La soustraction de données par l'employé au regard des art. 143 et 179^{novies} CP

ELODIE LE GUEN

Table des matières

I. Introduction

Afin de permettre à l'employé d'effectuer les tâches pour lesquelles il a été engagé, l'employeur lui communique, au cours des rapports de travail, de nombreuses informations, sous plusieurs formes, pouvant concerner tant son entreprise, ses autres employés, ses fournisseurs que ses clients et qui revêtent parfois un caractère confidentiel, voire secret. À l'heure du tout numérique, la communication de ces informations à l'employé passe généralement par l'octroi d'un accès au système informatique de l'employeur.

Pendant les rapports de travail, la loi impose à l'employé, de par son devoir de diligence et de fidélité, non seulement d'utiliser les systèmes informatiques et autres installations techniques mises à sa disposition pour l'exécution de son travail conformément aux instructions de son employeur, mais également de ne pas faire usage ni révéler des faits destinés à rester confidentiels dont il a pris connaissance au service de celui-ci.

À la fin des rapports, ce devoir de diligence et de fidélité se concrétise par l'obligation qui est faite à l'employé de restituer à son employeur toutes les données remises par celui-ci, quel que soit le support sur lequel elles se trouvent, cette obligation portant tant sur les données contenues sur des supports papier que celles enregistrées électroniquement dont l'employé ne peut, sauf convention contraire, garder copie. En outre, l'employé peut être tenu au maintien de la confidentialité même après la fin des rapports de travail, dès lors que l'intérêt légitime de l'employeur le requiert.

Mais qu'en est-il lorsque l'employé s'approprie des données appartenant à son employeur, contre sa volonté, en particulier lorsque l'employé conserve des données ou fait usage de ses accès au système informatique de son ancien employeur après la fin des rapports de travail ? À quelles conditions la commission d'une infraction pénale peut-elle être reprochée à l'employé indélicat ?

Partant de la constatation que la majorité des affaires de soustraction de données dont les tribunaux ont eu à connaître ces dernières années s'inscrit dans

un contexte de rapports de travail – et notamment à la fin de ceux-ci – la présente contribution entend examiner comment sont mises en œuvre les dispositions pénales applicables en la matière.

À cette fin, nous examinerons l'infraction de soustraction de données au sens de l'art. 143 CP (section II) et celle de soustraction de données personnelles au sens de l'art. 179novies CP (section III), puis nous présenterons une sélection de décisions rendues par les instances fédérales et cantonales afin de mettre en exergue les difficultés de mise en œuvre des dispositions pénales examinées (section IV).

II. Soustraction de données (art. 143 CP)

Classé parmi les infractions portant atteinte au patrimoine, l'art. 143 CP a été introduit dans le Code pénal dans le but de rendre punissable ce que l'on appelle communément le « vol de données », soit l'obtention illégitime de données incorporelles qui ne faisait précédemment l'objet d'aucune protection pénale[1].

Réprimant le fait de soustraire, pour soi-même ou pour un tiers, dans un dessein d'enrichissement illégitime, des données enregistrées ou transmises électroniquement ou selon un mode similaire qui n'étaient pas destinées à l'auteur et qui étaient spécialement protégées contre un accès indu de sa part, la soustraction de données est une infraction poursuivie d'office. Elle est passible d'une peine privative de liberté de 5 ans au plus ou d'une peine pécuniaire et constitue un crime selon l'art. 10 al. 2 CP.

L'art. 143 CP entend protéger le droit du bénéficiaire légitime des données d'en disposer librement : c'est en quelque sorte la paix informatique qui est ainsi protégée[2]. Aussi, lorsque c'est le support informatique (tels qu'une clé USB, un disque dur externe, un CD-Rom, etc.) sur lequel les données sont enregistrées qui est soustrait, les dispositions classiques réprimant l'appropriation illégitime (art. 137 CP) ou le vol (art. 139 CP) trouveront application selon les circonstances[3].

Afin de cerner plus précisément quel type de comportement le législateur a voulu réprimer, nous examinerons successivement les éléments constitutifs objectifs (cf. titre A) et les éléments constitutifs subjectifs (cf. titre B) de l'infraction, puis

1 Message concernant la modification du Code pénal suisse et du Code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991 (cité : Message CP 1991), p. 977.

2 Macaluso Alain/Moreillon Laurent/Queloz Nicolas (édit.), *Commentaire romand Code pénal II, Art. 111-392 CP,* Bâle 2017 (cité : CR CP II-AUTEUR), MONNIER, art. 143 CP, N 5.

3 Message CP 1991, p. 977.

nous rappellerons brièvement les principes applicables s'agissant du cas privilégié (cf. titre C) et de la qualité de partie plaignante (cf. titre D).

A. Éléments constitutifs objectifs

1. Des données informatiques enregistrées ou transmises électroniquement

L'art. 143 CP vise exclusivement à protéger des données en tant qu'objet immatériel de propriété. Lors de l'adoption de cette disposition, le législateur a volontairement fait le choix de ne pas introduire de définition de la notion de données dans le Code pénal, ceci afin de tenir compte des développements technologiques futurs[4].

Le Message apporte tout de même un début de définition en précisant que les données au sens de la disposition considérée doivent être comprises « *au sens large comme toutes informations relatives à un état de faits, représentées sous forme de lettres, de nombres, de signes, de dessins, etc., qui sont transmises, traitées ou conservées en vue d'une utilisation ultérieure* »[5].

Il est en outre unanimement admis par la doctrine que les logiciels entrent dans la notion de données protégées au sens de cette disposition, quand bien même ils ne fournissent pas d'informations sur un état de fait en tant que tel[6]. Il s'ensuit que la notion de données au sens de cette disposition est particulièrement large et va au-delà des seules informations relatives à un état de fait.

En outre, le législateur a voulu limiter le champ d'application de cette disposition aux seules données qui sont traitées, mémorisées et transmises automatiquement au moyen d'un ordinateur, sous une forme généralement codée et non directement perceptible à l'œil, au moyen des logiciels qui assurent le fonctionnement d'une telle installation[7]. L'on admettra que l'on est en présence de données informatiques dans un cas précis, s'il apparaît que les données ne sont exploitables que par le biais d'un traitement automatisé de données et si elles peuvent être transformées par ce biais en une forme lisible[8]. Ainsi, la donnée de base (tels qu'une photographie, un film, des plans ou encore des données

4 Message CP 1991, p. 951.
5 Message CP 1991, p. 952.
6 Niggli Marcel Alexander/Wiprächtiger Hans (édit.), *Basler Kommentar Strafrecht (Strafgesetzbuch, Jugendstrafgesetz),* Bâle 2019, (cité : BSK StGB-AUTEUR), WEISSENBERGER, art. 143 CP, N 7 ; voir aussi CR CP II-MONNIER, art. 143 CP, N 4.
7 Message CP 1991, p. 952.
8 BSK StGB-WEISSENBERGER, art. 143 CP, N 10.

financières) n'est pas protégée du seul fait de son existence mais elle le deviendra à partir du moment où elle sera enregistrée sur un support informatique[9].

