CHAMBRE DES RECOURS PENALE

Arrêt du 16 décembre 2025

Composition : M. KRIEGER, président
M. Maillard et M. Perrot, juges
Greffier : M. Jaunin

*****

Art. 197 al. 1, 263 al. 1 let. d CPP

Statuant sur le recours interjeté le 28 juillet 2025 par **H._____** contre l'ordonnance rendue le 15 juillet 2025 par le Ministère public central, division criminalité économique, dans la cause **n° PE24.*****, la Chambre des recours pénale considère :

En fait :

A. Depuis le 22 août 2024, le Ministère public central, division criminalité économique (ci-après : Ministère public), instruit une enquête contre B._____ et C._____ pour escroquerie. Il leur est reproché d'avoir, possiblement de concert avec d'autres personnes non encore identifiées,

mis en ligne, sous l'URL www..com, une plateforme d'investissement présentée comme permettant à des utilisateurs inexpérimentés d'administrer un compte de trading portant sur des indices boursiers, le Forex, des cryptomonnaies, des marchés boursiers, des matières premières et des métaux. Entre janvier 2024 et avril 2025, soixante-huit victimes, domiciliées en Suisse, de cette plateforme ont été identifiées. Seize d'entre elles ont déposé plainte pénale pour un préjudice total dépassant 1'700'000 fr. (cf. notamment, PV des opérations, mentions des 22.08.2024 et 21.05.2025).

Selon les investigations menées à ce jour, les victimes auraient été approchées par le biais de publicités diffusées sur les réseaux sociaux et sur Internet. Après avoir manifesté leur intérêt sur la plateforme www...com, elles auraient été contactées par un conseiller, utilisant un numéro de téléphone suisse et se présentant comme travaillant pour « ... ». Sur les recommandations de ce dernier, elles auraient, dans un premier temps, investi de petites sommes d'argent, de l'ordre de 250 fr., au moyen de virements bancaires ou de paiements par carte de crédit. Dans cette phase initiale, les victimes auraient, manifestement afin d'être mises en confiance, pu récupérer les bénéfices apparents de leurs premiers investissements. Par la suite, elles auraient été fortement incitées à verser des montants toujours plus importants, puis auraient été confrontées à des pertes sévères, accompagnées de pressions temporelles, notamment sous la forme d'appels de marge (« *margin calls* ») les poussant à réinvestir encore davantage. Certaines d'entre elles auraient en outre été menacées de poursuites civiles si elles n'assumaient pas les pertes prétendument subies sur leur compte. Dans un second temps, plusieurs victimes auraient été contactées par de pseudo-cabinets juridiques leur promettant mensongèrement de récupérer leurs avoirs moyennant le versement préalable de nouvelles sommes. L'une des victimes aurait ainsi subi un préjudice supplémentaire en versant des montants additionnels à ce faux cabinet juridique. Aucun versement des victimes n'aurait été investi dans les produits financiers prétendument proposés par la plateforme www...com (cf. P. 4, 8/1 et 91).

B. **a)** Par ordonnance du 15 juillet 2025, le Ministère public a ordonné aux sociétés D._____ SA, F._____ Sàrl, G._____ SA, J._____ SA, N._____ AG, K._____ SA, E._____ SA, L._____ AG, M._____ et H._____ AG, le séquestre immédiat des URL suivantes :

- *www..com,*
- *www..com,*
- *www..site,*
- *www..com,*
- *www..com,*
- *www..com,*
- *www..com,*
- *www..com,*
- *www..com,*
- *www..com*
- *www..com* (I),

a ordonné aux sociétés susnommées de transmettre sans délai, mais au plus tard dans un délai de 5 jours ouvrables, la confirmation de l'exécution de la décision de séquestre (II), a dit que le refus, par lesdites sociétés, de se conformer aux chiffres I et II de cette décision serait passible de la peine d'amende prévue à l'art. 292 CP (III) et a rappelé que la présente décision était immédiatement exécutoire nonobstant recours (IV).

