Ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg
Note sur la Loi du 18 juillet 2014

Par une Loi du 18 juillet 2014[1], le Luxembourg a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 (ci-après : la Convention de Budapest), ainsi que le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination de certains actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 18 janvier 2003[2].

Nous soulignons l'importance de la Convention de Budapest, alors que celle-ci a également été signée par des Etats non-membres à cette organisation[3], ce qui lui confère un champ d'application territorial très large.

Sous une première section, la Convention de Budapest énumère les comportements qui doivent être réprimés par les législations nationales. Ceux-ci étant déjà couverts par les articles 509-1 et suivants du Code pénal[4], la Loi du 18 juillet 2014 vise donc essentiellement à parfaire et à compléter les textes luxembourgeois (A).

Les modifications apportées par la nouvelle législation concernent principalement les règles de procédure pénale reprises sous la deuxième section de la Convention de Budapest. Tandis que certaines pratiques, implicitement couvertes par le Code d'instruction criminelle, sont désormais expressément consacrées, d'autres procédures ont été créées (B).

A. Les infractions

Le législateur luxembourgeois est intervenu en 1993 pour sanctionner les atteintes aux systèmes de traitement ou de transmission automatisé de données[5] (articles 509-1 et suivants du Code pénal). A cette époque, les réseaux de l'information et plus précisément Internet, étaient encore à leurs débuts. Leur développement a donné naissance à de nouvelles formes de criminalité qui n'ont pas pu être imaginées au début des années 90. A titre d'exemple, on peut citer les usurpations d'identité sur les réseaux sociaux.

---

[1] Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

[2] Les dispositions contenues dans le Protocole étant couvertes par les dispositions législatives actuellement en vigueur au Luxembourg aucune modification législative n'a été nécessaire.

[3] Les États-Unis d'Amérique ayant également ratifié cette convention (le 1er janvier 2007) ; parmi les autres pays signataires figurent notamment l'Argentine, l'Australie, le Canada, le Japon, le Mexique et l'Afrique du Sud

[4] Insérés dans le Code pénal par la Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique.

[5] Le législateur a maintenu la notion de « systèmes de traitement ou de transmission automatisé de données » dans nos textes, au détriment de celle de « système informatique » employée dans la Convention de Budapest. Malgré cette différence de terminologie, la même infrastructure est visée. Tombent notamment sous cette qualification, les serveurs, ordinateurs, tablettes et smartphones.

L'application de la législation actuelle a généralement permis de sanctionner les nouvelles formes de délits en ligne[6]. La loi pénale étant d'application stricte, certains comportements ont toutefois échappé à toute répression. Il s'est également avéré que certaines sanctions n'étaient plus adaptées au comportement visé.

La Loi du 18 juillet 2014 répond aux lacunes constatées en complétant certains textes existants (1) et en créant de nouvelles infractions (2).

1. L'adaptation des textes existants

a. *Une protection accrue de la clé électronique*

i. Le « phishing »

Le « phishing » ou « hameçonnage » désigne *« la pratique frauduleuse qui consiste à tenter d'obtenir des informations sensibles, telles que des mots de passe ou des coordonnées de cartes de crédit, en se faisant passer pour une personne de confiance dans le cadre d'une communication électronique »*[7].

Tandis que l'attaque de « phishing » qui aboutit à un accès au système informatique visé est notamment réprimée par l'article 509-1 du Code pénal (accès frauduleux à un système de traitement ou de transmission automatisé de données), un doute est apparu pour ce qui est de la manœuvre de « phishing » qui n'a pas abouti à un tel accès.

