C H A M B R E D E S R E C O U R S P E N A L E

Arrêt du 21 octobre 2024

Composition : M. KRIEGER, président
Mme Fonjallaz et M. Perrot, juges
Greffière : Mme Fritsché

*****

Art. 143bis al. 1 CP ; 310 et 393 ss CPP

Statuant sur le recours interjeté le 4 juillet 2024 par **X._____** contre l'ordonnance rendue le 20 juin 2024 par le Ministère public de l'arrondissement de Lausanne dans la cause **n° PE24.011614-JMU**, la Chambre des recours pénale considère :

E n f a i t :

A. Par acte du 28 mai 2024, X._____ a déposé plainte pénale contre l'un de ses anciens employés, S._____, encore en poste au moment des faits, pour gestion déloyale, abus de confiance, soustraction de données et accès indu à un système informatique. Dans sa plainte, X._____ expose notamment ce qui suit :

« a) M. S._____ s'est procuré la carte SIM (IMSI [...]) d'une manière inconnue, l'a insérée dans l'un des téléphones de test du magasin [...] (**IMEI [...]**) et a ensuite demandé à sa sœur, Mme B._____, de se faire passer pour Mme Z._____ et d'appeler le Call center en utilisant le téléphone de Mme B._____en mode masqué, ce que Mme B._____a fait.

b) Cette dernière a demandé à l'agente du Call center d'activer la carte SIM (IMSI [...]) sur le n° +[...]. Devant l'hésitation de l'agente du Call center à procéder à l'activation, M. S._____ est intervenu agressivement dans la conversation afin de l'agente s'exécute.

c) Pendant tout le temps de l'appel (de 10 :44 à 10 :52), M. S._____ était connecté (de 10 :40 à 11 :00) au compte de la cliente depuis un ordinateur dont l'adresse IP correspond au magasin [...]. Nous supposons donc que M. S._____ et Mme B._____ étaient dans le back-office du magasin lors de l'appel au Call center.

d) La carte SIM (IMSI [...]) a donc été activée sur le n° +[...] attribué à Mme Z._____ mais comme la carte SIM était insérée dans un téléphone qui n'était pas dans ses mains, mais très probablement dans les mains de M. S._____ (le téléphone de test), Mme Z._____ ne pouvait plus ni téléphoner ni recevoir d'appel (perte de réseau) ; tous les appels entrant sur le n° +[...] ainsi que toutes les éventuels SMS nécessaires à une double identification – réseaux sociaux, e-banking, etc...) ont été reçu sur le téléphone très probablement dans les mains de M. S._____, ceci entre le 13 février 2024 à 11 :02 jusqu'au 14 février 2024 vers midi (quand Mme Z._____ s'est rendue au magasin de [...] pour activer sa nouvelle carte SIM). (...) ».

Le 14 juin 2024, le Procureur du Ministère public de l'arrondissement de Lausanne (ci-après : le procureur) a informé X._____ que la plainte déposée le 28 mai 2024 avait été enregistrée sous n° PE24.011614-JMU et l'a invitée à faire valoir ses éventuelles prétentions civiles, pièces justificatives à l'appui.

B. Par ordonnance du 20 juin 2024, le procureur a refusé d'entrer en matière (I), a dit que la clé USB, enregistrée sous fiche n° 39970, contenant l'enregistrement au Call Center du 13 février 2024 était restituée à la partie plaignante une fois l'ordonnance définitive et exécutoire (II), et a laissé les frais à la charge de l'Etat (III).

S'agissant de l'infraction relative à l'art. 143bis CP, soit l'accès indu à un système informatique au moyen d'un dispositif de transmission de données, le procureur a relevé ce qui suit : « *(...) En l'espèce, en sa*

qualité d'employé de X._____, S._____ était autorisé à accéder au système informatique de la société. L'accès n'est donc pas indu. De plus l'accès s'est fait en se connectant physiquement au système informatique dans le magasin [...]. Il n'a donc pas accédé au système informatique au moyen d'un dispositif de transmission de données. L'accès indu à un système informatique n'est donc pas réalisé. (...) ».

C. Par acte du 5 juillet 2024, X._____, par l'intermédiaire de son conseil de choix, a recouru contre cette ordonnance en concluant à son annulation, à ce qu'il soit ordonné au Ministère public de l'arrondissement de Lausanne d'ouvrir une procédure d'instruction en vue d'instruire les faits dénoncés et à ce que les frais soient laissés à la charge de l'Etat. Elle a également conclu à l'allocation d'une indemnité d'un montant de 5'334 fr. 75, liste des opérations à l'appui, pour les dépenses occasionnées par la présente procédure de recours.

