Droit pénal (CP) - Strafrecht (StGB)

TDMAR P1 05 34

Jugement du juge des districts de Martigny et St-Maurice du 28 juin 2005, Ministère public et Y. SA c. X.

Violation du secret de fabrication ou du secret commercial; soustraction de données personnelles; violation du secret des postes et des télécommunications.

– Eléments constitutifs de la violation du secret des postes et des télécommunications (art. 321ter al. 1 CP); en l'espèce, employé d'une société active dans la création de sites internet et l'hébergement de messageries qui copie des fichiers et les transfère sur son PC privé (consid. 2).

– Eléments constitutifs de la violation du secret de fabrication ou du secret commercial (art. 162 CP; consid. 3 et 4).

– Eléments constitutifs de la soustraction de données personnelles (art. 179novies CP; consid. 3 et 5).

Verletzung des Fabrikations- oder Geschäftsgeheimnisses; unbefugtes Beschaffen von Personendaten; Verletzung des Post- und Fernmeldegeheimnisses.

– Tatbestandsmerkmale der Verletzung des Post- und Fernmeldegeheimnisses (Art. 321ter Abs. 1 StGB); vorliegend Fall eines Angestellten einer Gesellschaft, die Internetseiten herstellt und einen Mailservice betreibt, der Dateien kopiert und auf seinen privaten PC überträgt (E. 2).

– Tatbestandsmerkmale der Verletzung des Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB; E. 3 und 4).

– Tatbestandsmerkmale des unbefugten Beschaffens von Personendaten (Art. 179novies StGB; E. 3 und 5).

Considérants (extraits)

(...)

2. L'arrêt de renvoi dressé par la Chambre pénale du Tribunal cantonal le 19 mai 2005 retient à l'encontre de l'accusé l'infraction réprimée par l'art. 321ter al. 1 CP.

a) Aux termes de cette disposition, celui qui, en sa qualité de fonctionnaire, d'employé ou d'auxiliaire d'une organisation fournissant des services postaux ou de télécommunication, aura transmis à un tiers des renseignements sur les relations postales, le trafic des paie-

ments ou les télécommunications de la clientèle, ouvert un envoi fermé ou cherché à prendre connaissance de son contenu ou encore fourni à un tiers l'occasion de se livrer à un tel acte sera puni de l'emprisonnement ou de l'amende.

aa) Objectivement, cette infraction ne peut être commise que par une personne astreinte au secret des postes ou des télécommunications, du fait de son activité professionnelle. Ce devoir incombe à toutes les personnes physiques ou morales offrant des services de télécommunication; les premières, que ce soit en qualité de responsables ou d'auxiliaires. Ce secret couvre les télécommunications au sens des art. 2 et 3 let. c de la loi fédérale du 30 avril 1997 sur les télécommunications (LTC; RS 784.10). Il s'agit de toute transmission d'informations sur des lignes ou par ondes herziennes, au moyen de signaux électriques, magnétiques ou optiques ou d'autres signaux électromagnétiques (art. 3 let. c LTC). Les services de fournisseurs d'accès à internet font partie des services de télécommunication (ATF 126 I 50 consid. 5b; Corboz, Les infractions en droit suisse, vol. I, Berne 2002, n. 6 ad art. 321ter CP). Ils tombent sous le coup de la loi sur les télécommunications et sont soumis à l'obligation d'observer le secret (art. 43 LTC). Quant aux données couvertes par le secret, il ne s'agit pas seulement du contenu des messages, mais aussi de leur simple existence, de leur nombre, de l'heure des communications, de leur durée et de l'identité des interlocuteurs (Corboz, op. cit., n. 9 ad art. 321ter CP). Selon la doctrine, l'accès aux mots de passe - qui peuvent être englobés comme les «logins» dans la notion de «Randdaten» au sens large du terme - constitue en soi une atteinte au secret des télécommunications (Schneider, Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Ueberwachung des E-Mail-Verkehrs über das Internet, in PJA 2/2005, p. 188). Il en est de même du seul fait de s'aménager la possibilité d'avoir librement accès aux messages privés de tiers (ATF 130 III 28 consid. 4.3).