Par un arrêt du 14 juin 2010[8], la Cour d'appel avait en effet acquitté un prévenu de l'infraction d'escroquerie, en retenant que *« le mot de passe ne constitue pas un meuble au sens de l'article 496 du code pénal. En effet contrairement aux données ou programmes informatiques susceptibles d'être enregistrés, transmis ou reproduits sous la forme d'impulsions dans des circuits électroniques ou sur des bandes ou disques magnétiques et dont la délivrance peut dès lors être constatée matériellement, le mot de passe composé d'une suite de caractères servant de moyen d'authentification à son utilisateur ne constitue qu'une simple clé électronique n'ayant aucune présence matérielle et ne pouvant partant pas être remise ou délivrée à l'auteur de l'infraction »*.

Au regard du trouble causé par les attaques de « phishing », le législateur est dès lors intervenu pour compléter le texte sur l'escroquerie en y visant expressément la clé électronique comme « bien » susceptible d'appropriation (modification apportée à l'article 496 du Code pénal).

ii. Les infractions de vol, d'extorsion et d'abus de confiance

Suite aux observations du Conseil d'Etat[9], le législateur a également complété les textes sur le vol (article 461 du Code pénal), l'extorsion (article 470 du Code pénal) et l'abus de confiance (article 491 du Code pénal) en insérant la clé électronique dans la liste des objets susceptibles d'une appropriation frauduleuse.

---

[6] Pour un aperçu de jurisprudence, voir notamment : M. BRAUN, Les infractions en matière de cybercriminalité, JTL 18, 2011, p. 141 ss.

[7] Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité - COM/2007/0267 final, page 3

[8] CA 14 juin 2010, n° 261/10 X, JUDOC 99865656

[9] Doc. parl. n° 6514-2, Avis du Conseil d'Etat, p. 3

A ce sujet, nous tenons à relever un arrêt de la Cour de cassation du 3 avril 2014[10] qui pourrait mettre un terme aux hésitations existant en matière d'appropriation d'objets incorporels. Par cette décision, la Haute juridiction a en effet cassé un arrêt de la Cour d'appel, en retenant que :

> *« Attendu que les données électroniques enregistrées sur le serveur de la banque et qui sont juridiquement sa propriété exclusive constituent des biens incorporels qui peuvent faire l'objet d'une appréhension par voie de téléchargement ;*
>
> *qu'en retenant dès lors que par le fait de télécharger des données électroniques à partir du serveur de la banque, B) ne s'est pas approprié un meuble corporel, de sorte que l'élément matériel du vol fait défaut, la Cour d'appel a violé la disposition susvisée ;*
>
> *que l'arrêt encourt dès lors la cassation »*.

L'appropriation frauduleuse de biens incorporels appartenant à autrui tombe dès lors désormais sous l'infraction de vol.

iii. Augmentation de la peine prévue pour la contrefaçon et l'altération de clés

L'infraction de contrefaçon et d'altération de clés, y compris électroniques est désormais punie d'un emprisonnement de quatre mois à cinq ans et d'une amende de 1.250 à 30.000 euros (article 488 du Code pénal).

b. *Le blanchiment*

Les infractions informatiques ne figuraient pas dans la liste des infractions primaires de l'infraction de blanchiment prévue par les articles 506-1 et suivants du Code pénal. Tel est désormais le cas (article 3, point 7 de la Loi du 18 juillet 2014).

2. Les infractions créées par la Loi du 18 juillet 2014

a. *L'interception des données*

L'article 3 de la Convention de Budapest prévoit la pénalisation de l'interception illégale de données informatiques[11]. D'après le rapport explicatif de la Convention[12], cette disposition *« vise à protéger le droit au respect des données transmises »*. L'interception concerne *« l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu soit directement, au moyen de l'accès au système informatique et de son utilisation, soit indirectement, au moyen de l'emploi de dispositifs d'écoute. L'interception peut aussi consister en un enregistrement des données »*.

---

[10] Cass. 17 avril 2014, n° 17/2014 pénal

[11] Article 3 : *« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique »*.