Se fondant sur la jurisprudence et la doctrine, le procureur a considéré que les données informatiques, y compris les URL des sites web, pouvaient être assimilées à des objets et, partant, faire l'objet d'un séquestre. Il a en outre estimé qu'il était plus proportionnel de bloquer l'accès à un site plutôt que de séquestrer des serveurs de données. Sur cette base, il a retenu que les sites Internet susmentionnés avaient servi ou devaient servir à appâter des lésés domiciliés en Suisse en leur faisant miroiter de prétendus investissements dans des produits financiers, alors même que leurs auteurs n'avaient d'autre intention que de les dépouiller de leurs économies et que, malgré leurs tentatives, les victimes n'étaient pas parvenues à récupérer leurs avoirs. De tels agissements pouvant être constitutifs d'escroquerie, il a estimé qu'il y avait lieu d'ordonner, sur l'ensemble du territoire suisse, le séquestre des URL des sites précités, lesquelles avaient servi à commettre cette infraction, en vue de garantir leur éventuelle confiscation, par la suppression, dans les DNS, de la

correspondance entre ces URL et l'adresse IP ou par toute autre mesure technique appropriée.

b) Par courriers et courriels des 17, 18, 21, 22 juillet, 5 et 11 août 2025, F._____ Sàrl, E._____ SA, M._____, G._____ SA, N._____ AG, L._____ AG, D._____ SA, K._____ SA et J._____ SA ont confirmé que l'accès aux URL litigieux avait été bloqué sur leur système DNS (cf. P. 182,183, 184, 192, 196, 197, 218, 219 et 223).

C. Par acte du 28 juillet 2025, H._____ AG, par son conseil, a recouru contre cette ordonnance, concluant à son annulation, dès lors qu'elle « *se consid*[érait] *dans l'incapacité de se conformer à la décision du 15 juillet 2025, ce qui lui serait d'ailleurs interdit par la loi* ».

Par acte du même jour, H._____ AG, par son conseil, a requis que son recours soit assorti de l'effet suspensif.

Par ordonnance du 29 juillet 2025, le Président de la Chambre des recours pénale a accordé l'effet suspensif.

Le 23 octobre 2025, le Ministère public a déposé des déterminations et conclu au rejet du recours.

Le 24 novembre 2025, H._____ AG, par son conseil, a spontanément répliqué.

E n d r o i t :

1.

1.1 Aux termes de l'art. 393 al. 1 let. a CPP, le recours est recevable contre les décisions et actes de procédure de la police, du Ministère public et des autorités pénales compétentes en matière de contraventions. Une ordonnance de séquestre (art. 263 CPP) rendue par le Ministère public dans

le cadre de la procédure préliminaire est ainsi susceptible de recours selon les art. 393 ss CPP (Lembo/Nerushay, in : Jeanneret et al. [éd.], Commentaire romand, Code de procédure pénale suisse [ci-après : CR CPP], 2e éd., 2019, n. 4 ad art. 267 CPP ; Moreillon/Parein-Reymond, Petit Commentaire, Code de procédure pénale, 3e éd., 2025, n. 24 ad art. 263 CPP).

Le recours s'exerce par écrit, dans les dix jours, devant l'autorité de recours (art. 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 Interjeté en temps utile par H._____ AG, fournisseuse d'accès à Internet et destinataire de l'ordonnance entreprise, qui a un intérêt juridique à son annulation ou à sa modification (art. 382 al. 1 CPP), le recours est recevable.

2. Selon l'art. 197 al. 1 CPP, les mesures de contrainte ne peuvent être prises que si elles sont prévues par la loi (let. a), si des soupçons suffisants laissent présumer une infraction (let. b), si les buts poursuivis ne peuvent pas être atteints par des mesures moins sévères (let. c) et si elles apparaissent justifiées au regard de la gravité de l'infraction (let. d).

Aux termes de l'art. 263 al. 1 let. d CPP, des objets et des valeurs patrimoniales appartenant au prévenu ou à des tiers peuvent être mis sous séquestre, lorsqu'il est probable qu'ils devront être confisqués.

