infraction soit consommée.[122] S'agissant d'un site web falsifié pour Boog et Müller, il s'agit là également d'un faux matériel s'il permet à la dupe d'ouvrir une session de e-banking d'apparence identique à une ouverte sur le site web de l'institution bancaire légitime.[123] Subjectivement, l'intention de l'auteur doit être reconnaissable dans le courrier envoyé. Il doit ainsi avoir su et voulu créer un faux document digital, à partir du moment où il usurpe l'identité d'une institution légitime, par exemple une institution bancaire. L'avantage illicite pouvant être de n'importe quelle nature, l'auteur du phishing réalise cette condition s'il agit dans le but d'obtenir des renseignements de la part de sa victime afin de les utiliser ou de les revendre, indépendamment de vouloir payer des biens et des services.[124]

V. Crypto-monnaies

[31] Les *e-wallets*, à savoir les porte-monnaies digitaux en ligne de crypto-monnaies constituent une cible privilégiée des auteurs de phishing.[125] Au premier plan, en considérant l'anonymat conféré par la technologie des registres distribués de type blockchain[126], il est primordial pour

115 PC-CP ad art. 251 N 4.

116 Müller, p. 82, Spas, p.7.

117 ATF 138 IV 130, c. 3.2.4 ; ATF 100 IV 180, c. 3a et 3d.

118 Pour un avis favorable voir Markus Boog, BSK-StGB ad Art. 251 N 175, ainsi que Ammann, p. 201s, pour un avis plus nuancé voir Müller (2012), p. 82ss.

119 Art. 110 ch. 4 CP.

120 ATF 137 IV 167, c. 2.3.1 ; 128 IV 265, c. 1.1.1.

121 ATF 137 IV 167, c. 2.4.

122 Voir l'ATF 132 IV 57, c. 5.1.1., l'ATF 123 IV 17, c.2e ainsi que Boog, BSK-StGB ad Art. 251 N 72 et PC-CP ad art. 251 N 10

123 Boog, BSK-StGB ad Art. 251 N 175 et Müller (2012), p. 82s.

124 Müller (2012), p. 82s, Stoll, p. 104.

125 Fabian Teichmann/Léonard Gerber, « Les tokens et les risques de compliance au Liechtenstein », Jusletter du 24 février 2020, p. 5, ainsi que les références citées.

126 À noter toutefois que contrairement à ses utilisateurs, les transactions effectuées sur la blockchain sont publiquement consultables sur le site suivant : https://live.blockcypher.com (consulté le 6 avril 2021). Voir également Fabian Teichmann/Léonard Gerber, « La surveillance informatique », Jusletter du 12 novembre 2020, p. 3.

les utilisateurs de protéger la clé d'authentification privée d'être divulguée à des tiers non-autorisés.[127] Selon la juridiction concernée, un vide juridique peut néanmoins subsister notamment quant à la surveillance des prestataires de services liés aux crypto-monnaies, ainsi qu'aux standards de sécurité informatique à adopter et à l'efficacité de la protection de leurs utilisateurs.[128] À défaut de tels standards applicables, la sécurité informatique des services offerts par les prestataires de services liés aux crypto-monnaies est délaissée à la responsabilité purement privée des prestataires de services et de leurs utilisateurs.[129]

[32] Parallèlement, le recours à des agents financiers et à des personnes morales établies à l'étranger ainsi que les nombreuses possibilités d'internationaliser les infractions préalables et le blanchiment d'argent connexe à un phishing liés aux crypto-monnaies constituent les principales vulnérabilités.[130] Le recouvrement des valeurs patrimoniales en temps opportun ou la preuve d'une infraction préalable constituent un défi pour les autorités de poursuite pénale.[131] Il s'ensuit alors de longues procédures d'entraide pénale internationale.[132]

VI. Conclusion

[33] Aux vues des aspects internationaux de la cybercriminalité à plus fortes raisons de la criminalité par le biais d'internet, les demandes d'entraides judiciaires auprès de l'OFJ seront nécessaires.[133] Les sites de phishing sont souvent hebergés à l'étranger sur des serveurs piratés d'utilisateurs tiers. Les auteurs passent également par des services de proxy établi à l'étranger pour créer les pages de phishing. Les données volées sont souvent distribuées à d'autres personne dans l'optique d'un réemploi sur le marché noir.[134] Par conséquent, il y a une multiplication des juridictions touchées et potentiellement compétentes pour traiter ou enquêter sur les infractions d'un auteur de phishing. La CCC constitue donc une première réponse envers la cybercriminalité internationale et un renforcement de la coopération internationale ayant permi l'introduction de l'art. 18b EIMP en droit suisse.

[34] Plus intéressant à cet égard, le Conseil fédéral dans son message daté de 2010 considère qu'il faille à l'avenir doté les offices compétents de services spécialisés car ils représenteront un atout sur le plan pratique dans la lutte contre la cybercriminalité.[135] Plus généralement, l'emprise des technologies modernes et la propagation de la cybercriminalité solliciteront progressivement les

---

127 Voir notamment Claudia Keller/Martin Hess, Rechtliche Anforderungen an System- und Datensicherheit und Compliance für webbasierte und mobile Zahlungen, dans : Weber/Thouvenin (éd.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zurich 2015, ZIK, p. 181–205, p. 199, ainsi que Teichmann/ Gerber (Liechtenstein), p. 3 et 5.

128 Fabian Teichmann, « Financing terrorism through cryptocurrencies – a danger for Europe ? », 2018, Journal of Money Laundering Control, vol. 21, N. 4, p. 515.

129 S'agissant de risques informatiques, il pourra potentiellement en aller ainsi de la Suisse en considérant le message du Conseil fédéral du 27 novembre 2019 relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres distribués, publié à la FF 2020 223, p. 250.

130 Rapport du GCBF, p. 44ss. Voir également Fabian Teichmann, « Recent trends in money laundering and terrorism financing », 2019, Journal of Money Laundering Control, vol. 27, N. 1, p. 7ss.

131 Rapport du GCBF, p. 44ss.

132 Teichmann/Gerber (surveillance informatique), p. 5 ainsi que les références citées.

133 FF 2010 4275, 4318.

134 Voir par exemple Métille/Aeschlimann, p. 302s.

135 FF 2010 4275, 4318s.

forces de police et les autorités de poursuite pénale.[136] Au niveau Suisse pour lutter contre les fraudes sur internet, la Centrale d'enregistrement et d'analyse pour la sûreté de l'informatique (MELANI) a été missionnée de recenser les modes opératoires et émettre des recommandations de sécurité informatique.[137] MELANI offre des réponses adaptées à chaque nouvelle fraude. Il en va également de même pour le Service national de coordination de la lutte contre la criminalité sur internet (SCOCI), de la Prévention Suisse de la Criminalité (PSC) ainsi que le Préposé fédéral à la protection des données et à la transparence (PFPDT).[138]

Auteur : Fabian Teichmann, Teichmann International (Schweiz) AG

Co-auteur : Léonard Gerber, Teichmann International (Schweiz) AG

136 FF 2010 4275, 4318.

137 Rappo/Stojaniovic, p. 60.

138 Métille/Aeschlimann, p. 286.