101

PE12.016676-PGN

CHAMBRE DES RECOURS PENALE

Arrêt du 19 février 2016

Composition : M. ABRECHT, président
M. Meylan, juge et Mme Epard, juge suppléante
Greffière : Mme Joye

*****

Art. 319 CPP

Statuant sur le recours interjeté le 5 octobre 2015 par **C._____** contre l'ordonnance de classement rendue le 17 septembre 2015 par le Ministère public de l'arrondissement de Lausanne dans la cause **n° PE12.016676-PGN**, la Chambre des recours pénale considère :

En fait :

A. **a)** Le 31 août 2012, C._____ a, par son associée-gérante [...], déposé plainte contre U._____ pour accès indu à un système informatique (art. 143bis CP) et sous-traction de données (art. 143 CP), ainsi que toute autre infraction dont l'instruction révélera l'existence. En substance, la plaignante reproche à la prénommée, qui a été son

employée du 1er février 2011 au 10 juillet 2012, d'avoir accédé, sans autorisa-tion, au compte informatique de l'un de ses collègues, [...], d'avoir copié une conversation Skype de ce dernier, ainsi que son curriculum vitae, et d'avoir subtilisé et utilisé des données confidentielles de la société et/ou de l'un des clients de la société au moins; elle lui reproche également d'avoir effacé ou tenté d'effacer des fichiers compromettants à l'issue d'une réunion avec le responsable des ressources humaines qui s'est déroulée le 10 juillet 2012 et lors de laquelle l'intéressée a été sommée de s'expliquer sur ses agissements; enfin, la plaignante soupçonne son ex-employée d'avoir eu une activité professionnelle accessoire durant ses heures de travail et d'avoir collaboré avec une société concurrente.

b) Par mandat d'investigation du 29 août 2014, le procureur a chargé la Police cantonale de saisir et d'analyser le matériel informatique et/ou électrique utilisé par U._____ alors qu'elle était employée de C._____ (matériel consigné auprès du service de sécurité de l'EPFL) et d'entendre, le cas échéant, les différents protagonistes.

Le 20 avril 2015, le spécialiste informatique [...] de la Division criminalité informatique de la Police de sûreté, a déposé son rapport (P. 10). Après examen de l'ordinateur de bureau d'U._____ et des deux disques durs saisis, il a abouti aux conclusions suivantes :

« Le seul dossier partagé de l'ordinateur [...]-PC02 utilisé par Mme U._____ est accessible en lecture par tous les utilisateurs configurés sur le réseau de la société [...]. Ce dossier partagé contient tous les profils utilisateurs de la machine, et donc tous les documents, images, vidéos, téléchargements, et données d'applications (navigation, Internet, Skype, etc.) de ces différents utilisateurs. De plus, les comptes utilisateurs « Admin », « U._____» et « [...]» sont administrateurs de la machine. Ils peuvent donc accéder en lecture et en écriture à tous les fichiers du PC lorsqu'ils sont connectés sur celui-ci, en local ou à distance.

Il existe bien un fichier « 17.docx » sur le PC de Mme U._____. Ce fichier a été créé sur cet ordinateur le 7 mars 2012 à 16h44. Il contient bien un fil de discussion entre M. [...] et M. [...]. Nous avons également retrouvé une page Internet du cache du logiciel de navigation Firefox dans une sauvegarde du PC et dans laquelle on observe une utilisation de l'outil de traduction « Google Translate » sur un extrait de ce document. La personne enregistrée à ce moment-là sur son compte Google est « U._____». Mme U._____ a donc certainement traduit ce document, ou parties de ce document, en ligne à l'aide de l'outil « Google Translate ».

Des photos et des CV de MM. [...] et [...] ont été retrouvés sur le disque dur externe My passport noir de Mme U._____, mais nous n'en avons pas trouvé sur l'ordinateur [...]-PC02. Ce matériel est disponible sur Internet bien que les CV aient changé depuis 2012. Les deux enregistrements sonores créés le 6 juillet 2012 sont bien présents sur l'ordinateur [...]-PC02.

