Colloque Préparatoire.
24 – 27 Septembre 2013, Antalya (Turquie),
Section III: Société de l'information et droit pénal

RAPPORT BELGE*

Daniel DE WOLF*

(B). Questions d'ordre général

(1) Y a-t-il des définitions (juridique ou socio-juridique) actuelles pour les applications de l'informatique et des TIC dans le cadre de la procédure pénale (y compris criminalistique)? Comment ces définitions conceptuelles sont-elles reflétées dans la littérature, les lois, les décisions judiciaires et les pratiques pertinentes au sein de la procédure pénale?

Il est d'abord opportun de remarquer que dans la culture judiciaire belge, il est moins fréquent de définir des concepts ou d'analyser le droit au moyen de définitions conceptuelles. Deuxièmement, nous nous limiterons aux définitions dans le droit pénal ou dans le droit de procédure pénale.

Lors de l'adoption de la loi du 28 novembre 2000 relative à la criminalité informatique, qui comporte aussi bien un volet pénal matériel et un volet de procédure pénale, l'on a noté que la loi ne contient aucune définition. Cela était expliqué par le manque de « tradition juridique » et par le fait que des définitions peuvent produire un effet contreproductif vu l'évolution de la technologie. Le législateur a donc opté pour une approche neutre d'un point de vue technologique. Un « système informatique » a été expliqué comme « *tout système permettant le stockage, le traitement ou la transmission de données. À ce propos, on pense principalement aux ordinateurs, aux cartes à puce etc., mais également aux réseaux et à leurs composants ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information* »[1]. La doctrine n'a fait que reprendre ce passage des travaux parlementaires[2]. On l'utilise aussi en droit pénal pour définir l'infraction du faux en informatique et du « hacking » d'un système informatique[3]. D'autres auteurs[4] préfèrent la définition de la Convention sur la cybercriminalité du 23 novembre 2001, qu'il jugent plus précise, où un « système informatique » est désigné « *comme tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données* »[5]. L'on pourra donc désigner comme un système informatique les ordinateur, les réseaux informatiques, les cartes à puces, le système de télécommunications, les appareils photo digitaux, les caméras vidéos, les téléphones mobiles, le système de gestion automatique des ascenseurs, les centrales de système d'alarmes, les agendas électroniques, les e-books [6], un récepteur GPS, un terminal de paiement électronique, …[7]. Mais il n'y a pas, du moins entre pénalistes, de vrai débat conceptuel, ce qui est peu surprenant.

Dans les mêmes travaux parlementaires de la loi relative à la criminalité informatique, l'on retrouve la définition suivante concernant les « données » au sens de la loi : « *les représentations de l'information pouvant être stockées, traitées et*

---

* Attention: Le texte publié constitue la dernière version originale du rapport national envoyé par l'auteur, sans révision éditoriale de la part de la Revue.

* Dr. Daniel De Wolf. Maître de conférence. Vrije Universiteit Brussel (Université de Bruxelles/ University of Brussels). Faculté de Droit et de Criminologie, Unité de droit pénal. Avocat au Barreau de Bruxelles.

1 *Doc. Parl.,* Chambre 1999-2000, n° 50-0213/001 et 50-0214/001, 12.

2 Voir par exemple P. Van Linthout en J. Kerkhofs, « Cybercriminaliteit doorgelicht », (2010), 199; Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 393; comparez Ch. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *RDPC* 2001, 622-623.

3 O. Leroux, « Criminalité informatique », dans H.D. Bosly et Ch. De Valkeneer (ed.), *Les infractions contre les biens,* Bruxelles, 2008, 384-385 et 414.

4 Ch. Meunier, l.c., (2001), (2001), 623; O. Leroux, *o.c.,* (2008), 385.

5 Art. 1.a. Convention sur la cybercriminalité du 23 novembre 2001, Loi portant assentiment du 3 août 2012, entrée en vigueur le 1 décembre 2012.

6 Ch. Meunier, l.c., (2001), 623.

7 O. Leroux, *o.c.,* (2008), 414.

transmises par le biais d'un système informatique » [8] . La Convention sur la cybercriminalité définit les « données informatiques » comme « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction* ». Ces définitions ne sont pas ou peu utilisées en procédure pénale.

Dans la loi du 13 juin 2005 relative aux communications électroniques on retrouve de multiples définitions, ce qui n'est pas surprenant puisque cette loi est la transposition de directives Européennes. Pas moins de 72 termes y sont définis. On peut y lire les définitions suivantes :

- réseau de communications électroniques : les systèmes de transmission, et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes avec commutation de circuits ou de paquets, y compris l'Internet et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de radiodiffusion et de télévision;

- fourniture d'un réseau de communications électroniques : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques;

- service de communications électroniques : le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision;

- donnée de trafic : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication;

- donnée de localisation : toute donnée traitée dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public;

- service à données de trafic : un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

- service à données de localisation : un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;

- réseau public de communications électroniques : un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau;

- opérateur : toute personne ayant introduit une notification conformément à l'article 9 (La fourniture ou revente en nom propre et pour son propre compte de services ou de réseaux de communications électroniques ne peut débuter qu'après une notification);

On doit cependant constater qu'à l'exception de l'opérateur et du fournisseur de services – la loi ne parle que de fourniture d'un réseau de communications électroniques - ces termes sont peu ou pas utilisés en procédure pénale ou il n'y est pas fait référence. Le terme « *donnée de trafic »* n'est par exemple pas utilisé dans la pratique de la procédure pénale.

L'article 1.c. et d. de la Convention sur la cybercriminalité y ajoute :

- l'expression " fournisseur de services " désigne :

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

- l'expression " données relatives au trafic " désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Dans la loi relative à la procédure par voie électronique l'on ne retrouve aucune définition des expressions « voie électronique » ou « caractère électronique ». Les travaux parlementaires restent muets sur ce point. Il semble que la signification est tellement évidente qu'il ne fallait pas la définir.

[8] *Doc. Parl.,* Chambre 1999-2000, n° 50-0213/001 et 50-0214/001, 12.

Dans la loi du 31 mai 2007 réglant l'installation et l'utilisation de caméras de surveillance une caméra de surveillance est définie comme : « *tout système d'observation fixe ou mobile dont le but est de prévenir, de constater ou de déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou de maintenir l'ordre public, et qui, à cet effet, collecte, traite ou sauvegarde des images; est réputée mobile, la caméra de surveillance qui est déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions* » (article 2).

La jurisprudence ne s'est pas exprimée sur le « concept des TIC », ce qui serait assez difficile. Nous verrons dans la partie D du rapport que la jurisprudence et surtout la doctrine s'est exprimée, sans pour autant le placer dans un cadre plus large de l'utilisation des TIC dans la procédure pénale, sur la signification de termes comme « transmission », « données », « système informatique », « observation », « caméra », etc. . Nous y référons.

L'on pourra conclure que bien qu'il n'existe pas ou peu de débat, le législateur a d'un côté considéré que certains termes sont tellement clairs qu'ils ne devaient pas être définis et d'autre part que vu l'évolution des techniques il ne fallait pas les définir. Une définition large et neutre fut appliquée - *tout système permettant le stockage, le traitement ou la transmission de données* -, ce qui permet de couvrir toute forme de TIC. Cependant, dans le cadre des mesures de recherches, la jurisprudence et la doctrine ont été amenées à définir certain termes.

(2) Y a-t-il des institutions spécifiques et/ou des groupes de travail impliqués dans la mise en œuvre des TIC au sein du système de justice pénale?

Au *niveau de la police,* l'on peut signaler l'existence d'un ou plusieurs services qui se consacrent à la cybercriminalité, la criminalité informatique et la délinquance informatisée (pédophilie, fraudes). Au niveau de la police fédérale, au niveau national, il existe la « Federal Computer Crime Unit (FCCU) ». Ce service de police spécialisé est incorporé au sein de la direction de la lutte contre la criminalité financière Ecofin, elle-même faisant partie de la Direction générale de la police judiciaire.

Au niveau des arrondissements judicaires, les **CCU régionaux (RCCU)** apportent un appui aux autres services au sein de services déconcentrés sous l'autorité du directeur judiciaire.

La finalité des services est décrite comme suit :

- Une assistance efficiente et opportune aux services de police dans le cadre de dossiers judiciaires afin de détecter, de conserver et de fournir aux enquêteurs sous forme lisible toutes les informations pertinentes dans les environnements ICT.
- Une lutte efficace contre toute forme de criminalité ICT au travers de la spécialisation, de la prévention, des interventions proactives, pour que l'impact négatif de cette forme de criminalité sur la vie sociale soit au final le plus limité possible. Les services fournis doivent être d'une qualité procédurale et technique irréprochable et couvrir de la même façon le territoire belge dans son entièreté[9].

La FCCU est composée de 4 sections [10]:

*La section **« Gestion »** est responsable pour conseiller dans toute matière dans la recherche en milieu ICT, pour la détermination des méthodes et standards, pour l'achat de matériel spécifique et pour la formation.*

*La section **« Opérations »** :*

- *Fournit un appui spécialisé aux services de recherche opérationnels centraux et aux Regional Computer Crime Units (RCCU) pour les recherches dans les systèmes ICT dans le cadre de la criminalité « traditionnelle ».*
- *Assiste les RCCU dans le traitement des dossiers de la criminalité informatique et les fraudes aux télécommunications.*

*La section **« Recherches sur Internet »** traite en tant que Point de Contact Central pour la criminalité sur Internet les dénonciations qui sont reçues via www.ecops.be. La section collabore étroitement avec les autres services centraux de la Police judiciaire fédérale.*

*La section **« Intelligence** » s'occupe de la gestion de l'information et de la création d'images concernant la criminalité informatique.*

Les activités des RCCU portent sur l'analyse des TIC du type ordinateur ou autres supports de données et petits réseaux. Ceci dans une finalité de police judiciaire, c'est-à-dire la recherche des faits et l'identification des auteurs. La FCCU se concentre sur les plus grands réseaux.

Nous verrons que l'utilisation de moyens techniques, comme la vidéo surveillance est réservée aux unités spécialisées de la police fédérale (voir question D 4).

[9] Voir http://www.polfed-fedpol.be/org/org_dgj_FCCU_RCCU_fr.php.
[10] Voir http://www.polfed-fedpol.be/org/org_dgj_FCCU_RCCU_fr.php.

Au niveau du parquet, certains parquets opèrent avec des magistrats de référence en la matière. Ces magistrats des différents arrondissements se réunissent régulièrement. Dans la juridiction de la Cour d'appel de Gand, toutes les affaires en matière de TIC dans le ressort sont regroupées au parquet de Dendermonde, même si les faits ne se déroulent pas dans cet arrondissement. Vu le projet de réforme des arrondissements, il semblerait que cette manière d'organiser sera vraisemblablement suivie dans tous les ressorts.

Au niveau des juges d'instruction seuls certains juges se sont spécialisés dans les affaires « TIC ». Au sein des *tribunaux et des cours* aucune spécialisation n'existe dans ce domaine.

En matière de « know how » et de « R&D », l'on pourra certainement signaler le BCCE ou *Belgian Cybercrime Centre of Excellence for training, research & education*[11]. Il 's'agit d'une coopération d'universités (KUL, FUNDP, Tilburg), d'acteurs privés (Microsoft, Atos, Febelfin, …) et des autorités judiciaires, policières (FCCU, NICC, …) et publiques (SBF Intérieur et ICT). Son objectif est de fournir de la recherche et la formation de personnes dans les secteurs public (juges, …) et privé (avocats, entreprises, citoyens) ainsi que de servir comme plateforme de coopération.

En matière d'introduction des TIC, les choses sont bien moins organisées, l'on a parfois parlé d'un certain chaos qui régnait en la matière. Un comité « Phenix » avait été mis en place afin d'accompagner l'introduction des TIC dans la procédure par une firme privée. Après l'échec cuisant du projet « Phenix », le projet d'informatisation est maintenant mené au sein du Ministère de la Justice (Service fédéral Justice). Entre autres, le projet *JustScan* est en phase de développement (voir ci-dessus et aussi la partie F).

On peut encore mentionner ici la *Commission de Modernisation de l'Ordre judiciaire*[12], instituée auprès du Service public fédéral Justice, qui est chargé de l'amélioration des processus judiciaires et administratifs[13]. Un projet d'e-group d'informations a été réalisé afin d'améliorer la circulation de l'information au sein de l'organisation judiciaire par le biais d'« e-letters »[14] et de faciliter le dialogue entre magistrats[15]. En plus, un système « Ludexnet » a été réalisé en 2010. Il s'agit d'un site portail destiné à mettre des informations et de la documentation à la disposition de tous les magistrats du siège et du personnel des cours et tribunaux[16]. Les magistrats du siège ne disposaient pas comme les magistrats du parquet d'un système de ce genre.

La commission participe au projet *JustScan*. Il s'agit d'un projet informatique qui, «*conduit dans ses aspects techniques par le service d'encadrement ICT, a pour objet de :*

- *convertir les dossiers d'affaires judiciaires actuellement sur support papier en information sur support électronique;*
- *fournir un outil de recherche (dans des dossiers volumineux par exemple) à l'usage des magistrats et des autres clients internes (personnel des greffes ou des parquets) et externes (avocats, justiciables);*
- *rendre possible la délivrance de copies des dossiers judiciaires sur support électronique (DVD),*
- *faciliter la délivrance de copies papier, et plus généralement, diminuer le nombre des tâches de manutention liées à la procédure (transfert du dossier d'une instance à l'autre, photocopies multiples en vue de la communication du dossier aux parties)* »[17].

En outre, des *KnowledgeTrees* sont mis en œuvre pour les juridictions et les magistrats. Le but est de « *mettre à la disposition des juridictions une application leur permettant, facilement et en toute sécurité, de conserver des données sans devoir installer un programme et sans se préoccuper du stockage de ces données »* et puis de *« permettre de consulter les données depuis le domicile sans qu'aucune installation de programme ne soit requise* »[18].

---

[11] http://www.b-ccentre.be.
[12] http://www.cmro-cmoj.be/fr.
[13] Loi du 20 juillet 2006 instaurant la Commission de Modernisation de l'Ordre judiciaire et le Conseil général des partenaires de l'Ordre judiciaire. La commission veille à mener une réflexion générale portant sur la modernisation de la gestion de l'Ordre judiciaire; organiser et mener une réflexion portant sur les structures des organes de gestion du pouvoir judiciaire et les fonctions judiciaires; élaborer des projets d'harmonisation, d'amélioration et de modernisation de la gestion de l'Ordre judiciaire; concevoir des projets expérimentaux en matière de gestion de l'Ordre judiciaire élaborés au niveau fédéral ou local et en soutenir le développement; accompagner les expériences de transfert de compétences aux juridictions dans le cadre d'une décentralisation administrative; apporter un soutien méthodologique à la mise en oeuvre des projets expérimentaux en matière de gestion de l'Ordre judiciaire; proposer des méthodes pour optimiser l'utilisation des moyens consacrés au fonctionnement de l'institution judiciaire; créer et animer un réseau d'échange d'informations entre l'administration centrale du Service public fédéral Justice et les chefs de corps (article 3, § 1).
[14] Voir http://www.cmro-cmoj.be/fr/realisations/communication/creation_egroupes_information.
[15] Voir http://www.cmro-cmoj.be/fr/realisations/communication.
[16] Voir http://www.cmro-cmoj.be/fr/realisations/communication/iudexnet.
[17] Voir http://www.cmro-cmoj.be/fr/realisations/outils_de_travail/justscan.
[18] Voir http://www.cmro-cmoj.be/fr/realisations/outils_de_travail/knowledgetree_juridictions et http://www.cmro-cmoj.be/fr/realisations/outils_de_travail/knowledgetree_magistrats.

