REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

POUVOIR JUDICIAIRE

P/9480/2023 **ACPR/838/2024**

COUR DE JUSTICE

Chambre pénale de recours

Arrêt du mardi 12 novembre 2024

Entre

A_____ SA, représentée par Me Nicolas HOFFMANN, avocat, KELLERHALS CARRARD GENEVE SNC, rue François-Bellot 6, 1206 Genève,

recourante,

contre l'ordonnance de non-entrée en matière rendue le 1er octobre 2024 par le Ministère public,

et

LE MINISTÈRE PUBLIC de la République et canton de Genève, route de Chancy 6B, 1213 Petit-Lancy - case postale 3565, 1211 Genève 3,

intimé.

EN FAIT :

A. **a.** Par acte expédié le 14 octobre 2024, A_____ SA recourt contre l'ordonnance du 1er octobre précédent, notifiée le 2, par laquelle le Ministère public a décidé de ne pas entrer en matière sur sa plainte du 2 mai 2023.

La recourante conclut à l'annulation de ladite ordonnance, au renvoi de la cause au Ministère public pour instruction et à ce qu'il soit ordonné à cette autorité de procéder à divers actes d'enquête, qu'elle énumère. Elle conclut à l'octroi d'une juste indemnité pour les dépenses occasionnes par la procédure.

b. La recourante a versé les sûretés en CHF 1'500.- qui lui étaient réclamées par la Direction de la procédure.

B. Les faits pertinents suivants ressortent du dossier :

a. A_____ SA, société inscrite au registre du commerce du canton de Genève depuis le _____ 2020 et active dans le négoce international de matières premières dans le domaine de l'énergie, essentiellement de produits pétroliers et de gaz, a déposé plainte le 2 mai 2023 pour soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP), détérioration de données (art. 144bis CP), faux dans les titres (art. 251 CP), tentative d'escroquerie (art. 22 *cum* 146 CP) et tentative d'utilisation frauduleuse d'un ordinateur (art. 22 *cum* 147 CP), à la suite de trois attaques informatiques dont elle avait été victime entre les 2 et 10 février 2023.

Les auteurs de ces attaques avaient usurpé les adresses électroniques de son équipe financière afin de fournir des coordonnées bancaires erronées à un client. Lors de la première attaque, les auteurs avaient tenté de faire transférer USD 4'637'312.- et USD 6'716'701.- en faveur de [la banque] B_____, sise à C_____, au Mexique, lors de la seconde, USD 8'225'047.63, sur un compte de la banque D_____, à E_____, en Pologne. Dans le cadre de la troisième de ces attaques, les auteurs avaient adressé une facture falsifiée de USD 2'310'085.-, payable sur un compte ouvert auprès de [la banque] F_____, en République Tchèque. Elle avait pu déceler la fraude avant qu'il ne soit procédé à ces transferts, grâce à son système de "*call back*" consistant à demander au bénéficiaire du virement, à l'occasion d'un contact téléphonique, de confirmer la finalisation du paiement.

À la suite de ces attaques, elle avait mandaté une société active dans l'audit et le conseil dans le domaine de la cybersécurité, G_____ qui avait eu pour mission de lancer une action dite de "*take down*" des sites internet (web ou serveurs) utilisant son nom et son image, dans le but de les fermer. Cette action avait permis de faire fermer, le 19 février 2023, le site incriminé H_____.com [similaire à celui de A_____] (son nom de domaine à elle étant www.A_____.com).

b. Il ressort du rapport de renseignements du 14 juin 2023 de la Brigade des Cyber Enquêtes de la police judiciaire que la recherche dans ses bases de données n'avait pas révélé de cas similaires en lien avec les numéros de compte indiqués par la plaignante. Le nom de domaine H_____.com n'était plus accessible, en raison de l'action menée par G_____. Ce site avait été enregistré auprès de la compagnie américaine I_____ (J_____, USA) et les données publiques qui pouvaient avoir été mises à disposition lors de l'enregistrement de ce site étaient protégées par un service d'anonymisation basé en Islande (K_____). Cette société protégeait l'identité de ses clients en indiquant comme titulaire du site uniquement les coordonnées de "*Privacy service*". De plus, l'Islande avait une législation propre concernant la protection des données et il n'était pas possible à la police d'obtenir des informations auprès des autorités. Seule I_____ pourrait faire progresser l'enquête, mais cette compagnie ne répondait aux requêtes de la police que sur commission rogatoire internationale.