[12] Rapport explicatif de la Convention de Budapest, n° 53

Les textes luxembourgeois ne réprimaient pas expressément l'interception de données, de sorte que le législateur a complété l'article 509-3 du Code pénal par un alinéa 2, suivant lequel :

> « Sera puni des mêmes peines[13] celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données informatiques lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données ».

b. *L'abus de dispositifs*

L'alinéa 2 de l'article 509-4 du Code pénal réprimait ceux qui *« auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l'alinéa 1^er^ »*.

En visant uniquement les infractions prévues à l'article 509-4 alinéa 1^er^ du Code pénal[14], l'application du texte pénal était limitée aux outils malveillants ayant pour finalité de réaliser un transfert d'argent ou de valeur monétaire.

Cette restriction – qui semble avoir été introduite par erreur – a été levée par la Loi du 18 juillet 2014, qui réprime d'une façon générale *« le fait d'avoir, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition,*

- *un dispositif informatique destiné à commettre l'une des infractions visées aux articles 509-1 à 509-4; ou*
- *toute clef électronique permettant d'accéder, au mépris des droits d'autrui, à tout ou à partie d'un système de traitement ou de transmission automatisé de données »* (article 509-5 du Code pénal[15]).

Les développeurs de virus, de sites de « phishing » ou de malware tombent notamment sous cette infraction.

c. *L'usurpation du nom ou de l'identifiant d'autrui*

Le port public d'un nom appartenant à autrui est réprimé par l'article 231 du Code pénal. Pour que cette infraction soit donnée, il faut que l'auteur prenne publiquement un nom qui ne lui appartient pas. Le faux nom est un autre nom que celui qui figure dans l'acte de naissance.

Le texte existant a notamment permis de sanctionner l'inscription sous le nom d'autrui sur les réseaux sociaux ou l'utilisation de ce nom pour ouvrir des boîtes de courrier électronique[16].

La protection prévue par l'article 231 du Code pénal se limite toutefois au nom patronymique[17], de sorte que d'autres types d'identification sur les réseaux de l'information, tels que nom d'utilisateur ou pseudonyme, se sont pas couverts par ce texte.

---

[13] Emprisonnement de trois mois à trois ans et d'une amende de 1.250 à 12.500 euros ou d'une de ces peines seulement.

[14] Les infractions informatiques dans lesquelles il y eu transfert d'argent ou de valeur monétaire.

[15] L'article 509-4, alinéa 2 étant abrogé.

[16] TA Lux. 5 avril 2011, n° 1238/2011

[17] La Cour d'appel a notamment jugé que le port public d'un faux prénom, pris comme tel, n'est pas réprimé par l'article 231 du Code pénal (CA 27 février 2007, n° 125/07 V)

Le législateur est dès lors intervenu pour compléter le Code pénal par un article 231bis, qui prévoit que :

> *« Quiconque, dans le but de troubler la tranquillité d'un tiers, ou dans le but de porter atteinte à l'honneur ou à la considération d'un tiers, aura pris un nom ou un identifiant qui ne lui appartient pas sera puni d'un emprisonnement de trois mois à deux ans, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement »* (alinéa 1er).

Il est important de noter que la poursuite de l'infraction prévue par cet article exige une plainte de la victime, de son représentant légal ou de ses ayants droit (alinéa 2).

B. Les règles de procédure

Les infractions informatiques touchent généralement plusieurs pays. Ainsi, dans une fraude à la carte de crédit, une carte de crédit peut être soustraite dans un pays A, par un prévenu résidant dans un pays B, qui passe par la suite une commande moyennant cette carte auprès d'un vendeur résidant dans un pays C, alors que l'organisme de paiement a son siège social dans un pays D. Ce simple exemple illustre le caractère international de la cybercriminalité. Le nombre de pays impliqués pouvant être facilement démultiplié.

Les règles de compétence territoriale luxembourgeoises actuelles permettent d'appréhender cette problématique. La Loi du 18 juillet 2014 s'est dès lors limitée à consacrer le principe « aut dedere aut judicare » (extrader ou poursuivre) pour les infractions informatiques (1).