3) Y a-t-il des organisations (entreprises) privées (commerciales) qui offrent des services liés aux TIC dans le système de justice pénale? Si c'est le cas, pouvez-vous donner des exemples? Quelles limites doivent être respectées?

Oui, outre les partenaires privées du BCCE cité ci-dessus, deux types d'exemples peuvent être donnés. Il y a d'une part, la participation d'organismes ou entreprises privés à l'élaboration de l'informatique au sein de la justice pénale et d'autre part la participation d'experts lors des différents stades de la procédure pénale.

Exemples. Concernant la participation d'organismes ou entreprises privés à l'élaboration de l'informatique au sein de la justice pénale, il faut constater que les services de soutien du Ministère de la Justice (Service fédéral Justice) à l'ordre judiciaire ne sont pas en mesure, du point de vue de la connaissance ou de moyens humains, d'élaborer eux-mêmes des logiciels adaptés aux traitements électroniques d'informations ou de données. D'autre part, l'on ne peut jusqu'à présent que constater l'échec – l'exemple du projet « Phenix » est le plus flagrant - des différentes entreprises qui ont répondu aux différents appels d'offres. Sans doute, est-il exagéré de prétendre que les partenaires privés seraient les seuls responsables de l'échec. En plus, les problèmes d'informatisation ne sont pas limités au domaine de la justice puisque dans d'autres services publics, l'on constate les mêmes difficultés à informatiser les processus.

Peut-être pourrait-on saisir l'opportunité de signaler ici les conditions pour réussir une informatisation de la justice. Avant d'informatiser, il faut d'abord équiper les acteurs en « hardware », c'est-à-dire être sûr que chaque magistrat dispose d'un ordinateur. Puis le processus d'informatisation peut commencer. L'erreur ici est de se concentrer sur des questions techniques. Informatiser veut dire identifier les processus dans l'organisation, définir les missions et les objectifs et ensuite avec les moyens disponibles et, en tenant compte des missions en optimalisant les processus, introduire les TIC afin d'améliorer le fonctionnement, l'efficacité et la performance de la justice. Pour réussir l'informatisation, il est nécessaire de définir les bonnes pratiques (« best practices »), ce qui contribue à l'optimalisation de la procédure et la simplification de la législation, de rassembler les différentes visions dans un visions commune, de convaincre les utilisateurs de l'utilité des systèmes et de garantir la finition des différents stades de développements.

Récemment, une plate-forme de concertation stratégique (CSO) a été créée[19]. Ce comité a élaboré une stratégie pour l'informatisation de la justice (2012-2014)[20] et un planning opérationnel.

Le but est de travailler autour de quatre « piliers » [21]:

*- le **Carrefour Justice** : un système ad hoc structuré et automatisé **pour la consultation et l'échange d'informations par voie électronique** selon le principe de la 'source authentique' ;*

*- la **plate-forme collaborative** qui doit notamment permettre une **collaboration électronique** aisée dans un dossier ;*

*- la **plate-forme de communication** qui constitue la **porte d'accès électronique** à la Justice pour d'autres acteurs de la Justice et qui peut servir de source d'information pour le monde extérieur.*

*- du **business intelligence**, le dernier volet, qui doit fournir un instrument pour le **traitement électronique et l'analyse d'informations** avec comme objectif le développement de rapports de management ainsi que l'analyse de données internes et externes.*

Le carrefour justice aura pour but de recevoir des informations (par exemple des procès-verbaux des services de police, conclusions des avocats) mais aussi d'envoyer des documents à d'autres services (par exemple pour l'exécution des peines) et de consulter certaines banques de données (par exemple registre national, registre de l'office des étrangers, etc.).

La plate-forme collaborative sera l'environnement de travail des membres et collaborateurs de l'ordre judiciaire. Cette plate-forme pourra contenir des documents, mais aussi une liste d'objets concernant des dossiers (scellés par exemples). Le but est également d'archiver des dossiers. La plate-forme de communication permet l'accès (comme un intranet) à la plate-forme collaborative. Finalement, le business intelligence sert à collecter des informations en matière de fonctionnement et de gestion afin d'effectuer des choix (management)[22].

Tous ces projets sont le fruit d'une collaboration entre différents organes publics et le secteur privé, principalement des entreprises de développements de logiciels et de solutions en matière de TIC.

Concernant la participation d'experts lors des différents stades de la procédure pénale, il faut signaler qu'au niveau de la procédure belge, il n'est pas obligatoire qu'un expert soit un organisme public. Des personnes privées peuvent donc être nommées comme « experts » par la justice, ce qui n'empêche pas de considérer l'expertise comme un service public[23]. En plus, les parties peuvent désigner leur « conseil technique ». En matière de TIC, il est possible que des experts en informatique livrent leur opinion sur l'analyse de données ou répondent à une question de manipulation d'un élément de

[19] http://justice.belgium.be/fr/ordre_judiciaire/reforme_justice/nouvelles/news_2012-05-14. jsp

[20] http://justice.belgium.be/fr/binaries/Lignes%20de%20force%20strat%C3%A9giques%20pour%20l%27informatisation%20de %20l%27OJ%202012-2014 tcm421-175726.pdf

[21] *Ibid.*, p. 16-17.

[22] *Ibid.*, p. 17-28.

[23] H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 634 et 639.

preuve digital. Il se peut également que des experts utilisent des TIC lors de leur mission (voir ci-dessus question F.3.). Ces experts sont soit des professeurs d'université ou d'hautes écoles, soit des personnes qui à mi-temps ou à temps plein ont développé une activité commerciale d'expertises, soit encore des grandes entreprises qui disposent au sein de leur organisation d'une « *forensic* » division ou qui offrent des services d'expertises. La collaboration directe, même en dehors du cadre formel d'une expertise, entre personnes privés et le parquet et/ou la police, a été critiquée vu le coût exagéré auquel ces entreprises livrent leurs services.

Les limites. Les limites en matière de collaboration avec des organismes ou entreprises privés sont d'ordre divers, juridique, pratique, financier etc. Nous signalerons les règles de débat en droit public concernant les tâches réservées à l'Etat et les règles en matière de délégation ou de coopération (en Néerlandais « PPS ») avec des organismes privés. En outre, les règles en matière d'offres publiques règlent l'exécution de tâches par des personnes privées aux services de l'Etat. Ces sujets sont fort éloignés de notre sujet et nous ne les aborderons donc pas. Par contre, en matière d'expertise, il existe quelques règles procédurales qu'il pourrait être utile de signaler.

Il n'existe pas de règles concernant la désignation de l'expert. Dans ce domaine-là, le juge n'est soumis à aucune limite. Le juge est libre dans la désignation de la personne qu'il présume la plus indiquée pour remplir la mission[24].

L'expert ne peut pas refuser ni déléguer sa mission, ni même de sa propre initiative former un collège d'experts[25].

Sujet plus controversé[26], est celui que l'expert doit garder largement le secret au sujet de ses travaux [27]. Ce n'est que dans son rapport final que les parties pourront prendre connaissance de ses conclusions et les contester à l'audience.

L'expert ne peut pas s'installer à la place du juge. La mission dont l'expert est chargé est limitée à la collecte d'informations factuelles dont le juge aura besoin pour appliquer le droit. L'expert ne peut pas donner d'avis sur le bien-fondé de l'action intentée[28]. Les questions que l'expert doit résoudre ne peuvent coïncider avec celles du juge[29]. L'expert a pour mission de faire des constatations de faits ou de donner un avis technique, et non pas de donner des conseils sur le bien-fondé de l'action[30].

En conclusion, le droit belge permet la coopération de personnes privées avec les autorités judiciaires. Les limites imposées à cette coopération sont de natures diverses, mais une grande liberté y règne.

C. Informations et renseignements: postes d'information en construction pour l'application des lois

1. Introduction: remarques d'ordre général et sources législatives

La fonction de police guidée par l'information (*Intelligence Led Policing*) est un concept qui ne correspond à aucune règle juridique. Pour le policier, il s'agit d'une technique d'organisation policière qui est applicable aussi bien dans le domaine de la police administrative ou judicaire et qui aide la police dans l'accomplissement de tâches d'ordre répressive ainsi que préventive. La récolte et le traitement de données guident la police aux niveaux stratégique (politique criminelle), tactique (plans d'actions) et opérationnel (enquête)[31].

Pour le juriste belge, les distinctions entre police administrative et judiciaire, de répression ou de prévention restent essentielles, parce qu'elles règlent l'action et les compétences de la police (à interpréter ici au sens fonctionnel). C'est dans ce cadre-là, que nous aborderons ce chapitre. Il faudra donc différencier les réponses aux questions de recherche selon les différents cas de figures.

On peut effectivement distinguer la collecte de données ou d'informations d'ordre général afin de réunir des informations concernant des personnes ou phénomènes qui peuvent constituer un risque de sécurité (le terrain des services de renseignement et de sécurité ou de police, plus précisément au niveau stratégique et tactique), la collecte de données ou d'informations afin de prévenir la commission d'infractions ou de sanctionner des comportement illégaux ou des infractions administratives (le terrain de la police administrative) et la collecte de données ou d'informations afin de guider ou de conforter la recherche d'infractions et d'auteurs d'infractions et ceci dans un cadre réactif ou proactif (le terrain de la police judiciaire).

La première est régie par la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, par la loi 5 août 1992 sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux. La seconde est soit régie par la loi 5 août 1992 sur la fonction de police et la loi du 7 décembre 1998 organisant un

[24] Cass. 5 avril 1996, *Pas*. 1996, I, 283; 24 mai 2005, *Pas.* 2005, 1103; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert*, o.c.*, (2010), 636-637.
[25] Voir H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 639.
[26] Cour EDH Cottin c. Belgique 2 juin 2005, *RABG* 2005,184, note F. Van Volsem; voir aussi CC 30 avril 1997, *RW* 1997-98, 713 et 24 juin 1998, *RW* 1998-99, 1139, note B. De Smet en *JT* 1998, 551.
[27] Cass. 24 juin 1998, *AC* 1998, 746 en *JT* 1998, 640; 24 novembre 1998, *AC* 1998, 1068 et *RW* 1999-2000, 843, note B. De Smet; voir aussi A. Fettweis, "Le point sur le caractère contradictoire de l'expertise pénale", note sous Cass. 19 février 2003, *RDPC* 2004, 129-142
[28] Cass. 3 juin 2004, *AC* 2004, n° 303; 19 février 2010, C.08.127.F ; Corr. Nivelles 22 février 2007, *JT* 2007, 429.
[29] Cass. 13 février 2003, *AC* 2003, n° 118.
[30] Cass. 10 novembre 2006, *AC* 2006, n° 554; 7 juin 2007, *AC* 2007, n° 312.
[31] Voir http://www.polfed-fedpol.be/org/org_dgj_intelligence_fr.php.

service de police intégré (police administrative dite spéciale), soit par ou en combinaison avec les lois spéciales fédérales et décrets ou ordonnances des régions ou communautés concernant le secteur ou l'activité en question (police administrative dite spéciale, par exemple les polices sur les lois fiscales ou sociales ou du travail, la police d'urbanisme, la police de l'environnement, etc.). La troisième est principalement régie par le Code d'Instruction Criminelle, mais il existe aussi des lois spéciales fédérales (par exemple la loi du 22 mars 1999 relative à la procédure d'identification par analyse ADN en matière pénale).

En outre, des échanges d'informations peuvent sous certaines conditions avoir lieu entre ces différents services de renseignement et de sécurité, inspections administratives, autorités administratives, services de police et autorités judiciaires. Par exemple un service de renseignement et de sécurité peut obtenir des informations ou données que détiennent les autorités judiciaires ou des autorités administratives et vice versa. Une administration peut échanger des informations et des données avec le parquet et vice versa. Les conditions de ces transferts d'information sont régies par les lois citées ci-dessus. Il est très important de signaler ici que nonobstant cette possibilité d'exchange d'informations et de données, il est interdit d'utiliser des moyens spécifiques afin d'alimenter une autre procédure ou enquête d'un autre type ayant une autre finalité. Il est effectivement tentant d'utiliser les moyens plus étendus dont disposent uniquement certains services ou inspections spéciales. Les informations ou données sont alors transférées au service ou à l'autorité compétente suite à la découverte « *par hasard* » de nouveaux faits ou infractions. Ce type de problèmes se pose surtout entre la police administrative et la police judiciaire, mais est aussi envisageable dans d'autres cas de figures.

Enfin, certaines informations ou données peuvent être fournies ou doivent être fournies par des organismes privés aux autorités administratives ou judiciaires et dans une moindre mesure en sens inverse. Ici, ce sont des problèmes concernant le secret professionnel ou le devoir de confidentialité qui entrent en jeu.

Dans tous ces cas, il s'agit de traitement d'informations ou de données et donc régis par la législation en matière de protection de la vie privée, car à ce niveau-là aussi il existe des lois (principalement la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) ou dispositions générales ou spéciales (par exemple concernant les banques de données). Cette législation sera également déterminante pour la désignation des organes et mécanismes de contrôle. Alors que la loi du 8 décembre 1992 sur la vie privée instaure une Commission de la protection de la vie privée ou Commission de vie privée (en néerlandais *privacy-commissie*), différents autres organes de contrôle spéciaux existent (par exemple le Comité sectoriel de la Sécurité Sociale et de la Santé, le Comité sectoriel de la Banque-Carrefour des Entreprises, le Comité de surveillance sectoriel Phenix, etc.).

2. Questions de recherches

(1) Quelles sont les techniques liées aux TIC utilisées pour la construction de postes d'information pour les organismes d'application de la loi?

On peut constater qu'il existe plus au moins trois différentes techniques liées aux TIC qui peuvent être utilisées afin de constituer ou de traiter des informations : les banques de données, les systèmes de surveillance et la statistique. Comme indiquée ci-dessus, ces techniques peuvent être utilisées afin d'obtenir des informations et qui peuvent guider ou diriger les différents services et autorités afin d'établir un stratégie (niveau de gestion et de politique criminelle), une tactique (niveau des plans d'actions) ou une opération concrète (missions, contrôles, enquêtes). Les banques de données seront traitées dans le cadre de la question 2. Attardons-nous ici aux systèmes de surveillance et le traitement informatisé des statistiques.

- Systèmes de surveillances électroniques :

Deux types de surveillances pourront être mentionnés qui peuvent être traitées de manière électronique ou connectées à des banques de données : la vidéo-surveillance et l'imagerie satellite.

a. *Vidéo-surveillance* : Cette matière est régie par la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[32]. Nous traiterons d'abord brièvement le droit de récolte et de traitement de données par les services de police, puis l'installation de système de vidéo-surveillance par la police, pour ensuite cibler le phénomène des caméras dites « intelligentes » et leur légalité.

1. Les services de polices (police fédérale et locale) peuvent recueillir des données et donc des données recueillies par vidéo-surveillance. L'article 44/1 de la loi du 5 août 1992 sur la fonction de police stipule que dans l'exercice des missions qui leur sont confiées, les services de police peuvent recueillir et traiter des données à caractère personnel et des informations relatives notamment à des évènements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative et pour l'exécution de leurs missions de police judiciaire conformément aux articles 28bis, 28ter, 55 et 56 du Code d'instruction criminelle [33].

[32] Voir aussi A. Marut, « Bewakingscamera's », dans Postal memorialis, 2012.

[33] Il y a donc un droit ou même une obligation à s'informer et un droit de récolter des données à caractère personnels ou sur de évènements ou groupes et puis de les traiter. Voir Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 342-350; Ch. Caliman, « La gestion de l'information policière dans la loi du 7 décembre 1998 et les principes relatifs à la protection de la vie privée », RDPC 2000, 408-413.