Le journal d'événements de Windows enregistrant les connexions à distance via le protocole RDP est vide, ce qui indique que l'ordinateur de Mme U._____ n'a jamais été utilisé pour se connecter à distance sur un ordinateur au travers de ce protocole. Par contre, un autre ordinateur a pu être utilisé pour ces connexions à distance via le protocole RDP, pour autant que l'utilisateur connaisse les noms d'utilisateurs et mots de passe nécessaires. Mais dans ce cas, les traces informatiques se trouvent sur les ordinateurs vers lesquels les connexions à distance ont été effectuées, soient le PC [...]-PC03 et le serveur dmt.pc19. Nous ne possédons aucune de ces traces.

Le disque dur externe Western Digital My Passport de couleur noire a bien été connecté à l'ordinateur [...]-PC03 de M. [...] le 7 mars 2012 à 17h08. Des fichiers (modèles de CV et fichiers de code de programmation informatique) ont bien été copiés sur ce disque entre 17h08 et 17h10 à cette même date. Ils proviennent certainement de cet ordinateur. Par contre, nous ne pouvons pas établir avec certitude que ce même disque dur ait été connecté à l'ordinateur de Mme [...] faute de traces informatiques précises fournies par la plaignante.

Le 10 juillet 2012 après la réunion prévue ce jour-là, Mme U._____ s'est bien connectée à son ordinateur [...]-PC02. Mme [...] s'est également connectée à distance sur ce même ordinateur et a modifié/réinitialisé le mot de passe du compte « U._____». Mme U._____ s'est ensuite certainement reconnectée à l'ordinateur à l'aide des comptes utilisateurs « [...] » et « Guest » qui ne sont pas protégés par un mot de passe. Il n'y a pas eu de copie de fichiers sur les disques durs externes de Mme U._____. Il ressort de l'analyse des fichiers d'index $I30 que ce sont principalement les fichiers temporaires qui ont été effacés qui concernent les navigateurs Internet Firefox, Chrome et Internet Explorer, et certaines données applicatives telles que Adobe Flash Player ou Java. Nous n'avons pas observé d'effacements massifs de répertoires de documents de travail. ».

c) Par courrier du 17 juin 2015, la plaignante a requis que des questions complémentaires, dont il a précisé le contenu, soient posées à l'auteur du rapport, et qu'U._____ soit auditionnée.

Par courrier du 10 juillet 2015, U._____ s'est opposée aux réquisitions de la plaignante du 17 juin 2015, sauf à son audition, qu'elle a également appelé de ses vœux.

Par lettre du 13 juillet 2015, le procureur a informé la plaignante que les réquisitions qu'elle avait formulées étaient rejetées.

d) Le 28 août 2015, dans le délai de prochaine clôture, la plaignante s'est opposée au classement de la procédure, a réitéré sa demande tendant au complètement du rapport d'analyse du 20 avril 2015 et a requis l'audition d'U._____, d' [...], de [...], ainsi que celle de [...], dont elle a produit une déclaration écrite datée du 28 août 2015. Dans ce document, rédigé en anglais, [...], qui se présente comme un informaticien au bénéfice de quinze ans d'expérience et comme le responsable de la mise en place et de l'entretien de l'infrastructure informatique de C._____, relève l'existence de certaines inexactitudes dans le rapport d'analyse du 20 avril 2015, en particulier s'agissant de la présentation de l'environnement informatique de la société, des relations entre les trois ordinateurs [...]-PC01 (d' [...]), [...]-PC02 (d'U._____) et [...]-PC03 (de [...]) et des droits d'accès mis en place.

Par courriers des 28 août et 7 septembre 2015, U._____ a conclu au classement de la procédure dirigée contre elle et à l'octroi d'une indemnité de 4'623 fr. 50 en vertu de l'art. 429 al. 1 let. a et b CPP.

Le 18 septembre 2015, la plaignante a réitéré ses réquisitions du
28 août 2015.

B. Par ordonnance du 17 septembre 2015, le Ministère public de l'arron-dissement de Lausanne a ordonné le classement de la procédure pénale dirigée contre U._____ pour soustraction de données et accès indu à un système informatique (I), a rejeté la requête d'indemnité, au sens de l'art. 429 CPP, de la prénommée (II) et a laissé les frais de procédure à la charge de l'Etat (III).

Dans son ordonnance, le procureur a d'abord rejeté les réquisitions présentées par la plaignante dans son écriture du 28 août 2015, considérant, d'une part, que les auditions demandées étaient inutiles dès lors que les éléments constitutifs objectifs des infractions dénoncées n'étaient pas réalisées, et, d'autre part, qu'il n'y avait pas lieu de procéder à des « corrections » du rapport de la Police cantonale sur la

base des déclarations écrites de [...], estimant que les « constations objectives » faites par la Police cantonale devaient être privilégiées par rapport au témoignage d'un « membre » de la société plaignante, lequel devait être pris avec réserve.