De telles commissions rogatoires pourraient [également] être adressées au Mexique, en Pologne et en République tchèque, afin d'obtenir les auditions des personnes en lien avec les comptes bancaires [censés recevoir les montants litigieux].

C. Dans son ordonnance querellée, le Ministère public retient que malgré une enquête de police, les auteurs n'avaient pas pu être formellement identifiés. Seul l'envoi de demandes d'entraide internationale au Mexique, en Pologne, aux USA et en République Tchèque permettrait éventuellement de faire avancer les investigations. Or, au vu des intérêts en jeu, un tel acte serait disproportionné et le Ministère public pouvait y renoncer. Il ne disposait ainsi d'aucun élément susceptible d'orienter des soupçons sur un ou des auteurs et ne pouvait procéder.

D. **a.** À l'appui de son recours A_____ SA fait valoir une violation de l'art. 310 al. 1 let. b CPP, dans la mesure où il n'existait pas d'empêchement de procéder, ainsi qu'une violation du principe de proportionnalité. Les attaques cybercriminelles qu'elle dénonçait n'avaient rien à voir avec la situation objet de l'arrêt du Tribunal fédéral 1B_67/2012 sur lequel s'était basé le Ministère public pour refuser d'adresser des commissions rogatoires dans les pays concernés. De telles attaques avaient connu une hausse significative depuis 2012 (+66 % en 2024 par rapport à 2022 pour les usurpations de systèmes de paiement ou d'identité), alors que, dans le même temps, les efforts d'investigation s'étaient vraisemblablement estompés, ce qui conduisait les victimes à ne pas déposer plainte (seules environ 10 à 20 % le faisant). Les victimes se trouvaient ainsi démunies et les auteurs impunis. Par ailleurs, l'absence d'enquêtes menées jusqu'à leur terme violait l'art. 13 de la Convention internationale sur la cybercriminalité, ratifiée par la Suisse en 2012. La Pologne, les USA et la République tchèque en faisaient également partie. Selon cette Convention (art. 25 et 31), les États s'accordaient l'entraide la plus large possible aux fins d'investigation. Sans tentative d'utilisation des instruments prévus par cette Convention, nul ne pouvait anticiper le résultat des demandes d'entraide internationale requises. Pour le Mexique et les USA, il existait un Traité d'entraide (RS 0.351.956.3 et 0.351.933.6).

La police avait *in casu* sollicité la transmission de demandes d'entraide pour que les autorités requises procèdent à l'audition des personnes en lien avec les comptes bancaires censés recevoir les montants litigieux, portant sur plusieurs millions de dollars. Vu ces instruments internationaux, les enjeux importants en lien avec la cybercriminalité et la nature des actes à effectuer, ces demandes avaient de grandes chances d'aboutir.

Enfin, les montants en jeu n'étaient pas négligeables et ce n'était que grâce aux procédures de sécurité qu'elle avait mises en place qu'elle avait pu déceler les fraudes avant qu'elles ne fussent consommées. Son dommage était certain et important, dès lors qu'elle s'était vue contrainte de mandater la société G_____ pour mettre des mesures de sécurité en place. Ses intérêts étaient multiples, à savoir dissuader les auteurs de ces attaques de même que d'autres auteurs potentiels, obtenir une aide étatique dans la très complexe lutte contre la cybercriminalité et prévenir le risque de futurs dommages.

En termes d'actes d'instruction, elle demandait en outre que le Ministère public ordonne l'extraction des données de son système informatique en lien avec les faits dénoncés et procède à leur analyse, ainsi qu'une surveillance du trafic de réseau de son système informatique, afin de détecter des éventuels serveurs externes.

b. À réception des sûretés, la cause a été gardée à juger sans échange d'écritures, ni débats.

