La pénétration du droit pénal dans l'espace privé: la captation de données informatiques

Matthieu Audibert

La pénétration du droit pénal dans l'espace privé
La captation de données informatiques

Par

MATTHIEU AUDIBERT[1]
Officier de gendarmerie

Comme le proclame l'article 9 du code civil, « *chacun a droit au respect de sa vie privée* ». Le Conseil constitutionnel précise en outre « *qu'aux termes de l'article 2 de la Déclaration des droits de l'Homme et du citoyen : « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la sûreté, et la résistance à l'oppression » ; que la liberté proclamée par cet article implique le respect de la vie privée »*[2]. A cet égard, la protection de la vie privée découle implicitement du principe constitutionnel de liberté individuelle.

Ainsi historiquement, le domicile a fait très tôt l'objet de protections spécifiques en procédure pénale, notamment pour les perquisitions et visites domiciliaires[3], principalement au cours de l'enquête préliminaire[4]. Le droit européen participe également à la protection du domicile. Dans son arrêt Keegan contre Royaume-Uni, la Cour européenne des droits de l'homme rappelle que l'inviolabilité est une prérogative rattachée au domicile[5].

Dans le même temps, avec l'émergence d'Internet et des connexions à haut débit, les outils numériques sont devenus des produits de consommation courant. Leur usage ne cesse de se développer. L'écrasante majorité de la population française dispose d'un accès à Internet, les trois quarts de la population disposent d'au moins un téléphone portable connecté à Internet. Ainsi en 2019, 94% de la population d'Europe occidentale est utilisateur d'Internet, 95% de l'Amérique du Nord. Enfin, 92% de la population française utilise Internet[6]. Dans le même temps, l'émergence de la téléphonie mobile et les évolutions technologiques relatives aux réseaux mobiles ont entraîné une connectivité toujours plus importante et surtout presque permanente. Les arrivées de la 4G[7] et bientôt de la 5G[8] ont modifié les usages si bien que l'ordinateur personnel perd chaque année du terrain face aux smartphones. Il est ainsi aisé de réaliser un grand nombre de tâches depuis son domicile, plus largement depuis n'importe où.

[1] Officier de gendarmerie, l'auteur prépare une thèse de doctorat en droit privé et sciences criminelles au sein du Centre de droit pénal et de criminologie de l'Université Paris Nanterre. L'auteur s'exprime à titre personnel et dans le cadre de ses travaux universitaires. Ses propos, thèses ou opinions n'engagent en aucune façon la gendarmerie nationale.
[2] Cons. const., 23 juillet 1999, n°99-416, §45
[3] Article 59 du code de procédure pénale
[4] Article 76 du code de procédure pénale
[5] CEDH 18 juillet 2006, n°28867/03, Keegan c/ Royaume Uni, §29. Voir aussi, CEDH, 9 novembre 2006, n°7615/02, Imakaïeva c/ Russie
[6] AMSILI Sophie et MAUSSION Florian, *L'usage d'Internet dans le monde en cinq chiffres,* Les Échos, 9 février 2019
[7] La 4G correspond à la quatrième génération des standards pour la téléphonie mobile, c'est surtout la première qui propose des vitesses de connexion supérieures aux connexions ADSL.
[8] La 5G correspond à la cinquième génération des standards pour la téléphonie mobile. Encore en développement, elle promet des débits jusqu'à 100 fois plus rapides que la 4G et aura des impacts plus larges que le simple usage de la téléphonie mobile.

Par ailleurs, les applications de messageries instantanées sont en développement croissant. Les objets connectés connaissent un développement fulgurant. Les délinquants se sont eux aussi emparés de ces nouvelles technologies avec notamment le recours massif aux techniques de chiffrement. Autrefois réservée à la criminalité organisée, cette fonctionnalité concerne désormais tous les utilisateurs. En effet, suite aux révélations sur les programmes d'interceptions américains, les opérateurs et les fabricants de supports numériques ont procédé à la généralisation du chiffrement des communications et ce dernier est même devenu un argument commercial.

La problématique du chiffrement est donc devenue un enjeu de plus en plus prégnant pour la réussite des enquête judiciaires. Comme le notent Benoist Hurel et Vincent Lemonier, « *Aujourd'hui, il n'est malheureusement pas exagéré d'affirmer que des enquêtes portant sur des structures criminelles majeures sont rendues impossibles, ou sont extrêmement ralenties, par l'utilisation de messageries cryptées que les enquêteurs ne peuvent pas intercepter en temps réel* »[9].