Il convient en revanche de relever que pour bénéficier de la protection de la loi, les données n'ont pas besoin de revêtir une valeur particulière, ni de constituer des informations privées, intimes ou secrètes[10]. Il n'est pas non plus nécessaire que les données soient une œuvre protégée par le droit d'auteur[11].

En guise de synthèse, on retiendra donc que l'art. 143 CP porte sur toutes données pouvant faire l'objet d'une communication humaine[12], pour autant qu'elles puissent être traitées, enregistrées ou transmises sous forme codée par un système de traitement de données informatiques[13].

2. Des données non destinées à l'auteur

Afin de réaliser les conditions de l'infraction, les données soustraites ne doivent pas être destinées à l'auteur[14]. On exclut ainsi les données qui sont librement accessibles à tout un chacun[15]. Il faut donc que l'auteur se procure lesdites données sans avoir le droit d'en disposer, étant précisé que le droit de disposition est en principe indépendant de la qualité d'auteur des données ou de celle de propriétaire du système de traitement de données[16]. De ce fait, les droits de la personnalité ou les droits d'auteur ne justifient pas à eux seuls un droit de disposition. Il faudra bien plutôt déterminer si le bénéficiaire légitime des données a voulu les mettre à la disposition de l'auteur ou si, au contraire, il a voulu l'en priver.

À cet égard, MONNIER cite l'exemple du patient qui s'introduit dans le système informatique de son médecin pour consulter les données médicales. Quand bien même les données ainsi consultées par l'auteur le concernent directement, il doit être admis que l'accès au système informatique n'a pas été autorisé par le médecin. Par conséquent, les données médicales qui y figurent n'ont pas été mises à la disposition de l'auteur et ne lui étaient donc pas destinées[17]. Cet exemple nous paraît convaincant et l'on peut soutenir, de manière analogue, que l'employé qui s'immisce dans le dossier informatique de son employeur pour prendre connaissance de son dossier personnel en brisant les protections informatiques mises en

9 CR CP II-MONNIER, art. 143 CP, N 5.
10 CR CP II-MONNIER, art. 143 CP, N 5.
11 Message CP 1991, p. 978.
12 CR CP II-MONNIER, art. 143 CP, N 4.
13 BSK StGB-WEISSENBERGER, art. 143 CP, N 8.
14 CORBOZ Bernard, *Les infractions en droit suisse,* vol. I, 3e éd., Berne 2010, art. 143 CP, N 6, p. 285 et N 7, p. 287.
15 CORBOZ, *op. cit.*, art. 143 CP, N 6, p. 286.
16 BSK StGB-WEISSENBERGER, art. 143 CP, N 15.
17 CR CP II-MONNIER, art. 143 CP, N 13.

place accède à des données qui ne lui étaient pas destinées, si l'employeur a voulu en limiter l'accès aux seules personnes autorisées du département des ressources humaines. Dans ce cas, le droit évident de l'employé à pouvoir accéder à son dossier personnel en vertu de l'art. 8 LPD n'empêche pas, à notre sens, la réalisation de l'infraction.

Déterminer si les données étaient ou non destinées à l'auteur dépendra ainsi des circonstances, mais il peut toutefois être retenu que l'absence de droit de disposition sur les données, de même que l'absence d'octroi d'un droit d'accès aux données, permettra généralement d'aboutir à la conclusion que les données n'étaient pas destinées à l'auteur de l'infraction.

3. Des données spécialement protégées

Outre le fait que les données ne doivent pas être destinées à l'auteur, la réalisation de l'infraction impose que les données fassent l'objet d'une protection spéciale contre un accès indu de sa part[18]. Cette protection contre les attaques extérieures doit être reconnaissable par l'auteur de l'infraction[19].

La loi n'apporte cependant pas de précision quant au degré de protection requis par l'art. 143 CP. La mesure de ce qui constitue une protection spéciale dépendra des circonstances du cas d'espèce, mais il est généralement admis qu'une mesure de protection sera suffisante si elle est de nature, dans le cas considéré, à empêcher les personnes non autorisées à accéder aux données, ou à tout le moins à en rendre l'accès beaucoup plus difficile[20]. Au titre des exemples de critères pouvant être utilisés pour apprécier de la suffisance de la protection mise en place, certains auteurs citent le standard habituel dans le domaine en question ou la branche considérée ainsi que la sensibilité des données à protéger[21].

En revanche, l'appréciation du caractère suffisant de la protection mise en place est indépendante des capacités de l'auteur concerné : il n'est ainsi pas attendu du bénéficiaire des données qu'il dispose de compétences informatiques plus importantes que l'auteur de l'infraction[22].

En ce qui concerne les mesures de protection spéciale à mettre en œuvre, on pense en premier lieu à une protection de type informatique intégrée dans le logiciel ou le système de traitement des données, tels que les mots de passe, les

18 CORBOZ, *op. cit.*, art. 143 CP, N 6, p. 285 et N 7, p. 287.
19 BSK StGB-WEISSENBERGER, art. 143 CP, N 18 ; CORBOZ, *op. cit.*, art. 143 CP, N 7, p. 286.
20 BSK StGB-WEISSENBERGER, art. 143 CP, N 19.
21 *Ibidem.*
22 MÉTILLE Sylvain/AESCHLIMANN Joanna, *Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ?, in* RPS 132 3, p. 291.

codes, le cryptage[23] ou encore la fragmentation des données empêchant le recoupement de celles-ci. L'utilisation de pare-feu ainsi que l'accès par carte magnétique ou par clés biométriques (avec reconnaissance des empreintes digitales, de la rétine, de la signature ou de la voix) sont autant de mesures de protection qui peuvent être mises en place dans ce contexte[24].

Quand bien même la disposition vise à protéger les données qui sont enregistrées ou transmises au moyen d'un système informatique, la doctrine admet qu'il n'est pas nécessaire que la barrière mise en place par le bénéficiaire des données soit de nature informatique. Une protection physique des données informatiques est déjà en soi suffisante, pour autant qu'elle soit reconnaissable pour l'auteur[25]. On citera à titre d'exemple l'ordinateur contenant les données qui serait conservé dans un coffre ou dans une armoire ou un bureau fermé à clé[26].

A contrario, si l'auteur s'est vu remettre, par le bénéficiaire des données, un accès à celles-ci (par exemple au moyen de mot de passe, d'une clé ou encore en lui accordant le droit de les consulter), on admettra alors que les données ne sont pas protégées contre l'accès de l'auteur même s'il ne respecte pas les éventuelles restrictions d'utilisation qui ont pu être prévues et que, ce faisant, il outrepasse ses droits. Une interdiction d'accès qui ne serait prévue que par la loi, la morale ou un contrat ne constitue pas une protection spéciale au sens de cette disposition. Dans un tel cas, l'infraction ne sera pas réalisée, le simple « détournement de données » ne tombant pas sous le coup de l'art. 143 CP, pas plus que le comportement de celui qui s'est vu accorder un accès à un logiciel protégé par le droit d'auteur et en fait des copies non autorisées[27].