L'intervention législative a été plus importante pour adapter les règles de procédure actuelles – notamment sur l'administration de la preuve – aux nouvelles réalités technologiques (2).

1. La compétence territoriale des autorités judiciaires luxembourgeoises

L'article 22, point 1 de la Convention de Budapest dispose en premier lieu que les autorités judiciaires luxembourgeoises doivent être compétentes pour connaître des infractions informatiques commises sur son territoire. Cette condition – qui consacre le droit commun luxembourgeois – se trouve évidemment remplie.

La compétence territoriale doit également être donnée si une de ces infractions est commise par un ressortissant luxembourgeois, *« si l'infraction est punissable également là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat »*. Cette extension de la compétence des juridictions nationales pour les infractions commises par un luxembourgeois à l'étranger est réglée par l'article 5 du Code d'instruction criminelle.

Le législateur a encore complété l'article 7-4 du Code d'instruction criminelle en prévoyant que les infractions en matière informatique commises à l'étranger pourront être poursuivies au Luxembourg lorsque le suspect n'est pas extradé par le pays requis. Le Luxembourg élève ainsi la criminalité informatique aux affaires relavant du principe « aut dedere aut judicare » (extrader ou poursuivre)[18].

[18] Conformément à l'article 22, point 3 de la Convention de Budapest.

2. Les moyens d'enquête

a. *La conservation rapide et la saisie des données informatiques*

Un facteur primordial dans la poursuite d'infractions en matière informatique est le temps. Les réseaux de l'information et les infrastructures informatiques fonctionnent de façon instantanée ; dès qu'une demande est adressée à ces systèmes, la réponse est immédiate. De l'autre côté, les autorités policières et judiciaires travaillent à la vitesse de l'être humain. Autrement dit, pendant le temps nécessaire à la préparation d'une ordonnance de saisie ou de perquisition, des systèmes informatiques peuvent avoir été radicalement modifiés.

L'impératif de célérité dans la collecte des données informatiques ne saurait toutefois aboutir à priver les citoyens des garanties offertes par le Code d'instruction criminelle (notamment en matière de saisies ou de perquisitions).

Le système instauré par la Convention de Budapest prévoit partant une procédure en deux étapes : une première qui consiste à conserver des données pendant une certaine période (i), une deuxième qui permet de saisir ces données suivant les procédures de droit (ii).

i. La conservation rapide de données informatiques stockées et la conservation et divulgation de données relatives au trafic

La conservation rapide des données est prévue par un nouvel article 48-25 du Code d'instruction criminelle qui dispose que :

> *« Lorsqu'il y a des raisons de penser que des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, le procureur d'Etat ou le juge d'instruction saisi peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, de ces données »*[19].

Cette disposition permet la conservation rapide de données dans le cadre du flagrant délit ou de l'enquête préliminaire par le procureur d'Etat et dans le cadre de l'instruction par le Juge d'instruction. La procédure pourra être utilisée aussi bien au niveau national qu'au niveau international dans le cadre de commissions rogatoires internationales[20].

Il est important de noter que les informations conservées en application de l'article 48-25 du Code d'instruction criminelle restent entre les mains de la personne requise (notamment un hébergeur).

Ce n'est que dans une deuxième étape que les données seront saisies au sens des règles applicables à l'enquête de flagrance, à l'enquête préliminaire, ainsi qu'à l'instruction judiciaire.

ii. La saisie proprement dite des informations

La saisie des données informatiques peut être ordonnée directement ou à la suite d'une demande de conservation rapide de données (voir le point i. ci-dessus).