EN DROIT :

1. Le recours est recevable pour avoir été déposé selon la forme et dans le délai prescrits (art. 385 al. 1 et 396 al. 1 CPP), concerner une ordonnance sujette à recours auprès de la Chambre de céans (art. 393 al. 1 let. a CPP) et émaner de la plaignante qui, partie à la procédure (art. 104 al. 1 let. b CPP), a qualité pour agir, ayant un intérêt juridiquement protégé à la modification ou à l'annulation de la décision querellée (art. 382 al. 1 CPP).

2. La Chambre pénale de recours peut décider d'emblée de traiter sans échange d'écritures ni débats les recours manifestement irrecevables ou mal fondés (art. 390 al. 2 et 5 *a contrario* CPP). Tel est le cas en l'occurrence, au vu des considérations qui suivent.

3. La recourante reproche au Ministère public de ne pas avoir donné suite à sa plainte.

3.1. Selon l'art. 310 al. 1 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 (let. a) ou qu'il existe des empêchements de procéder (let. b).

3.2. Des motifs de fait peuvent également justifier la non-entrée en matière. Il s'agit des cas où la preuve d'une infraction, soit de la réalisation en fait de ses éléments constitutifs, n'est pas apportée par les pièces dont dispose le Ministère public. Il faut que l'insuffisance de charges soit manifeste. De plus, le Ministère public doit examiner si une enquête, sous une forme ou sous une autre, serait en mesure d'apporter des éléments susceptibles de renforcer les charges contre la personne visée. Ce n'est que si aucun acte d'enquête ne paraît pouvoir amener des éléments susceptibles de renforcer les charges contre la personne visée que le Ministère public peut rendre une ordonnance de non-entrée en matière. L'impossibilité d'identifier l'auteur constitue également un motif de fait justifiant la non-entrée en matière (Y. JEANNERET / A. KUHN / C. PERRIER DEPEURSINGE (éds), *Commentaire romand : Code de procédure pénale suisse*, 2ème éd., Bâle 2019, n. 9a *ad* art. 310). Tel est le cas lorsque l'identité de l'auteur de l'infraction ne peut vraisemblablement pas être découverte et qu'aucun acte d'enquête raisonnable ne serait à même de permettre la découverte des auteurs de l'infraction. Il en va ainsi, par exemple, si les investigations possibles doivent se dérouler, sur commissions rogatoires, dans un pays étranger pour tenter de découvrir les auteurs de l'infraction. Cela pourrait concerner notamment des détenteurs d'adresses IP, celles-ci pouvant vraisemblablement être localisées dans d'autres contrées, voire ne plus exister actuellement. Il sied dans un tel cadre de mettre en balance les intérêts en jeu (arrêt du Tribunal fédéral 1B_67/2012 du 29 mai 2012 consid. 3.2; ACPR/402/2019 du 31 mai 2019 consid. 3.1 et 3.2; ACPR/472/2021 du 14 juillet 2021 consid. 5.4).

Lorsque, pour tenter d'identifier l'auteur de l'infraction, des actes d'instruction doivent se dérouler, sur commissions rogatoires, à l'étranger, les critères à prendre en compte dans la pesée des intérêts sont les suivants : la perspective que la demande d'entraide internationale aboutisse (ACPR/434/2023 du 9 juin 2023, consid. 3.3, ACPR/251/2023 du 6 avril 2023, consid. 2.3, ACPR/195/2023 du 16 mars 2023, consid. 2.4 ainsi qu'ACPR/888/2021 précité, consid. 3.3, tous rendus en matière de crypto-monnaies); l'utilité des informations susceptibles d'être obtenues pour découvrir l'auteur (*ibidem*); la quotité du dommage subi par le plaignant – étant relevé que des préjudices de CHF 12'000.- (arrêt du Tribunal fédéral 1B_67/2012 précité) et CHF 61'450.- (ACPR/888/2021 précité, consid. 3.3) ont été jugés insuffisants pour justifier, à eux seuls, l'envoi de commissions rogatoires –.