Le séquestre en vue de confiscation prévu par l'art. 263 al. 1 let. d CPP consiste à séquestrer des biens en raison de leur origine criminelle ou du danger qu'ils représentent pour la sécurité, l'ordre public ou encore la morale. Il a pour but de préparer la confiscation au sens des art. 69 et 70 CP (Moreillon/Parein-Reymond, op. cit., n. 19 ad art. 263 CPP). Il s'agit d'une mesure conservatoire provisoire fondée sur la vraisemblance (ATF 143 IV

357 consid. 1.2.3 et les arrêts cités). Un séquestre est proportionné lorsqu'il porte sur des objets ou avoirs dont on peut admettre, prima facie, qu'ils pourront être confisqués en application du droit pénal fédéral (ATF 144 IV 285 consid. 2.2, JdT 2019 IV 3 ; TF 7B_622/2024 du 10 décembre 2024 consid. 4.3.2 ; TF 1B_343/2020 du 3 septembre 2020 consid. 3.1).

3.

3.1 Dans un premier moyen, la recourante fait valoir qu'elle est uniquement une fournisseuse d'accès à Internet et non un bureau d'enregistrement de noms de domaine (« *registrar* »), de sorte qu'elle n'aurait aucun accès aux domaines Internet visés par l'ordonnance. À cet égard, elle explique que son serveur DNS, comme celui de tout fournisseur d'accès, ne fait que traduire temporairement un nom de domaine en adresse IP afin de permettre à l'utilisateur d'accéder au site souhaité. Pour ce faire, son serveur DNS interroge les serveurs « *faisant autorité* » du registre des domaines concernés, seuls à contenir les données originales. Les informations ne seraient conservées chez elle qu'en cache, pour une durée très courte (au maximum 24 heures et seulement si un client a effectivement consulté le domaine), puis supprimées. Dans la mesure où elle ne disposerait pas durablement des données visées par l'ordonnance de séquestre, elle soutient ne pas avoir la capacité d'exécuter la mesure ordonnée. À toutes fins utiles, elle requiert qu'une expertise soit mise en œuvre sur le fonctionnement du système DNS, ainsi que sur les questions de savoir si les fournisseurs d'accès à Internet gèrent les domaines Internet et si elle a accès au registre des domaines concernés.

3.2 En l'espèce, et contrairement à ce que paraît soutenir la recourante, le séquestre en cause ne vise pas à saisir les noms de domaine auprès d'un « *registrar* », mais à imposer aux fournisseurs d'accès de neutraliser, au niveau de leurs propres résolveurs DNS, la correspondance entre les URL concernées et les adresses IP auxquelles elles renvoient. Autrement dit, il s'agit, pour les fournisseurs d'accès, d'empêcher leurs serveurs DNS de fournir à leurs clients l'adresse IP associée aux domaines en cause, ou de mettre en place une mesure équivalente, par exemple une redirection vers une page d'information. Le grief de la recourante tiré du

fait qu'elle n'est pas un bureau d'enregistrement de noms de domaine repose ainsi sur une compréhension erronée de l'objet du séquestre et doit dès lors être rejeté.