Le 8 octobre 2024, le Ministère public a indiqué qu'il renonçait à se déterminer. Cette correspondance a été transmise à la recourante le lendemain.

En droit :

1.

1.1 Les parties peuvent attaquer une ordonnance de non-entrée en matière rendue par le Ministère public en application de l'art. 310 CPP dans les dix jours devant l'autorité de recours (art. 310 al. 2, 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 d'introduction du Code de procédure pénale suisse du 19 mai 2009 ; BLV 312.01] ; art. 80 LOJV [loi vaudoise d'organisation judiciaire du 12 décembre 1979 ; BLV 173.01]).

1.2 La recourante, en sa qualité d'exploitante d'un système de traitement de données et de fournisseur de télécommunications, est titulaire du bien juridiquement protégé par l'art. 143bis al. 1 CP. Elle a

donc la qualité pour recourir (TF 6B_456/2007 du 18 mars 20218 consid. 4.2)**.** Partant, interjeté en temps utile auprès de l'autorité compétente par la partie plaignante qui a qualité pour recourir (art. 382 al. 1 CPP et TF 6B_456/2007 précité) et satisfaisant aux exigences de forme prescrites (art. 385 al. 1 CPP), le recours est recevable.

2. Conformément à l'art. 310 al. 1 let. a CPP, le Ministère public rend immédiatement une ordonnance de non-entrée en matière s'il ressort de la dénonciation ou du rapport de police que les éléments constitutifs de l'infraction ou les conditions à l'ouverture de l'action pénale ne sont manifestement pas réunis. Cette disposition doit être appliquée dans le respect de l'adage in dubio pro duriore. Celui-ci découle du principe de la légalité (art. 5 al. 1 Cst. [Constitution fédérale de la Confédération suisse du 18 avril 1999 ; RS 101] et art. 2 al. 2 CPP en relation avec les art. 319 al. 1 et 324 al. 1 CPP ; ATF 138 IV 86 consid. 4.2) et signifie qu'en principe, un classement ou une non-entrée en matière ne peuvent être prononcés par le Ministère public que lorsqu'il apparaît clairement que les faits ne sont pas punissables ou que les conditions de la poursuite pénale ne sont pas remplies (ATF 143 IV 241 consid. 2.2.1 ; ATF 138 IV 86 consid. 4.1.2 et les références citées ; TF 7B_24/2023 du 22 février 2024 consid. 3.2). En d'autres termes, il faut être certain que l'état de fait ne constitue aucune infraction. Une ordonnance de non-entrée en matière ne peut être rendue que dans les cas clairs du point de vue des faits, mais également du droit ; s'il est nécessaire de clarifier l'état de fait ou de procéder à une appréciation juridique approfondie, le prononcé d'une ordonnance de non-entrée en matière n'entre pas en ligne de compte. En règle générale, dans le doute, il convient d'ouvrir une enquête pénale (ATF 143 IV 241 consid. 2.2.1 ; ATF 138 IV 86 précité consid. 4.1.2 ; ATF 137 IV 285 consid. 2.3 et les références citées, JdT 2012 IV 160). En revanche, le Ministère public doit pouvoir rendre une ordonnance de non-entrée en matière dans les cas où il apparaît d'emblée qu'aucun acte d'enquête ne pourra apporter la preuve d'une infraction à la charge d'une personne déterminée (TF 6B_541/2017 du 20 décembre 2017 consid. 2.2).

3.

3.1 La recourante conteste uniquement le raisonnement du Ministère public relatif à l'infraction d'accès indu à un système informatique au sens de l'art. 143bis al. 1 CP. Elle invoque à cet égard que les prévenus se sont introduits, d'une part, dans le compte client [...] de l'ex-compagne du prévenu par le biais d'un ordinateur et, d'autre part, dans les données de l'utilisatrice en raccordant son numéro de téléphone portable à une carte SIM en leur possession. Ils auraient eu ainsi accès à toutes les données privées de la cliente et auraient notamment été en mesure d'intercepter les communications qu'elle recevait, empêchant en outre celle-ci de bénéficier des prestations liées à son abonnement (téléphone, messagerie, accès aux réseaux sociaux). Dans la mesure où le numéro de téléphone attribué à un client serait relié à une carte SIM protégée par un code et que le compte-client serait sécurisé par un mot de passe, les prévenus auraient délibérément franchi des barrières d'accès au traitement des données par une tromperie opérée auprès d'une employée du Call Center de l'entreprise, en vue d'obtenir le transfert du numéro de téléphone de la cliente sur une nouvelle carte SIM. Un tel comportement n'entrerait manifestement pas dans les attributions de S._____ lorsqu'il était au service de la plaignante, de sorte qu'il y aurait bien un accès indu aux données privées de la cliente.