Il en découle que le principe de proportionnalité a une portée en la matière, lui qui s'applique à toutes les activités de l'État (art. 5 al. 2 Cst.), y compris à l'activité du ministère public et donc aux investigations pénales (Y. JEANNERET / A. KUHN / C. PERRIER DEPEURSINGE (éds), *op.cit.*, n. 10d *ad* art. 310). Le caractère proportionné de l'enquête à mener est aussi reconnu par la jurisprudence relative à

l'art. 4 CEDH qui impose "*une exigence de célérité et de diligence raisonnable*" (CourEDH Rantsev c. Chypre et Russie du 7 janvier 2010, requête no 25965/04).

3.3. Les États parties à la Convention internationale sur la cybercriminalité (dont la plupart des États européens, les USA, le Canada, l'Australie et le Japon) ont constaté que les technologies modernes de communication et de traitement des données constituent un défi pour la lutte contre la cybercriminalité et la criminalité informatique. Les données électroniques, quel que soit leur lieu d'origine ou de stockage, sont envoyées en quelques secondes à n'importe quel destinataire dans le monde entier ou diffusées à un grand nombre de personnes et d'entités. Les informations stockées dans les systèmes informatiques peuvent être rendues accessibles à un groupe de personnes déterminé ou indéterminé, recherchées de manière ciblée et téléchargées en conséquence. Les frontières nationales ne constituent plus un obstacle à la circulation des informations à l'ère d'Internet, et les nouvelles technologies font que les lieux d'activité et de réussite des comportements délictueux peuvent être de plus en plus éloignés géographiquement. Étant donné que le champ d'application des législations étatiques est limité par le principe de territorialité, la poursuite pénale dans le domaine de la cybercriminalité doit être soutenue par des instruments adéquats du droit pénal international (ATF 141 IV 108 consid. 5.4 et références citées).

3.4. En l'occurrence, si les tentatives du ou des auteurs de faire verser sur des comptes bancaires à l'étranger, par trois fois en quelques jours en février 2023, pour un montant total de près de USD 22'000'000.-, au préjudice de la recourante, active dans le négoce international de matières premières, après falsification de factures et piratage d'adresses e-mails d'employés de son équipe financière, paraissent avérées, il y a lieu de constater qu'aucun acte d'enquête en Suisse, pas plus que les démarches entreprises par la plaignante avec une société spécialisée (G_____), n'ont permis d'en découvrir l'auteur. Il s'agit là au demeurant du but précisément recherché par le ou les auteurs qui profitent des possibilités offertes par Internet. La Brigade des Cyber Enquêtes a suggéré au Ministère public l'envoi de plusieurs commissions rogatoires internationales. L'une, aux USA, concernerait la société I_____ ayant enregistré le site H_____.com par lequel les auteurs auraient agi. La police précise toutefois que les données mises à disposition lors de cet enregistrement seraient protégées par un service d'anonymisation en Islande. Il en résulte qu'il n'est pas possible de déterminer les informations que cet acte d'enquête serait effectivement à même de fournir. Quant aux commissions rogatoires qui seraient adressées au Mexique, en Pologne et en République tchèque, il n'est pas évident qu'elles conduiraient à l'identification, puis à l'audition, des bénéficiaires effectifs des montants devant parvenir sur les comptes bancaires ouverts dans ces pays, pas plus que des personnes ayant conçu de fausses factures et adresses e-mail. Aussi, s'il ne peut être dit que les démarches du Ministère public sont restées sans résultat, il appert que les seules investigations qui pourraient, le cas échéant, faire avancer l'enquête, seraient à tout le moins l'envoi de quatre commissions rogatoires

internationales dont l'admission par les pays concernés, quand bien même certains sont partie à la Convention internationale sur la cybercriminalité, n'est pas garantie. En effet, si les montants en jeu sont très importants, il doit être tenu compte du fait que les infractions en cause n'en sont restées qu'au stade de la tentative, grâce au contrôle "*call back*" en vigueur dans la société plaignante, contrôle qui semble indispensable lorsque les transactions qu'une telle société effectue se montent chacune à plusieurs millions d'USD. Dans le cas d'espèce, au regard du dommage effectivement subi par la plaignante (frais liés à l'intervention de G_____) et dans la mesure où la possibilité d'identifier les auteurs restera manifestement vaine, le principe de proportionnalité autorisait le Ministère public à ne pas entrer en matière.