Ces informations et données ne peuvent être communiquées qu'aux autorités visées à l'article 5, aux services de police belges ou étrangers, au Service d'Enquêtes du Comité permanent P, au Service d'Enquêtes du Comité permanent R, ainsi qu'à l'Organe de coordination pour l'analyse de la menace, à l'inspection générale de la police fédérale et de la police locale ainsi qu'aux services de renseignements et de sécurité au Comité permanent P et au Comité permanent R qui en ont besoin pour l'exécution de leurs missions. Elles peuvent également être communiquées aux organisations internationales de coopération policière à l'égard desquelles les autorités publiques ou les services de police belges ont des obligations. Le Roi détermine à quelles autres autorités publiques (même à la Poste) ces mêmes données et informations peuvent également être communiquées.

L'article 44/5 y ajoute que, lorsque dans le cadre de l'exercice de leurs missions de police administrative, les services de police acquièrent connaissance d'informations intéressant l'exercice de la police judiciaire, ils en informent sans délai ni restriction les autorités judiciaires compétentes. Lorsque dans le cadre de l'exercice de leurs missions de police judiciaire, les services de police acquièrent la connaissance d'informations intéressant l'exécution de la police administrative et qui peuvent donner lieu à des décisions de police administrative, ils en informent les autorités administratives compétentes, sauf si cela peut porter atteinte à l'exercice de l'action publique, mais sans préjudice des mesures indispensables à la protection des personnes[34].

2. La décision d'installer une ou plusieurs caméras de surveillance dans un lieu ouvert est soumise à un avis positif du conseil communal de la commune où se situe ce lieu. Le responsable du traitement appose à l'entrée du lieu ouvert, un pictogramme signalant l'existence d'une surveillance par caméra (article 5, §§ 1-3).

Le visionnage de ces images en temps réel n'est admis que sous le contrôle des services de police et dans le but de permettre aux services compétents d'intervenir immédiatement en cas d'infraction, de dommage, de nuisance ou d'atteinte à l'ordre public et de guider au mieux ces services dans leur intervention. Un arrêté royal délibéré en Conseil des ministres, dont le projet est soumis pour avis à la Commission de la protection de la vie privée, détermine les conditions auxquelles les personnes susceptibles d'être habilitées à pratiquer le visionnage doivent satisfaire. Il désigne ces personnes, qui agissent sous le contrôle des services de police.

L'enregistrement d'images n'est autorisé que dans le but de réunir la preuve de nuisances ou de faits constitutifs d'infraction ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes. Si ces images ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne peuvent permettre d'identifier un auteur, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois (article 5, § 4).

Les caméras de surveillance ne peuvent ni fournir d'images qui portent atteinte à l'intimité d'une personne, ni viser à recueillir des informations relatives aux opinions philosophiques, religieuses, politiques ou syndicales, à l'origine ethnique ou sociale, à la vie sexuelle ou à l'état de santé (article 9). Toute personne filmée a un droit d'accès aux images. Elle adresse à cet effet une demande motivée au responsable du traitement, conformément aux articles 10 et suivants de la loi du 8 décembre 1992 (article 11).

Les services de police peuvent avoir recours aux caméras de surveillance mobiles dans le cadre de grands rassemblements, tels que visés à l'article 22 de la loi du 5 août 1992 sur la fonction de police. Il s'agit exclusivement de missions non permanentes et dont la durée d'exécution est limitée. Des caméras de surveillance mobiles peuvent être utilisées dans un lieu ouvert ou dans un lieu fermé accessible au public (art. 7/1).

La décision de recourir à des caméras de surveillance mobiles dans un lieu ouvert est prise par l'officier de police administrative à qui la responsabilité opérationnelle est confiée conformément aux articles 7/1 à 7/4 de la loi du 5 août 1992 sur la fonction de police. Il en informe le bourgmestre ou les bourgmestres concernés dans les plus brefs délais. La décision de recourir aux caméras de surveillance mobiles dans un lieu fermé accessible au public est prise par le bourgmestre. Uniquement en cas d'extrême urgence, l'officier de police administrative peut décider seul de recourir à l'utilisation de caméras mobiles. Il en informe le bourgmestre concerné sur le champ. L'officier de police administrative visé aux paragraphes 1er et 2e, veille aussi à ce que l'utilisation des caméras soit ciblée et efficace et qu'elle soit conforme aux principes définis dans la loi du 8 décembre 1992. Lorsque l'officier de police administrative décide de recourir à l'utilisation de caméras mobiles, il notifie sa décision au plus tard la veille du jour dudit rassemblement à la Commission de la protection de la vie privée sauf en cas d'urgence.

Le visionnage de ces images en temps réel par les services de police n'est admis que dans le but de permettre aux services compétents d'agir préventivement et d'intervenir immédiatement en cas d'infraction, de dommage, de nuisance ou d'atteinte à l'ordre public, et de guider au mieux ces services dans leur intervention.

L'enregistrement d'images n'est autorisé que dans le but :

- de prendre des mesures préventives destinées à éviter une perturbation de l'ordre public;

- de réunir la preuve de faits constitutifs d'une infraction ou d'une atteinte à l'ordre public;

[34] Voir Ch. De Valkeneer, *o.c.,* (2006), 350-355.

- de réunir la preuve de faits constitutifs de dommages ou de nuisances;

- de rechercher et d'identifier un auteur des faits, un perturbateur de l'ordre public, des témoins ou des victimes.

Si les images ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne peuvent permettre d'identifier un auteur, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois (article 7/2). Toute utilisation cachée de caméras de surveillance est interdite (article 8).

Il peut en plus exister des règles spécifiques (article 3, al. 2, 1° loi du 21 mars 2007). Par exemple, l'Arrêté Royal du 22 février relatif à l'installation et au fonctionnement de caméras de surveillance dans les stades de football règle l'utilisation de caméras dans les stades de football. Les organisateurs doivent équiper leurs stades de caméras (art. 2). Ces caméras doivent pouvoir réaliser un plan rapproché permettant d'identifier chaque spectateur. Les caméras dirigées vers les places debout et assises doivent pouvoir réaliser un plan rapproché afin de filmer le visage des spectateurs présents dans le stade au moins au moment où ils regardent le terrain de jeu. Les caméras doivent être pourvues d'un système d'enregistrement automatique des images. L'installation doit permettre en outre l'impression immédiate des images enregistrées (articles 3-4)[35]. En cas d'infractions, les services de polices peuvent saisir les images. Les images doivent être conservées pendant une période de 6 mois (article 11). Le public est informé de la présence de caméras par un règlement d'ordre intérieur.

Des règles spécifiques existent aussi en matière de roulage, plus spécifiquement l'utilisation de caméras automatiques (loi du 4 août 1996). L'on pourra aussi équiper des drones ou des policiers de caméras. Ces utilisations ne sont pas réglées par la loi, ce qui pose problème sous l'angle de l'article 8 CEDH.

3. Les caméras « intelligentes » sont des caméras auxquelles on ajoute un système informatique afin de pouvoir stocker et traiter les images et même de les connecter avec d'autres données. Ces systèmes de vidéo-surveillances permettent de reconnaître des objets, de compter des personnes ou véhicules, de suivre des personnes ou véhicules indiquées par un opérateur, de mesurer la vitesse de personnes ou véhicules ou de constater la relative immobilité de personnes.

Récemment, des caméras intelligentes ont été introduites afin de contrôler un véhicule sur un trajet. Dans certaines villes, des caméras suivent tous les mouvements de citoyens et de véhicules 24 heures sur 24 sans aucune restriction. Certains corps de polices se sont équipés de voitures qui permettent de scanner des plaques minéralogiques de voitures et à l'aide d'un lien avec une banque de données reconnaitre les voitures volées ou signalées.

4. Pour conclure, l'on peut se demander quelle est la légalité de ce type de caméra. La lecture des dispositions qui précèdent permet de conclure que la loi du 27 mars 2007 et la loi du 8 décembre 1992 sont applicables[36]. Ceci implique que l'utilisation de caméras mobiles en dehors du cadre de l'article 7 de la loi du 27 mars 2007 est défendue. Si les règles de l'article 5 de la loi sont respectées, l'installation de caméras intelligentes est légale si la police respecte les conditions de la loi du 8 décembre 1992 sur le traitement de données à caractère privées[37]. La question se pose cependant si ces dispositions vagues qui ne se réfèrent nullement aux caméras dites intelligentes sont une base suffisante et ceci vu l'impact considérable sur la vie privée (nombre et caractère des données). L'article 9 est clair sur ce point, que les caméras ne peuvent ni fournir d'images qui portent atteinte à l'intimité d'une personne, ni viser à recueillir des informations relatives aux opinions philosophiques, religieuses, politiques ou syndicales, à l'origine ethnique ou sociale, à la vie sexuelle ou à l'état de santé. Il est donc interdit de scanner des véhicules à l'entrée d'une ville, de les suivre, puis de constater qu'ils s'arrêtent devant le bâtiment d'un syndicat ou d'un bâtiment religieux ou philosophique et de stocker ces données dans une base de données. Par contre, il sera possible de signaler automatiquement la présence de véhicules volées ou de personnes signalées et puis de diriger des patrouilles afin d'intercepter ou interpeller ces véhicules ou personnes. L'article 44/1 et 5 de la loi sur la fonction de la police permet d'utiliser ces informations pour les fonctions de police administratives ou judiciaires et de transmettre ces données à un nombre important des services et autorités publiques.

L'introduction des TIC dans ce domaine a créée des possibilités énormes en matière de récolte d'informations, mais ceci donne lieu à d'importantes questions juridiques et non-juridiques. Plus de recherches devraient s'y attarder.

- *Images satellites* :

Les autorités régionales dans le cadre de leur compétences en matière d'urbanisme ou d'environnement pourraient par le biais de photos aériennes ou provenant de satellites civils dresser un inventaire des bâtiments existant et comparer de

[35] Afin de garantir la qualité de l'identification et des images, les caméras doivent être réglées de façon à ce qu'il soit parfaitement possible de lire, sur les moniteurs et sur les images imprimées, un chiffre ou une lettre de 20 centimètres de hauteur et de deux centimètres de largeur, placé(e) à une hauteur de 80 centimètres au-dessus de chaque place assise et à une hauteur de 1,70 mètre au-dessus de chaque place debout ou endroit situé en dehors des tribunes et ce, quelles que soient les conditions météorologiques et de luminosité (article 4, § 3).

[36] La loi de 1992 n'est cependant pas intégralement applicable, voir Ch. De Valkeneer, *o.c.,* (2006), 348-349.

[37] Voir aussi A. Marut, *o.c.,* B193 / 30.2, qui cite la recommandation n° 04/2012 d.d. 29 février 2012 CBPL (réf. CO-AR-2011-11), « *Het gebruik van mobiele bewakingscamera's met nummerplaatherkenning met het oog op onder meer de opsporing van gestolen voertuigen, geseinde personen, enzovoort, is met andere woorden de lege lata problematisch gelet op deze recente aanpassing van de camerawet. Het gebruik van vaste bewakingscamera's met nummerplaatherkenning is volgens de camerawet daarentegen wel mogelijk (bv. aan sommige op- en afrittencomplexen of bij binnenkomst van een stad of gemeente) en is juridisch sluitend* ».

manière électronique ou manuelle celui-ci avec les registres des permis (informatisés ou pas, voir aussi ci-dessus la question 2) et les permis eux-mêmes. Certaines données de ces satellites sont même accessibles au grand public comme « Google-Earth ». Les autorités pourraient les utiliser pour récolter des informations[38]. Dans un avis du 12 juillet 2006, la Commission vie privée a rendu un avis dans la matière[39]. La Commission estime que des prises de photo par satellite de parcelles dont les propriétaires sont identifiables et ceci à des fin de constatation d'infractions en matière d'urbanisme tombe sous la loi du 8 décembre 1992. L'article 8 de cette loi stipule que les autorités compétentes ont le droit de traiter des informations judiciaires. Vu la finalité des images et le fait qu'en Flandre les infractions à la règlementation en matière d'urbanisme sont punissables pénalement, les autorités compétentes pourront utiliser les prises de vue par satellite. Cependant, dans la mesure où cette recherche serait une enquête pro active dans le sens de l'article 28bis CIC, les conditions de cet article doivent être suivies. En plus, le public (avant) et les propriétaires (après) devront en être informés.

- *Traitement informatisé des statistiques* :

Le domaine des statistiques criminelles en Belgique est bien vaste, mais surtout très désordonné et lacunaire. Le chaos y semble maître. Cette constante n'est pas sans importance, puisque la gestion (le management des ressources) ou l'élaboration de la politique criminelle est largement tributaire (*evidence based policy*) de données concernant l'ampleur des phénomènes criminels, l'efficacité du « système » pénal et l'utilisation de ressources financières, humaines et logistiques. Par exemple, depuis longtemps des statistiques sont établis concernant la survenance géographique de la délinquance. Ceci permet d'orienter des patrouilles ou de renforcer la présence policière dans certains quartiers plus que d'autres. La question qui se pose ici est si l'introduction des TCI a changé ou amélioré l'établissement des statistiques.

L'exemple d'une recherche récente en matière d'infractions aux lois de l'urbanisme que nous avons menée nous-même peut illustrer le problème. Alors qu'au niveau des autorités locales ou des services de police (locale ou fédérale) aucune statistique n'existe, les données de la Région Flamande et des parquets divergeaient énormément. Plus loin dans la « chaine pénale », les données manquaient de nouveau ou étaient très fragmentaires. Il a fallu travailler avec quelques données recueillies auprès de certains magistrats du parquet ou du siège. Bien qu'il existe des statistiques concernant les cours et tribunaux et l'exécution de peines, les infractions urbanistiques n'étaient pas répertoriées. Vu le caractère hautement lacunaire, nous avions conseillé d'améliorer l'établissement de statistiques en cette matière. Ceci est certainement anecdotique et la situation est parfois moins confuse en matière d'infractions plus générales comme les vols ou les infractions concernant les stupéfiants.

Le traitement informatisé des statistiques a cependant apporté des améliorations, mais a aussi apporté ses propres problèmes. Quelques exemples.

L'existence d'une banque de données au sein du Bureau de statistiques permet de récolter un nombre important de données concernant les enquêtes et ensuite d'effectuer des analyses sur mesure en fonction des besoins de gestion. Les possibilités de combinaison de paramètres sont très larges.

Mais tout cela a ses limites et de nombreux problèmes surgissent. Dans la recherche citée ci-dessus, nous avions constaté avec l'aide des analystes du collège des procureurs-généraux que la comparaison entre les données du parquet et de l'administration compétente était impossible vu que par exemple les traitements n'utilisaient pas la même référence temporelle. La récolte et le traitement des données au sein du parquet étaient fragilisés par le système de volontariat à envoyer les données au Bureau de statistiques et par des différences d'interprétation des différentes catégories lors de l'encodage des données matérielles dans le système informatique. Il y a certainement le problème général d'interprétation des statistiques, mais les manipulations et les calculs des analystes sont parfois fort compliqués à comprendre pour de simples juristes ou fonctionnaires ce qui peut conduire à des erreurs d'interprétations. Les données récoltées sont fortement liées au travail du parquet et sont d'ordre quantitatif ; par ailleurs, elles ne reflètent pas nécessairement des phénomènes criminels, qui sont des données d'ordre qualitatif.

On peut notamment lire dans le Plan d'action 2012-2014 de Lutte contre la traite et le trafic des êtres humains en Belgique que : « *L'arrêté Royal du 16 mai 2004 royal relatif à la lutte contre le trafic et la traite des êtres humains (M.B. 28/05/2004) devait mener à la création d'un Centre d'information et d'analyse en matière de trafic et de traite des êtres humains (CIATTEH). … Pour pouvoir effectuer des analyses pertinentes, le CIATTEH doit rassembler des informations provenant de différents services et départements et se baser sur ces dernières afin de pouvoir procéder à une analyse stratégique pertinente. … Une première tentative d'analyse a mené au constat que plusieurs problèmes empêchent d'obtenir un résultat effectif. La* ***seule possibilité*** *d'atteindre les objectifs du CIATTEH est que la législation permette d'utiliser des* ***données personnelles*** *au lieu de données anonymes* »[40].