En effet, le législateur a considéré qu'il n'était pas nécessaire – car le besoin ne s'en faisait pas sentir ni en Suisse ni à l'étranger – de pénaliser le comportement de celui qui est habilité à disposer des données mais qui outrepasse les limites de son droit d'utilisation[28]. Ce que l'on pourrait qualifier d'« abus de confiance informatique » n'est ainsi pas visé par l'art. 143 CP et ne constitue pas un comportement pénalement répréhensible en droit suisse.

4. Une soustraction

Contrairement à ce qui prévaut pour le vol au sens de l'art. 139 CP, la soustraction de données ne requiert pas que les données soient enlevées à leur possesseur

23 CR CP II-MONNIER, art. 143 CP, N 6.
24 BSK StGB-WEISSENBERGER, art. 143 CP, N 20.
25 CR CP II-MONNIER, art. 143 CP, N 6.
26 *Ibidem* ; voir aussi BSK StGB-WEISSENBERGER, art. 143 CP, N 20.
27 BSK StGB-WEISSENBERGER, art. 143 CP, N 16.
28 Message CP 1991, p. 978.

légitime et qu'il ne puisse plus en disposer. En ce sens, les données peuvent être soustraites même si leur titulaire légitime en a toujours la maîtrise[29]. Il suffit en effet pour réaliser le comportement typique de l'infraction que l'auteur acquière – lui aussi – la maîtrise des données en question, c'est-à-dire qu'il soit en mesure de les utiliser pour lui-même. Le fait que l'auteur ait pu lire les données en question est par conséquent suffisant pour que la maîtrise des données lui soit acquise[30].

B. Éléments constitutifs subjectifs

1. Intention

La soustraction de données est une infraction intentionnelle, le dol éventuel suffit. La simple négligence n'est en revanche pas punissable[31].

2. Dessein d'enrichissement

L'intention de l'auteur doit également porter sur un dessein d'enrichissement illégitime, soit sur sa volonté d'agir dans le but de se procurer ou de procurer à un tiers un enrichissement illégitime. Par enrichissement, il faut entendre tout avantage économique selon la doctrine[32]. Selon la définition classique qui en est donnée, l'enrichissement consiste soit à une augmentation de l'actif, à une diminution du passif, à une non-diminution de l'actif ou à une non-augmentation du passif[33].

Le dessein d'enrichissement illégitime sera évidemment réalisé lorsque l'auteur soustrait les données dans le but de les revendre à un tiers intéressé par celles-ci. On peut également citer le cas des données commerciales ou secrets techniques qui ne peuvent être développés qu'au prix de gros efforts[34]. Il suffit ainsi que ce faisant, l'auteur veuille s'épargner une dépense, par exemple les frais de recherches et de développement d'un produit pharmaceutique, pour que le dessein d'enrichissement illégitime soit réalisé[35].

29 CR CP II-MONNIER, art. 143 CP, N 12-13.
30 *Ibidem.*
31 BSK StGB-WEISSENBERGER, art. 143 CP, N 27.
32 CORBOZ, *op. cit.*, art. 138 CP, N 14, p. 237.
33 *Ibidem.*
34 BSK StGB-WEISSENBERGER, art. 143 CP, N 29.
35 CORBOZ, *op. cit.*, art. 143 CP, N 11, p. 287.

C. Cas privilégié

La soustraction de données commise au préjudice des proches (soit le conjoint, le partenaire enregistré, les parents en ligne directe, les frères et sœurs germains, consanguins ou utérins ainsi que les parents, frères et sœurs et enfants adoptifs[36]) ou des familiers (soit les personnes qui font ménage commun avec l'auteur[37]) ne sera poursuivie que sur plainte, conformément à l'art. 143 al. 2 CP, ce qui impliquera de respecter le délai de 3 mois prévu par l'art. 31 CP, sous peine de déchéance.

Si dans le contexte d'une relation de travail il est probable que cette disposition n'aura qu'une portée très limitée, elle pourra trouver application lorsque l'employeur et l'employé doivent être qualifiés de proches au sens de l'art. 110 al. 1 CP.

S'agissant de la qualité de familiers, soit le fait de vivre durablement en communauté de toit, de lit et de table et d'entretenir des relations personnelles étroites, analogues à une communauté familiale[38], elle ne devrait, à notre sens, être admise que de manière exceptionnelle, en présence d'un employé vivant au quotidien au domicile de son employeur, comme cela peut-être le cas de l'employé en charge de la garde des enfants ou du gardiennage. Dans ce cas, nous sommes d'avis que la qualité de familiers ne pourra être admise que pour autant que la relation présente une importante proximité[39] (par exemple lorsque la personne en charge de la garde des enfants prend ses repas avec la famille, part en vacances avec celle-ci et participe à la vie familiale) et que l'employé et l'employeur aient noué une relation personnelle dépassant le seul rapport de travail. À défaut d'une telle relation personnelle, le privilège de l'art. 143 al. 2 CP ne devrait, selon nous, pas trouver application dès lors que le ménage commun ne constituera, dans la plupart des cas, qu'une modalité de l'exécution du travail et non la manifestation d'une volonté de créer une communauté de vie analogue à celle d'une famille.

D. Qualité de partie plaignante

La qualité de partie plaignante en cas de soustraction de données doit être reconnue à toute personne qui, selon les règles de droit civil ou de droit public, est

36 Art. 110 al. 1 CP.
37 Art. 110 al. 2 CP.
38 Moreillon Laurent/Macaluso Alain/Queloz Nicolas/Dongois Nathalie (édit.), *Commentaire romand Code pénal I, Art. 1-110 CP,* Bâle 2021 (cité : CR CP I-AUTEUR), JEANNERET, art. 110 al. 2 CP, N 2.
39 CR CP I-JEANNERET, art. 110 al. 2 CP, N 4.

autorisée à disposer des données[40]. Il peut ainsi s'agir de l'exploitant du système de traitement de données mais pas nécessairement[41].

La qualité de partie plaignante doit ainsi être admise à l'employeur, qu'il soit une personne physique ou une personne morale, en tant que les données soustraites lui appartiennent, que celles-ci concernent son entreprise, ses produits ou services, ses employés ou ses clients.

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

L'art. 179^novies CP a été introduit en parallèle à la LPD et reprend par conséquent dans une très large mesure les notions contenues dans celle-ci.

Contrairement à l'art. 143 CP qui vise à protéger le droit du lésé à disposer librement de ses données informatiques, le but de l'art. 179^novies CP, à l'instar de la LPD, est de protéger la personne concernée par les données personnelles soustraites dans son droit fondamental à la protection de sa personnalité[42].

Le comportement réprimé consistant à soustraire d'un fichier des données personnelles sensibles ou des profils de la personnalité non librement accessibles n'est poursuivi, contrairement à l'art. 143 CP, que sur plainte et est passible d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Selon la systématique du Code pénal, l'infraction doit ainsi être qualifiée de délit conformément à l'art. 10 al. 3 CP.

Nous nous proposons d'examiner ci-après les éléments constitutifs objectifs (cf. titre A) et les éléments constitutifs subjectifs (cf. titre B) de l'infraction puis d'évoquer brièvement la qualité de partie plaignante (cf. titre C) et les modifications qui seront apportées à l'art. 179^novies CP à compter de l'entrée en vigueur de la nLPD (cf. titre D).