Par ailleurs, la mise en place d'un filtrage/blocage DNS constitue une fonctionnalité courante des fournisseurs d'accès à Internet (cf. par exemple : https://.wikipedia.org/wiki/Blocage_DNS), que ce soit pour exécuter des obligations légales, notamment en matière de lutte contre la pédopornographie, ou pour appliquer des politiques de sécurité (filtrage anti-malware/anti-phishing, contrôle parental, etc.). Au demeurant, la loi fédérale sur les jeux d'argent du 29 septembre 2017 (LJAr ; RS 935.51) impose expressément aux fournisseurs de services de télécommunication de bloquer l'accès aux offres de jeux d'argent en ligne non autorisées en Suisse (art. 86 LJAr). De même, la note de l'Office fédéral de la justice du 4 juillet 2017 intitulée *« Le blocage de sites Internet et ses alternatives »* (cf. P. 248/1), rédigée dans le cadre des travaux préparatoires de cette loi, décrit en détail ce mécanisme, en se référant à la pratique des autorités fédérales dans le domaine de la pédopornographie et de la pornographie dure : le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) tient une liste noire d'URL sur son propre serveur, à laquelle seuls les fournisseurs d'accès peuvent se connecter. Cette liste, qui se présente sous la forme d'un simple fichier texte, dans lequel chaque ligne correspond à l'adresse d'une page Internet, leur est transmise automatiquement, et le blocage des sites se fait ensuite également de manière automatisée. Selon la technique choisie par chaque fournisseur, le blocage peut viser soit l'URL précise, soit l'ensemble du nom de domaine correspondant (ch. 2.2, p. 3). Enfin, à l'ATF 148 II 392, traduit au JdT 2023 I 3, le Tribunal fédéral a eu l'occasion de présenter, sous l'angle de la LJAr, les différentes possibilités de blocage DNS offertes aux fournisseurs d'accès à Internet, pour leur permettre d'empêcher qu'un utilisateur puisse accéder à la page visée (cf. consid. 7). Il a en outre jugé que, même si son efficacité était limitée, le blocage DNS constituait une mesure proportionnée (cf. consid. 8).

Au vu de ce qui précède, la recourante, active de longue date sur le marché suisse et soumise aux mêmes obligations que ses

concurrents, ne saurait être suivie lorsqu'elle prétend qu'elle serait incapable, sur le plan technique, d'exécuter le blocage ordonné. De même, le caractère temporaire du cache DNS, qu'elle met en avant, ne fait pas obstacle au blocage, puisqu'il s'agit précisément de modifier la réponse fournie par le résolveur (ou de ne plus répondre) lorsqu'un client sollicite la résolution d'un des domaines visés. La mise en œuvre d'un tel blocage ne suppose pas que la recourante conserve durablement les données originales du registre, mais seulement qu'elle adapte le comportement de son serveur DNS pour certaines requêtes. Le dossier montre au demeurant que les autres fournisseurs d'accès à Internet destinataires de la décision ont exécuté sans difficulté le blocage demandé (cf. P. 182,183, 184, 192, 196, 197, 218, 219 et 223).

Enfin, l'expertise requise par la recourante est superflue, les conditions posées par l'art. 182 CPP n'étant au surplus manifestement pas réalisées. En effet, la recourante se borne à solliciter, de manière générale, une expertise sur le fonctionnement du système DNS et sur le rôle des fournisseurs d'accès, respectivement des « *registrars* » en matière de gestion des domaines. Or, ces éléments sont notoires et ressortent en outre déjà suffisamment des propres explications de la recourante et de celles du Ministère public. Pour le reste, la recourante ne soutient pas que l'expertise devrait porter sur la faisabilité, pour un fournisseur d'accès, de procéder à un blocage, alors qu'il s'agit-là du point effectivement contesté. A cet égard, et comme on l'a vu, la capacité technique des fournisseurs d'accès à mettre en œuvre un blocage DNS ne fait aucun doute, de sorte qu'elle ne nécessite pas de clarifications techniques supplémentaires.

Le moyen, fondé sur l'impossibilité d'exécuter l'ordonnance faute d'accès aux domaines, doit dès lors être rejeté.

4.

4.1 La recourante fait ensuite valoir qu'un domaine Internet ne pourrait pas faire l'objet d'un séquestre au sens des art. 263 ss CPP mais tout au plus d'un blocage. Elle s'appuie à cet égard sur la définition du séquestre donnée par le dictionnaire Larousse ainsi que sur les art. 46 LTC

(loi fédérale sur les télécommunications du 30 avril 1997 ; RS 784.10) et 86 LJAr, pour en conclure que le législateur n'a jamais employé le terme « *séquestre* » pour désigner le blocage d'un site Internet. Elle soutient en outre, à titre subsidiaire, que l'art. 263 CPP ne constituerait pas une base légale suffisante pour contraindre un fournisseur d'accès à Internet à bloquer un domaine Internet, dès lors que celui-ci ne serait ni un bien ni une valeur patrimoniale, mais une inscription dans un registre.