[38] Voir P. Michielsen, « De overheid bekijkt u vanuit de lucht », *Juristenkrant* 2006, n° 134, p. 5..
[39] Avis n° 26/2006 du 12 juillet 2006 « Adviesaanvraag inzake het gebruik van satellietbeelden bij de opsporing en de vaststelling van bouwovertredingen ».
[40] P. 39-40, voir http://www.dsb-spc.be/web/index.php?option=com_content&task=view&id=55&Itemid=80& lang=french.

En guise de conclusion, on peut dire que les avantages du traitement informatisé sont l'automatisation des manipulations et calculs, l'interconnections de données et la plus grande capacité de stockage et de calcul. Mais l'introduction de l'informatique a créé de nouveaux problèmes : le besoin d'encodage manuel à la base, l'interprétation différente des catégories lors de l'encodage des données, les difficultés à traiter des données qualitatives, le manque d'interconnectibilité entre différentes banques de données, entre différents services et administrations et le besoin de données personnelles, ce qui pose problème en matière de protection de la vie privée[41].

(2) A quel type de bases de données publiques (bases de données ADN par exemple) et privées (par exemple, PNR ou des données financières telles que les données SWIFT), la loi donne-t-elle une autorisation d'accès aux agences d'exécution de la loi ?

1. Il y a d'abord les banques de données publiques qui sont accessibles à tous en donc aussi aux autorités. Signalons par exemple qu'en Flandre une banque de donnée GIS, maintenant GDI et GRB[42] rassemble les données existantes en matière d'urbanisme en Flandre. Il existe même la volonté d'améliorer l'interconnectivité des données par le projet G-scan[43].

2. Puis il y a de nombreuses banques de données et systèmes d'informations publiques gérés par des autorités judiciaires ou publiques et non-accessible au public, mais à un nombre restreint de personnes, possédant souvent une autorité publique. Deux banques de données sont plus élaborées du point de vue juridique, il s'agit de la banque de donnée nationale générale de la police et la banque de données ADN.

La banque de donnée nationale générale. Nous avons déjà signalé plus haut que les policiers ont explicitement le droit par l'article 44/1 de la loi sur la fonction de police de récolter et de traiter des informations. Ces activités tombent en plus sous le coup de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel. Les travaux de la commission d'enquête parlementaire instaurée suite à l'enlèvement et la séquestration d'enfants avaient rappelé le besoin d'une circulation d'informations entre services de polices. La loi du 7 décembre 1998 sur la police intégrée a complété les dispositifs par la création d'une banque de donnée centrale au sein de la police[44]. Ajoutons que l'intégration de la gendarmerie, avec un système de récolte d'informations assez poussé, dans une police intégrée a renforcé le besoin d'un système de collecte d'informations au niveau de la police.

La loi du 7 décembre 1998 part du principe du besoin de circulation maximale des informations. Pour cela une banque de donnée est créée au niveau fédéral, plus précisément au sein de la police fédérale, mais en coopération avec la police locale qui reste le pourvoyeur principal en information. La création d'un carrefour d'informations d'arrondissement est la pierre angulaire de ce système[45]. Les différents services et les autorités judiciaires doivent bénéficier d'un accès facile aux informations. L'introduction et l'accès aux informations judiciaires sont considérés comme trop sensibles et peuvent être restreints par le magistrat compétent[46]. Enfin un organe de contrôle, présidé par un magistrat fédéral et composé d'un policier fédéral et local et d'un expert désigné conjointement par les Ministres de la Justice et de l'Intérieur, doit veiller à la bonne gestion de la banque[47]. Cet organe ne peut pas intervenir au niveau de l'introduction des données, mais uniquement au niveau de la gestion de la banque[48].

Les Ministres de la Justice et de l'Intérieur sont respectivement pour la police judiciaire et la police administrative chacun compétents pour orienter la récolte d'informations par le biais de directives (art. 5 et 44/3 loi sur la fonction de la police)[49]. La loi a prévu la centralisation, le stockage, le traitement et l'aiguillage des informations vers les différents acteurs dans et à partir d'une banque de données (art. 44/4, al. 1 loi sur la fonction de la police)[50]. L'architecture de cette banque s'appuie sur l'idée d'une structure intégrée où toutes les informations circulent librement et sur l'idée de l'accessibilité totale pour toutes les autorités. L'on pourra bien limiter en l'accès, par exemple au moyen de systèmes de sécurité et moduler l'accès selon la sensibilité des données, mais l'on pourra aussi réaliser une interconnexion avec d'autres banques de données (par exemple des détenus)[51]. La centralisation est acquise par la règle que, sauf pour des situations particulières où une banque de données séparée peut-être instaurée, toutes les données doivent être introduites dans une seule et unique banque. En cas

---

[41] Voir les différentes contributions dans Ch. Vanneste, F. Vestini, J. Louette et B. Mine (ed.), *De Belgische strafrechtelijke statistieken ten tijde van de informatisering. Uitdagingen en perspectieven,* Gent, Academia press, 2012, 148 p.

[42] Voir « Geo-loket Vlaanderen » http://www.agiv.be/gis/diensten/geo-vlaanderen/?catid=24 et http:// ogc.beta.agiv.be/gdiviewer/?simple=true

[43] http://www.agiv.be/gis/projecten/?artid=1931.

[44] Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 341; voir aussi H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 494-495; R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, 237-240.

[45] Pour plus d'informations Ch. De Valkeneer, *o.c.,* (2006), 342 et 360.

[46] Voir Ch. De Valkeneer, *o.c.,* (2006), 342 et 359.

[47] Voir Ch. De Valkeneer, *o.c.,* (2006), 342, 357 et 359. Cet organe peut s'appuyer sur le soutien de l'inspection générale de la police.

[48] Ch. De Valkeneer, *o.c.,* (2006), 357.

[49] Voir Ch. De Valkeneer, *o.c.,* (2006), 355-356.

[50] Voir Ch. De Valkeneer, *o.c.,* (2006), 356.

[51] Voir Ch. De Valkeneer, *o.c.,* (2006), 356-357.

d'instauration d'une banque de données séparée, l'organe de contrôle doit en être averti (art. 44/7 loi sur la fonction de la police). Ceci n'empêche pas la conservation locale d'un extrait de la banque[52]. Une autorisation de l'organe de contrôle est en principe nécessaire afin de pouvoir omettre l'introduction de données, mais les Ministres compétents peuvent par une directive générale décider quelles données ne doivent pas figurer dans la banque[53]. Sauf en cas de décision d'un magistrat concernant des données judiciaires sensibles, l'introduction des données doit être immédiate. La rétention et l'omission d'introduction sont punissables sous certaines conditions (art. 41/11 loi sur la fonction de la police).

Les banques de données ADN. Au sein de l'INCC (Institut National de Criminalistique et de Criminologie) deux banques de données ont été créées afin de centraliser les données en matière de recherche de profils ADN, la banque « criminalistique » et la banque « condamnée »[54]. La loi du 22 mars 1999 relative à la procédure d'identification par analyse ADN en matière pénale règle la matière. Cette loi a été amendée par la loi du 7 novembre 2011, mais, par une technique devenue habituelle en droit belge, cette loi n'est à ce jour pas encore entrée en vigueur. Notre analyse portera sur le droit belge en vigueur.

a. La banque de données « criminalistique » contient les profils ADN de traces de cellules humaines découvertes lors d'enquêtes ainsi que certaines données personnelles et liées à l'enquête et certains liens d'identification positifs. Ces données ne peuvent être utilisées qu'aux fins d'établir un lien d'identification entre des profils ADN de traces de cellules humaines découvertes ou entre ceux-ci et des profils ADN d'échantillons prélevés sur des personnes lors d'une enquête ou d'une instruction. Le stockage d'échantillons sans lien avec des profils stockés dans la banque n'est pas autorisé à ce jour. Pour comparer un profil avec des traces d'infractions futures, il est nécessaire que la personne soit condamnée[55].

Le ministère public ou le juge d'instruction, selon le cas, peuvent, par décision motivée, ordonner à un expert attache à l'Institut national de Criminalistique et de Criminologie de comparer le profil ADN des traces de cellules découvertes ou le profil ADN de l'échantillon de cellules humaines prélevé avec les données contenues dans la banque de données. Ces seuls magistrats peuvent prendre connaissance de l'identité de la personne à laquelle se rapportent les profils ADN pertinents de la banque de données. Remarquons que le juge d'instruction devra tenir compte de sa saisine *in rem,* ce qui l'empêchera de faire comparer des traces d'autres affaires[56].

L'expert présente un rapport motivé sur l'exécution de sa mission. Dans le cas où la comparaison établit un lien positif avec d'autres profils ADN stockés dans la banque de données, il en informe d'office les magistrats compétents (article 4).

Les profils ADN et les données y relatives visés au présent article sont effacés de la banque de données ADN « Criminalistique » sur ordre du ministère public, dès lors que leur conservation dans la banque de données n'est pas ou n'est plus utile aux fins de la procédure pénale.

Les profils ADN et les données y relatives sont de toute façon effacés de la banque de données, selon le cas :

1° 30 ans après leur enregistrement dans la banque de données, pour les profils ADN qui n'ont pas été identifiés;

2° dès qu'une décision judiciaire passée en force de chose jugée est intervenue dans le dossier pour lequel le profil ADN a été obtenu, pour les profils ADN qui ont été identifiés (art. 4, § 4).

b. La banque de données « commandées » contient le profil ADN de chaque personne qui, pour avoir commis une des infractions visées à l'une des dispositions énumérées ci-dessous, a été condamnée définitivement à une peine d'emprisonnement ou à une peine plus lourde (avec ou sans sursis)[57], ainsi que de chaque personne à l'égard de laquelle une mesure d'internement a été ordonnée de manière définitive pour avoir commis une de ces infractions. Certaines données de l'enquête y sont aussi ajoutées (art. 5, § 1).

Donnent lieu à un enregistrement dans la banque de données, les infractions visées :

1° à l'article 347bis du Code pénal (prise d'otage);

2° aux articles 368 et 369 du même Code (certain cas d'enlèvement de mineurs);

---

[52] Ch. De Valkeneer, *o.c.,* (2006), 358.
[53] Ch. De Valkeneer, *o.c.,* (2006), 358.
[54] Voir Ch. De Valkeneer, *o.c.,* (2006), 440-446; J.-M. Hausman, « Tests et banques de données ADN en matière pénale: modes de régulation et de contrôle », *RDPC* 2005, 387-400; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 470-471 et 630-631; M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale,* Bruxelles, Larcier, 2006, 316-317 et 729-730; R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, 304-305; C. Meunier, **«** L'analyse génétique en procédure pénale », dans X., *Le point sur les procédures*, Commission Université-Palais (CUP), n° 38, 257-299; B. De Smet, *Vergelijkend DNA onderzoek in strafzaken*. *CABG* 2003, 53 p. ; R. Decorte, E. Jehaes et J. Cassiman, « Mogelijkheden en beperkingen van het DNA-onderzoek in het gerechtelijk onderzoek", *Vigiles* (N) 2000, 109-119; B. Renard, P. Van Renterghem et A. Leriche, « Een bespreking van de wet betreffende de identificatieprocedure via DNA-onderzoek in strafzaken", *Vigiles* (N) 2000, 120-132 et err. 2001, 40; J. Meese, « Een eerste commentaar bij de Wet van 22 maart 1999 betreffende de identificatieprocedure via DNA-onderzoek in strafzaken », *RW* 1999-00, 1041-1052.
[55] Ch. De Valkeneer, *o.c.,* (2006), 443.
[56] Voir Ch. De Valkeneer, *o.c.,* (2006), 442.
[57] Voir Ch. De Valkeneer, *o.c.,* (2006), 445.

3° aux articles 372 à 378 du même Code (attentat à la pudeur et viol);

4° aux articles 393 à 397 du même Code (meurtre, homicide volontaire et assassinat);

5° aux articles 400 et 401 du même Code (coups et blessures qualifiés;

6° à l'article 438 du même Code (cas de torture);

7° aux articles 471 à 475 du même Code (certains vols qualifiés);

8° à l'article 477sexies du même Code (certains vols de matériel nucléaire);

9° aux articles 518, 531 et 532 du même Code (certains cas d'incendie et de destruction).

Si, dans le cadre de la procédure qui a conduit à la condamnation ou à la décision d'internement, un profil ADN de l'intéressé a été dressé, ce profil ADN est enregistré dans la banque de données ADN sur ordre du ministère public. L'intéressé en est informé. Si le profil ADN de l'intéressé n'a pas été dressé, le profil sera dressé sur ordre du ministère public, si nécessaire par la force. Le ministère public désigne un expert attaché à un des laboratoires agréés par le Roi pour établir le profil ADN du condamné ou de l'interné et présenter un rapport motivé de sa mission. Le résultat est enregistré dans la banque de données.
L'expert détruit immédiatement l'échantillon des cellules prélevées. Dans le mois, il informe le ministère public que l'échantillon de cellules prélevées a été détruit (art. 5, § 2).

L'utilisation de ces données est limitée exclusivement afin de pouvoir identifier directement ou indirectement des personnes concernées par une infraction. Le ministère public ou le juge d'instruction, selon le cas, peuvent, par décision motivée, ordonner à un expert attaché à l'Institut national de Criminalistique et de Criminologie de comparer le profil ADN des traces de cellules humaines découvertes avec les données contenues dans la banque de données. Le cas échéant, seul le ministère public ou le juge d'instruction peuvent prendre connaissance de l'identité de la personne à laquelle se rapportent les profils ADN pertinents de la banque de données. L'expert présente un rapport motivé sur l'exécution de sa mission.

Les données suivantes sont également enregistrées avec les données relatives aux profils ADN pertinents de la banque de données « Criminalistique » :

1° le cas échéant, le lien positif avec d'autres profils ADN stockés dans la banque de données;

2° le cas échéant, le numéro de code attribué par le magistrat et reliant le profil ADN au nom de la personne concernée.

Si la comparaison avec d'autres profils ADN stockés dans la banque de données établit un lien positif, l'expert en informe d'office les magistrats compétents à cet égard (art. 5, §§ 3 et 4).

Les données de la banque de données ADN « Condamnés » sont effacées sur ordre du ministère public dix ans après le décès de la personne à laquelle elles se rapportent (art. 5, § 5).

L'article 6 punit quiconque qui, sans y être autorisé, aura pris sciemment connaissance des résultats de l'analyse ADN. En plus sera puni quiconque, alors qu'il y était autorisé, aura pris connaissance des résultats de l'analyse ADN, et les aura sciemment utilisés à d'autres fins qu'aux fins de la procédure pénale.

Notons enfin que l'arrêté royal du 4 février 2002 pris en exécution de la loi du 22 mars 1999 relative à la procédure d'identification par analyse ADN en matière pénale contient différentes règles concernant la gestion des banques de données et la protection de la vie privée. On y prescrit que les profils ADN sont enregistrés dans un fichier électronique qui offre les plus grandes garanties en matière de sécurité et de confidentialité du traitement envisagé. Ces garanties, ainsi que les exigences concernant la gestion des banques de données seront décrites dans un arrêté royal (articles 13 et 14). Malheureusement cet arrêté n'existe toujours pas. La Cour de Cassation a décidé que l'absence d'effectivité des normes relatives aux garanties de traitement des traces d'échantillons de cellules et aux exigences en matière de gestion des banques de données n'implique pas, en soi, l'illégalité de la preuve résultant de l'analyse d'échantillons de cellules conservées dans une banque de données ni ne prive le juge du pouvoir d'apprécier la régularité de la preuve ainsi produite[58].

Les membres du personnel de l'Institut national de Criminalistique et de Criminologie qui ont accès aux banques de données sont soumis au secret professionnel et ne peuvent pas prendre part à l'exécution des analyses ADN. Le gestionnaire responsable des banques de données ADN fixe les modalités d'accès pour chaque utilisateur des banques de données ADN en fonction des responsabilités et des tâches de celui-ci.