Sur le fond, le procureur a constaté, en substance, que le curriculum vitae de [...] était accessible sur internet, que si le fichier « 17.docx » contenant la retranscription de la conversation Skype du prénommé semblait bien avoir été créé par la prévenue, le rapport d'analyse avait démontré que l'univers informatique de la société plaignante n'était pas sécurisé, si bien que le fichier en question était accessible par d'autres personnes au sein de la société, et, enfin, qu'il n'avait pas été constaté que la prévenue aurait effacé de manière massive des répertoires de documents à l'issue de la réunion du 10 juillet 2012. Le procureur a conclu de ces constations que les éléments constitutifs des infractions prévues aux art. 143 et 143bis CP n'étaient pas réalisés et a considéré que le classement de la procédure devait être ordonné. S'agissant de l'indemnité réclamée par la prévenue en vertu de l'art. 429 CPP, le procureur a estimé que celle-ci n'avait pas fourni les éléments justifiant ses prétentions.

Par ordonnance du 22 septembre 2016, le Ministère public a rectifié celle rendue le 17 septembre 2015 en ce sens qu'il a ordonné le maintien au dossier, à titre de pièce à conviction, du CD-Rom inscrit sous fiche N° 60'380 (I), a confirmé l'ordonnance du 17 septembre 2015 pour le surplus (II) et a dit que le prononcé rectificatif était rendu sans frais (III).

C. Par acte du 5 octobre 2015, C._____ a recouru auprès de la Chambre des recours pénale du Tribunal cantonal contre l'ordonnance de classement du 17 septembre 2015, en concluant, avec dépens, à son annulation, la cause étant renvoyée au ministère public pour qu'il procède à la reprise de l'instruction dans le sens des considérants et rende une nouvelle décision.

U._____ s’est déterminée le 28 janvier 2016. Elle a conclu, avec dépens, au rejet du recours et à la confirmation de l’ordonnance de classement attaquée.

Par courrier du 28 janvier 2016, le Ministère public a renoncé à déposer des déterminations.

Dans une écriture du 16 février 2016, la recourante a confirmé ses conclusions du 5 octobre 2015.

E n d r o i t :

1. Les parties peuvent attaquer une ordonnance de classement rendue par le ministère public en application des art. 319 ss CPP (Code de procédure pénale suisse du 5 octobre 2007; RS 312.0) dans les dix jours devant l’autorité de recours (art. 322 al. 2 et 396 al. 1 CPP; cf. art. 20 al. 1 let. b CPP), qui est, dans le canton de Vaud, la Chambre des recours pénale du Tribunal cantonal (art. 13 LVCPP [loi vaudoise du 19 mai 2009 d’introduction du code de procédure pénale suisse; RSV 312.01]; art. 80 LOJV [loi vaudoise du 12 décembre 1979 d’organisa-tion judiciaire; RSV 173.01]).

Interjeté dans le délai légal auprès de l’autorité compétente par la partie plaignante, qui a la qualité pour recourir (cf. art. 382 al. 1 CPP; CREP 19 novembre 2014/828), et satisfaisant aux conditions de forme posées par la loi (cf. art. 385 al. 1 CPP), le recours est recevable.

2.

2.1 Selon l'art. 319 al. 1 CPP, le ministère public ordonne le classement de tout ou partie de la procédure lorsqu'aucun soupçon justifiant une mise en accusation n'est établi (let. a), lorsque les éléments constitutifs d'une infraction ne sont pas réunis (let. b), lorsque des faits justificatifs empêchent de retenir une infraction contre le prévenu (let. c), lorsqu'il est établi que certaines conditions à l'ouverture de l'action pénale

ne peuvent pas être remplies ou que des empêchements de procéder sont apparus (let. d) ou lorsqu'on peut renoncer à toute poursuite ou à toute sanction en vertu de dispositions légales (let. e).