4.2 La recourante soutient que la loi ne permettrait qu'un séquestre au sens d'une « *saisie* » et non un « *blocage* » de l'accès à un site Internet. Cette interprétation doit être écartée. En effet, le séquestre se définit comme une « *mise sous main de justice des éléments de preuve découverts lors d'une perquisition ou en cours d'enquête, avec le consentement ou contre la volonté de leur détenteur, en vue de leur conservation pour les besoins du procès et de leur production ultérieure devant la juridiction de jugement ou pour procéder à leur confiscation ou leur dévolution à l'Etat* » (Moreillon/Parein-Reymond, op. cit., n. 2 ad rem. prél. aux art. 263 à 268 CPP ; Piquerez, Traité de procédure pénale suisse, 2e éd., Genève 2006, n. 911, p. 589), et non comme une façon précise de s'emparer matériellement d'un objet ou d'une valeur. Du reste, la jurisprudence et la doctrine ont admis, s'agissant de données informatiques, que celles-ci pouvaient être assimilées à des objets matériels et faire l'objet d'un séquestre, respectivement d'un blocage (TPF BV.2004.26 ; TF 1B_142/2016 du 16 novembre 2016 ; TF 1B_185/2016 du 16 novembre 2016 ; CREP 18 juin 2014/250 ; TACC 3 avril 2008/197 ; Benhamou, Blocage de sites web en droit suisse, des injonctions civiles et administratives de blocage au séquestre pénal, in : Droit d'auteur 4.0 Genève [éd.], Genève 2018, pp. 11 à 14). Dans la pratique, lorsque le séquestre porte sur un compte bancaire, il se traduit par un blocage comptable, et non par la remise matérielle des billets et pièces à l'autorité ; de même, lorsqu'il porte sur un bien numérique, la mise sous main de justice passe nécessairement par une neutralisation de l'accès ou de l'usage. D'autre part, le fait que le législateur emploie, dans des lois spéciales telles que la LTC ou la LJAr, les termes de « *blocage* » ou de « *suppression* » pour désigner certains mécanismes administratifs de filtrage ne signifie pas qu'un blocage ordonné dans le

cadre d'une procédure pénale constituerait une mesure d'une autre nature qu'un séquestre au sens des art. 263 ss CPP. En l'occurrence, le blocage DNS n'est que la modalité technique choisie pour réaliser l'effet recherché par l'art. 263 al. 1 let. d CPP, à savoir la mise hors d'usage, en vue de leur éventuelle confiscation, des URL utilisées comme instruments d'une éventuelle escroquerie. La distinction que tente d'opérer la recourante entre « *séquestre* » et « *blocage* » repose ainsi sur une conception excessivement formaliste et matérialiste de la notion de séquestre, laquelle ne tient pas compte des progrès de la technique. Ce moyen, de même que celui tiré de l'absence de base légale, doit dès lors être rejeté.

5.

5.1 La recourante fait valoir que son serveur DNS ne contient que des données temporaires et non les « *données originales* ». Dès lors, même à supposer qu'un séquestre soit possible, celui-ci ne pourrait porter que sur les données disponibles au moment de l'entrée en vigueur de la décision, et non sur les nouvelles données qui seraient enregistrées à l'avenir sur le serveur. Elle ajoute que ces données ne sont qu'en transit pour permettre la consultation des sites par les clients, de sorte que pour y accéder, les autorités devraient recourir à la LSCPT (loi fédérale sur la surveillance de la correspondance par poste et télécommunication ; RS 780.1), et non au séquestre.