La structure de l'information à transférer sera déterminée dans un arrêté royal (inexistant à ce jour). Des copies électroniques des données ADN sont enregistrées régulièrement dans le seul but de pouvoir recharger ces données en cas de perte accidentelle. Chaque document ordonnant l'effacement de données des banques de données « Criminalistique » et « Condamnés » conformément aux articles 4, § 4, et 5, § 5, de la loi du 22 mars 1999 est conservé à l'Institut national de Criminalistique et de Criminologie pendant trois ans à dater de l'exécution de l'ordre. Le document mentionnant cet effacement de données est rédigé par l'Institut national de Criminalistique et de Criminologie et sera conservé pendant la période précitée (article 15).

[58] Cass. 22 septembre 2005, P.05.1266.F.

Chaque utilisateur des banques de données est désigné par un code d'identification unique. Chaque accès aux banques de données ADN « Criminalistique » et « Condamnés » et chaque enregistrement, modification ou effacement de données sont inscrits dans l'agenda électronique (article 16).

Autres banques de données publiques. On pourra encore citer les banques de données ou systèmes d'information publics suivants[59] :

- le casier policier, le casier judiciaire, le bulletin d'information communale ;
- le bulletin de recherche et d'information (également la documentation concernant les auteurs inconnus et les délinquants en fuite) ;
- les informations concernant les véhicules volés ;
- l'identité judiciaire (empreintes digitales);
- le registre central d'armes ;
- la documentation financière ;
- la documentation concernant les documents d'identité faux et falsifiés (SNDIFF); concernant le faux monnayage (OCRFM); concernant les œuvres d'art et les antiquités ;
- les informations venant de la Sureté de l'Etat, le Service général du renseignement et de la sécurité des Forces armées, de l'OCAM ;
- les systèmes d'information internationaux comme Schengen, Europol et Interpol;
- le registre national[60];
- registre de l'office des étrangers, le système d'information « *Print track »* (empreintes digitales concernant des personnes étrangères) ;
- les informations de la Cellule de traitement des informations financières (CTIF) ;
- les informations auprès des inspections (ISI, administrations fiscales et des douanes et accises, inspections sociales, économiques, etc.) ;
- registre des véhicules inscrits (DIV) ;
- les données d'enregistrement de voyageurs auprès des fournisseurs d'hébergements[61].

En dehors de la sphère justice-intérieur d'importantes banques de données existent ou les autorités judiciaires ou parfois administratives peuvent avoir accès. On citera ici la banque carrefour de la sécurité sociale[62] et la banque carrefour des entreprises[63].

3. *Les banques de données privées.*

Sauf accord de la personne, l'on ne saura recourir à l'utilisation de moyens coercitifs (saisie de données article 35 CIC, collecte d'informations bancaires – par exemple l'historique des transactions sur un compte- article 46quater CIC[64]) en dehors d'une enquête. En d'autres mots, les pouvoirs des autorités judiciaires sont limités par la finalité judiciaire. Même une enquête proactive a une finalité judicaire[65], ce qui exclut une exploration de données afin de former un « poste d'information » (voir aussi question 4).

Certains organismes de contrôle (contrôle des institutions et marchés financiers) ou administratives (des inspection peuvent par une loi spéciale avoir accès à des banques de données de personnes privées si cela est dans leur compétence et nécessaire à l'exercice de ce contrôle) peuvent obtenir des données. Mais là encore, leurs pouvoirs sont restreint à leur compétence en matière de police administrative. Il est interdit d'utiliser ces pouvoirs à des fins exploratrices en récoltant des informations sur un tiers lors d'un contrôle d'une personne privée.

La question se pose si des données qui ont été obtenues par les autorités compétentes lors d'une procédure pénale ou administrative, peuvent être stockées et ensuite être utilisées ultérieurement pour créer « des postes d'informations » concernant ces personnes ou des tiers. Là encore, nous pensons qu'il s'agit d'une dérive de la finalité originale. L'article 4, § 1, 2° de la loi du 8 décembre 1992 stipule que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

---

[59] Voir H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 500-504.
[60] Loi du 8 août 1983 organisant un registre national des personnes physiques.
[61] Art. 141-145 de la loi du 1er mars 2007 portant dispositions diverses.
[62] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité Sociale.
[63] Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions.
[64] Voir Ch. De Valkeneer, *o.c.,* (2006), 452-457..
[65] Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 13.

Notons que les institutions financières sont obligées de transmettre des données en cas de soupçon de blanchiment d'argent ou de comportement similaires[66].

La transmission des données de vols des passagers ou données PNR (*Passenger Name Record*) est réglée par l'arrêté royal du 11 décembre 2006 concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers. Cet arrêté est pris sur base de l'article 5 de la loi du 27 juin 1937 portant révision de la loi du 16 novembre 1919 relative à la réglementation de la navigation aérienne, qui réalise ainsi la conversion de la directive UE 2004/82/CE**.** Les transporteurs aériens transmettent à la demande du Ministre qui a l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers dans ses compétences ou de son délégué, avant la fin de l'enregistrement, les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire belge (article 3, §1). Les données à caractère personnel visées à l'article 3, § 1er, sont transmises aux autorités chargées du contrôle des personnes aux frontières extérieures, qui les utilisent pour faciliter l'exécution de ces contrôles frontaliers, dans le but de lutter plus efficacement contre l'immigration illégale. Les transporteurs recueillent et transmettent ces données par voie électronique ou, en cas d'échec, par tout autre moyen approprié. Les autorités chargées du contrôle des personnes aux frontières extérieures conservent les données dans un fichier temporaire. Une fois les passagers entrés sur le territoire, les autorités chargées du contrôle des personnes aux frontières extérieures effacent les données dans les 24 heures qui suivent la transmission, à moins que ces données ne soient nécessaires ultérieurement pour leur permettre d'exercer leurs pouvoirs légaux ou réglementaires en matière de lutte contre l'immigration illégale. Les transporteurs effacent, dans les 24 heures suivant l'arrivée du vol, les données à caractère personnel qu'ils ont recueillies et transmises aux autorités chargées du contrôle des personnes aux frontières extérieures. Les transporteurs fournissent aux passagers les informations conformément à l'article 9 de la loi du 8 décembre 1992 (article 4). Là encore, ce sont les autorités privées qui doivent transmettre les données. En cas de contrôle, les autorités administratives peuvent consulter les données, mais là nous nous trouvons de nouveau en dehors de la collecte d'informations, puisque la consultation se fait dans un but précis.

Signalons enfin qu'à la requête d'un service de renseignement ou de sécurité, selon la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris des services de police, communiquent au service de renseignement et de sécurité concerné, dans le respect de la présente loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités responsables, les informations utiles à l'exécution de ses missions. Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions (art. 14)

Conformément à l'article 3, § 4, de la loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les services de renseignement et de sécurité peuvent solliciter les informations nécessaires à l'exercice de leurs missions, y compris des données à caractère personnel, auprès de toute personne ou organisme relevant du secteur privé (article 16).

(3) Quelles techniques catégorisées comme l'exploration de données et de la recherche de correspondances de données peuvent être appliquées? Si oui, ces techniques sont utilisées pour créer les profils des auteurs potentiels ou des groupes à risque? Si c'est le cas, les services répressifs disposent-ils d'outils spéciaux mis au point pour eux?

On pourra fournir différents exemples d'applications, nous en donnerons deux :

- Il y a d'abord la technique du « datamining », l'interconnexion de données qui vont diriger des contrôles administratifs ; l'administration fiscale applique cette technique pour sélectionner les dossiers ; l'idée est que certains paramètres sont de meilleurs indicateurs de fraude que d'autres ;
- En matière d'ILP on citera au niveau opérationnel l'élaboration d'un profil du suspect (« *profiling* »), appuyé ou non par les TIC, ou au niveau stratégique l'élaboration d'une politique à partir d'analyses de suspects ou de la criminalité; ces analyses se basent sur différentes sources comme la banque de donnée nationale générale de la police, le travail sur le terrain des agents de quartier, les informations recueillies lors de contrôles dits intégrés ; l'on donnera comme exemple l'élaboration d'un plan contre les bandes itinérantes[67] ; cet approche peut résulter dans d'une enquête proactive, qui elle-même peut mener à une enquête réactive.

(4) Les mesures coercitives (par exemple l'interception des télécommunications) peuvent-elles être utilisées pour construire des postes d'information?

Non, ces mesures sont pour la plupart des pouvoirs exclusifs au juge d'instruction et qu'exceptionnellement au procureur du Roi. Dans le premier cas (l'instruction du juge d'instruction), l'utilisation dans une phase proactive est exclue, dans le second,

[66] Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.
[67] Voir http://www.polfed-fedpol.be/crim/pdf/BandesItinerantes_FR.pdf.

il est néanmoins nécessaire qu'il y ait une finalité judiciaire et que les conditions (flagrant délit, cas d'urgence, etc.) ne se prêtent pas à un but de récolte d'informations (voir partie D ci-dessus).

Les méthodes particulières de recherche par contre peuvent être appliquées lors de la phase proactive. Ceci présuppose quand même aussi une finalité judiciaire, ce qui exclut un objectif exploratoire ou de police administrative[68]. On pourra donc ici aussi l'exclure du champ d'action de la collecte d'informations.

(5) Quels sont les acteurs privés (fournisseurs d'accès internet par exemple ou entreprises de télécommunications) qui conservent ou sont obligés de conserver des renseignements pour les organismes d'application des lois?

1. Nous avons déjà défini les opérateurs et fournisseurs de services ci-dessus (voir question B.1.). Les opérateurs sont les compagnies de téléphonie, dont l'opérateur historique, qui fournissent aussi des services internet. Selon un des auteurs, les fournisseurs de services sont les fournisseurs de courriers électroniques, de forums, d'encryptage, services bancaires etc., mais non les cybercafés[69].

Par la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, tout prestataire d'un service de la société de l'information assure un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, au moins : son nom ou sa dénomination sociale, l'adresse géographique où le prestataire est établi, ses coordonnées, y compris son adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec lui, le cas échéant, le registre de commerce dans lequel il est inscrit et son numéro d'immatriculation (art. 7). Cette obligation est pénalement sanctionnée (art. 24, voir aussi l'article 22 à propos la procédure d'avertissement et la mise en conformité).

2. Le problème de la conservation tient au fait que la conservation de données se faisait dans un but de facturation. Après le règlement de la facture, les opérateurs ou fournisseurs ne gardaient pas les données. Avec l'apparition des forfaits pour une connection internet, les opérateurs et fournisseurs ne gardaient plus les données concernant le moment et la durée de la connection[70]. Pour remédier à ce problème et en exécution de la législation européenne, la Belgique a introduit une obligation de conservation par la loi du 28 novembre 2000. La loi du 13 juin 2005 a modifié la formulation des dispositions.

L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques stipule actuellement que par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du Ministre de l'intérieur et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut. Les opérateurs font en sorte que les données soient accessibles de manière illimitée de Belgique.

La loi soumet l'obligation de conservation à une condition de finalité (en vue de la poursuite et la répression d'infractions pénales) et limité à des cas déterminés par un arrêté d'exécution[71]. Une durée de conservation d'au minimum 12 mois est stipulé, ce qui parait nécessaire du point de vue pratique des enquêtes pénales où la découverte des faits n'interviendrait que beaucoup de temps après ceux-ci[72].

A ce jour, aucun arrêté d'exécution n'a été pris.

(6) Quels sont les acteurs privés qui peuvent ou doivent fournir des informations aux organismes d'application de la loi?

On touche ici à un domaine aussi vaste que le droit même. Des entreprises doivent déposer leurs comptes annuels à la Banque Nationale, chaque personne qui veut développer une activité de prestations de services doit s'inscrire auprès du carrefour des entreprises, les employeurs doivent fournir un nombre important de données concernant leur employés (système DIMONA), les agriculteurs doivent remplir d'innombrables formulaires concernant leurs activités agricoles et concernant le traitement du fumier, les banques et un nombre croissant de personnes privées doivent informer la cellule de traitement des informations financières (CTIF), etc. Les autorités administratives et judiciaires peuvent puiser dans ces (banques de) données (voir ci-dessus la question 2 pour les données « PNR » ou les informations bancaires). Le manque à

[68] Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 13.
[69] Ch. Meunier, l.c., (2001), 657.
[70] Ch. Meunier, l.c., (2001), 654.
[71] Ch. Meunier, l.c., (2001), 655-656.
[72] Ch. Meunier, l.c., (2001), 657.

l'obligation de fournir des informations est très souvent pénalement ou administrativement puni. Signalons que ceci pose des problèmes concernant le droit de ne pas devoir s'incriminer compris dans l'article 6.1. CEDH.

(7) Y a-t-il un contrôle judiciaire sur les postes d'information en construction?

Oui, mais les mécanismes dépendront des matières et le contrôle n'est pas d'ordre pénal, mais civil ou administratif. Un exemple cependant.

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel dispose qu'une Commission de la protection de la vie privée est institué auprès de la Chambre des représentants (art. 23). Sans préjudice de toute action devant les tribunaux et sauf si la loi en dispose autrement, la Commission examine les plaintes signées et datées qui lui sont adressées. Ces plaintes peuvent avoir trait à sa mission de protection de la vie privée à l'égard des traitements de données à caractère personnel ou à d'autres missions qui lui sont confiées par la loi. Si la plainte est recevable, la Commission accomplit toute mission de médiation qu'elle juge utile. En cas de conciliation des parties, fondée sur le respect de la vie privée, elle dresse un procès-verbal dans lequel la solution retenue est explicitée. En l'absence de conciliation, la Commission émet un avis sur le caractère fondé de la plainte. Son avis peut être accompagné de recommandations à l'intention du responsable du traitement. Les décisions, avis et recommandations de la Commission sont motivés. Une copie de la décision, de l'avis des recommandations est adressée au Ministre de la Justice (art. 31). L'article 31 est par exemple applicable au traitement de données personnelles par les services de police[73]. La loi institue au sein de la Commission des comités sectoriels compétents pour instruire et statuer sur des demandes relatives au traitement ou à la communication de données faisant l'objet de législations particulières, dans les limites déterminées par celle-ci (art. 31bis). Chacun peut aussi se tourner vers le Tribunal de première instance et si nécessaire même en référée.

Différentes infractions à la loi du 8 décembre 1992 sont punies pénalement (art. 39). Dans ce cas, le contrôle est exercé par le juge pénal, mais il s'agit qu'un contrôle indirect. En condamnant du chef d'une infraction à l'article 39, le juge peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou ordonner l'effacement de ces données. La confiscation ou l'effacement peuvent être ordonnés même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné. L'article 8, § 1er, de la loi du 29 juin 1964 concernant la suspension, le sursis et la probation n'est pas applicable à la confiscation ni à l'effacement ordonnés conformément aux alinéas 1er et 2e. Les objets confisqués doivent être détruits lorsque la décision est passée en force de chose jugée (art. 41, § 1).

Le tribunal peut, lorsqu'il condamne du chef d'une infraction à l'article 39, interdire de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel (art. 41, § 2). Toute infraction à l'interdiction édictée par le § 2 est punie d'un emprisonnement de trois mois à deux ans et d'une amende de cent francs à cent mille francs (à lire comme euros en augmentant avec les décimes additionnels) ou d'une de ces peines seulement (art. 41, § 3).

D. Les TIC dans l'enquête criminelle

(1) Les organismes d'application de la loi peuvent-ils procéder à des interceptions en temps réel des a) données d'e-trafic; b) données de contenu?

a) L'interception en temps réel des données d'e-trafic

Oui, il est possible d'intercepter les données dites dynamiques en temps réel.

