TCVS P3 05 28

ATC (Chambre pénale) du 19 mai 2005, Office du ministère public du Bas-Valais c. Office du juge d'instruction du Bas-Valais.

Opportunité d'établir l'arrêt de renvoi (art. 113 ch. 1 let. d CPP).

– Compétence de la Chambre pénale en la matière (consid. 1).

– Distinction entre arrêt de renvoi et arrêt de non-lieu (consid. 2).

– Définition des infractions de soustraction de données et d'accès indu à un système informatique (art. 143 et 143bis CP; consid. 3a); application de ces dispositions en l'espèce (consid. 3b).

Möglichkeit des Erlasses des Überweisungsbeschlusses (Art. 113 Ziff. 1 lit. d StPO).

– Kompetenz der Strafkammer zum Erlass des Überweisungsbeschlusses (E. 1).

– Unterscheidung zwischen Einstellungs- und Überweisungsbeschluss (E. 2).

– Erläuterung der Widerhandlungen der unbefugten Datenbeschaffung (Art. 143 StGB) und des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB; E. 3a); Anwendung dieser Bestimmungen im vorliegenden Fall (E. 3b).

Faits (résumé)

A. La société Y. SA est une société active dans le domaine des services internet, notamment dans la création de sites internet et l'hébergement de messagerie. Dès juin 2001, X., diplômé de l'école d'informatique de Sierre, a travaillé en qualité d'informaticien-stagiaire dans cette entreprise. Sa tâche a consisté au développement des sites internet. A la suite de problèmes de réseau interne survenus à la fin janvier 2002, les responsables de cette compagnie ont procédé à des contrôles techniques. Les résultats de leurs recherches les ont conduits à suspecter X. d'avoir accédé de façon indue à un domaine du réseau interne dont l'accès était, selon eux, spécifiquement protégé et d'avoir effectué des copies de logiciels (figurant sous «Back Office») de la société, évalués alors au bilan à ..... fr., ainsi que d'autres données confidentielles de celle-ci et de ses clients. Il a encore été constaté que X. avait envoyé, dans le courant du mois de janvier 2002, les fichiers copiés, via courrier électronique, à son adresse privée.

B. En raison de ces soupçons, Y. SA a déposé, le 12 mars 2002, plainte pénale contre X. pour soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143 bis CP) et violation du secret de fabrication ou du secret commercial (art. 162 CP), subsidiai-

rement pour tentative de cette infraction. Le lendemain, le juge d'instruction du Bas-Valais (ci-après: le juge d'instruction) a ordonné la visite domiciliaire et la perquisition dans tous les locaux et véhicules de l'intéressé ainsi que le séquestre de tous objets en relation avec des infractions.

Interrogé, X. a soutenu ne pas avoir transmis à des tiers les données soustraites auprès de son employeur. Il a prétendu avoir agi de la sorte, soit pour continuer son travail à domicile, soit par curiosité. Le dossier ne révèle pas qu'il ait fait usage des données en question ou les ait divulguées.

C. X. a été inculpé de soustraction de données (art. 143 CP), d'accès indu à un système informatique (art. 143bis CP), de violation du secret commercial (art. 162 CP) et de violation du secret postal (art. 321ter CP). Le 23 juin 2003, il a fait l'objet d'une inculpation complémentaire pour soustraction de données personnelles (art. 179novies CP).

Après administration des moyens de preuve complémentaires proposés par la lésée et l'inculpé, le magistrat instructeur a prononcé, par ordonnance du 29 août 2003, la clôture de l'instruction de la cause et transmis le dossier au ministère public en vue de l'établissement de l'arrêt de renvoi. Au terme de son écriture du 28 novembre 2003, le procureur du Bas-Valais, estimant injustifiée une mise en accusation fondée sur les art. 143, 143bis et 321ter CP, a proposé au magistrat instructeur de rendre un non-lieu sur ces points et de reprendre le dossier pour la rédaction d'une ordonnance de renvoi en relation avec les art. 5 et 23 LCD. Après avoir recueilli l'avis des autres parties, le juge d'instruction a, par lettre du 3 février 2005, demandé à la Chambre pénale de mettre fin à la divergence en tranchant au moyen d'un arrêt de non-lieu ou de renvoi.