De manière générale, les motifs de classement sont ceux « qui déboucheraient à coup sûr ou du moins très probablement sur un acquittement ou une décision similaire de l'autorité de jugement » (Message du Conseil fédéral relatif à l'unification du droit de la procédure pénale du 21 décembre 2005, FF 2006 pp. 1057 ss, spéc. 1255). Un classement s'impose donc lorsqu'une condamnation paraît exclue avec une vraisemblance confinant à la certitude. La possibilité de classer la procédure ne saurait toutefois être limitée à ce seul cas, car une interpréta-tion aussi restrictive imposerait un renvoi en jugement, même en présence d'une très faible probabilité de condamnation (ATF 138 IV 86 consid. 4.1.1). Le principe « *in dubio pro duriore* » exige donc simplement qu'en cas de doute, la procédure se poursuive. Pratiquement, une mise en accusation s'impose lorsqu'une condamnation apparaît plus vraisemblable qu'un acquittement. En effet, en cas de doute, ce n'est pas à l'autorité d'instruction ou d'accusation mais au juge matériellement compétent qu'il appartient de se prononcer (ATF 138 IV 86 consid. 4.1.1; cf. ég. ATF 138 IV 186 consid. 4).

2.2 En vertu de l’art. 143 CP, se rend coupable de soustraction de données celui qui dans le dessein de se procurer un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électro-niquement qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part. Cette disposition réprime un comportement couramment désigné par les termes de « vol de données » et protège le droit du bénéficiaire légitime de disposer des données informatiques à sa guise (Dupuis et alii, Petit commentaire du Code pénal, Bâle 2012, n. 1 ad art. 143 CP).

Selon l’art. 143bis CP, se rend coupable d’accès indu à un système informatique quiconque s'introduit sans droit, au moyen d'un dispositif de trans-mission de données, dans un système informatique

appartenant à autrui et spéciale-ment protégé contre tout accès de sa part. Cette disposition incrimine le piratage informatique (« hacking »), à savoir l'intrusion illicite dans un système informatique appartenant à autrui (Dupuis et alii, op. cit., n. 1 ad art. 143bis CP).

Tant l'art. 143 CP que l'art. 143bis CP disposent que les données doivent être spécialement protégées. Il faut ainsi qu'une protection informatique soit mise en place. Une interdiction morale ou contractuelle ne suffit pas (Dupuis et alii, op. cit., n. 14 ad art. 143 CP).

Aux termes de l'art. 179^{novies} CP, se rend coupable de soustraction de données personnelles celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la personnalité qui ne sont pas librement accessibles. Pour que cette infraction soit objectivement réalisée, il faut que l'auteur ait soustrait des données contenues dans un fichier, qu'il s'agisse de données personnelles sensibles ou de profils de la personnalité et que ces données soient non librement accessibles. Par données personnelles sensibles, on entend les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime, l'appartenance à une race, les mesures d'aide sociale, les poursuites ainsi que les sanctions pénales ou administratives (art. 3 let. c LPD [Loi fédérale sur la protection des données; RS 235.1]; Corboz, op. cit., n. 3 ad art. 179^{novies} CP; Dupuis et alii, op. cit., n. 7 ad art. 179^{novies} CP). La notion de données non librement acces-sibles de l'art. 179^{novies} CP est explicitement plus large que celle de protection contre tout accès. Si les art. 143 et 143bis CP impliquent la manifestation d'une fermeture, il n'en va pas de même de l'art. 179^{novies} CP. Cet article s'appliquera quand bien même l'auteur ne ferait que franchir une interdiction contractuelle (Dupuis et alii, op. cit., n. 10 ad art. 179^{novies} CP).

2.3 En l'espèce, il ressort du rapport d'analyse du 20 avril 2015 que les données informatiques litigieuses, en particulier la retranscription d'une conversation Skype de [...], ont bien été trouvées dans l'ordinateur de la prévenue, dans un fichier « 17.docx », et qu'elle a traduit ladite

conversation, au moins partiellement. D'après la plaignante, cette retranscription contiendrait des informations nécessaires pour accéder au serveur d'un client de la société, lequel abriterait des données confidentielles particulièrement sensibles.

Pour déterminer si un comportement pénalement répréhensible pourrait être reproché à la prévenue, la question centrale à examiner est celle de savoir si elle disposait d'un droit d'accès au dossier partagé où étaient initialement enregistrées les données litigieuses, en particulier la conversation Skype de [...], ou si, au contraire, cet accès était protégé.