Le comportement punissable consiste, dans la première hypothèse, de la part de la personne astreinte au secret, à communiquer ou rendre accessible à un tiers non autorisé l'information couverte par le secret. Dans la seconde hypothèse, la personne astreinte au secret doit percer elle-même le secret qu'elle devait respecter; il suffit, selon le texte légal, qu'elle cherche à prendre connaissance du contenu du message protégé pour que l'infraction soit consommée (Corboz, op. cit., n. 21 et 23 ad art. 321ter CP).

bb) Subjectivement, contrairement à l'art. 179 CP, il n'est pas nécessaire que l'auteur ait ouvert le pli (ou la session informatique) fermé dans l'intention de prendre connaissance de son contenu (Donatsch/Wohlers, Strafrecht IV, Delikte gegen die Allgemeinheit, 3e éd. 2004, p. 496).

b) Dans le cas d'espèce, il a été retenu, en faits, qu'Y. SA est une société inscrite auprès de l'office fédéral de la communication en qualité de fournisseur de services de télécommunication, qui est active, notamment, dans la création de sites internet et l'hébergement de messageries. En qualité d'employé de cette société, l'accusé était donc astreint au secret des postes et des télécommunications. Les données transférées par l'intéressé sur son PC privé, à son domicile, étaient également couvertes par le secret des télécommunications, puisqu'il s'agissait de fichiers contenant des adresses e-mail des abonnés au service de messagerie «A.ch», des «logins» (nom d'utilisateur) et des mots de passe permettant d'accéder aux boîtes de messagerie de ces abonnés et de prendre connaissance du contenu de leurs messages et des fichiers rattachés, ainsi que de la liste des clients d'un site mis à disposition par Y. SA à l'un de ses clients sans doute les plus importants. L'accusé, qui a reconnu avoir suivi des cours de droit qui ont également (et inévitablement) porté sur la protection des données, a admis avoir pris connaissance, à une ou deux reprises, de la liste des différentes personnes se trouvant dans le fichier «... Zip». Ce seul comportement réalise déjà les conditions objectives et subjectives de l'infraction réprimée par l'art. 321ter CP.

De toute manière, en copiant ces fichiers et en les transférant à son domicile privé, l'intéressé avait la possibilité, en consultant ces données, d'accéder librement à des messages de caractère privé et à des listes d'abonnés d'Y. SA. Peu importe qu'il n'ait éventuellement pas pris connaissance de certains de ces messages ou que son seul but, selon ses dires, était de connaître les adresses e-mail d'éventuels amis d'enfance. En effet, il a, par son comportement, cherché à prendre connaissance de données qui étaient couvertes par le secret des télécommunications, auquel il était astreint, ce qu'il ne pouvait décemment pas, de par sa position d'employé d'une société informatique et eu égard à sa formation professionnelle, ignorer. Le seul fait, pour l'accusé, de s'être aménagé la possibilité (soit par dol éventuel) de consulter ces données constitue une violation de l'art. 321ter al. 1 CP. Il doit donc être reconnu coupable de violation du secret des postes et des télécommunications au sens de cette disposition.

3. a) L'ordonnance d'inculpation retient à charge de l'accusé les infractions de violation du secret de fabrication ou du secret commercial (art. 162 CP) et de soustraction de données personnelles (art. 179novies CP), poursuivies toutes deux sur plainte.

Le droit de porter plainte se prescrit par trois mois, le délai courant du jour où l'ayant droit a connu l'auteur de l'infraction (art. 29 CP; ATF 101 IV 113 consid. 1b).

b) En l'occurrence, Y. SA a déposé plainte le 12 mars 2002, manifestant l'intention de voir poursuivre l'inculpé pour avoir accédé de façon indue à un domaine du réseau interne dont l'accès était spécifiquement protégé contre tout accès indu, effectué des copies des «Back Office» ainsi que des autres données strictement confidentielles de la société et de ses clients et envoyé par e-mail les fichiers copiés à son adresse e-mail privée, faits qui se seraient produits dans le courant du mois de janvier 2002 et qu'elle aurait découverts dès le 26 janvier 2002, lors de contrôles effectués au sein de la société. Le 2 décembre 2002, le mandataire de la plaignante a sollicité que l'instruction porte également sur les faits révélés ultérieurement par l'enquête, soit que l'accusé avait également soustrait et transféré un fichier «... zip». La plainte, intervenue dans le délai légal de trois mois, est donc valable.