Considérants (extraits)

1. En cas de divergence entre le ministère public et le juge d'instruction sur la justification d'une mise en accusation, le dossier est adressé à la Chambre pénale qui tranche elle-même par un arrêt de non-lieu ou de renvoi (art. 113 ch. 1 let. d CPP).

2. Si la condamnation paraît vraisemblable, il y a lieu de dresser l'arrêt de renvoi, qui a pour effet de provoquer la saisine de l'autorité de jugement. Au contraire, le non-lieu est l'acte par lequel l'autorité judiciaire décide de renoncer à la continuation de la poursuite, c'est-à-dire de traduire l'inculpé en jugement, soit en raison d'une insuffisance des charges, soit pour un motif de droit. Il y a motivation en

droit du non-lieu quand, sur le vu des éléments du dossier, le juge arrive à la conclusion que les faits sur lesquels porte l'instruction ne constituent pas une infraction ou, dans le cas où elle est objectivement réalisée, que les conditions de la poursuite ne sont pas réunies en raison d'un moyen libératoire ou d'un fait justificatif comme la mort du prévenu, la prescription, le retrait de la plainte ou l'exception de chose jugée (RVJ 1997 p. 301 consid. 2a; Piquerez, Procédure pénale suisse, Zurich 2000, n° 2942 ss; Hauser/Schweri/Hartmann, Schweizerisches Strafprozessrecht, 6e éd., § 78 n. 3 ss; Schmid, Strafprozessrecht, 4e éd., n. 796 s.).

3. A l'occasion de la révision du titre IIe de la partie spéciale du Code pénal, entrée en vigueur le 1er janvier 1995, le législateur a introduit de nouvelles dispositions, tels les art. 143, 143bis et 144bis, afin de mieux réprimer la criminalité informatique.

a) L'art. 143 CP punit de la réclusion jusqu'à cinq ans au plus ou de l'emprisonnement celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait des données enregistrées ou transmises électroniquement, qui ne lui étaient pas destinées et étaient spécialement protégées contre tout accès indu de sa part. Sont visées les données elles-mêmes et aussi les programmes ou les logiciels, soit les procédés permettant de les traiter (FF 1991 II 954). La donnée ne doit pas être destinée à l'auteur et, de surcroît, être protégée contre tout accès indu de sa part. A cet égard, le législateur a précisé qu'il ne s'agissait pas de protéger indistinctement l'ensemble des données appartenant à autrui. Si l'auteur est habilité à disposer des données mais outrepasse les limites de son droit d'utilisation, en accédant à des données qui ne lui sont en aucun cas destinées, l'art. 143 CP n'est pas applicable, l'abus de confiance portant sur des données ne tombant donc pas sous le coup de cette disposition (FF 1991 II 978; Weissenberger, Commentaire bâlois, Strafgesetzbuch II, n. 11 ad art. 143 CP; Trechsel, Schweizerisches Strafgesetzbuch Kurzkommentar, 2e éd., n. 6 1e partie ad art. 143 CP). La soustraction des données pénalement répréhensible suppose ainsi l'existence d'une protection dite spéciale, à définir de cas en cas, en fonction des standards habituels de sécurité (Schmid, Computer- sowie Check- und Kreditkarten-Kriminalität, Zurich 1994, § 4 n. 30; pour une description détaillée de telles mesures, cf. n. 33 à 38); l'appréciation y relative ne saurait dépendre de la capacité de l'auteur à déjouer le dispositif mis en

place (Stratenwerth/Jenny, Schweizerisches Strafrecht, Besonderer Teil I, 6e éd., § 14 n. 28). Ne constituent pas une sécurité suffisante des instructions voire des interdictions orales ou écrites, ni des mesures d'organisation en vue de séparer les fonctions au sein du personnel (cf. Schmid, op. cit., § 4 n. 39).