Face à ces nouveaux comportements et défis technologiques, le législateur a entrepris dès 2011 de renforcer les moyens d'investigation à la disposition des enquêteurs. Si le chiffrement fait obstacle aux interceptions judiciaires ou à leur exploitation ultérieure dans le cadre d'une opération criminalistique, il faut donc récupérer les éléments de preuve numérique directement à la source : quand l'utilisateur utilise son terminal numérique quand bien même cette utilisation a lieu depuis son domicile, plus généralement en tout lieu et à toute heure.

Ainsi, la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 (n°2011-267) va permettre le recours à la captation des données informatiques. Comme évoqué précédemment, « *l'utilité du dispositif ainsi déployé se situe au-delà et en amont des procédés préexistants* »[10]. Il ne s'agit pas avec cette nouvelle technique spéciale d'enquête de procéder à une perquisition au sein du domicile et ce, de manière visible selon les modalités prévues par le régime légal de la perquisition. Il va s'agir ici dans la plus grande discrétion de récupérer des éléments de preuve numérique, notamment en contournant le chiffrement, de manière totalement invisible pour l'utilisateur[11].

Or, cette nouvelle forme d'investigation numérique repose sur une technologie redoutable qu'il est possible de qualifier « d'armes d'intrusion massive » au regard des risques d'atteintes portées à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme.
S'agissant de la mise en œuvre de cette technique spéciale d'enquête par les autorités publiques, le professeur Jean-Christophe Saint-Pau évoque l'existence d'un conflit de normes entre investigations judiciaires numériques et le droit au respect de la vie privée. Ce conflit de

[9] HUREL B., et LEMONIER V., *L'enquête pénale à l'épreuve du chiffrement*, Délibérée, vol. 4, no. 2, 2018, pp. 53-57.
[10] HENNEQUIN S., *Quid de la captation de données informatiques,* Recueil Dalloz 2011, p.1358
[11] Ibid.

normes devant être impérativement résolu par les caractères nécessaire et proportionné qui doivent être énoncés dans la loi et effectivement vérifiés par un juge[12].
A cet égard, la Cour européenne des droits de l'homme « *observe que la protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part.*[13] »

Après avoir présenté les modalités de mise en œuvre de la captation des données informatiques sous le prisme de la pénétration du droit pénal dans l'espace privé et au travers d'un exemple opérationnel (I), nous verrons, qu'eu égard à son caractère extrêmement intrusif, cette technique spéciale d'enquête est particulièrement encadrée pour concilier la nécessité d'identifier les auteurs d'infraction et la protection de la vie privée (II).

[12] SAINT-PAU Jean-Christophe, *Les investigations numériques et le droit au respect de la vie privée,* AJ Pénal 2017, p. 321
[13] CEDH, 4 décembre 2018, n°30562/04 et 30566/04, S. et Marper c/ Royaume-Uni, §112

I. La captation des données informatiques : une approche fonctionnelle de la pénétration quasi-ultime de l'espace privé par le droit pénal.

A l'origine peu connue dans les milieux judiciaires, la captation des données informatiques présente un intérêt de plus en plus marqué eu égard aux dernières évolutions technologiques (A). Sa mise en œuvre souvent envisagée sous un angle théorique peut désormais être illustrée au travers de l'étude d'un cas opérationnel récent (B).

A) La création d'une technique spéciale d'enquête particulièrement intrusive en écho aux évolutions technologiques

Les moyens de communication modernes irriguent profondément nos sociétés et ont profondément bouleversé les méthodes d'enquêtes policières s'agissant de l'interception des correspondances. En effet, si le domicile fait l'objet d'une protection particulière en procédure pénale eu égard à la protection de la vie privée, il s'agit ici d'intercepter et donc de traiter les informations entrantes et sortantes de ce domicile, et même au-delà, sans pour autant y pénétrer.

Le développement des moyens de communication a entraîné une pénétration non physique mais numérique de plus en plus forte de la vie privée par la procédure pénale au cours de l'enquête et de l'instruction. Historiquement, les interceptions de correspondances émises par la voie des communications électroniques ont fait l'objet d'un premier encadrement en 1991[14] et ont évolué au regard du souhait du législateur d'accroitre cette capacité pour les services d'enquêtes. Ces interceptions sont actuellement possibles aussi bien en enquête préliminaire[15], de flagrance[16] que dans le cadre d'une information judiciaire[17].