1. *Objet.* Par données dynamiques on peut entendre les données qui ont trait à une certaine période dans le temps (par exemple l'utilisation d'une adresse IP dans un certain laps de temps), alors que les données statiques ont trait à des données ponctuelles et limitées dans le temps (par exemple l'identité d'un abonné correspondant à l'octroi d'une adresse IP à un certain moment précis)[74]. Le droit belge, plus spécialement l'article 88bis du Code d'Instruction Criminelle (CIC), permet la recherche et la localisation des télécommunications. Ceci veut dire la recherche de personnes qui communiquent entre eux, quand et où ces communications ont eu lieu[75]. En d'autres mots, le moment, la durée, la localisation et les correspondants[76]. La loi permet de requérir ces données auprès des opérateurs et fournisseurs de services internet[77]. En pratique, l'on peut ainsi obtenir les données concernant le trafic GSM ou internet, la localisation d'un GSM à partir d'une antenne, les communications passant par une antenne[78], la géolocalisation d'une voiture (volée) si cette voiture est équipée

[73] Voir Ch. De Valkeneer, *o.c.,* (2006), 349.
[74] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 191, note 3.
[75] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
[76] Ch. De Valkeneer, *Manuel de l'enquête pénale,* Bruxelles, Larcier, 2006, 319.
[77] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
[78] Voir aussi Th. Freyne, « Knelpunten en recente evoluties betreffende de telecommunicatiemaatregelen in het strafrechtelijk vooronderzoek », dans X., *Liber amicorum Alain De Nauw*, Brugge, Die Keure, 2011, 302.

d'un système spécial de transmission de données GPS vers une centrale, etc.[79]. Les données concernant le trafic internet sont par exemple l'adresse IP [80], les adresses e-mail utilisées, les sites « web » visités[81] ou inversement les utilisateurs qui ont visités un site déterminé[82], les serveurs connectés (FTP-servers), l'utilisation de ou la connection (« logins ») à des sites privées (« online, web-based ou ISP-based e-mail », « file sharing », « peer-to-peer », « torrents », etc.), l'historique des connections (boîtes de messages éléctroniques [83], « blogs », forums, médias sociaux, etc.)[84]. Si nécessaire, le juge d'instruction peut par la suite ou simultanément combiner une demande au sens de l'article 88bis CIC avec une demande au sens de l'article 46bis du CIC afin d'obtenir l'identité des correspondants[85]. Plus délicates sont des données du type de « noms électroniques » (« ID » ou « username ») et les adresses e-mails qui y sont connectées (médias sociaux, « webmails », « file-sharing »,…), les fichiers consultés ou même les données téléchargées (download). Ces données doivent probablement être considérées comme étant des données de contenu[86] ou même l'objet d'une identification et ne peuvent alors pas être obtenus au moyen d'une demande visée par l'article 88bis du CIC. Ceci est certainement vrai pour les messages privés envoyés ou écrits (« blog », « forum » « social media », …). Plus difficile encore est de délimiter la mesure d'identification (art. 46bis CIC) et la recherche de communications (art. 88bis CIC), ce qui pose des problèmes concernant l'identification d'adresses IP dynamiques (voir ci-dessous point 3). Signalons aussi que les données d'ordre financier (payements en ligne, utilisation de carte de crédit) ne peuvent être obtenues par l'article 88bis du CIC, mais peuvent faire l'objet d'une mesure distincte visée par l'article 46 quater CIC. Nous nous limiterons ici au repérage de communications « belges » et par le biais d'opérateurs et fournisseurs belges[87].

2. *Règlementation.* L'article 88bis a été inséré en 1991 afin de règlementer le repérage de communications téléphoniques[88]. Par la loi du 10 juin 1998 l'article fut élargi à toutes formes de télécommunications, dont les TIC[89]. L'article 88bis, § 1, al. 1 du Code d'Instruction Criminelle stipule que lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaires à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication, soit au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, soit à la localisation

[79] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192; voir aussi B. De Smet, "Registratie en lokalisatie van telecommunicatie", *Comm. strafrecht en strafvordering*, Antwerpen, Kluwer, 2008, 7-12.

[80] M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale,* Bruxelles, Larcier, 2006, 482.

[81] Ch. Meunier, l.c., (2001), 653; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 651.

[82] H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 651.

[83] H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 651.

[84] Voir Larry E. Daniel and Lars E. Daniel, *Digital forensics for legal professionals,* Syngress-Elsevier, Waltham, MA, USA, 2012, 139-143 et 156.

[85] Ch. Meunier, l.c., (2001), 653.

[86] F. Deruyck, « De wet van 11 februari 1991 tot invoeging van een artikel 88bis in het Wetboek van Strafvordering betreffende het opsporen van telefonische mededelingen », *RW* 1991-92, 10.

[87] Sur la question de l'applicabilité sur des opérateurs et fournisseurs étrangers voir Th. Freyne, *o.c.,* (2011), 295-297; P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 191; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 650; O. Leroux, « *Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation », JT* 2012, 839-843; P. De Hert en G. Boullet, « Yahoo! moet meewerken met Belgische procureur », *Juristenkrant* 2012, n° 253, 8 ; L. Kerzman « L'affaire Yahoo! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46bis du Code d'instruction criminelle? », *RDTI* 2011, 116-123 ; N. Vandezande, « Yahoo! als operator of verstrekker », *AM* 2011, 220-223 ; S. Kang, «Yahoo!'s Legal Battle in France and in the USA, LIEI 2002, afl. 2, 195-203 ; E. De Busser, « Yahoo weigert IP-adressen door te spelen aan Belgisch gerecht », *Juristenkrant* 2009, afl. 186, 3 ; P. Van Linthout, « Yahoo is geen verstrekker van elektronische communicatiedienst », *Juristenkrant* 2010, afl. 216, 4-5 en err. Juristenkrant 2010, afl. 217, 9 ; K. Deschepper, « Identificatie van de gebruiker van een telecommunicatiemiddel. Medewerking in een virtuele context? Ya! Hoo echter afdwingen? », *AM* 2012, afl. 2-3, 239-243 ; P. Van Linthout, « Webmailproviders en de wettelijke medewerkingsplicht in de zin van artikel 46bis Sv. », *T.Strafr.* 2011, 136-137.

[88] Voir F. Deruyck, "De wet van 11 februari 1991 tot invoeging van een artikel 88bis in het Wetboek van Strafvordering betreffende het opsporen van telefonische mededelingen", *RW* 1991-92, 10-15; voir aussi H.D. Bosly et D. Vandermeersch, "La loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », *RDPC* 1995, 301-343; L. Huybrechts, "Het gerechtelijk afluisteren in het Belgisch recht na de nieuwe afluisterwet", *Panopticon,* 1995, 41-85; Th. Freyne, « De bewaking van privécommunicatie en –telecommunicatie in strafonderzoeken : een stand van zaken », *T. Strafr.* 2008, 165-182.

[89] Voir A. Sadzot, « Les écoutes, la prise de connaissance et l'enregistrement des (télé)communications privées après la loi du 10 juin 1998 », dans CUP, *Formation permanente*, vol. 38, *Les points sur les procédures*, 2000, 223-256; D. Vandermeersch, « Les modifications en matière de repérage et d'écoute de (télé)communications introduites par la loi du 10 juin 1998 », *RDPC* 1998, 1061-1074 ; J. Meese, « De Wet van 10 juni 1998 tot wijziging van de Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie », in X., *Recente Wetgeving*, Gent, Mys & Breesch, 1999, 164-166.

de l'origine ou de la destination de télécommunications. Le juge indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi (art. 88bis, § 1, al. 3 CIC).

3. *Autorité compétente.* Il s'agit en fait d'un pouvoir uniquement attribué au juge d'instruction ; ni le parquet, ni les services de polices n'ont ici en principe des pouvoirs. L'intervention d'un juge d'instruction suppose l'ouverture d'une instruction (l'article 55 CIC) ou d'une mini-instruction (l'article 28septies)[90]. La mini-instruction implique que le procureur du Roi requiert du juge d'instruction l'accomplissement d'un acte d'instruction pour lequel seul le juge d'instruction est compétent. Après l'exécution de l'acte d'instruction accompli par le juge d'instruction, celui-ci décide s'il renvoie le dossier au procureur du Roi qui est responsable de la poursuite de l'information ou si, au contraire, il continue lui-même l'enquête. L'intervention nécessaire d'un juge d'instruction exclut l'application de la mesure lors d'une enquête proactive[91]. Celle-ci n'est pas possible dans le cadre d'une instruction.

Cependant l'article 88bis, § 1, al. 5 et 6 CIC prévoit trois exceptions à cette règle: deux cas de flagrants délits concernant des infractions graves ou le cas d'harcèlement téléphonique à la demande de la victime. En cas de flagrant délit, le procureur du Roi peut premièrement ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4 CIC, c'est-à-dire les infractions pour lesquelles une mesure d'écoute est possible (voir infra question D.1.b). Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction. Selon certains auteurs le texte de la loi doit être compris dans ce sens qu'il ne s'agit pas d'un contrôle a posteriori par le juge d'instruction pour la période révolue, mais d'une délivrance d'autorisation pour la période après les premières vingt-quatre heures[92]. Deuxièmement, s'il s'agit toutefois de l'infraction visée à l'article 347bis (prise d'otages) ou 470 (l'extorsion) du Code pénal, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction soit nécessaire. Troisièmement, le procureur du Roi peut ordonner la mesure si le plaignant la sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques (harcèlement téléphonique)[93].

Soulignons aussi que l'article 46 du CIC permet au juge d'instruction et au magistrat du parquet de requérir l'identification d'un utilisateur d'un service de télécommunication ou d'internet[94]. Dans ce cas, il s'agit des données dites statiques, ce qui exclut la recherche en temps réel. Cet article est dans la pratique fort utilisé, non seulement parce que l'intervention d'un juge d'instruction n'est pas nécessaire, mais surtout par ce qu'il permet l'identification à partir d'une adresse IP, d'une adresse e-mail, d'un numéro de téléphone, d'un numéro IMEI, d'une carte SIM retrouvée dans un GSM[95]. Certains auteurs sont d'avis que l'identification des adresses IP pendant un laps de temps (donc dynamique et non statique) « s'assimile » à un repérage de communications et nécessite l'ordonnance d'un juge d'instruction[96]. D'autres auteurs prétendent que le schéma de la carte de couverture d'une antenne pour le réseau de GSM (en néerlandais « dekkingsplan »), peut même être obtenue par simple demande (par le biais de la recherche d'infractions prévu par l'article 8 du CIC) sans que l'on doive recourir aux articles 46 ou 88bis du CIC[97]. Les autorités judicaires peuvent aussi utiliser leurs pouvoirs de recherches « normaux » et peuvent par exemple saisir la facture d'un opérateur ou fournisseur de services où certaines données seront mentionnées[98].

En outre, la recherche des données dites dynamiques prévu par l'article 88bis du CIC est possible en temps réel, mais la jurisprudence estime que la demande peut aussi concerner des données dynamiques pour une période révolue. Dans ce cas, l'ordonnance du juge ne doit pas être motivée[99]. Cependant, la mesure reste un pouvoir exclusivement attribué au juge

---

[90] Ch. De Valkeneer, *o.c.,* (2006), 321.
[91] Ch. De Valkeneer, *o.c.,* (2006), 320; autrement B. De Smet, *o.c.,* (2008), n°. 64.
[92] Ch. De Valkeneer, *o.c.,* (2006), 322, note 680.
[93] Les pouvoirs du procureur du Roi ont souffert entre 2005 et 2008 d'un imbroglio législatif, voir Th. Freyne, *o.c.,* (2011), 304-305; M. Nihoul en C. Visart de Bocarmé, « Le risque accru de légiférer par référence au droit pénal : un exemple récent en matière d'écoutes téléphoniques », *JT* 21002, 318-320; B. Mabilde, « Alleen onderzoeksrechter kan nog elektronische belagers opsporen », *Juristenkrant* 2007, n° 154, 6; N. Banneux et L. Kezelmann, « Le mal nommé 'harcèlement téléphonique': chronique des tribulations législatives d'une infraction moderne », *RTDI* 2009, n° 34, p. 29-45.
[94] Voir P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 191; Ch. De Valkeneer, *o.c.,* (2006), 324; B. De Smet, *o.c.,* (2008), n°. 45.
[95] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 191.
[96] O. Leroux, « *Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation », JT* 2012, (839), 842.
[97] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
[98] Ch. De Valkeneer, *o.c.,* (2006), 321; B. De Smet, *o.c.,* (2008), n° 35; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 651. Mais il est vrai que les autres moyens de recherche comme une perquisition ne suffisent pas à tout repérage des communications (voir B. De Smet, *o.c.,* (2008), n° 6).
[99] Cass. 16 avril 2003, *Pas.* 2003, n° 258 et *RDPC* 2003, 1183; 21 avril 2004, *Pas.* 2004, n° 211, *JT* 2004, 820, obs. L. Kennes et *JLMB* 2004, 1369; 19 janvier 2005, *Pas.* 2005, n° 37, avec le conclusions de l'avocat-général Loop, *JT* 2005, 289, *RDPC* 2005, 819, obs. X, « Le ministère public et le repérage téléphonique », *JLMB* 2005, 1405 et Vigiles 2005, 97, note S. Vandromme; voir aussi Cass. 23 juin 1999, *Pas.* 1999, I, n° 392, p. 975.

d'instruction[100]. Dans la mesure où la recherche pour une période révolue ne peut être basée sur l'article 88bis CIC et que l'on doit se contenter d'articles d'ordre général, l'on peut se demander si cela correspond à l'exigence de l'égalité ordonnée par l'article le 8 CEDH[101]. L'article 88bis permet donc aussi bien d'obtenir les données d'appels pendant la durée où des échanges d'e-mails ont eu lieu, que la liste des adresses IP d'ordinateurs s'étant connectés sur le net (appelé « logs » ou « log-books ») [102]. Ici il n'y a pas de limitations dans le temps, mais en pratique on devra se limiter à 6 mois puisque les opérateurs et fournisseurs ne conservent les données que pendant une période de 6 mois [103].

Une discussion similaire est née concernant la localisation d'appareils mobiles (GSM). La jurisprudence avait dans un premier temps considéré que la localisation d'un téléphone mobile (GSM) avec l'aide de l'Institut belge des services postaux et de télécommunications n'est pas assujettie à l'article 88bis du Code CIC. Le raisonnement était qu'il n'y avait pas de communications en donc pas de localisation[104]. Par la suite, la jurisprudence a considéré que tant que l'appareil est en mode de fonctionnement, une ordonnance du juge d'instruction, visée par l'article 88bis du CIC, est nécessaire même si l'appareil ne transmet aucune communication[105]. La distinction entre celle-ci et une recherche pour une période donnée est qu'ici non seulement l'article 88bis CIC est applicable, mais qu'une ordonnance motivée du juge d'instruction est obligatoire. Par contre, certains auteurs ont, face à cette nouvelle jurisprudence, considéré qu'une ordonnance du juge d'instruction est bien requise, mais non pas au sens de l'article 88bis du CIC, mais parce qu'une simple requête sans aucune forme du juge suffit. Un article général concernant la recherche des infractions et les pouvoirs du juge d'instruction dans une instruction, l'article 56 CIC, fournirait dans ce cas une base légale suffisante au sens de l'article 8 CEDH[106].

Enfin, les données bancaires peuvent selon l'article 46quater CIC être obtenues par le procureur du Roi ou le juge d'instruction (article 56, § 1, al. 3 *juncto* 46quater CIC) s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

Vu la question, nous nous limiterons à l'article 88bis CIC concernant la recherche de données dynamiques en temps réel.

4. *Portée.* L'article 88bis CIC ne permettant pas l'interception de données de contenu[107], à cet effet une mesure d'écoute devra être ordonnée, le cas échéant simultanément avec une mesure de recherche ou de localisation prévue par l'article 88 CIC. C'est la raison pour laquelle la mesure de l'article 88 CIC est – à notre avis, relativement – peu utilisée en pratique[108].