Il n'y a pour le surplus pas de raisons que le Ministre public entreprenne les autres actes d'enquête proposés par la recourante sur son propre système informatique (extraction de données, leur analyse et surveillance du trafic de réseau), dès lors qu'elle est la mieux à même d'y procéder. Si ces investigations devaient le cas échéant révéler des éléments de nature à faire significativement progresser l'enquête, la procédure pourrait toujours être reprise (art. 323 al. 1 let. b CPP).

Dès lors, faute de soupçon sur un individu, c'est à bon droit que le Ministère public a renoncé à entrer en matière sur les infractions dénoncées et aucune mesure d'instruction proportionnée ne paraît être à même de modifier ce constat. La volonté de la recourante de dissuader les auteurs de ces attaques, de même que d'autres auteurs potentiels, d'obtenir une aide étatique dans la lutte contre la cybercriminalité et de prévenir le risque de futurs dommages est certes compréhensible, mais n'y change rien. Elle a au demeurant pu prendre, en mandatant une société spécialisée, les mesures pour les actions de "*take down*" et mis en place par son intermédiaire, selon ses dires, des mesures de sécurité pour parer à de nouvelles attaques.

4. Il résulte de ce qui précède que l'ordonnance querellée doit être confirmée.

5. La recourante, qui succombe, supportera les frais envers l'État, fixés en totalité à CHF 1'500.- (art. 428 al. 1 CPP et 13 al. 1 du Règlement fixant le tarif des frais en matière pénale, RTFMP ; E 4 10.03).

6. Corrélativement, aucun dépens ne lui sera alloué (ATF 144 IV 207 consid. 1.8.2).

PAR CES MOTIFS,
LA COUR :

Rejette le recours.

Condamne A_____ SA aux frais de la procédure de recours, arrêtés à CHF 1'500.-.

Dit que ce montant sera prélevé sur les sûretés versées.

Notifie le présent arrêt, en copie, à A_____ SA, soit pour elle son conseil, et au Ministère public.

Siégeant :

Madame Corinne CHAPPUIS BUGNON, présidente; Madame Valérie LAUBER et Monsieur Vincent DELALOYE, juges; Monsieur Julien CASEYS, greffier.

Le greffier :	La présidente :
Julien CASEYS	Corinne CHAPPUIS BUGNON

Voie de recours :

Le Tribunal fédéral connaît, comme juridiction ordinaire de recours, des recours en matière pénale au sens de l'art. 78 de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF; RS 173.110); la qualité et les autres conditions pour interjeter recours sont déterminées par les art. 78 à 81 et 90 ss LTF. Le recours doit être formé dans les trente jours qui suivent la notification de l'expédition complète de l'arrêt attaqué.

Le recours doit être adressé au Tribunal fédéral, 1000 Lausanne 14. Les mémoires doivent être remis au plus tard le dernier jour du délai, soit au Tribunal fédéral soit, à l'attention de ce dernier, à La Poste Suisse ou à une représentation diplomatique ou consulaire suisse (art. 48 al. 1 LTF).

P/9480/2023 **ÉTAT DE FRAIS**

COUR DE JUSTICE

Selon le règlement du 22 décembre 2010 fixant le tarif des frais en matière pénale (E 4 10.03).

Débours (art. 2)		
- frais postaux	CHF	10.00
Émoluments généraux (art. 4)		
- délivrance de copies (let. a)	CHF	
- délivrance de copies (let. b)	CHF	
- état de frais (let. h)	CHF	75.00
Émoluments de la Chambre pénale de recours (art. 13)		
- décision sur recours (let. c)	CHF	1'415.00
Total	CHF	**1'500.00**