Il s'agit d'écouter, de retranscrire les paroles ou messages émis en tout temps et en tout lieu via une interception réalisée chez les opérateurs téléphoniques par le biais de la plateforme nationale des interceptions judiciaires[18]. Toutefois, les évolutions technologiques récentes ont entrainé de nombreux bouleversements dans cette capacité que la procédure pénale a pour pénétrer la vie privée. En effet, depuis les révélations d'Edward Snowden le 5 juin 2013, les différents fournisseurs de solutions de communications électroniques ont massivement recours au chiffrement, qui est maintenant présenté comme argument commercial.

Ainsi, de nos jours, il est possible, depuis son domicile, plus largement depuis n'importe où, de converser de manière totalement chiffrée avec un tiers sans prendre le risque de voir ses propos interceptés même par des systèmes mis en œuvre par les autorités publiques. Au titre de la protection de la vie privée, cette possibilité se justifie aisément et est même saine dans une société démocratique. Toutefois elle va constituer un obstacle majeur à la réussite des enquêtes judiciaires[19].

---

[14] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques

[15] Article 706-95 du code de procédure pénale

[16] Ibid.

[17] Article 100 du code de procédure pénale

[18] Article 230-45 du code de procédure pénale

[19] HUREL B., et LEMONIER V., *L'enquête pénale à l'épreuve du chiffrement*, Délibérée, vol. 4, no. 2, 2018, pp. 53-57.

Pour contourner cet obstacle et procéder à des investigations en toute discrétion, le législateur a prévu, pour un champ infractionnel spécifique[20], un certain nombre de techniques spéciales d'enquête, qui vont chacune à divers degrés comporter un caractère intrusif dans la vie privée. Il est par exemple possible de recourir à l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique[21], d'utiliser un imsi-catcher pour récupérer des données de connexion ou intercepter des correspondances[22]. Dans le même temps, il est possible de procéder à une sonorisation du domicile ou du véhicule du mis en cause[23].

Ces techniques spéciales d'enquête sont particulièrement intrusives mais pas nécessairement efficientes. Dans l'hypothèse d'une conversation, il y a un émetteur et un récepteur. L'émetteur d'une conversation peut voir son domicile sonorisé. Néanmoins, cette sonorisation ne permettra pas de récupérer des messages textuels ou encore, dans l'hypothèse d'une conversation vocale, de récupérer les propos tenus par l'autre participant à la conversation. En outre, si la communication est chiffrée, l'imsi-catcher ne présente aucune utilité au même titre qu'une interception de correspondances mise en œuvre sur les réseaux de communications électroniques[24].

De plus, une exploitation forensique post-mortem[25] du terminal numérique peut éventuellement permettre de récupérer des éléments de preuve. Deux écueils peuvent toutefois être relevés : si le terminal est chiffré, il peut être particulièrement long et complexe de récupérer les données intéressant l'enquête, en particulier si le mis en cause ne coopère pas en communiquant la clé de déchiffrement de son terminal[26]. Surtout, les enquêteurs et les magistrats ne peuvent disposer en temps réel d'éléments susceptibles d'intéresser les investigations en cours[27].

Prenant la mesure de ces contraintes opérationnelles, le législateur, via la loi d'orientation et de programmation pour la performance de la sécurité intérieure[28] a ainsi créé une nouvelle technique spéciale d'enquête relative aux captations des données informatiques, prévues par les articles 706-102-1 à 706-102-5 du code de procédure pénale. A l'origine réservée à l'information judiciaire, elle a été étendue aux enquêtes en 2016[29]. Enfin, elle a été dernièrement modifiée en 2019 afin de renforcer son efficacité[30].

Ainsi, cette technique spéciale d'enquête permet de mettre en place un « *dispositif technique ayant pour objet sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont*

[20] Articles 706-73 et 706-73-1 du code de procédure pénale
[21] Article 706-95 du code de procédure pénale
[22] Article 706-95-20 du code de procédure pénale
[23] Article 706-96 du code de procédure pénale
[24] Articles 100 et 706-95 du code de procédure pénale
[25] Après une interpellation
[26] Article 434-15-2 du code pénal
[27] JEANDIDIER Wilfrid, *Criminalité et délinquance organisées,* Rép. Pén. Dalloz, janvier 2017, §96
[28] Loi n°2011-267 du 14 mars 2011 dite loi « LOPPSI 2 »
[29] Loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
[30] CHOPIN Frédérique, *Cybercriminalité,* Rép. Pén. Dalloz, janvier 2020, §463

stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques[31]. »