3.2 Aux termes de l'art. 143bis al. 1 CP, quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Cette disposition protège la paix informatique et plus particulièrement le droit du titulaire du système informatique d'en maîtriser l'accès et de le contrôler à sa guise (Dupuis et al. [éd.], Petit commentaire, Code pénal, 2e éd., Bâle 2017, n. 2 ad art. 143bis CP et les références citées). Elle protège ainsi les systèmes de traitement de données contre les intrus (appelés pirates informatiques) qui cherchent à déjouer les systèmes de sécurité pour s'introduire dans des systèmes de données sécurisés et dont l'activité s'est révélée être la source de perturbation et de danger considérables pour le bon fonctionnement des grandes installations notamment. Le

législateur a délibérément subordonné la punissabilité en vertu de l’art. 143bis al. 1er CP au fait qu’un système de protection de l’accès ait été contourné. En tant qu’acte préparatoire à une soustraction de données au sens de l’art. 143 CP, l’infraction d’accès indu à un système informatique au sens de l’art. 143bis al. 1 CP suppose déjà – de manière d’ailleurs analogue à la violation de domicile (art. 186 CP) – une intrusion dans un système informatique appartenant à autrui. Font l’objet de l’attaque les systèmes ou installations de traitement de données et non pas les données qui y sont stockées. C’est la liberté qu’a l’ayant droit de décider qui peut accéder à une installation informatique sécurisée et aux données qui y sont stockées qui est protégée (ATF 145 IV 185 consid. 2.1 et les références citées, JdT 2019 IV 312).

Tombe sous le coup de cette disposition la personne qui parvient à pénétrer dans un système informatique protégé contre tout accès indu. Il faut donc qu'il existe une protection de nature informatique et non physique, comme un codage, un cryptage ou un mot de passe (TF 6B_241/2015 du 26 janvier 2016 consid. 1.3.3 ; Dupuis et al., op. cit., n. 11 ad art. 143bis CP et n. 13 ad art. 143 CP). La notion de protection spéciale est analogue à celle prévue à l'art. 143 CP : si la barrière consiste uniquement dans une interdiction morale ou contractuelle d'utiliser un code dont on dispose ou dont on a disposé légitimement, l'art. 143 CP ne sera pas applicable ; celui qui outrepasse les limites de son droit de disposer des données ou utilise abusivement des données accessibles, à savoir "*l'abus de confiance informatique*", n'est pas punissable (Dupuis et al., op. cit., n. 11 ad art. 143bis CP et n. 14 ad art. 143 CP et les références citées).

Selon le Tribunal fédéral, celui qui se connecte à un compte de courrier électronique à l’aide d’un mot de passe accède aussi en même temps au système informatique en tant que tel. Le mot de passe permet ainsi au titulaire de définir l’accès non seulement au compte de courrier électronique, mais également à l’installation de traitement de données en tant que telle (TF 6B_456/2007 du 18 mars 2008 consid. 4.1).

3.3 En l'espèce, il est vrai, comme le relève le Ministère public, qu'à l'époque des faits, S._____ était employé chez X._____ et disposait ainsi de certains accès informatiques au réseau de l'entreprise. Toutefois, il apparaît qu'il n'aurait pas agi dans le cadre autorisé, et aurait franchi non pas de simples obstacles moraux, légaux ou contractuels, mais de véritables barrières de sécurité, puisque les codes et mots de passe des clients ne sont en principe pas connus du personnel. Selon la plaignante, l'intrusion aurait été rendue possible par une tromperie menée de concert par le prévenu et sa sœur, cette dernière s'étant fait passer pour Z._____ auprès d'une collaboratrice travaillant au call center de X._____ dans le but de transférer le numéro de la prénommée sur une autre carte SIM afin de pouvoir accéder à ses données.