5.2 En l'espèce, la recourante part d'une prémisse inexacte quant à l'objet de la mesure litigieuse. L'ordonnance de séquestre ne vise pas à s'emparer des données techniques stockées temporairement dans le cache de son serveur DNS. Elle a pour objet les URL en cause, en tant qu'instruments de l'infraction présumée, et tend à leur mise hors d'usage par le biais d'un blocage d'accès. En d'autres termes, ce qui est demandé à la recourante n'est pas de conserver des données DNS existantes ou futures, mais d'adapter le comportement de ses serveurs lorsqu'un client sollicite la résolution de l'un des domaines visés, pour qu'aucune adresse IP ne soit fournie ou qu'une page d'information s'affiche. Mal fondé, le moyen doit donc être rejeté.

Pour le surplus, le renvoi à la LSCPT n’est pas pertinent. En effet, l’ordonnance querellée ne tend nullement à permettre aux autorités pénales d’accéder aux données de télécommunication de la recourante ou à des journaux de requêtes DNS, mais uniquement à empêcher que ses clients puissent continuer à atteindre certains sites soupçonnés de servir à la commission d’une escroquerie.

6.

6.1 La recourante invoque enfin le principe de neutralité du réseau et ses engagements contractuels, en soutenant qu’elle est tenue d’offrir à ses clients un accès Internet ouvert et sans restriction, de sorte qu’un blocage de domaines sans base légale constituerait une violation tant de ses obligations légales que contractuelles.

6.2 La recourante se prévaut de l’art. 12e al. 1 LTC, qui impose aux fournisseurs d’accès à Internet de transmettre les informations sans faire de distinction, sur le plan technique ou économique, entre émetteurs, destinataires, contenus, services, classes de services, protocoles, applications, programmes ou terminaux. Cette règle n’est toutefois pas absolue. En effet, l’art. 12e al. 2 LTC prévoit expressément que les fournisseurs peuvent traiter les informations de manière différenciée lorsque cela est nécessaire pour respecter une disposition légale ou une décision rendue par un tribunal.

En l’espèce, et comme on l’a vu, l’art. 263 CPP, qui permet de restreindre la garantie de la propriété (Moreillon/Parein-Reymond, op. cit., n. 3 ad rem. prél. aux art. 263 à 268 CPP), constitue une base légale suffisante pour permettre le blocage des URL litigieuses, de sorte que, pour ce motif déjà, le moyen doit être rejeté. A cela s’ajoute que l’on se trouve précisément dans le cas où l’exception à l’Internet ouvert prévue à l’art. 12e al. 2 LTC trouve application. Dans ce cadre, l’invocation du principe de neutralité des réseaux ne saurait faire obstacle à l’exécution de l’ordonnance, mais confirme au contraire que le législateur a prévu la possibilité de blocages ciblés lorsqu’ils sont fondés sur une base légale.

Quant aux engagements contractuels de la recourante envers ses clients, ils ne peuvent évidemment primer sur des obligations découlant directement de la loi ou d'une décision judiciaire. Les utilisateurs ne peuvent d'ailleurs pas s'attendre à un accès illimité à tout contenu en ligne indépendamment des restrictions prévues par le droit fédéral, comme le montrent déjà les mécanismes de blocage imposés notamment en matière de jeux d'argent en ligne (art. 86 LJAr) ou de lutte contre la pédopornographie.

Partant, le moyen tiré d'une violation du principe de neutralité du réseau, respectivement d'obligations contractuelles envers la clientèle, doit être rejeté.

7. En définitive, le recours doit être rejeté et l'ordonnance entreprise confirmée.

Vu le sort du recours, les frais de la procédure, constitués en l'espèce de l'émolument d'arrêt, par 1'210 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 mis à la charge d'H._____ AG, qui succombe (art. 428 al. 1 CPP).

Par ces motifs,
la Chambre des recours pénale
prononce :

I. Le recours est rejeté.
II. L'ordonnance du 15 juillet 2025 est confirmée.
III. Les frais d'arrêt, par 1'210 fr. (mille deux cent dix francs), sont mis à la charge d'H._____ AG.

IV. L’arrêt est exécutoire.

Le président : Le greffier :

Du

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

- Me Simon Schlauri, avocat (pour H._____ AG),
- M. le Procureur du Ministère public central, division affaires spéciales,

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).

Le greffier :