En d'autres termes, il devient techniquement et surtout juridiquement possible de prendre connaissance, en tout temps et tout lieu, du contenu d'un texte ou d'une conservation vocale avant qu'ils ne soient chiffrés, par la mise en place d'un logiciel espion sur le terminal cible ou sur le réseau de communications électroniques utilisé par le suspect[32]. Ce dispositif technique permet alors de prendre connaissance non seulement des textes insérés par l'utilisateur puis transporter par un périphérique externe[33] mais également les sons, images émis ou reçus lors de l'utilisation d'un service en ligne. Cette précision est importante parce qu'elle permet d'inclure tous les services de communication ne rentrant pas dans la catégorie des opérateurs téléphoniques[34]. Il est ainsi possible de cibler des services de communications tels que WhatsApp, Signal, Telegram, Skype, etc.

En outre, analysée sous l'angle du droit pénal spécial, la captation des données informatiques correspond en réalité à une atteinte à un système de traitement automatisé de données prévue et réprimée par les articles 323-1 et suivants du code pénal et à plusieurs infractions portant atteinte à la vie privée au sens des articles 226-1 à 226-7 du code pénal.

La captation des données informatiques est donc une forme de perquisition informatique à distance, continue mais réalisée à l'insu de la personne objet des investigations et sans témoins. Si elle vise par un exemple un téléphone portable, elle sera fonctionnelle lorsque le suspect est à son domicile et quelle que soit l'heure. Dès lors, il s'agit d'une pénétration extrême de la vie privée par la procédure pénale mais elle présente néanmoins un intérêt opérationnel certain qui mérite d'être illustré au travers d'un exemple concret.

B) Quel intérêt fonctionnel pour la captation des données informatiques ?

Le 2 juillet 2020, Europol et Eurojust diffuse un communiqué de presse pour annoncer la réussite d'une opération majeure contre le crime organisé[35]. Ce communique souligne que depuis plusieurs années, les pays européens sont touchés par des groupes criminels organisés qui sont particulièrement résilients et omniprésents. Les organismes européens de coopération policière et judiciaire relèvent que les technologies de communication chiffrées constituent un élément clé dans la réussite de leurs activités criminelles.

Ainsi, en 2017, la gendarmerie nationale et les magistrats français constatent au cours de différentes opérations que des malfaiteurs utilisent des téléphones chiffrés dotés d'un outil spécifique de communication : Encrochat. Cet outil était censé garantir un anonymat parfait. Il s'agissait d'un système d'exploitation installé en double sur un téléphone portable

[31] Article 706-102-1 alinéa 1 du code de procédure pénale
[32] CHOPIN Frédérique, *Cybercriminalité,* Rép. Pén. Dalloz, janvier 2020, §463
[33] Clé USB par exemple
[34] Article L. 33-1 du code des postes et des communications électroniques.
[35] https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

fonctionnant sous Android. Ce système était masqué pour un utilisateur non averti et nécessitait une combinaison de touches spéciales pour être activé.

En outre, il disposait de plusieurs fonctionnalités visant à assurer une certaine impunité à ses utilisateurs : suppression automatique des messages, code spécifique permettant d'effacer les données présentes sur le terminal ou encore effacement automatique de celles-ci en cas de saisies d'un mauvais code. Ces éléments permettaient en cas d'arrestation de rendre impossible la récupération d'éléments de preuve par les enquêteurs[36]. Par ailleurs, ces téléphones spécifiques étaient dépourvus de caméra, de micro et de GPS. Ils étaient donc utilisés dans un objectif bien précis, ce qui était illustré par les typologies de dossiers au sein desquels ces téléphones étaient retrouvés par les différents services d'enquête européens.

Les spécificités techniques de ce système rendaient impossible l'utilisation des méthodes d'investigation traditionnelles : les interceptions téléphoniques étaient inefficaces, les téléphones étant chiffrés. Leur fonctionnement rendait impossible toute géolocalisation et en l'absence d'informations précises sur les utilisateurs, il était impossible d'envisager des sonorisations. Dès lors, les magistrats et les enquêteurs ont décidé de recourir à la captation des données informatiques afin de contourner l'obstacle constitué par le chiffrement et accéder à des données informatiques, éléments de preuve, de manière invisible pour l'utilisateur[37].