---

[19] Article prévu dans un nouveau chapitre X, intitulé *« De la conservation rapide des données informatiques »*, figurant dans le Livre Premier, Titre II du Code d'instruction criminelle

[20] Doc. parl. n° 6514, exposé des motifs, p. 13

Le législateur est intervenu à plusieurs niveaux pour adapter les règles existantes aux saisies informatiques. En premier lieu, les articles 33 et 66 du Code d'instruction criminelle prévoient désormais expressément la saisie des *« données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données »*. Cette précision permet essentiellement de souligner la portée de ces textes, alors que la saisie de données informatiques se pratiquait déjà en application des textes originaires.

Nous insistons plus particulièrement sur les aspects suivants :

- la possibilité de saisir les données de télécommunications dans le cadre d'une mini-instruction définie par l'article 24-1 du Code d'instruction criminelle,
- la faculté de saisir une copie des données,
- la possibilité de procéder à l'effacement de celles-ci,
- la nomination d'un expert en matière de cryptologie.

- la possibilité de saisir les données de télécommunications dans le cadre d'une mini-instruction définie par l'article 24-1 du Code d'instruction criminelle

L'article 24-1 du Code d'instruction criminelle permet au procureur d'Etat de requérir du juge d'instruction d'ordonner une perquisition, une saisie, l'audition d'un témoin ou une expertise sans qu'une instruction préparatoire ne soit ouverte[21].

Les pouvoirs attribués au Juge d'instruction en application de l'article 67-1 du Code d'instruction criminelle (saisie de données de télécommunication) n'étaient toutefois pas visés par ce texte. Autrement dit, pour pouvoir ordonner un repérage ou une localisation de données de télécommunication, une instruction judicaire a toujours dû être ouverte.

Cette obligation a mené à un formalisme important en matière d'infractions liées à la cybercriminalité. La problématique s'est notamment posée avec les dossiers dans lesquels les repérages n'ont donné aucun résultat. Ce constat, qui aurait engendré un simple classement au parquet, a systématiquement engendré une procédure de non-lieu devant la Chambre du conseil en application des articles 127 et 128 du Code d'instruction criminelle.

Afin d'éviter ces inconvénients, la saisie de données de télécommunication peut désormais être ordonnée dans le cadre d'une mini-instruction pour les infractions énumérées à l'article 24-1, alinéas 1 et 2 du Code d'instruction criminelle.

- la faculté de saisir une copie des données

En matière de saisie de biens corporels, le détenteur du bien visé par l'enquête ou l'instruction en est matériellement dessaisi au détriment des autorités judiciaires.

En matière informatique, une prise de possession matérielle de données informatiques est uniquement possible en saisissant l'infrastructure sur laquelle ces données sont stockées (p.ex. un ordinateur). Cette saisie peut s'avérer fastidieuse à plusieurs égards :

- les données litigieuses peuvent être stockées sur un serveur qui abrite les données d'autres personnes que celle visée par l'enquête ou l'ordonnance de saisie. Tel est notamment le cas

[21] Cette faculté étant limitée aux infractions visées par l'article 24-1 du Code d'instruction criminelle (presque tous les délits et certains crimes).

pour les serveurs hébergeant une multitude de sites Internet. La saisie du serveur perturbe alors également les services de personnes tierces[22] ;

- le fonctionnement d'infrastructures informatiques peut être très complexe. A titre d'exemple, on peut citer les services de stockage dans le nuage (angl. « cloud »), où les données d'un même utilisateur peuvent être stockées sur une multitude de serveurs. Ce ne sont que les logiciels de ces opérateurs qui permettent d'afficher les données d'un utilisateur ensemble.

- les données litigieuses se trouvent sur l'infrastructure d'un opérateur non visé par l'enquête ou l'instruction. Pour saisir les données de son client, il faudrait partant saisir son matériel.

Le législateur a partant adapté la législation luxembourgeoise aux réalités en matière informatique, en prévoyant que *« la saisie des données stockées, traitées ou transmises dans un système informatique peut se faire, soit par la saisie du support physique de ces données, soit par une copie de ces données » (article 33, point 5 ; article 66, point 3)*.