D'après le rapport d'analyse de la police, tous les utilisateurs du réseau informatique de la société plaignante – en particulier la prévenue – avaient accès aux données enregistrées dans le volume partagé de chacun des ordinateurs du réseau. Ce constat est toutefois contredit par l'informaticien [...], responsable de la mise en place et de l'entretien de l'infrastructure informatique de la société plaignante; en effet, dans sa déclaration écrite du 28 août 2015, il indique que, contrairement à ce qui ressort du rapport précité, les trois ordinateurs [...]-PC01, [...]-PC02 et [...]-PC03 n'étaient pas constitués en réseau global, l'erreur de l'analyste de la police provenant, à son avis, probablement du fait que celui-ci a supposé que les ordinateurs de la société étaient connectés à un serveur Windows avec un « Domaine Windows », ce qu'il dit ne pas être le cas; [...] précise que toutes les autorisations d'accès aux dossiers des divers utilisateurs, y compris les dossiers partagés, étaient « locales » et qu'U._____ n'avait pas de compte local – et donc pas de droit d'accès – sur l'ordinateur [...]-PC03 de [...] et en particulier sur le dossier partagé où était enregistrée la conversation Skype de son collègue.

Contrairement à ce qu'a considéré le procureur, les indications données par l'informaticien qui a installé le système informatique de la plaignante – lesquelles touchent à des questions déterminantes pour l'instruction de la cause – ne peuvent pas être écartées au bénéfice du

rapport d'analyse de la police du 20 avril 2015. On ne saurait en effet ignorer ses constatations pour le motif qu'il travaille ou a travaillé pour la société plaignante, rien ne permettant par ailleurs de douter de ses compé-tences. [...] doit donc être auditionné et l'analyste [...] interpellé afin qu'il puisse se déterminer sur les informations fournies par le prénommé, ce qui pourrait permettre d'éviter la mise en œuvre d'une expertise. Il y aura également lieu, le cas échéant, d'auditionner U._____ et [...], éventuellement [...]. Enfin, le procureur devra examiner si les données litigieuses, en particulier le contenu de la conversation Skype, sont des « données personnelles sensibles » au sens de l'art. 179^{novies} CP.

3. Le recours doit ainsi être admis, l'ordonnance du 17 septembre 2015, de même que celle du 22 septembre 2015 qui la confirme, annulées et le dossier de la cause renvoyé au Ministère public de l'arrondissement de Lausanne pour qu'il procède dans le sens des considérants.

Les frais de la procédure de recours, constitués de l'émolument d'arrêt, par 1'100 fr. (art. 20 al. 1 TFIP [Tarif des frais de procédure et indemnités en matière pénale du 28 septembre 2010, RSV 312.03.1]), seront mis à la charge de l'intimée, U._____, qui succombe dès lors qu'elle a conclu au rejet du recours (art. 428 al. 1 CPP).

S'agissant des dépens réclamés par la recourante, il appartiendra, le cas échéant, à cette dernière d'adresser à la fin de la procédure ses prétentions à l'autorité pénale compétente selon l'art. 433 al. 2 CPP (CREP 16 avril 2013/279 consid. 4 et les références citées).

Par ces motifs,
la Chambre des recours pénale
prononce :

I. Le recours est admis.
II. Les ordonnances des 17 et 22 septembre 2015 sont annulées.

III. Le dossier de la cause est renvoyé au Ministère public de l'arrondisse-ment de Lausanne pour qu'il procède dans le sens des considérants.

IV. Les frais d'arrêt, par 1'100 fr. (mille cent francs), sont mis à la charge d'U._____.

V. Le présent arrêt est exécutoire.

Le président : La greffière :

Du

Le présent arrêt, dont la rédaction a été approuvée à huis clos, est notifié, par l'envoi d'une copie complète, à :

- M. Boris Vittoz, avocat (pour C._____),
- M. Lê-Bihn Hoang, avocat (pour U._____),
- Ministère public central,

et communiqué à :

- M. le Procureur de l'arrondissement de Lausanne,

par l'envoi de photocopies.

Le présent arrêt peut faire l'objet d'un recours en matière pénale devant le Tribunal fédéral au sens des art. 78 ss LTF (loi du 17 juin 2005 sur le Tribunal fédéral – RS 173.110). Ce recours doit être déposé devant le Tribunal fédéral dans les trente jours qui suivent la notification de l'expédition complète (art. 100 al. 1 LTF).

La greffière :