Cette opération de captation a permis de récupérer, à l'insu des malfaiteurs, l'ensemble des données échangées pendant la période autorisée par les magistrats : plus d'une centaine de millions de messages a pu ainsi être récupérée en temps réel avant leur chiffrement. Fort de ces éléments, les enquêteurs de différents pays de l'Union européenne ont pu interpeller de nombreux suspects, saisir plusieurs milliers de kilos de drogues, des armes, des avoirs criminels ou encore découvrir des chambres de torture[38].

En d'autres termes, cela signifie que pendant cette opération de captation, les enquêteurs ont pu lire en temps réel les messages échangés via le système Encrochat mais également récupérer les données stockées sur les terminaux. Il s'agit donc de la pénétration complète d'un système informatique, et d'un réseau illégal de communications électroniques, par les enquêteurs au plus proche des utilisateurs ciblés.

Du fait de cet aspect extrêmement intrusif, il convient à présent d'étudier quelles sont les garanties procédurales encadrant cette technique spéciale d'enquête, notamment au regard du nécessaire équilibre entre protection de la vie privée et recherche des auteurs d'infractions, objectif de valeur constitutionnelle[39].

---

[36] MANACH Jean-Marc, *La gendarmerie a (de nouveau) cassé des messages chiffrés*, NextInpact, 3 juillet 2020
[37] Ibid.
[38] STROOBANTS Jean-Pierre, *Aux Pays-Bas, la police découvre une salle de torture en enquêtant sur un réseau de trafiquants*, Le Monde, 8 juillet 2020.
[39] Conseil constit. 16 juillet 1996, n°96-377 DC, §16

II. L'encadrement de la captation des données informatiques au regard de la nécessaire conciliation entre recherche des auteurs d'infractions et protection de la vie privée

Cette technique spéciale d'enquête fait l'objet d'un double encadrement : au moment de la conception d'un outil de captation (A) et au moment de son utilisation (B).

A) La fabrication d'un dispositif de captation, un fait justificatif extrêmement encadré

Au titre de la protection de la vie privée, le droit pénal sanctionne différents types d'atteintes à celle-ci. Ainsi, la fabrication d'un appareil ou d'un dispositif technique ayant pour objet la captation des données informatiques en l'absence d'autorisation ministérielle y compris lorsque ces faits sont commis par négligence, est punie de cinq ans d'emprisonnement et de 300 000 euros d'amende[40].

Pour réaliser les opérations techniques permettant la conception du dispositif technique de captation, le procureur de la République ou le juge d'instruction peuvent désigner une personne physique ou morale habilitée et inscrite comme expert[41]. Ils peuvent également prescrire le recours aux moyens de l'État soumis au secret de la défense nationale[42].

Toutefois, le risque d'atteinte à la vie privée étant particulièrement important, un dispositif réglementaire vient encadrer cette fabrication. En vertu de l'article R. 226-1 du code pénal, un arrêté du Premier ministre établit les appareils concernés. Il s'agit ainsi des « dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un tel système, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels, opérations ayant pour objet la captation de données informatiques[43] ».

La fabrication de ceux-ci est soumise à une autorisation[44] délivrée par une commission instituée auprès du Premier ministre[45]. Une demande d'autorisation doit être déposée auprès du directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour chaque type d'appareil ou de dispositif technique[46]. L'ANSSI va ensuite auditer l'appareil ou le dispositif technique afin de délivrer le cas échéant une autorisation pour une durée maximale de six ans. Certains services de l'État pouvant recevoir une autorisation de plein droit pour fabriquer de tels appareils ou dispositifs techniques[47].

---

[40] Article 226-3 du code pénal
[41] Au titre de l'article 157 du code de procédure pénale
[42] Article 706-102-1 alinéa 2 du code de procédure pénale
[43] Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal. JORF n°0177 du 1er août 2012
[44] Article R. 226-3 du code pénal
[45] Article R. 226-2 du code pénal
[46] Article R. 226-4 du code pénal
[47] Article R. 226-5 du code pénal

En outre, s'agissant de la captation des données informatiques en matière judiciaire[48], l'État a décidé de centraliser la conception de ces outils au sein d'un service à compétence national dénommé « service technique national de captation judiciaire (STNCJ)[49] » rattaché au directeur technique de la direction générale de la sécurité intérieure. Ses activités et son organisation sont couvertes par le secret de la défense nationale[50]. Toutefois, les travaux de conception et les opérations de mise en œuvre des outils de captation sont placés sous le contrôle de deux personnalités qualifiées. Elles sont respectivement désignées par le ministre de l'intérieur et le ministre de la justice[51].
Ainsi, la simple conception d'un outil de captation est particulièrement encadrée, l'absence d'autorisation de fabrication constituant une infraction pénale. Les articles R. 226-1 et suivants du code pénal constitue un fait justificatif s'agissant de l'infraction prévue par l'article 226-3 du code pénal.