A. Éléments constitutifs objectifs

1. Des données contenues dans un fichier

Les données personnelles protégées par cette disposition doivent en premier lieu être contenues dans un fichier, ce par quoi on entend « *tout ensemble de données*

40 BSK StGB-RAMEL/VOGELSANG, art. 143 CP, N 35.
41 Message CP 1991, p. 979.
42 Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988 (cité : Message LPD 1988), p. 496.

personnelles dont la structure permet de rechercher les données par personne concernée » (art. 3 lit. g LPD).

Cette notion englobe toute forme de stockage d'informations qui permet d'effectuer une recherche en fonction de la personne physique ou morale au sujet de laquelle des données sont traitées[43]. Est déterminante la structure du fichier, indépendamment de la manière dont il est organisé. La recherche de personnes dans le fichier peut ainsi être aménagée grâce à des index, des numéros d'identification personnels, des codes ou autres[44].

MONNIER n'exclut pas que la notion de fichier puisse inclure également un fichier qui ne concernerait qu'une seule personne[45]. Nous partageons cet avis et considérons que le dossier individuel de l'employé préparé et conservé par l'employeur constitue déjà en soi un fichier même s'il ne concerne qu'un seul employé.

L'art. 179novies CP ne requiert pas que les données soient traitées et enregistrées de manière informatique[46]. Les données personnelles protégées par cette disposition peuvent ainsi être contenues dans un dossier papier, à la différence de l'art. 143 CP qui implique nécessairement un traitement informatique des données protégées.

2. *Des données personnelles sensibles ou des profils de la personnalité*

La soustraction réprimée par l'art. 179novies CP ne concerne pas toutes les données personnelles au sens de la LPD mais seulement celles qui requièrent une protection particulière car elles sont soit sensibles soit constitutives d'un profil de la personnalité.

La notion de données personnelles est définie à l'art. 3 lit. a LPD comme étant toutes les informations qui se rapportent à une personne identifiée ou identifiable. On admettra que la personne concernée par la donnée est identifiée si les données en question mentionnent son identité, alors qu'elle sera seulement identifiable si la personne qui traite les données peut l'identifier, pour autant que dite identification n'entraîne pas un travail disproportionné par rapport à

43 CORBOZ, *op. cit.*, art. 179novies CP, N 7, p. 688.
44 CR CP II-MONNIER, art. 179novies CP, N 3.
45 CR CP II-MONNIER, art. 179novies CP, N 2.
46 CORBOZ, *op. cit.*, art. 179novies CP, N 7, p. 688 ; BSK StGB-RAMEL/VOGELSANG, art. 179novies CP, N 21.

celui que le maître du traitement, respectivement le maître du fichier, mettrait lui-même en œuvre[47].

Une donnée personnelle est considérée comme « sensible » lorsqu'elle a trait à l'un ou l'autre des éléments exhaustivement listés à l'art. 3 lit. c LPD. Il s'agit ainsi des données concernant une personne identifiée ou identifiable qui se rapportent à ses opinions ou activités religieuses, philosophiques, politiques ou syndicales, à sa santé, sa sphère intime ou son appartenance à une race, aux mesures d'aide sociale ainsi qu'aux poursuites ou aux sanctions pénales et administratives la concernant.

On a affaire à un profil de la personnalité en présence d'« *un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique* » conformément à la définition prévue à l'art. 3 lit. d LPD.

Enfin, comme pour l'art. 143 CP, l'infraction de soustraction de données personnelles ne requiert pas que les données personnelles en question soient secrètes[48].

3. Des données non librement accessibles

Selon l'art. 179^novies^ CP, il faut encore que les données personnelles visées par la disposition ne soient pas librement accessibles à l'auteur. La définition du caractère non librement accessible des données fait l'objet d'une controverse doctrinale au sujet de laquelle le Tribunal fédéral n'a, à ce jour, pas encore eu à se prononcer.

Certains auteurs considèrent en effet que la protection pénale mise en œuvre par l'art. 179^novies^ CP nécessite que les données personnelles soient spécialement protégées contre un accès indu, à l'instar de ce qui prévaut pour l'art. 143 CP[49]. D'autres auteurs admettent en revanche qu'une protection spéciale de type technique ou physique n'est pas requise et qu'une interdiction contractuelle ou morale suffit[50].

---

47 CR CP II-MONNIER, art. 179^novies^ CP, N 5.

48 BSK StGB-RAMEL/VOGELSANG, art. 179^novies^ CP, N 20.

49 Corboz, *op. cit*., art. 179^novies^ CP, N 8, p. 688 ; BSK StGB-RAMEL/VOGELSANG, art. 179^novies^ CP, N 21 ; sans autre examen de la question : MÉTILLE/AESCHLIMANN, p. 295.

50 Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan, *Schweizerisches Strafgesetzbuch Handkommentar,* 4^e^ éd., Berne 2020 (cité : HK StGB-AUTEUR), art. 179^novies^ CP, N 2 ; MONTAVON Michel, *in* RFJ 2021, pp. 27 ss., 32-33 ; CELLINA Eva, *La commercialisation des données personnelles. Aspects de droit contractuel et de protection des données,* thèse de doctorat, Genève/Zurich/Bâle 2020, N 68, p. 20.

Se fondant sur une comparaison des textes des art. 143 et 179novies CP, MONNIER est en particulier d'avis qu'admettre la nécessité d'une protection spéciale contre un accès indu aux données personnelles reviendrait à introduire dans la loi une condition supplémentaire que le législateur n'a pas voulu[51]. Cet auteur retient, contrairement à ce qui prévaut pour l'art. 143 CP, que la protection de l'art. 179novies CP devrait trouver application même en présence d'une seule interdiction contractuelle[52], soit une barrière morale.

Nous partageons cet avis à la lumière des considérations suivantes.

D'une part, non seulement les textes des deux dispositions diffèrent dans leur version française, mais ils sont également différents dans leur version allemande. Ainsi, dans la version allemande de l'art. 143 CP, il est fait référence aux données « *die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind* » alors qu'à l'art. 179novies CP, il est fait mention des données « *die nicht frei zugänglich sind* ». Il ne s'agit ainsi pas d'une erreur de traduction entre la version allemande et la version française.

D'autre part, il convient de rappeler que le bien juridiquement protégé par ces deux dispositions n'est pas le même : alors que l'art. 143 CP entend réprimer le fait de porter atteinte au patrimoine du titulaire des données en troublant son droit d'en disposer librement, l'art. 179novies CP a été introduit afin de protéger, en tant que droit fondamental, la personnalité des personnes concernées par les données personnelles protégées. Les intérêts juridiques protégés par les deux normes étant différents, l'on ne peut partir du principe que le législateur a voulu imposer les mêmes conditions à la répression des deux infractions considérées.

Du reste, à teneur du Message, rien ne laisse penser qu'une protection spéciale serait nécessaire à la réalisation de l'infraction : « […] *est punissable celui qui a eu connaissance de ces données en s'introduisant dans des locaux ou des installations dont l'accès lui était interdit. L'auteur de l'infraction peut parvenir à prendre connaissance des données de différentes manières : il peut dérober des dossiers entiers ou partie de ceux-ci, il peut s'introduire dans le système à partir d'un terminal, ou encore il peut intercepter des transmissions de données* »[53]. Le Conseil fédéral n'a ainsi aucunement fait référence à la nécessité de protéger les données personnelles par l'instauration d'une barrière physique ou technique.