L'article ne permet pas le contrôle discret d'une personne par le biais de ses communications, comme par exemple le suivi d'une voiture. Pour cela, les pouvoirs en matière de méthodes particulières de recherche devront être appliqués[109]. La mesure ne peut pas être appliquée dans une recherche dite proactive (voir aussi ci-dessus)[110].

Les personnes et moyens de communications ont été développé ci-dessus (point 2).

Conditions. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi (art. 88bis, § 1, al. 4 CIC). La mesure doit être nécessaire à la manifestation de la vérité (art. 88bis, § 1, al. 1 CIC).

Bien que l'article 88bis du CIC ne subordonne à ce jour[111] pas expressément la mesure à de conditions de subsidiarité ou de proportionnalité[112], la notion de nécessité à la manifestation de la vérité, qui est assurément bien large, semble quand même impliquer un certain contrôle de subsidiarité et de proportionnalité pour les besoins de l'instruction. Mais il est vrai que le juge ne devra pas vérifier si d'autres mesures seraient ou se sont relevées inefficaces[113]. La mesure n'est même pas limitée à certaines infractions, mais vu l'obligation de requérir un juge d'instruction, la mesure n'est pas possible en matière de

---

[100] Cass. 19 janvier 2005, *Pas.* 2005, n° 37, avec le conclusions de l'avocat-général Loop, *JT* 2005, 289, *RDPC* 2005, 819, note. X, « Le ministère public et le repérage téléphonique », *JLMB* 2005, 1405 et Vigiles 2005, 97, note S. Vandromme ; voir aussi B. De Smet, *o.c.,* (2008), n° 33.
[101] Ch. De Valkeneer, *o.c.,* (2006), 319.
[102] Ch. Meunier, l.c., (2001), 653.
[103] B. De Smet, *o.c.,* (2008), n° 14.
[104] Voir Cass. 10 novembre 2009, P.09.1584.F., *Pas.* 2009, 2579, *RW* 2010-11, note B. De Smet, « Opvangen van signalen van gsm-toestellen als onderzoeksdaad", *NC* 2010, 291, *RABG* 2010, 873 et RDPC 2010, 682.
[105] Cass. 24 mai 2011, P.11.0761.N, P.11.0909.N et P.11.0921.N, *Juristenkrant* 2011, n° 231, 3, obs. S. Vandromme, *T. Strafr.* 2011, 208, note F. Schuermans; voir aussi Th. Freyne, *o.c.,* (2011), 302-303.
[106] F. Schuermans, note sous Cass. 24 mai 2011, *T. Strafr.* 2011, 210.
[107] F. Deruyck, *l.c.,* (1991), 10; B. De Smet, *o.c.,* (2008), n° 3.
[108] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
[109] P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
[110] Ch. De Valkeneer, *o.c.,* (2006), 320.
[111] L'article 16 de la loi du 27 décembre 2004 prévoit que dans le futur le juge d'instruction devra également préciser le caractère proportionnel eu égard à la vie privée ainsi que le caractère subsidiaire par rapport aux autres mesures d'enquêtes. Cette disposition n'est pas entrée en vigueur.
[112] Ch. De Valkeneer, *o.c.,* (2006), 319.
[113] Ch. De Valkeneer, *o.c.,* (2006), 320.

contraventions sauf s'ils sont connexes à des délits ou des crimes[114]. La nécessité devra cependant découler de la motivation[115]. Le juge peut pour cela se baser sur la gravité des infractions [116].

Si les communications sont en rapport avec un dépositaire du secret professionnel, le respect de ce secret s'impose. Certains auteurs sont d'opinion que l'avis du bâtonnier ou le président du conseil de l'ordre est nécessaire[117]. Sauf pour éviter la commission d'infractions graves, la recherche concernant les sources d'informations de journalistes n'est pas autorisée[118].

Durée. Dans son ordonnance motivée le juge d'instruction précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement (art. 88bis, § 1, al. 4 CIC). Ceci veut dire que l'ordonnance autorise les recherches en temps réel pour une période de maximum deux mois. Cependant cette autorisation peut être renouvelée de façon illimitée[119]. On peut donc en théorie rechercher de manière illimitée dans le temps pour autant qu'au moins tous le deux mois une nouvelle ordonnance soit délivrée. On peut penser que les principes de subsidiarité et de proportionnalité sous-entendus dans l'article 88bis n'autorisent pas ce genre de recherche illimité dans le temps, mais limite celle-ci nécessairement au temps nécessaire à la recherche d'infractions et des auteurs.

Rapportage. Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal (art. 88bis, § 1, al 2 CIC). L'on considère qu'il suffira de mentionner dans le procès-verbal les données utiles. L'ensemble des données recueillies pourront être stockées sur un support digital qui sera conservé au greffe[120]. Si un GSM a été désactivé, il suffira que l'on en fasse mention[121].

Formalités. Sanction et preuve. Les formalités ne sont pas prescrites à peine de nullité. En cas de violations, le juge du fond ne doit pas exclure les éléments de preuves ainsi obtenus[122], sauf si cela rendait la procédure inéquitable ou entacherait la fiabilité de la preuve[123]. Il sera fort difficile pour la défense de démontrer que la fiabilité est atteinte. Il semble même que les résultats des repérages interdits dans la phase dite proactive (voir ci-dessus), ne devront pas être exclus[124]. Le manque de motivation n'aura donc en principe aucune conséquence[125] et certainement pas sur la recevabilité des poursuites[126]. La Cour de Cassation a souligné que le juge d'instruction qui fait procéder à un repérage de communications téléphoniques peut se fonder sur la gravité particulière de l'infraction pour laquelle cette mesure s'avère nécessaire[127]. Le manque de communication au procureur du Roi n'aura aucune répercussion sur la licéité de la preuve[128]. La violation du secret professionnel semble cependant conduire à l'exclusion de la preuve ainsi obtenue[129].

b) L'interception en temps réel des données de contenu

Oui, il est permis d'intercepter les données de contenu en temps réel.

1. *Objet.*

Le droit Belge, plus spécialement l'article 90ter et quater CIC, permet la prise de connaissance du contenu de communications électroniques (en néerlandais « informaticatap »). La doctrine a décrit cette mesure comme le fait « d'écouter, de prendre connaissance ou d'enregistrer pendant leur transmission et à l'aide d'un appareil quelconque des communications ou des télécommunications privées »[130]. Le terme « prendre connaissance » est bien plus large que le

---

114 Dans ce sens B. De Smet, *o.c.,* (2008), n° 3.
115 Ch. De Valkeneer, *o.c.,* (2006), 320.
116 Voir Cass. 11 octobre 2000, *Bull.* et *Pas.* 2000, n° 542 et *RDPC* 2001, 849.
117 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 650.
118 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 650; voir la loi du 7 avril 2005 et K. Lemmens, « La protection des sources journalistiques », *JT* 2005, 669-676.
119 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.
120 Ch. De Valkeneer, *o.c.,* (2006), 323.
121 Cass. 17 avril 2012, P.12.0348.N.
122 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192; B. De Smet, *o.c.,* (2008), n° 7-8.
123 Voir Cass. 14 octobre 2003, *RW* 2003-04, 67 avec les conclusions du procureur-général M. De Swaef et observations D. De Wolf, *RW* 2003-04, 1235-1239.
124 B. De Smet, *o.c.,* (2008), n°. 65.
125 Voir aussi Ch. De Valkeneer, *o.c.,* (2006), 320 et Cass. 3 mai 2005, *Pas.* 2005, n° 261 et 22 juin 2005, *Pas.* 2005, n° 364, *RDPC* 2006, 189, *JLMB* 2005, 1413 et *NC* 2008, 271; comparez cependant H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 653; R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, n° 932, p. 460.
126 Voir Cass. 15 juni 2005, *RDPC* 2005, 1117.
127 Cass. 11 octobre 2000, *Pas.* 2000, n° 542 et *RDPC* 2001, 849, avec note A. Jacobs.
128 Voir Cass. 3 mai 2005, *Pas.* 2005, n° 267.
129 B. De Smet, *Nietigheden in het strafproces,* Antwerpen, Intersentia, 2011, 63-64.
130 H.-D. Bosly et D. Vandermeersch, "La loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », *RDPC* 1995, 304; Ch. Meunier, l.c., (2001),661.

terme « écouter ». Ceci permet d'inclure la communication électronique ou digitale[131], par exemple la transmission électronique de données sous toutes ses formes notamment des images ou des messages[132]. Il peut donc s'agir de photos, vidéos[133], messages, conversations par messagerie électronique[134], e-mails, fichiers, logiciels, etc. Tous les moyens de communication tombent sous le coup, comme l'internet, la transmission par fax ou téléphone, par ligne de téléphone fixe ou mobile, etc. Cependant la mesure visée par l'article 90ter et quater CIC ne s'applique qu'aux communications en phase de transmission et non ceux qui ont été communiqués[135]. Les messages non privés ne tombent *a contrario* pas sous le coup de l'article 90ter CIC[136]. D'autres mesures permettent la recherche informatique - ce qui est en fait simplement une perquisition - et l'extension de la recherche du réseau (en néerlandais « netwerkzoeking »). La différence entre ces différentes mesures semble claire et aisée, dans la pratique la différence entre ces mesures est particulièrement difficile à tracer[137].

Une certaine doctrine considère que les données sont en transmission quand l'ordre d'envoi est lancé, mais qu'elles sont stockées en vue de l'envoi proprement dit ou que les données sont arrivées à destination, par exemple dans la boîte e-mail ISP et que les données ne « bougent » plus, mais que l'utilisateur ne les a pas encore reçues par le bais du logiciel sur son ordinateur[138]. D'autres considèrent que les messages stockés auprès d'un fournisseur de messagerie en attente d'être livrées au destinataire ne sont plus en transmission[139]. Encore d'autres émettent des réserves quant aux e-mails qui résident sur le serveur de l'ISP ou dans le « webmail », l'article 8 CEDH supposant un texte clair et précis afin de s'immiscer dans la vie privée alors que l'article 90ter du CIC est assez vague sur ce point[140]. Ne sont clairement[141] pas en transmission, les messages en phase de rédaction dans le logiciel sur un ordinateur, sur internet, dans une application de « chat », de messagerie, etc. ou l'encodage d'un message dans un téléphone mobile sans que ce message soit envoyé. Il en va de même pour les messages qui sont définitivement transmis, c'est-à-dire les messages de type e-mail reçus sur l'ordinateur de l'utilisateur par le bais d'un logiciel, la réception du message dans un « webmail » ou la réception d'un message dans une boîte vocale[142]. Dans cette optique, il semble sans importance que le destinataire du message a effectivement lu le message, pourvu que le message ait été transmis sur son ordinateur, tablette, GSM-Smartphone, dans le « webmail » ou dans la boîte vocale[143]. Une certaine jurisprudence considère que la transmission n'est pas encore terminée aussi longtemps que le destinataire n'a pas lu ces messages[144]. Ceci est peu convaincant. Mais il semble assez correct de dire que dans le cas où le message n'est pas encore arrivé sur l'ordinateur, l'utilisateur peut déjà avoir eu pris connaissance de ce message par un service de type « webmail » et que dans ce cas-là la transmission est terminée[145]. Afin d'éviter toute discussion et difficulté de preuve une certaine doctrine propose de parler de « station finale normalement indicée » (en néerlandais « geïndiceerd noodzakelijk eindstation »). Ce qui signifierait que dans le cas d'un e-mail type ISP, la transmission prend fin au moment où le message est chargé sur l'ordinateur, dans le cas d'un « webmail », au moment de l'accessibilité dans le « webmailbox ». Dans le cas d'accessibilité d'un e-mail type ISP par un webmail, ceci restera le moment où le message est chargé sur l'ordinateur[146].

Nous ne traiterons pas ici les problèmes liés à l'interception des télécommunications dans le cadre international[147].

---

131 Cass. 26 mars 2003, *Pas.* 2003, 664, *JT* 2003, 626, *RDPC* 2003, 1080, note T. Henrion et *Vigiles* 2003, 145, note S. Vandromme.
132 Voir Ch. Meunier, l.c., (2001), 661.
133 *Contra* R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, n° 941, p. 464, qui considère que la loi ne s'applique pas aux images visuelles bien que la transmission d'images par voie de communication tomberait sous le coup de la loi.
134 Chambre de mise en acc. Gand 27 septembre 2007, *T. Strafr.* 2008, 129.
135 Ch. Meunier, l.c., (2001), 661.
136 R. Verstraeten, *o.c.*, (2005), n° 942.
137 Voir Ph. Van Linthout et J. Kerkhofs, « Internetrecherche : informaticatap en netwerkzoeking, licht aan het einde van de tunnel », *T. Strafr.* 2008, 79-95.
138 Ph. Van Linthout et J. Kerkhofs, Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel, *T. Strafr*. 2008, p. 85, n° 25.
139 D. Vandermeersch, « Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs) – la procédure pénale », dans X., *Internet sous le regard du droit,* Ed. du Jeune Barreau de Bruxelles, 1997, 252-253; voir dans ce sens *Travaux Parl.* de la Chambre 1996-97, n° 1075/17, p. 10.
140 Th. Freyne, *o.c.,* (2011), 309 et 316.
141 Voir les doutes de R. Verstraeten, *o.c.*, (2005), n° 943.
142 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 86, n° 27; Th. Freyne, *o.c.,* (2011), 307; voir aussi Ch. De Valkeneer, *o.c.,* (2006), 325, note 686.
143 Ph. Van Linthout et J. Kerkhofs (*l.c.,* (2008), p. 80, n° 6) semblent par contre indiquer que dans le cas d'un webmail le message doit être lu, alors que dans le cas d'un e-mail de type ISP il suffit que le message est transmis sur l'ordinateur. Ici aussi les doutes de R. Verstraeten, *o.c.,* (2005), n° 943.
144 Corr. Leuven 4 décembre 2007, *T. Strafr.* 2008, 223, note L. Ceulemans, « De kennisname van e-mails 'tijdens de overbrenging', een verduidelijking van het telecommunicatiegeheim ».
145 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 86-87, n° 29.
146 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 87, n° 30-31.
147 Voir art. 90ter, § 6-7 CIC et Ch. De Valkeneer, *o.c.,* (2006), 335-339.

2. *Règlementation.* Les articles 90ter et quater du CIC ont été insérés en 1994 et amendés en 1998[148] et depuis ponctuellement amendés par différentes lois[149]. L'article 90ter CIC stipule que lorsque les nécessités de l'instruction l'exigent, le juge d'instruction peut, à titre exceptionnel, écouter, prendre connaissance et enregistrer, pendant leur transmission, des communications ou des télécommunications privées, s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité. La mesure de surveillance ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou de télécommunication régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut l'être également à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect[150].

Toute mesure de surveillance sur la base de l'article 90ter est préalablement autorisée par une ordonnance motivée du juge d'instruction, que celui-ci communique au procureur du Roi (article 90quater, § 1, al. 1 CIC).

3. *Autorité compétente.* Ici aussi il s'agit d'un pouvoir uniquement attribué au juge d'instruction[151], ni le parquet, ni les services de polices n'ont ici en principe des pouvoirs. La possibilité d'une mini-instruction est même exclue par la loi (l'art 28septies CIC)[152]. La mesure suppose donc toujours une instruction (l'article 55 CIC). L'intervention nécessaire d'un juge d'instruction exclut de nouveau l'application de la mesure lors d'une enquête proactive.

La loi ne permet qu'une exception. En cas de flagrant délit et tant que la situation de flagrant délit perdure, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 347bis (prise d'otages) ou 470 (extorsion) du Code pénal (art. 90ter, § 5 CIC). La confirmation par le juge d'instruction dans les 24 heures a été supprimée par la loi du 27 décembre 2012.