Enfin, l'installation et l'usage du dispositif technique font également l'objet d'un encadrement très important.

B) La mise en œuvre d'une captation des données informatiques : technique d'enquête la plus intrusive et par conséquent la plus contrôlée

Comme cela été précisé, la captation des données informatiques est possible en enquête de flagrance, en enquête préliminaire et dans le cadre de l'information judiciaire. La loi du 23 mars 2019 est venue réorganiser les dispositions relatives à l'encadrement des techniques spéciales d'enquête[52].

Ainsi, la captation des données informatiques est limitée aux d'infractions d'une *« particulière gravité et complexité*[53] » qui doivent nécessairement entrer dans le champ d'application des articles 706-73 et 706-73-1 du code de procédure pénale et si les nécessités de l'enquête ou de l'information l'exigent[54]. Autrement dit, il faut préalablement justifier dans la procédure la nécessité de recourir à cette technique spéciale d'enquête avant de solliciter toute demande d'autorisation.

Cette autorisation est obligatoirement délivrée par un magistrat du siège : dans le cadre de l'enquête, par le juge des libertés et de la détention à la requête du procureur de la République, dans le cadre de l'information, par le juge d'instruction, après avis du procureur de la République[55]. Ensuite le juge doit impérativement rendre une ordonnance écrite et motivée comportant des éléments de fait et de droit pour justifier que cette opération est nécessaire[56].

[48] La captation des données informatiques est également possible au titre de l'article L. 853-2 du code de la sécurité intérieure.
[49] Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire ». JORF n°0107 du 10 mai 2018
[50] Ibid. Article 3
[51] Ibid. Article 7
[52] Loi n°2019-222 du 23 mars 2019 et articles 706-95-11 à 706-95-19 du code de procédure pénale
[53] Conseil constit. 21 mars 2019, n°2019-778 DC, §162
[54] Article 706-95-11 du code de procédure pénale
[55] Article 706-95-12 du code de procédure pénale
[56] Article 706-95-13 du code de procédure pénale

En raison du caractère secret de la procédure, cette ordonnance ne constitue pas un acte juridictionnel et n'est donc pas susceptible de recours. Elle pourrait éventuellement faire l'objet d'une requête ultérieure en nullité[57]. Le juge des libertés et de la détention ainsi que le juge d'instruction conservent donc l'entière maîtrise de l'opportunité d'ordonner une captation des données informatiques[58].

La captation des données informatiques est aussi limitée dans le temps. Dans le cadre de l'enquête, l'autorisation est délivrée pour une durée maximale d'un mois, renouvelable une fois. Dans le cadre de l'information, elle est délivrée pour une durée maximale de quatre mois et renouvelable sans que la captation n'excède une durée de deux ans[59].
Une fois l'autorisation générale autorisant le recours au dispositif de captation délivrée, une autorisation spéciale va préciser les modalités d'implémentation du dispositif technique. L'article 706-102-5 du code de procédure pénale prévoit plusieurs hypothèses en vue de l'installation du dispositif technique qui font chacune l'objet d'un contrôle renforcé en fonction du degré d'atteinte à la vie privée.

Ainsi, le juge des libertés et de la détention, à la requête du procureur de la République, ou le juge d'instruction peut autoriser l'introduction dans un véhicule ou dans un lieu privé en vue de l'installation du dispositif, y compris en dehors des heures légales[60]. Cette opération a lieu à « l'insu ou sans le contentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur celui-ci[61] ».

Le domicile fait l'objet d'une protection renforcée, le juge des libertés et de la détention devant impérativement délivrer une autorisation si le lieu visé est un lieu d'habitation et que l'opération d'installation a lieu en dehors de la période légale prévue par l'article 59 du code de procédure pénale. Le juge des libertés et de la détention étant saisi à cette fin par le procureur de la République ou le juge d'instruction[62]. Dans cette hypothèse, le juge des libertés et de la détention, tel un véritable juge de l'enquête et de l'opportunité des moyens intrusifs à employer, intervient donc dans tous les cas. Deux ordonnances seront alors nécessaires : la première étant celle du juge d'instruction qui autorise le recours à la technique spéciale d'enquête[63] et la seconde étant celle du juge des libertés et de la détention qui autorise l'entrée dans un local d'habitation en dehors des heures légales[64].