L'on peut souhaiter que le Tribunal fédéral ait à connaître prochainement de cette question afin de mettre un terme à la controverse doctrinale qui subsiste.

---

51 CR CP II-MONNIER, art. 179novies CP, N 8 ; dans le même sens : ERARD Frédéric, *Soustraction de données personnelles en milieu hospitalier,* 20 août 2021 *in* www.swissprivacy.law/85in www.swissprivacy.law/85.

52 CR CP II-MONNIER, art. 179novies CP, N 8 ; dans le même sens : ERARD Frédéric.

53 Message LPD 1988, p. 496.

4. Une soustraction

L'infraction est caractérisée par un comportement de soustraction. La notion étant la même que celle de l'art. 143 CP[54], il est ici renvoyé à ce qui a été dit précédemment (cf. p. 409).

B. Éléments constitutifs subjectifs

Tout comme pour la soustraction de données, la soustraction de données personnelles est une infraction intentionnelle et le dol éventuel suffit[55]. En revanche, à la différence de l'art. 143 CP, l'auteur n'a pas besoin d'avoir un dessein d'enrichissement illégitime pour réaliser l'infraction.

C. Qualité de partie plaignante

Comme mentionné plus haut, l'art. 179^{novies} CP a été introduit dans le but d'accroître la protection de la personnalité des personnes faisant l'objet des données personnelles soustraites. Aussi, la qualité pour déposer plainte appartient en premier lieu aux personnes dont les données personnelles ont été dérobées[56]. En l'état actuel du droit, tant les personnes physiques que les personnes morales concernées par les données personnelles soustraites ont la qualité de partie plaignante[57] mais cela est amené à changer prochainement, comme nous le verrons plus loin (cf. p. 417).

La doctrine est divisée s'agissant de la qualité de plaignant – et partant de lésé – du maître du fichier qui détient les données personnelles qui ne le concernent pas personnellement, certains auteurs reconnaissant une telle qualité et d'autres la niant[58]. CORBOZ, en particulier, considère que l'exploitant doit se voir accorder la qualité de plaignant dès qu'il peut être civilement responsable[59]. Nous sommes d'avis que l'employeur devrait pouvoir se constituer partie plaignante du seul fait que sa responsabilité civile pourrait être engagée lorsque les données personnelles soustraites concernent des tiers. Une précision du Tribunal fédéral serait toutefois bienvenue à cet égard également.

---

54 CR CP II-MONNIER, art. 179^{novies} CP, N 9.
55 CR CP II-MONNIER, art. 179^{novies} CP, N 10.
56 CR CP II-MONNIER, art. 179^{novies} CP, N 11.
57 La LPD protège les données personnelles des personnes physiques et des personnes morales : art. 2 al. 1 LPD.
58 CR CP II-MONNIER, art. 179^{novies} CP, N 11 et les références citées.
59 CORBOZ, *op. cit.*, art. 179^{novies} CP, N 11, p. 689.

D. Révision totale de la loi sur la protection des données : modification de l'art. 179novies CP

Avec l'entrée en vigueur de la nLPD annoncée au 1er septembre 2023, l'art. 179novies CP subira également des modifications. Sa nouvelle teneur sera la suivante : « *Celui qui aura soustrait des données personnelles sensibles qui ne sont pas accessibles à tout un chacun sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire* »[60].

Avec l'entrée en vigueur du nouveau droit, l'infraction sera toujours constitutive d'un délit. Elle ne concernera en revanche plus les données personnelles des personnes morales, ces dernières n'étant plus soumises à la protection de la loi[61].

Les références au profil de la personnalité et au fichier seront par ailleurs supprimées de l'art. 179novies CP, pour faire suite à l'abrogation de ces notions dans la nLPD. Seules les données personnelles sensibles seront protégées par le nouvel art. 179novies CP, soit les données listées de manière exhaustive à l'art. 5 lit. c nLPD : les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'origine raciale ou ethnique, les données génétiques, les données biométriques identifiant une personne physique de manière univoque, les données sur des poursuites ou sanctions pénales et administratives et les données sur des mesures d'aide sociale.

Il est intéressant de constater que, dans sa nouvelle teneur, l'art. 179novies CP ne fera plus référence aux données « *qui ne sont pas librement accessibles* », cette notion étant remplacée par l'expression « *qui ne sont pas accessibles à tout un chacun* »[62]. Le Message ne précise pas ce qu'il faut entendre par cette nouvelle formulation. Cela étant, nous sommes d'avis que le choix du législateur d'opter pour une formulation différente de celle utilisée à l'art. 143 CP confirme la position soutenue dans la présente contribution selon laquelle il ne peut être requis, afin de réaliser l'infraction réprimée par l'art. 179novies CP dans sa version actuelle, que les données soustraites aient fait l'objet de mesures de protection de nature physique ou technique, une interdiction « morale » ou contractuelle devant suffire. Il devra, selon nous, en aller de même avec la modification de l'art. 179novies CP.

60 FF 2020 7397, 7445.

61 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017 (cité : Message LPD 1997), p. 6741 ; voir aussi art. 2 al. 1 nLPD.

62 Message LPD 1997, p. 6741.

IV. Application pratique des art. 143 et 179^{novies} CP dans le cadre de la relation de travail

Les conditions nécessaires à la réalisation des infractions de soustraction de données et de soustraction de données personnelles ayant été rappelées, nous résumerons dans le présent chapitre quelques décisions topiques dans lesquelles ces infractions ont été examinées dans le cadre de rapports de travail (cf. titre A), ce qui nous amènera ensuite à faire un certain nombre de constats s'agissant de la mise en œuvre de ces dispositions (cf. titre B).

A. Aperçu de jurisprudence

1. Jugement de la Cour des affaires pénales du Tribunal pénal fédéral SK.2014.46 du 27 novembre 2015 (art. 143 CP)

Dans cette affaire, il était reproché à un ancien employé de la banque pour laquelle il travaillait en qualité d'informaticien, d'avoir soustrait, au cours des rapports de travail, sur une période de plus de deux ans, de très nombreuses données détenues par la banque employeuse concernant en particulier l'identité de ses clients, leurs avoirs, le montant de leurs investissements ainsi que le type d'investissements effectués, en les transférant et les enregistrant sur ses propres supports informatiques. L'employé indélicat avait ensuite tenté de vendre ces données à plusieurs banques et organismes étatiques étrangers.

Selon le Ministère public de la Confédération, qui soutenait que le comportement reproché au prévenu était constitutif – entre autres – d'une soustraction de données au sens de l'art. 143 CP, les données dérobées auraient fait l'objet de trois niveaux de protection que l'employé serait parvenu à briser. Premièrement, les données étaient fragmentées, c'est-à-dire que les données personnelles des clients n'étaient jamais mises en relation avec les données patrimoniales de ceux-ci. Deuxièmement, les données étaient soit fictives, soit soumises à un programme de cryptage ou d'anonymisation. Troisièmement, l'extraction de données était interdite par la réglementation interne de la banque employeuse ainsi que par la configuration des appareils utilisés.

