MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

La MInute Cyber 07

DÉCISION DE LA COUR DE CASSATION RELATIVE AUX CONDITIONS DE CAPTATION DE DONNÉES INFORMATIQUES

Les enquêteurs français peuvent-ils procéder à une captation de données informatiques sur le fondement de l'article 706-102-1 du Code de procédure pénale dès lors que le support électronique concerné se trouve à l'étranger ? Oui, répond la chambre criminelle de la Cour de cassation dans un arrêt du 17 juin 2025, tout en précisant les exigences procédurales lorsque les États concernés sont membres de l'Union européenne (Cour de cassation - Chambre criminelle - 17 juin 2025 - n° 24-87.110).

Dans le cadre d'une information judiciaire ouverte notamment des chefs d'importation de stupéfiants en bande organisée, infractions aux législations sur les stupéfiants et sur les armes, association de malfaiteurs, et blanchiment aggravé, les enquêteurs avaient implanté dans le téléphone mobile d'un suspect un dispositif de captation de données informatiques en temps réel leur permettant d'accéder en permanence à l'ensemble de celles-ci et de les exploiter, y compris quand le mis en cause se trouvait hors du territoire national, voyageant dans divers pays, parmi lesquels deux États-membres de l'Union européenne.

Mis en examen par le magistrat instructeur à l'issue des investigations, le mis en cause demandait à la chambre de l'instruction l'annulation des pièces de la procédure relatives à cette captation informatique soutenant parmi divers autres moyens que le principe de souveraineté des États interdisait aux officiers de police judiciaire de réaliser, fût-ce sur autorisation d'un juge d'instruction français, des actes d'investigations en dehors du territoire national.

La chambre de l'instruction rejetait ce moyen en considérant que *« s'il est recommandé de recueillir l'autorisation de l'État étranger même a posteriori, en cas de poursuite au-delà des frontières d'une géolocalisation déjà engagée sur le territoire national, aucun texte ni aucune jurisprudence concernant en propre la captation de données informatiques ne subordonne la validité de l'exploitation des données captées par un key logger lorsque le téléphone se trouve à l'étranger, à l'autorisation de l'État étranger, dès lors que la mesure n'a pas nécessité l'assistance technique du pays où se trouvait le boîtier »*.

Le mis en examen introduisait alors un pourvoi en cassation considérant que les principes de territorialité et de souveraineté des États excluaient que les enquêteurs français soient compétents pour accomplir le moindre acte d'enquête portant atteinte à la vie privée en dehors des frontières nationales, *a fortiori* en exploitant un dispositif de captation de données informatiques sur un support se trouvant en dehors du territoire national français sans l'autorisation expresse de l'État concerné.

La Chambre criminelle de la Cour de cassation rejetait ce pourvoi en précisant que la captation des données informatiques, prévue à l'article 706-102-1 du Code de procédure pénale qui autorise l'accès, en tous lieux, à celles-ci, s'était effectuée dans le cas d'espèce sans l'assistance technique des pays dans lesquels le téléphone, objet de la mesure, avait été déplacé, par l'effet du dispositif technique consistant à transmettre les données vers le territoire national, le simple transit de celles-ci par le réseau d'un opérateur de l'État étranger ne caractérisant pas une atteinte à la souveraineté de cet État, de sorte qu'il n'y avait pas lieu de requérir l'autorisation de ce dernier.

Toutefois, la Chambre Criminelle rappelait que la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014, concernant la décision d'enquête européenne en matière pénale, prévoit en son article 31, paragraphe 1, que, lorsque l'autorité compétente d'un État membre a autorisé, aux fins d'enquête, une interception de télécommunications et que l'adresse de communication de la cible de l'interception est utilisée sur le territoire d'un autre État membre dont l'assistance technique n'est pas nécessaire pour cette interception, l'État membre interceptant notifie cette interception à l'autorité compétente de l'État membre concerné.

Considérant qu'une mesure liée à l'infiltration d'appareils terminaux visant à extraire des données de communication, de trafic et de localisation, à partir d'un service de communication fondé sur l'internet, s'assimile, selon une interprétation autonome et uniforme propre au droit de l'Union, à une mesure d'interception de télécommunications au sens de l'article 31, paragraphe 1, de la directive précitée (CJUE, arrêt du 30 avril 2024, M. N., C-670/22, § 114), la Cour de cassation exige que les États concernés, dès lors qu'ils sont membres de l'Union européenne reçoivent notification de la mesure de captation informatique en cours.

Ayant vérifié qu'une telle notification avait eu lieu dans l'affaire en question par l'émission et la transmission aux deux États-membres de l'Union européenne concernés, par le juge d'instruction, de décisions d'enquête européenne, et que ces États n'avaient pas demandé en retour l'interdiction ou la restriction d'utilisation des données informatiques captées, la Cour de cassation valide l'ensemble des actes accomplis dans le cadre de l'instruction préparatoire.

Visite du général d'armée Hubert BONNEAU, Directeur général de la gendarmerie nationale au COMCYBER-MI

Le 4 juillet dernier, le COMCYBER-MI a eu l'honneur d'accueillir le général d'armée Hubert BONNEAU, Directeur général de la gendarmerie nationale (DGGN).

Accompagné du général de corps d'armée Lionel Lavergne, Directeur des opérations et de l'emploi (DOE), et du général de division Sylvain Noyau, préfigurateur de l'UNPJ (Unité nationale de police judiciaire), il a été accueilli par le commandant du COMCYBER-MI, le général de division Christophe Husson, dans les locaux à Sèvres (92).