De plus, l'installation du dispositif de captation fait également l'objet d'un encadrement précis s'agissant des services, unités et organismes autorisés à y procéder[65]. Ces entités sont limitativement listées à l'article D. 15-1-6 du code de procédure pénale.

---

[57] Articles 170 et 802 du code de procédure pénale
[58] MEINDL Thomas, *Procédure applicable à la criminalité et la délinquance organisée,* JCP. Procédure pénale, Art. 706-73 à 706-106, fasc. n° 20, § 59, 31 janvier 2020
[59] Article 706-95-16 du code de procédure pénale
[60] Article 59 du code de procédure pénale
[61] Article 706-102-5 alinéa 1 du code de procédure pénale
[62] Ibid.
[63] Article 706-95-12 du code de procédure pénale
[64] Article 706-102-5 alinéa 1 du code de procédure pénale
[65] Article 706-95-17 alinéa 2 du code de procédure pénale

Il s'agit ici de l'implémentation physique du dispositif technique de captation. La loi autorise également une implémentation à distance, notamment par la « *transmission par un réseau de communications électroniques de ce dispositif*[66] ». Dans ce cas, l'autorisation est délivrée par le juge des libertés et de la détention, à la requête du procureur de la République, ou par le juge d'instruction. En revanche, le juge des libertés ne rend pas une seconde ordonnance comme dans l'hypothèse évoquée précédemment. Cela peut se justifier dans la mesure où il ne s'agit pas d'une pénétration physique dans un lieu d'habitation et ce en dehors des heures légales.

Dans ces deux hypothèses d'implémentation, l'ensemble des opérations d'installation et de désinstallation du dispositif technique est placé sous l'autorité et le contrôle du juge des libertés et de la détention s'agissant de l'enquête ou du juge de l'instruction s'agissant de l'information. En outre, « *ces opérations ne peuvent avoir d'autre fin que la mise en place du dispositif technique*[67] » de captation.

Il est également important de relever que certains lieux sont par nature exclus. Ainsi, un système de traitement automatisé de données présent dans un cabinet d'avocat ou à son domicile, des locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne, d'une agence de presse, les véhicules professionnelles de ces entreprises, le domicile d'un journaliste, un cabinet médical, d'un notaire, d'un avoué ou d'un huissier ne peut faire l'objet d'une opération de captation[68]. C'est également le cas s'agissant d'un tel système présent dans un véhicule, le bureau ou le domicile d'un député, d'un sénateur ou d'un magistrat.

Le contrôle par un magistrat du siège demeure continu tout au long des opérations, en particulier dans le cadre de l'enquête[69]. A cet effet, le juge des libertés et de la détention doit être informé sans délai des actes accomplis, les procès-verbaux dressés en exécution de son ordonnance doivent lui être communiqués[70]. Il exerce également un contrôle qualitatif des opérations. Si celles-ci ne se sont pas déroulées conformément à son ordonnance ou que les prescriptions légales n'ont pas été respectées, le juge des libertés et de la détention ordonne la destruction des procès-verbaux et des enregistrements effectués[71]. Enfin, la loi prévoit, à peine de nullité, que l'ensemble des opérations de captation ne peut avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat[72]. En revanche, le fait que ces opérations aient révélé des infractions autres que celles visées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes[73].

Une fois la captation fonctionnelle, la loi prévoit un encadrement spécifique s'agissant des informations recueillies. Ainsi les données recueillies utiles à la manifestation de la vérité sont transcrites dans un procès-verbal versé au dossier[74]. Aucune information relative à la vie

[66] Article 706-102-5 alinéa 2 du code de procédure pénale
[67] Article 706-102-5 alinéa 1 du code de procédure pénale
[68] Article 706-102-5 alinéa 3 du code de procédure pénale
[69] Article 706-95-14 alinéa 2 du code de procédure pénale
[70] Article 706-95-14 alinéa 3 du code de procédure pénale
[71] Ibid.
[72] Article 706-95-14 alinéa 4 du code de procédure pénale
[73] Ibid.
[74] Article 706-95-18 alinéa 3 du code de procédure pénale

privée et étrangère aux infractions visées dans les ordonnances du juge des libertés et de la détention ou du juge d'instruction ne peut être conservée dans la procédure[75].