S'agissant de la première mesure de protection invoquée par l'accusation, il a été reconnu que les données personnelles et les données patrimoniales des clients de la banque faisaient bien l'objet d'une ségrégation. Le Tribunal pénal fédéral a toutefois considéré que même si une telle fragmentation était utile, elle ne constituait pas, à elle seule, une mesure de protection suffisante au sens de l'art. 143 CP dès lors que l'employé détenait une multitude de mots de passe lui permettant d'accéder aux données personnelles mais également aux données

financières de clients. De plus, l'instruction n'avait pas permis d'établir à quels systèmes informatiques de la banque et, cas échéant, à quels moments, l'employé avait eu accès pendant ses rapports de travail. Or, dans la mesure où d'anciens collègues avaient déclaré qu'il était normal que le prévenu ait accès, à tout le moins temporairement, à plusieurs des fichiers retrouvés sur ses supports informatiques privés, il ne pouvait être retenu qu'il aurait soustrait des données qui ne lui étaient pas destinées et qui auraient été protégées contre son accès. Il s'est de surcroît avéré que la fragmentation des données était en réalité inopérante, la preuve ayant pu être apportée que certains rapprochements pouvaient être effectués entre les données personnelles et les données financières des clients au moyen de simples recherches par mots-clés dans les documents.

Pour ce qui est ensuite de la deuxième protection spéciale tenant au fait que seules des données fictives, cryptées ou anonymisées auraient été utilisées pour travailler, cette preuve n'avait pas pu être apportée lors de l'instruction dès lors qu'il ressortait de certains fichiers que des données réelles concernant des clients étaient enregistrées sans autre protection.

Enfin, la troisième protection alléguée par l'accusation selon laquelle les règles internes de la banque interdisaient aux employés d'extraire des données et de les enregistrer sur des supports privés ne constituait pas une protection spéciale au sens de l'art. 143 CP.

Fort de ces constatations, le Tribunal pénal fédéral a retenu que les protections alléguées par l'accusation ne constituaient pas une protection spéciale suffisante au sens de l'art. 143 CP et a donc acquitté l'employé du chef de l'infraction de soustraction de données, sans autre examen.

2. Décision de la Cour des plaintes du Tribunal pénal fédéral BB.2019.248-249 du 26 janvier 2021 (art. 143 CP)

Les recourants – soit la société employeuse et l'un de ses administrateurs – prétendaient que leur ancien employé aurait piraté le système informatique de la société, ce qui lui aurait permis d'accéder puis de copier l'intégralité des données confidentielles contenues sur les serveurs du groupe auquel la société appartenait.

Le Ministère public de la Confédération soutenait, quant à lui, que, si l'employé avait bien transféré un grand nombre d'informations appartenant à la société employeuse, il avait été en mesure de le faire car il avait été mis en possession des mots de passe des ordinateurs de deux des administrateurs de la société. De plus, aucun élément ne laissait apparaître que les données provenant du serveur de la société auraient fait l'objet d'une protection spécifique. Faute pour les

données d'avoir été spécialement protégées, le Ministère public de la Confédération a refusé d'étendre l'instruction ouverte contre l'employé à la soustraction de données au sens de l'art. 143 CP.

À l'appui de leur recours contre cette décision, les recourants reprochaient au Ministère public de la Confédération de ne pas avoir instruit la question de savoir si l'employé disposait de mots de passe et, cas échéant, dans quelles circonstances lesdits mots de passe lui auraient été confiés, ni à quel contenu ils lui auraient permis d'accéder.

Procédant à l'examen du dossier, le Tribunal pénal fédéral a relevé qu'il appartenait aux recourants, en tant qu'ils alléguaient que leurs propres données auraient été « volées », d'apporter les précisions utiles sur la manière dont était géré le parc informatique de la société, sur la configuration des appareils, sur les procédés techniques mis en place afin d'empêcher un accès aux données et sur la manière dont l'employé avait eu accès à ces données.

Quand bien même les plaignants avaient produit des rapports d'analyse de la boîte email ainsi que l'ordinateur professionnels de l'employé (desquels il ressortait notamment que celui-ci aurait enregistré des données sensibles de la société sur Dropbox, qu'il aurait transféré des données entre ses boîtes email professionnelle et privée et que, dans les vingt-quatre heures précédant la fin de ses rapports de travail avec la société, il aurait connecté des clés USB et un Blackberry à son ordinateur professionnel), ces rapports n'apportaient aucune information sur les mesures de sécurité mises en place au sein de la société ni sur la protection que le prévenu aurait dû surmonter pour avoir accès aux données.

Retenant que l'employé avait été mis en possession des mots de passe pour accéder aux ordinateurs de deux des administrateurs de la société, le Tribunal pénal fédéral a considéré qu'il n'existait en réalité pas de protection suffisante au sens de l'art. 143 CP et a confirmé la décision du Ministère public de la Confédération de ne pas étendre son instruction à l'infraction de soustraction de données.

3. Arrêt de la Cour de justice de la République et canton de Genève ACPR/94/2020 du 5 février 2020 (art. 143 CP)

La société employeuse reprochait à son ancien employé, engagé en qualité de technicien, d'avoir accédé à son système informatique, quelques jours après la fin des rapports de travail, au moyen de son identifiant informatique qui n'avait pas été désactivé. Elle en avait déduit que l'employé aurait prélevé des données confidentielles appartenant à la société qu'il aurait transférées tant sur son téléphone portable que sur son ordinateur personnel.

Le Ministère public avait d'emblée rendu une ordonnance de non-entrée en matière, faute d'éléments permettant la mise en prévention de l'employé.

La société employeuse a recouru contre cette ordonnance devant la Cour de justice et faisait grief au Ministère public de ne pas avoir retenu que son ancien employé s'était connecté à son système informatique 7 jours après la fin du contrat de travail entre les parties, qu'il avait agi de manière intentionnelle, preuve en était qu'il avait refusé de signer le courrier que la société lui avait remis le dernier jour des rapports de travail lui rappelant son obligation de diligence et de fidélité et qu'il avait produit, dans une procédure prud'homale opposant les parties, des documents appartenant à la société.

Le Ministère public considérait, de son côté, que même si les éléments du dossier avaient pu confirmer qu'une personne s'était connectée au système de la société employeuse avec l'identifiant de l'ancien employé quelques jours après la fin des rapports de travail, rien ne permettait d'établir qu'il s'agissait effectivement de l'ancien employé. De surcroît, la société avait elle-même précisé, dans sa plainte, avoir « déduit » que son ancien employé avait transféré des données de la société sur son téléphone portable et sur son ordinateur. Ses accusations ne reposaient ainsi que sur des suppositions et non pas sur des éléments objectifs.

Examinant les griefs soulevés par la recourante, la Cour de justice a relevé que la société n'avait pas rendu vraisemblable l'existence d'un quelconque enrichissement illégitime de son ancien employé. Pour ce motif déjà, il n'existait pas de prévention pénale suffisante de la commission de l'infraction de soustraction de données.