4. a) Aux termes de l'art. 162 CP, celui qui aura révélé un secret de fabrication ou un secret commercial qu'il était tenu de garder en vertu d'une obligation légale ou contractuelle, ou qui aura utilisé cette révélation à son profit ou à celui d'un tiers, sera, sur plainte, puni de l'emprisonnement ou de l'amende.

L'application de cette disposition suppose la réunion de plusieurs éléments objectifs, parmi lesquels celui de la divulgation du secret à une tierce personne.

b) En l'espèce, il a été retenu, en faits, que l'instruction n'avait pas permis d'établir si l'accusé avait transmis ou révélé à des tiers le contenu des données qu'il avait copiées sur son ordinateur privé. En conséquence, l'une des conditions objectives n'étant déjà pas remplie, l'accusé doit être libéré du chef d'inculpation de violation du secret de fabrication ou du secret commercial prévu à l'art. 162 CP.

5. a) L'art. 179novies CP punit de l'emprisonnement ou de l'amende, celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la personnalité qui ne sont pas librement accessibles.

Par «donnée personnelle», il faut entendre toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 let. a LPD). Les données personnelles ne sont protégées que si elles sont sensibles. Sont ainsi visées les données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'appartenance à une race, ou encore les données sur des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives (art. 3 let. c LPD). Par «profils de la personnalité», il faut entendre un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (Corboz, op. cit., n. 3 à 5 ad art. 179novies CP). La donnée soustraite doit se trouver dans un fichier qui n'est pas librement accessible. Cela suppose, d'une part, que l'auteur n'a pas le droit d'y accéder et, d'autre part, que les données soient protégées contre un accès indu, par exemple en plaçant le fichier dans un local interdit au public, dans un tiroir ou une armoire fermés à clé ou encore en rendant nécessaire l'utilisation d'un code d'accès secret (Corboz, op. cit., n. 8 ad art. 179novies CP; Stratenwerth/Jenny, Schweizerisches Strafrecht, BT I, 6e éd. 2003, n. 74 p. 257). L'accessibilité libre est déterminée en fonction de l'autorisation d'accès aux locaux ou annexes dans lesquels les données se trouvent (Von Ins/Wyder, Basler Kommentar, Bâle/Genève/Munich 2003, n. 16 ad art. 179novies CP). Il est nécessaire, comme à l'art. 143 CP, que les données soient particulièrement protégées (Rehberg/Schmid, Strafrecht III, Delikte gegen den Einzelnen, 7e éd. 1997, p. 336). Cette condition est également réalisée lorsque l'auteur doit surmonter des obstacles de nature technique pour se procurer les données. Tel n'est pas le cas lorsque l'auteur parvient à convaincre une personne physique qui a accès au fichier de lui transmettre certaines données (Favre/Pellet/Stoudmann, Code pénal annoté, 2e éd. 2004, n. 1.3 ad art. 179novies CP).

b) En l'occurrence, il a été retenu, en faits, que l'inculpé avait un accès «libre» aux serveurs de la société plaignante. En effet, les données soustraites par ce dernier se trouvaient dans son environnement de travail. Comme l'a déclaré le directeur C., l'inculpé n'a pas dû franchir de «barrière interdite» pour réaliser ses opérations, car les employés travaillaient dans un climat de confiance, seul un «contrat moral» les liant et les limitant à utiliser les seules données nécessaires à leur propre travail. Ainsi l'inculpé, en étant simplement au bénéfice d'un mot de passe qui lui permettait d'effectuer son travail au sein de la société plaignante, a pu accéder aux serveurs contenant les don-

nées dont il s'est emparé ensuite, sans difficulté. Comme les serveurs ne faisaient pas l'objet de mesures de protection spéciales contre des intrusions indues, il n'a rencontré aucune mesure de sécurité particulière l'entravant dans l'accès aux logiciels du «Back Office» recherché ou aux autres données copiées (adresses e-mail, liste de clients, «logins» et mots de passe), ni aucun obstacle technique, puisqu'il lui a simplement suffi de se renseigner auprès d'un collaborateur pour parvenir à y accéder rapidement. C'est dire que les données soustraites étaient librement accessibles pour l'inculpé, de sorte que l'un des éléments objectifs de l'infraction prévue à l'art. 179novies CP n'est pas réalisé. Partant, l'inculpé doit être libéré du chef d'inculpation de soustraction de données personnelles.