Enfin, au titre de la protection des données personnelles, la captation des données informatiques fait également l'objet d'un encadrement en raison de son caractère intrusif intrinsèque. Celle-ci reposant sur la collecte plus ou moins massive de données dans le cadre d'une enquête judiciaire. Ces données collectées sont nécessairement à caractère personnel et pour pouvoir les exploiter de manière efficace, c'est-à-dire rechercher tous les éléments utiles à la manifestation de la vérité, il est nécessaire de les ordonner dans un traitement informatisé.

Ainsi, au titre de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un dispositif réglementaire vient encadrer l'usage de ces données et précise quels sont les accédants et les destinataires des informations collectées dans le traitement informatique mis en œuvre[76]. Conformément à la loi relative à l'informatique, aux fichiers et aux libertés et à la délibération de la Commission Nationale de l'informatique et des Libertés (CNIL)[77], la mise en œuvre d'un tel traitement nécessite l'envoi à la CNIL d'un engagement de conformité accompagné d'un dossier technique de présentation du traitement. Au titre de la protection des données, le rôle du juge des libertés et de la détention et du juge d'instruction est également souligné.

Pour conclure, comme cela a été démontré, il appert que la captation des données informatiques est une technique spéciale d'enquête particulièrement intrusive, qu'il est possible de qualifier d'exemple topique de la pénétration du droit pénal dans l'espace privé. Il s'agit de la technique spéciale d'enquête qui fait l'objet de l'encadrement le plus strict en procédure pénale.

Pour autant, les finalités liées à la prévention des atteintes à l'ordre public et à la recherche des auteurs d'infractions qui sont, pour le Conseil constitutionnel, nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle[78], ne peuvent tout justifier. Il s'agit donc d'assortir cette pénétration du droit pénal dans l'espace privé de solides garanties procédurales. Ainsi, cette pénétration si absolue du droit pénal dans l'espace privé ne peut s'envisager que si elle est nécessaire, proportionnée[79] au titre de la gravité des infractions et de la durée des mesures mises en œuvre. En outre, ces mesures doivent faire l'objet d'un fort contrôle juridictionnel. Même si l'article 8 de la convention européenne de sauvegarde des droits de l'Homme n'exige pas cette garantie de manière explicite, la loi et la jurisprudence prévoient ce contrôle par un magistrat indépendant[80].

---

[75] Ibid.

[76] Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale. JORF n°0295 du 20 décembre 2015

[77] Délibération 2019-119 du 26 septembre 2020 portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2018 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale.

[78] Conseil *const*., 30 juillet 2010, n° 2010-14/22-QPC, AJDA 2010, p. 1556

[79] CEDH, 2 septembre 2010, n°35623, Uzun c/ Allemagne, D. 2011. 724, obs. S. Lavric

[80] Par exemple sur la géolocalisation, Crim. 22 octobre 2013, n°13-81.946, Bull. crim., n°197

Comme le souligne le professeur Jean-Christophe Saint-Pau, « *les investigations numériques sont le siège d'un conflit d'intérêts fondamentaux, en ce qu'elles poursuivent un objectif de sécurité et de lutte contre le terrorisme, mais qu'elles sont, par nature, attentatoires à la liberté individuelle et au droit au respect de la vie privée.*[81]» Il poursuit en expliquant que « *la recherche de l'équilibre entre ces objectifs d'identique valeur normative n'est pas complètement aboutie dans le dispositif légal*.[82] ». En effet, la principale garantie tient au droit, pour la personne visée par ces investigations, de solliciter la nullité des actes[83]. Or la loi ne prévoit aucune modalité s'agissant de l'information des personnes concernées.

Pour ces raisons, il sera particulièrement intéressant de suivre les évolutions des différents recours déposés au titre de l'exercice effectif des droits de la défense et du droit au respect de la vie privée[84].

[81] SAINT-PAU Jean-Christophe, *Les investigations numériques et le droit au respect de la vie privée,* AJ Pénal 2017, p. 321
[82] Ibid.
[83] Articles 170 et 802 du code de procédure pénale
[84] FOLLOROU Jacques, *Piratage d'EncroChat : les recours se multiplient contre la justice française,* Le Monde, 10 mars 2021