De surcroît, selon la Cour de justice, même à supposer que l'ancien employé se serait effectivement connecté au système informatique de la société et aurait soustrait à cette occasion des documents confidentiels, la simple utilisation de son identifiant informatique et de son mot de passe – qui n'avaient pas été modifiés par la société à la fin des rapports de travail – lui aurait suffi à accéder aux serveurs contenant les données. Ce faisant, il n'aurait rencontré aucune mesure de sécurité spécifique lui entravant l'accès aux données et n'aurait pas dû surmonter un quelconque obstacle de sécurité mis en œuvre volontairement par la société. Le simple fait que les rapports de travail existant entre la société et l'employé aient pris fin au moment du téléchargement de données ne suffisait pas à retenir un accès indu, faute de sécurité suffisante, de type technique, permettant de remplir les réquisits posés par l'art. 143 CP. Le recours de la société a donc été rejeté et l'ordonnance de non-entrée en matière confirmée.

4. Jugement du Juge des districts de Martigny et St-Maurice TDMR P1 05 34 du 28 juin 2005 – in RVJ 2006, pp. 222 ss. (art. 143 et 179^{novies} CP)

Une société active dans le domaine des services internet, notamment dans la création de sites internet et l'hébergement de messagerie, a suspecté son employé (engagé en qualité d'informaticien-stagiaire), en raison d'un contrôle technique fortuit, d'avoir accédé de façon indue à un domaine de son réseau interne et d'avoir effectué des copies de logiciels ainsi que d'autres données confidentielles de la société et de ses clients. Il a encore été constaté que l'employé s'était envoyé les fichiers copiés sur son adresse email privée. L'employé soutenait qu'il n'avait pas transmis à des tiers ni fait usage des données soustraites et prétendait avoir agi de la sorte soit pour pouvoir continuer à travailler depuis son domicile, soit par curiosité.

À la suite de la plainte pénale déposée par l'employeur, l'employé a notamment été mis en prévention de soustraction de données au sens de l'art. 143 CP ainsi que de soustraction de données personnelles au sens de l'art. 179^{novies} CP.

Amené à se prononcer sur les infractions devant faire l'objet de la mise en accusation, le Juge des districts de Martigny et St-Maurice a relevé que c'était parce que l'employé avait été mis au bénéfice du mot de passe qui lui permettait de s'acquitter de ses obligations contractuelles à l'égard de son employeur qu'il avait été en mesure d'accéder aux serveurs contenant les données dont il s'était ensuite emparé. Bien que les serveurs en question fussent protégés contre des intrusions externes au moyen notamment de contrôles d'accès biométriques et de pare-feu, l'employé n'avait rencontré aucune mesure de sécurité spécifique entravant son accès aux logiciels de l'employeur ou aux données de ce dernier. Compte tenu de cette absence de barrière technique, les éléments constitutifs de l'art. 143 CP n'étaient pas réalisés et un renvoi en jugement fondé sur cette disposition ne se justifiait dès lors pas.

Dans un *obiter dictum,* le Juge des districts de Martigny et St-Maurice a laissé entendre que le même raisonnement devait s'appliquer s'agissant de la soustraction de données personnelles au sens de l'art. 179^{novies} CP, considérant qu'il était nécessaire que les données personnelles soient particulièrement protégées, ce qui impliquait pour l'auteur de devoir surmonter des obstacles de nature technique pour se procurer les données. Or, il était ressorti de l'instruction que l'employé avait un accès « libre » aux serveurs de son employeur, que les données soustraites se trouvaient dans son environnement de travail et qu'il n'avait pas dû franchir de « barrière interdite » pour réaliser ses opérations, les employés travaillant dans un climat de confiance, seul un « contrat moral » leur

imposant d'utiliser les seules données nécessaires à leur propre travail. L'infraction de soustraction de données personnelles n'était par conséquent pas non plus réalisée.

5. *Arrêt de la Cour d'appel pénal du Tribunal cantonal de Fribourg 501 2020 136 du 9 juin 2021 – in RFJ 2021, pp. 27 ss. (art. 179novies CP)*

Une patiente avait déposé une plainte pénale pour soustraction de données personnelles au sens de l'art. 179novies CP contre une médecin-assistante à qui elle reprochait d'avoir accédé, sans motif légitime, à son dossier médical informatisé. En l'occurrence, le dossier médical en question se trouvait sur un site différent de celui sur lequel était occupée la médecin-assistante. Selon le système mis en place par le réseau hospitalier concerné, pour accéder à un dossier médical qui ne faisait pas partie de son périmètre, un employé devait se connecter au réseau informatique au moyen de son identifiant et de son mot de passe personnels puis indiquer la raison pour laquelle il souhaitait accéder au dossier en question. S'agissant de la justification de la consultation du dossier à apporter, il suffisait que l'employé inscrive n'importe quel motif dans un champ prévu à cet effet. Le champ en question était généralement incomplet, vide, voire incompréhensible.

Se prononçant sur les conditions d'application de l'art. 179novies CP, le Tribunal cantonal fribourgeois a retenu que « *des données ne sont pas librement accessibles au sens de cette disposition lorsque l'auteur doit surmonter des obstacles de nature technique pour se les procurer. Si les données soustraites sont librement accessibles à l'auteur et qu'il n'a pas dû déjouer de barrière technique pour y accéder mais uniquement la barrière que représente l'être humain, l'infraction de l'art. 179novies n'est pas réalisée* »[63].

Dans cet arrêt, le Tribunal cantonal fribourgeois a constaté que l'accès par un employé aux dossiers médicaux qui se trouvaient hors de son périmètre était techniquement possible dès lors que la seule limitation à cet accès était la confiance et la conscience professionnelle du collaborateur. Se référant à la décision du Juge des districts de Martigny et St-Maurice dans l'affaire résumée plus haut (cf. p. 422), le Tribunal cantonal fribourgeois est parvenu à la conclusion que la médecin-assistante n'avait pas eu à franchir de « barrières interdites » pour accéder aux données médicales litigieuses dès lors qu'il lui avait suffi de se connecter au moyen de ses propres accès et d'indiquer le motif pour lequel elle désirait

63 Arrêt de la Cour d'appel pénal du Tribunal cantonal de Fribourg du 9 juin 2021 (501 2020 136), c. 2.2.2 ; voir aussi résumé et critique de cet arrêt par MONTAVON Michael, *in* RFJ 2021, pp. 27 ss.

accéder à ce dossier, tout en sachant qu'aucune autre exigence technique n'était posée quant à la justification de cette consultation. Les conditions objectives nécessaires à la réalisation de l'infraction de soustraction de données personnelles selon l'art. 179^{novies} CP n'étaient par conséquent pas réunies.

B. Commentaire des arrêts choisis

L'examen des décisions rendues ces dernières années en lien avec l'infraction de soustraction de données au sens de l'art. 143 CP met en lumière le fait qu'il n'est de loin pas aisé de démontrer la réalisation des conditions objectives de l'infraction, en particulier la protection spéciale des données prétendument soustraites. Dans chacun des cas examinés, l'accusation, mais également l'employeur en tant qu'il participe comme plaignant à la procédure pénale dirigée contre un employé indélicat, se sont heurtés à la difficulté d'apporter la preuve du fait que des mesures de protection suffisantes avaient été mises en place et que celles-ci étaient à même d'empêcher l'employé d'accéder aux données dont la soustraction lui était reprochée.