Quant à l'art. 143bis CP, il concerne plus spécifiquement le pirate (hacker) qui s'introduit, à l'aide d'un dispositif de transmission de données, dans un système informatique, lequel doit aussi être «spécialement protégé contre tout accès de sa part» (Corboz, Les infractions en droit suisse, vol. I, Berne 2002, n. 5 et 6 ad art. 143bis CP).

b) En l'espèce, il est constant qu'en étant simplement au bénéfice du mot de passe lui permettant de s'acquitter de ses obligations contractuelles, X. a pu accéder aux serveurs contenant les données dont il s'est ensuite emparé. Bien que lesdits serveurs aient fait l'objet de diverses protections contre des intrusions de l'extérieur (chambre forte, contrôles d'accès biométriques, pare-feu), cet employé n'a rencontré aucune mesure de sécurité spécifique lui entravant l'accès aux logiciels du «Back Office» recherchés ou encore aux données d'Y. SA relatives aux adresses e-mail des abonnés au service de messagerie A.ch, de même que celles afférentes à la liste des clients du site B., le tout «logins» et mots de passe compris. C'est ainsi que, d'après le directeur C., rien qu'avec le «Back Office» dont il a pu entrer en possession, qui lui permettait de réaliser des sites internet dans des conditions très favorables, X. aurait été en mesure d'ouvrir sa propre entreprise ou de vendre à un concurrent des données évaluées alors à .....francs. A cet égard, comme on l'a déjà remarqué ci-dessus, il importe peu qu'en fonction de la formation ou des capacités de celui-ci, voire des renseignements fournis par des collègues mieux aguerris en ce domaine, l'employé indélicat ait mis plus ou moins de temps pour trouver le chemin des données recherchées, dès lors l'intéressé n'a dû surmonter aucun obstacle de sécurité mis en œuvre volontairement par son employeur. Au contraire, faisant prévaloir des raisons de rentabilité dont il n'appartient pas à la cour de vérifier le bienfondé, les organes d'Y. SA ont opté pour une barrière dite morale, qui ne suffit évidemment pas à réunir les réquisits posés à l'art. 143 CP, lors même - tel que déjà évoqué en droit - que cette barrière aurait été assortie d'instructions voire d'interdictions orales ou écrites. Lesdits réquisits sont donc bien plus sévères que ceux posés à l'art. 186 CP ou encore à l'art. 179 CP. Certes, avec la société

lésée, qui cherche en vain à démontrer une analogie étroite entre les conditions d'application de ces dispositions, on peut s'interroger sur le sens de la protection pénale restreinte ainsi accordée par le législateur, dans sa volonté de renoncer à réprimer ce qui équivaut à un abus de confiance au sens large du terme. C'est bien la raison pour laquelle ont déjà été relevés le peu d'incidence pratique de l'art. 143 CP et même le caractère dépassé des moyens légaux mis en œuvre dès 1995 pour lutter contre la criminalité informatique (cf. Moreillon, Nouveaux délits informatiques sur Internet, Medialex 2001 p. 21). Il suit de là qu'un renvoi en jugement fondé sur l'art. 143 CP ne saurait se justifier.

Pour des motifs similaires, l'application de l'art. 143bis CP n'entre pas en ligne de compte, outre que l'activité de l'employé X. ne peut être assimilée à celle d'un «hacker» qui visite le site d'autrui en vue d'en percer les défenses et, selon l'expression de Moreillon (op. cit., p. 22), d'en violer le domicile informatique.

Note

La cause pénale concernant X. a en revanche été renvoyée à jugement s'agissant de la violation du secret des postes et des télécommunications. Quant aux deux chefs d'accusation fondés sur les art. 162 et 179 novies CP, au sujet desquels le ministère public s'était dispensé de toute appréciation, il n'appartenait pas à la Chambre pénale de statuer sur ces questions dans le cadre spécifique de la procédure prévue à l'art. 113 ch. 1 let. d CPP.

Par jugement du 28 juin 2005, destiné à publication dans la RVJ 3/2006, le Juge des districts de Martigny et St-Maurice s'est prononcé sur la réalisation des conditions des art. 179 novies et 321 ter al. 1 CP.