En outre, la condition de l'utilisation d'un dispositif de transmission de données paraît également réalisée, le comportement incriminé étant intervenu par le biais d'un téléphone et d'un ordinateur. En effet, il semble que S._____ et sa sœur B._____ se soient introduits, d'une part, sur le compte client [...] de Z._____ par le biais d'un ordinateur et auraient, d'autre part, accédé aux données de Z._____ en raccordant son numéro de téléphone portable à une carte SIM en leur possession. Ce faisant, ils auraient eu accès à toutes les données privées de la cliente de la plaignante et auraient été en mesure d'intercepter les communications qu'elle recevait. Par ailleurs, cette manière de procéder aurait empêché Z._____ de se connecter à différents services en ligne qui nécessitaient la double identification par le biais d'un envoi de SMS (e-banking, messagerie électronique, Paypal, etc.). A cela s'ajoute que le compte client d'un fournisseur de télécommunication et le raccordement téléphonique attribué à celui-ci constituent des systèmes de transmission de données visés par l'infraction de l'art. 143bis al. 1 CP (cf. consid. 3.2 supra).

Au regard de ce qui précède et en application du principe *in dubio pro duriore*, le Ministère public ne pouvait, à ce stade, rendre une ordonnance de non-entrée en matière s'agissant de l'infraction à l'art. 143bis CP. Il lui appartiendra donc d'ouvrir une instruction pénale à

l’encontre de S._____ et de B._____, d’identifier les manipulations effectuées par les parties ayant mené au résultat dénoncé, et de bien circonscrire le rôle exact joué par B._____, celle-ci étant totalement extérieure à l’entreprise et ne pouvant de toute manière pas se prévaloir d’un quelconque droit d’accès aux données électroniques des clients de la recourante.

4. Au vu de ce qui précède, le recours doit être admis et l’ordonnance annulée, d’une part en tant qu’elle vaut non-entrée en matière sur l’infraction d’accès indu à un système informatique (art. 143bis al. 1 CP), et, d’autre part, en tant qu’elle prévoit la restitution à la plaignante de la clé USB, enregistrée sous fiche n° 39970, contenant l’enregistrement de l’appel au Call Center du 13 février 2024. L’ordonnance sera maintenue pour le surplus et le dossier de la cause renvoyé au Ministère public pour qu'il procède dans le sens des considérants.

Vu l’admission du recours, les frais de la procédure, constitués en l’espèce du seul émolument d'arrêt, par 880 fr. (art. 20 al. 1 TFIP [tarif des frais de procédure et indemnités en matière pénale du 28 septembre 2010 ; BLV 312.03.1]), seront laissés à la charge de l’Etat (art. 428 al. 4 CPP).

La recourante, qui a procédé avec l'assistance d'un conseil de choix et qui a obtenu gain de cause, a droit, de la part de l'Etat, à une indemnité pour les dépenses occasionnées par la procédure de recours (art. 433 al. 1 let. a CPP, applicable par renvoi de l'art. 436 al. 1 CPP). Elle a conclu à l'allocation d'une indemnité d'un montant de 5'334 fr. 75 correspondant à 11h45 de travail d’avocat au tarif horaire de 400 fr. à 235 fr. de frais forfaitaires et à 399 fr, 75 de TVA. C’est excessif. En effet, compte tenu de la nature de l'affaire et de l'acte de recours déposé, cette indemnité sera fixée à 1’500 fr., correspondant à 5h00 d'activité nécessaire d'avocat au tarif horaire de 300 fr. (art. 26a al. 3 TFIP), montant auquel il convient d'ajouter des débours forfaitaires à concurrence de 2 % des honoraires admis (art. 19 al. 2 TDC [tarif des dépens en matière civile

du 23 novembre 2010 ; BLV 270.11.6], applicable par renvoi de l'art. 26a al. 6 TFIP), par 30 fr., plus la TVA au taux de 8,1 % sur le tout, par 123 fr. 95, soit à 1'654 fr. au total en chiffres arrondis.

Par ces motifs,
la Chambre des recours pénale
prononce :

I. Le recours est admis.

II. L'ordonnance est annulée en tant qu'elle vaut non-entrée en matière sur l'infraction d'accès indu à un système informatique (art. 143bis al. 1 CP), d'une part, et restitution de la clé USB enregistrée sous fiche de pièce à conviction n° 39970, d'autre part.

L'ordonnance est maintenue pour le surplus.

III. Une indemnité de 1'654 fr. (mille six cent cinquante-quatre francs) est allouée à X._____ pour la procédure de recours, à la charge de l'Etat.

IV. Les frais d'arrêt, par 880 fr. (huit cent huitante francs), sont laissés à la charge de l'Etat.

V. L'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 :

- Me Pascal de Preux, avocat (pour X._____),
- 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 :