La charge de la preuve de la soustraction de données repose en effet dans une large mesure sur le plaignant, soit l'employeur dans de nombreux cas. Quand bien même l'infraction est poursuivie d'office, il est attendu du plaignant qu'il collabore proactivement à l'instruction en fournissant les informations pertinentes sur les mesures de protection mises en place, dès lors qu'il sera généralement la personne la plus à même d'expliquer – et de prouver – le fonctionnement de ses installations et la sécurisation mise en œuvre pour empêcher un accès indu à ses données.

La collaboration attendue du plaignant à l'établissement des faits sera d'autant plus importante que les faits reprochés s'inscrivent dans un rapport de travail. En effet, dans ce cas, l'employé, en tant qu'il est intégré dans l'organisation de travail de son employeur, se sera généralement vu accorder certains droits d'accès aux données de ce dernier afin de pouvoir effectuer ses tâches, contrairement à ce qui prévaut pour un tiers externe à l'entreprise. Dans ce contexte, il est essentiel que l'employeur – s'il veut que sa plainte ait des chances de déboucher sur une mise en accusation – puisse identifier et exposer précisément, déjà au stade du dépôt de la plainte pénale, i) quelles sont les données auxquelles l'employé avait accès, ii) quand et comment cet accès lui a été accordé, iii) quelles sont les données auxquelles l'accès lui était interdit, iv) par quelles mesures les données auxquelles l'employé n'avait pas accès étaient protégées et v) comment l'employé est parvenu à briser la protection mise en place. Une telle démonstration nécessitera, selon nous, très souvent la mise en œuvre d'une analyse forensique des systèmes informatiques de l'employeur. Or, une telle analyse ne sera ordonnée par le Ministère public que si celui-ci décide d'ouvrir une procédure, ce qui

n'est pas garanti compte tenu des difficultés exposées ci-avant. Aussi, l'employeur pourrait devoir faire le choix de mandater un expert privé, lui permettant de corroborer les faits qu'il dénonce à l'appui de sa plainte pénale. Une telle analyse peut toutefois se révéler très onéreuse et dissuader l'employeur d'y recourir à ses propres frais, réduisant ainsi ses chances de provoquer l'ouverture d'une procédure pénale contre l'employé.

Lorsqu'une violation de l'art. 143 CP est en cause, il appartiendra en outre à l'employeur de rendre à tout le moins vraisemblable le dessein d'enrichissement illégitime de l'employé ou ancien employé concerné, en indiquant aux autorités pénales les preuves dont l'administration est requise à cet égard. L'employeur ne pourra en effet pas se contenter de démontrer que des données ont été soustraites contre son gré mais devra également expliquer pourquoi ces données constituent un avantage économique pour l'employé. À défaut, la plainte de l'employeur aura de grandes chances d'aboutir à une ordonnance de non-entrée en matière ou de classement.

L'on constate par ailleurs qu'il ne suffit pas pour le plaignant – soit l'employeur dans le contexte qui nous occupe – d'invoquer l'existence de mesures de protection, encore faut-il que les mesures en question soient réellement mises en œuvre au sein de son organisation. Le doute devant profiter à l'accusé, si la mise en œuvre des mesures de protection technique ou organisationnelle n'est pas démontrée ou si les mesures mises en place s'avèrent finalement inopérantes, la soustraction ne sera pas admise.

Comme l'a rappelé récemment le Tribunal pénal fédéral : « *Il n'y a 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. Les instructions, les interdictions orales ou écrites, ou encore les mesures d'organisation visant à séparer les fonctions au sein du personnel ne constituent pas des mesures de sécurité suffisantes au sens de l'art. 143 CP* […] »[64].

Dans le contexte de rapports de travail, il ne suffira ainsi pas que l'employé se soit engagé contractuellement à une utilisation diligente et précautionneuse des moyens de communication et appareils électroniques mis à sa disposition et à garder confidentielle toute information en lien avec son employeur, même après la fin des rapports de travail. De telles clauses contractuelles ne permettent pas de protéger les données contre un accès indu au sens de l'art. 143 al. 1 CP[65].

Les constatations qui précèdent vaudront probablement lorsque la violation de l'art. 179novies CP est en cause, même si le Tribunal fédéral n'a, pour l'instant, pas tranché la controverse qui subsiste en doctrine s'agissant du niveau de protection

64 TPF 2019 248-249 du 26 janvier 2021, c. 4.2.
65 TPF 2019 248-249 du 26 janvier 2021, c. 4.5.6.

nécessaire à la réalisation de soustraction de données personnelles. Cela étant, les quelques décisions rendues par les tribunaux cantonaux vont plutôt dans le sens d'une interprétation identiques des deux dispositions en ce qui concerne le niveau de protection requis. Bien que cette solution ne nous paraisse pas conforme au but de l'art. 179^novies^ CP, les décisions cantonales examinées retiennent que l'art. 179^novies^ CP impose, de la même manière que l'art. 143 CP, que les données soustraites fassent l'objet d'une protection spécifique – de nature technique ou physique – et pas uniquement d'une « barrière morale ». Le plaideur prudent sera donc bien avisé de faire état, au stade de la plainte, des mesures de protection techniques ou physiques qu'il a mises en place pour empêcher l'accès aux données personnelles s'il allègue une violation de cette disposition.

Enfin, lorsque le comportement reproché par l'employeur consiste à accéder à des données ou à les conserver après la fin des rapports de travail, en violation des dispositions contractuelles applicables ou des instructions données, les conditions des dispositions examinées ne seront pas réalisées si l'employé a pu accéder aux données ou les copier parce qu'il a été mis en possession des moyens d'accès utiles à cet effet par l'employeur et ce, même si la collecte de données par l'employé porte sur un très grand nombre de données, s'est déroulée durant de nombreuses années, était systématique et a été réalisée dans un dessein d'enrichissement illégitime.

V. Conclusion

Après avoir procédé à l'examen des décisions rendues ces dernières années par les instances fédérales et cantonales, force est de constater que les art. 143 et 179^novies^ CP ne permettront que très difficilement à l'employeur de faire constater l'existence d'un comportement pénalement répréhensible de l'employé, peu importe que les faits reprochés aient lieu pendant ou après les rapports de travail. Au vu des difficultés d'application des dispositions examinées, l'on peut douter du caractère réellement dissuasif de celles-ci.

De surcroît, même dans les cas où l'employeur parvient, malgré les difficultés de preuve discutées, à obtenir la condamnation de son employé ou ancien employé, il faudra bien admettre que le but de la protection mise en œuvre n'aura pas été atteint.

Aussi, si l'on peut regretter que le Conseil fédéral n'ait pas jugé utile de pénaliser le comportement de celui qui, malgré une interdiction légale ou contractuelle, copie ou conserve des données, il apparaît que la prévention de la « fuite » de données passera nécessairement par la mise en place par l'employeur de mesures techniques et organisationnelles efficaces – particulièrement en cas de résiliation des rapports de travail – plutôt que par la menace d'une sanction pénale.