- *la possibilité de procéder à l'effacement de celles-ci*

Les articles 33, point 5) et 66, point 3) prévoient également que : *« si une copie est réalisée, le juge d'instruction [respectivement le Procureur d'Etat lors de l'enquête de flagrance] peut ordonner l'effacement définitif sur le support physique, lorsque celui-ci se trouve au Grand-Duché de Luxembourg et qu'il n'a pas été placé sous la main de la justice, des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens »*.

Cette disposition permet d'effacer des données stockées, traitées ou transmises dans un système informatique dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens. L'effacement se fait dans le cadre d'une saisie judiciaire et exige qu'une copie des données à effacer soit préalablement établie.

A côté des impératifs en matière de preuve, la copie ainsi établie permettrait encore de rétablir les données effacées en cas d'annulation de la décision d'effacement par la Chambre du conseil ou par les juridictions du fond, ainsi qu'en cas de non-lieu ou d'acquittement prononcé sur le fond de l'affaire[23].

Il est important de noter que le texte relatif à l'effacement s'applique uniquement aux données dont le support physique se trouve au Grand-Duché de Luxembourg.

L'utilité du nouveau texte est multiple. En premier lieu, il permet de faire cesser des atteintes contre d'autres systèmes informatiques. Nous pensons notamment aux dispositifs informatiques destinés à commettre l'une des infractions visées aux articles 509-1 à 509-4 du Code pénal[24]. Il permet également de retirer du contenu illégal, tel que des images ou vidéos pédopornographiques.

- *la nomination d'un expert en matière de cryptologie*

L'article 66, point 4) du Code d'instruction criminelle prévoit désormais que :

---

[22] Sur ces aspects, voir également B. LOSDYCK, Les saisies et perquisitions de matériel informatique : les « gardes-fous » entourant leur mise en œuvre, RDTI n° 52, 3/2013, p. 36

[23] Cette problématique a notamment été soulevée par le Conseil d'Etat dans son premier avis du 16 avril 2013, Doc. parl. n° 6514-2, p. 6, point 4

[24] Voir nos développements au sujet de l'article 509-5 du Code pénal, exposés ci-dessus

> *« Le juge d'instruction peut, par ordonnance motivée, enjoindre à une personne, hormis la personne visée par l'instruction, dont il considère qu'elle a une connaissance particulière du système de traitement ou de transmission automatisé de données ou du mécanisme de protection ou de cryptage, qu'elle lui donne accès au système saisi, aux données saisies contenues dans ce système ou aux données saisies accessibles à partir de ce système ainsi qu'à la compréhension de données saisies protégées ou cryptées. Sous réserve des articles 72, 73 et 76 ci-dessous, la personne désignée est tenue de prêter son concours ».*

Cette disposition est importante en matière d'infractions informatiques, étant donné que l'accès aux réseaux et donc aux données exige souvent l'intervention de personnes hautement spécialisées qui ont elles-mêmes programmé et configure les logiciels et sont souvent détentrices de mots de passe ou de codes sans lesquels un accès est impossible[25].

b. *Les repérages et localisations de télécommunications*

L'article 67-1 du Code d'instruction criminelle sur les repérages et localisations de télécommunications a été adapté, afin de rendre compte de l'introduction de la nouvelle procédure de l'article 48-25 du Code d'instruction criminelle (conservation rapide de données) et de la modification de l'article 24-1 du même code (mini-instruction) qui prévoient désormais la possibilité du repérage même en absence d'une instruction préparatoire.

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques a également été modifiée en ce sens.

c. *L'infiltration*

Le Juge d'instruction peut désormais ordonner des infiltrations en matière de criminalité informatique (article 48-17 du Code d'instruction criminelle).

26 juillet 2014

Par Max BRAUN
Magistrat

[25] Doc. parl. n° 6514, exposé des motifs, p. 14