Après une visite des espaces de travail et une présentation, par le général de division Christophe HUSSON, du COMCYBER-MI, de ses missions, de son activité et de ses objectifs, ainsi que du personnel et des profils qui le composent (militaire et personnel civil – dont un magistrat et un commissaire divisionnaire de la police nationale, adjoints au chef du COMCYBER-MI), le DGGN a évoqué longuement les ambitions qui doivent animer ce service à compétence nationale, chargé d'assurer la cohérence, la performance et la lisibilité du dispositif global du ministère face aux cybermenaces. Il a notamment souligné l'intérêt majeur de la prospective juridique, de même qu'en matière d'intelligence artificielle (IA), et a également insisté sur l'importance de lier le domaine cyber aux territoires et de connaître, par exemple, finement les menaces qui pèsent sur les opérateurs d'importance vitale (OIV), mais aussi sur les petites et moyennes entreprises (PME) et les très petites entreprises (TPE).

Le DGGN a ensuite pris le temps de répondre aux sujets d'interrogations du personnel présent.

Enfin, la matinée s'est conclue, autour d'un café accompagné de viennoiserie, permettant des échanges entre les équipes et les hauts dirigeants présents.

Le COMCYBER-MI et l'Adan présents à la 8e édition de l'Ethereum Community Conference

Le 30 juin 2025, les analystes – référents cryptoactifs du département de la prévention et de la cyber-résilience de la division de la connaissance de l'anticipation et de la gestion de crise du COMCYBER-MI étaient présents, à Cannes, lors de la 8e édition de l'Ethereum Community Conference, un événement réunissant plusieurs milliers de professionnels du secteur des cryptoactifs.

Au cours d'une conférence ayant trait à la sécurité des personnes et des fonds, les experts du COMCYBER-MI, ont évoqué, aux côtés des représentants de l'association pour le développement des actifs numériques (Adan), des mesures de prévention et de protection visant à renforcer la sécurité des acteurs de l'économie numérique.

Cette intervention s'inscrivait plus globalement dans le cadre des actions partenariales entreprises avec l'Adan, et qui font suite à la désignation, le 16 mai dernier, du COMCYBER-MI en tant que pilote d'un groupe de travail ayant pour objectif le déploiement de mesures de court terme pour prévenir, dissuader et entraver les actes criminels visant les professionnels du secteur des cryptoactifs.

POUR ALLER + LOIN…

Arrestation d'un membre du groupe criminel LockBit

Début août, la section J3 du Parquet de Paris, spécialisée dans la lutte contre la cybercriminalité, indiquait qu'un des membres du groupe LockBit avait été interpellé en Ukraine par l'Unité nationale cyber de la Gendarmerie nationale (UNCyber). LockBit, organisation criminelle spécialisée dans les rançongiciels, est responsable de plus de 2 500 cyberattaques en 2024 (200 en France), dont l'hôpital de Corbeil-Essonnes en août 2022. Cette opération internationale a permis de saisir des serveurs informatiques, de geler des comptes en cryptomonnaies et d'interpeller plusieurs autres membres du groupe.

Le Parquet de Paris a tenu à saluer le travail de transversalité entre équipes et services, qui s'est avéré déterminant, alors que M. Aurélien Brouillet, substitut du procureur à la section J3, a pour sa part indiqué que s'il y a bien eu *« un coup qui a stoppé un certain nombre d'attaques avec ce logiciel, la voie est encore longue […] quand on voit tous les logiciels et rançongiciels encore disponibles »*.

Recommandations de la CNIL sur le développement des systèmes d'IA

Le 22 juillet dernier, la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité administrative indépendante chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés, publiait ses dernières fiches IA (Intelligence Artificielle) en précisant les conditions d'applicabilité du règlement général de protection des données (RGPD) aux modèles. Elle précise également les impératifs de sécurité et les conditions d'annotation des données d'entraînement, tout en annonçant poursuivre ses travaux avec des analyses sectorielles et des outils d'évaluation de la conformité.

En effet, les concepteurs et développeurs de systèmes d'intelligence artificielle indiquent régulièrement à la CNIL que l'application du RGPD pose des difficultés, notamment pour l'entraînement des modèles. Par conséquent, l'autorité indépendante a rédigé une documentation qui vise à combattre cette idée et à aider les professionnels à concilier innovation et respect des droits des personnes.

Il est à noter que les recommandations formulées prennent en considération le nouveau règlement européen sur l'intelligence artificielle adopté à l'été 2024. Il est vrai que lorsque des données personnelles sont utilisées pour le développement d'un système d'IA, le RGPD et le règlement sur l'IA s'appliquent tous deux. Les recommandations de la CNIL ont donc été élaborées pour compléter ces dernières de manière cohérente sur le volet relatif à la protection des données.

Les recommandations de la CNIL sont consultables sur son site internet :

https://www.cnil.fr/fr/ia-finalisation-recommandations-developpement-des-systemes-ia

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 07 - JUILLET - AOÛT 2025
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : Mr J. MARILLY - CEN D. MALET - CEN N. PETITPAS
Conception graphique et maquettage : Mme M. BARREAU

En attendant le prochain numéro de La MInute Cyber, suivez notre actualité :

sur LinkedIn et sur X (ex-Twitter) :
@ComCyberMI