Quand la transmission est terminée, les autorités peuvent utiliser leurs pouvoirs de recherches « normaux ». Un e-mail (imprimé)[153] ou la casette d'un répondeur téléphonique[154] par exemple peuvent être saisis lors d'une perquisition. Un autre exemple sont les rubriques « Phonebook » et « Call Log » d'un GSM[155]. Selon le cas, il s'agira d'une saisie et donc un pouvoir du parquet et des services de polices (art. 87 et 88 CIC), d'un perquisition ou d'une recherche informatique et donc du pouvoir du juge d'instruction (voir ci-dessous question 2).

4. *Portée.* Les personnes et les moyens de communications ont déjà été indiqués ci-dessus (voir point 2). La mesure n'est de nouveau pas possible au cours de la phase dite proactive. Mais elle comporte aussi bien l'écoute par le captage des transmissions avec l'aide d'opérateurs ou de fournisseurs de services, que l'écoute directe et discrète chez l'utilisateur. En vue de permettre l'écoute, la prise de connaissance ou l'enregistrement direct de communications ou télécommunications privées à l'aide de moyens techniques, le juge d'instruction peut également à l'insu ou sans le consentement de l'occupant, du propriétaire ou de ses ayants droit, ordonner la pénétration, à tout moment, dans un domicile ou dans un lieu privé (article 90ter, § 1, al. 2 CIC). Ces moyens techniques peuvent êtres des micros-espions ou capteurs placés sur ou à l'intérieur des moyens de communications ou des micros paraboliques placés en dehors de l'endroit privé[156]. En matière de TIC, l'on peut se poser la question si des instruments ou des logiciels, voire des virus, ne pourraient pas être utilisés pour capter le contenu des communications électroniques. La loi permet de placer les moyens techniques, même pendant la nuit[157]. Pour le reste, la loi semble assimiler en tout point l'écoute directe avec l'écoute par le biais d'opérateurs ou fournisseurs de services[158]. Les tâches concernant le placement de ces moyens techniques semblent être réservées au domaine des unités

---

[148] Voir H.-D. Bosly et D. Vandermeersch, "La loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », *RDPC* 1995, 301-343; T. Herion, « Les écoutes téléphoniques », JT 1995, 205-213; L. Huybrechts, "Het gerechtelijk afluisteren in het Belgisch recht na de nieuwe afluisterwet", *Panopticon,* 1995, 41-85; A. Sadzot, « Les écoutes, la prise de connaissance et l'enregistrement des (télé)communications privées après la loi du 10 juin 1998 », dans CUP, *Formation permanente*, vol. 38, *Les points sur les procédures*, 2000, 223-256; D. Vandermeersch, « Les modifications en matière de repérage et d'écoute de (télé)communications introduites par la loi du 10 juin 1998 », *RDPC* 1998, 1061-1074 ; J. Meese, « De Wet van 10 juni 1998 tot wijziging van de Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie », in X., *Recente Wetgeving*, Gent, Mys & Breesch, 1999, 164-166.

[149] Voir Th. Freyne, « De bewaking van privécommunicatie en –telecommunicatie in strafonderzoeken: een stand van zaken », *T. Strafr.* 2008, 165-182.

[150] Pour plus de détails voir Th. Freyne, « De bewaking van privécommunicatie en –telecommunicatie in strafonderzoeken : een stand van zaken », *T. Strafr.* 2008, 170-171.

[151] R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, n° 940.

[152] Ch. De Valkeneer, *o.c.,* (2006), 327; M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006), 483.

[153] Ch. De Valkeneer, *o.c.,* (2006), 325; Th. Freyne, *o.c.,* (2011), 307.

[154] Cass. 27 octobre 1999, *Pas.* 1999, n° 559, *JT* 2000, 522 et *RDPC* 2000, 733.

[155] Cass. 31 mars 2010, P.10.0054.F.

[156] Ch. De Valkeneer, *o.c.,* (2006), 334.

[157] Ch. De Valkeneer, *o.c.,* (2006), 334.

[158] Ch. De Valkeneer, *o.c.,* (2006), 334.

spécialisées de la police fédérale, mais la loi ne le prescrit pas[159]. De toute façon, les noms des officiers de polices qui « assistent » à l'exécution de la mesure ne doivent pas figurer dans le dossier[160]. La Cour de Cassation a jugé que ne méconnaissaient pas l'inviolabilité du domicile, l'écoute, la prise de connaissance ou l'enregistrement de conversations de deux ou plusieurs personnes dans un domicile, réalisés sans introduction dans celui-ci ou à l'aide d'un moyen technique utilisé hors de celui-ci[161].

Conditions. L'on peut faire une distinction entre les conditions de fond et de forme[162]. Trois conditions de fond sont applicables[163]. *Premièrement,* la mesure est uniquement possible (proportionnalité) s'il y a des indices sérieux que les faits constituent des infractions dites graves d'une part limitativement énumérées au § 2 de l'article 90ter du CIC, y inclus les tentatives de ces infractions (§ 3) ; d'autre part, les infractions visées aux articles 322 ou 323 du Code pénal (association de malfaiteurs) peuvent également justifier une mesure de surveillance, pour autant que l'association soit formée dans le but de commettre un attentat contre les personnes ou les propriétés visées au § 2 ou de commettre le fait punissable visé à l'article 467, alinéa 1er, du Code pénal (certains vols qualifiés) (§ 4). Signalons que dans la liste du § 2 se trouve l'adhésion à une organisation criminelle qui peut être constituée dans le but de commettre des infractions punissables de plus de 3 ans d'emprisonnement (art. 324bis CP) et que la loi du 28 novembre 2000 concernant la criminalité informatique a complété cette liste des infractions[164] visées par les articles 210bis (faux en informatique), 504quater (fraude informatique), 550bis (hacking) et 550ter (sabotage informatique) du Code Pénal. Les articles 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques s'y retrouvent aussi.

Deuxièmement, la mesure ne peut être qu'ordonnée qu'à titre exceptionnel, - ce qui est juridiquement difficilement contrôlable[165] -, si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité (subsidiarité) (art. 90 ter, § 1, al. 1 et 90quater, § 1 CIC). Il n'est pas exigé d'avoir eu recours sans succès à d'autres moyens, il suffit qu'il ne soit pas raisonnablement probable que les autres moyens seront fructueux[166]. Le juge fournira une motivation *in abstracto*[167]. Satisfait à cette obligation, le juge d'instruction qui constate, dans son ordonnance, que les moyens ordinaires d'investigation seraient inopérants, notamment au regard des faits à élucider ou de la manière dont ils se commettent[168].

Troisièmement, la mesure de surveillance ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou de télécommunication régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut l'être également à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect (art. 90ter, § 1, al. 3 CIC). Cette troisième condition n'est à vrai dire pas une condition, mais indique la portée de la mesure[169].

Le juge d'instruction veillera en outre, sous contrôle de la Chambre des mises en accusation et du juge à l'audience, que les écoutes ne seront pas en rapport avec des conversations qui relèvent du secret professionnel. Les communications ou télécommunications couvertes par le secret professionnel ne peuvent pas être consignées dans le procès-verbal (art. 90sexies, al. 3 CIC).

Pour les moyens de communications, locaux ou résidence utilisés par les avocats et médecins, l'avis du bâtonnier ou du président du conseil de l'ordre est prévu par la loi (art. 90octies CIC). Ici aussi, l'on doit respecter la protection des sources journalistiques[170].

Quant aux conditions de forme, la loi oblige le juge à prendre une ordonnance motivée[171]. Cette motivation est prescrite ici – à la différence de l'article 88bis CIC - à peine de nullité. Différentes formes doivent être constatées (voir ci-dessous *Formalités*). La motivation doit comporter une partie factuelle. Le juge devra mentionner les indices ainsi que les faits

---

159 Voir Ch. De Valkeneer, *o.c.,* (2006), 335.

160 Cass. 27 avril 2010, P.10.0103.N. Il est peut-être plus judicieux de dire que des raisons d'ordre public autorisent à ne pas mentionner les noms des agents des services spécialisés.

161 Cass. 26 maart 2003, RDPC 2003, 1080, note T. Henrion.

162 Voir aussi Th. Freyne, « De bewaking van privécommunicatie en –telecommunicatie in strafonderzoeken : een stand van zaken », *T. Strafr.* 2008, 170-177.

163 F. Deruyck, *Syllabus strafprocesrecht*, Brussel, VUB-uitgaven, 2010, 127.

164 Ch. Meunier, l.c., (2001), 662.

165 M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),484, note 365.

166 Voir Ch. De Valkeneer, *o.c.,* (2006), 326; Th. Freyne, *l.c.,* (2008), p. 172-173, n° 18.

167 Ch. De Valkeneer, *o.c.,* (2006), 326; voir Cass. 5 octobre 2005, *Pas.* 2005, n° 483, *RDPC* 2006, 208 et *T. Strafr.* 2006, 20, note P. Van Walleghem, « Over de motiveringsverplichting bij direct afluisteren »; 26 décembre 2006, P.06.1621.F; 4 september 2007, *Pas.* 2007, n° 385 et *NC* 2008, 192; Bruxelles 24 décembre 2003, *RDPC* 2004, 742; Corr. Anvers 14 septembre 2005, *Vigiles* 2006, 58, note H. Berkmoes.

168 Cass. 4 septembre 2007, *Pas.* 2007, n° 385 et *NC* 2008, 192; 16 septembre 2008, *Pas.* 2008, n° 477, *T. Strafr.* 2009, 306 et *RW* 2009-2010, p. 834, note F. Vanneste, "De motivering van het subsidiariteitsbeginsel bij een afluistermaatregel"; 18 mai 2011, P.11.0138.F.

169 Ch. De Valkeneer, *o.c.,* (2006), 327-328.

170 Voir au sujet de tous ces point M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),484; Th. Freyne, *l.c.,* (2008), p. 177-178.

171 Voir pour plus de détails A. Jacobs, « L'exigence de motivation des décisions ordonnant un repérage ou une écoute téléphonique », RDPC 2001, 854-864; Th. Freyne, *l.c .,* (2008), p. 173-175.

concrets et propres à la cause qui justifient la mesure. Ceci implique que le juge, d'une part, constate l'existence d'indices sérieux, ce qui implique une référence aux pièces du dossier, et, d'autre part, qu'il indique les faits et circonstances propres à l'affaire[172]. Il faut éviter que la mesure soit purement exploratrice[173]. D'autre part, la motivation devra comporter les raisons pour lesquelles la mesure s'est avérée nécessaire à la manifestation de la vérité (art. 90quater, § 1 CIC), ce qui réfère aux conditions de fond, proportionnalité[174] et subsidiarité[175].

Durée. La mesure ne peut excéder un mois à compter[176] de la décision ordonnant la mesure (art. 90quater, § 1 CIC). Le juge d'instruction peut prolonger une ou plusieurs fois les effets de son ordonnance pour un nouveau terme qui ne peut dépasser un mois, avec un maximum de six mois, sans préjudice de sa décision de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparues (art. 90quinquies, al. 1 CIC).

Rapportage. L'analyse complète des règles en cette matière dépasse largement notre sujet[177]. Nous nous limiterons ici à quelques règles générales et aux spécificités en matière de TIC.

Les officiers de police judicaire commis font rapport par écrit au moins tous les cinq jours au juge d'instruction sur l'exécution de l'ordonnance (art. 90quater, § 3, dernier al. CIC, voir aussi l'art. 90septies, al. 1 CIC). Toutes les (télé)communications doivent être enregistrées dans leur entièreté[178] afin de préserver le droit de la défense, de garantir la manifestation de la vérité et d'éviter toute manipulation[179]. Là encore, la jurisprudence est assez coulante vu qu'en cas de perte des enregistrements, il suffira de prendre connaissance des transcriptions actées dans les procès-verbaux[180]. Les enregistrements sont transcrits et si besoin est traduits. C'est au cours de cette phase, qu'une sélection peut être faite[181]. A la fin de la mesure, les officiers de police judiciaire commis transmettent les enregistrements (art. 90sexies, al.1 CIC) accompagnés de la transcription des communications et télécommunications estimées pertinentes pour l'instruction, de leur traduction éventuelle et de l'indication des sujets abordés et des données d'identification du moyen de télécommunication à partir duquel ou vers lequel il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes. Le juge d'instruction peut faire réduire cette sélection[182] ou la compléter s'il estime cela pertinent pour l'instruction (al. 2). Pertinent signifie utile comme élément à charge, mais aussi à décharge[183]. Les parties peuvent aussi le demander au juge d'instruction (art. 90septies, al. 6-8 CIC).

Les enregistrements non pertinents et tout ce qui s'y rapporte sera détruit. Les autres enregistrements accompagnés de la transcription des communications et télé-communications estimées pertinentes avec traduction éventuelle, de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, et des copies des procès-verbaux sont conservés au greffe sous pli scellé. Le greffier mentionne dans un registre spécial tout évènement concernant ces scellés (art. 90septies, al. 2-4 CIC). Les parties peuvent demander de consulter les enregistrements (art. 90septies, al. 6-8 CIC). Le juge à l'audience n'a cependant ici aucun pouvoir.

Les moyens appropriés seront utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription ou de leur traduction ainsi que pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ils remplacent la conservation sous pli scellé ou le registre spécial.

Afin d'en garantir la conservation et le pouvoir de les consulter, il est important d'utiliser des supports qui ne permettent pas de les effacer[184]. Si le matériel technique est disponible, les TIC offrent ici de meilleures garanties de conservation et de consultation que l'enregistrement sur bande. L'on pourra aussi plus facilement faire une copie aux fins de la consultation en gardant l'original ou une autre copie en réserve. Cela permettra également un gain de place. La conservation devra se faire dans des conditions de température et d'humidité appropriées et de sécurité (incendie, effacement magnétique, etc.), ce qui n'est pas toujours aisé lorsque les bâtiments sont vétustes et mal sécurisés. Ici les TIC ne diffèrent pas d'autres supports, comme les bandes magnétiques, tout aussi sensibles.

---

172 Cass. 26 octobre 2010, P.10.0834.N; Th. Freyne, *o.c.,* (2011), 310-11.
173 Bruxelles 9 juin 2008, JLMB 2008, 32.
174 Cass. 5 octobre 2005, P.05.1056.F.
175 Voir la jurisprudence citée ci-dessus.
176 Cass. 25 novembre 2008, P.08.1050.N.; voir pour plus de détails Th. Freyne, *o.c.,* (2011), 313-314.
177 Voir par exemple Th. Freyne, *l.c.,* (2008), p. 178-180.
178 Ch. De Valkeneer, *o.c.,* (2006), 331.
179 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 676-677.
180 Cass. 29 mai 2001, *T. Strafr.* 2002, 37.
181 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 677.
182 Cass. 26 mai 2004, *Pas.* 2004, n° 286; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 677.
183 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 677.
184 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 677, note 742.

Formalités. Sanction et preuve. A la différence de la mesure de recherches de communications, différentes formes sont prescrites à peine de nullité. L'ordonnance doit être datée et indique les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90ter, les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité, la personne, le moyen de communication ou de télécommunication ou le lieu soumis à la surveillance, la période pendant laquelle la surveillance peut être pratiquée et qui ne peut excéder un mois à compter de la décision ordonnant la mesure et les nom et la qualité de l'officier de police judiciaire commis pour l'exécution de la mesure (art. 90quater, § 1 CIC)[185]. Ceci n'est pas sans importance puisque la jurisprudence actuelle considère que les preuves obtenues illégalement ne peuvent être exclues que si les formes sont entre autres prescrites à peine de nullité[186]. Il faut cependant souligner que la jurisprudence s'efforce à contourner ces formes, ce qui rend la mesure bien sûr légale. Cependant, l'examen de cette jurisprudence, sauf quelques exemples ci-dessus, dépasserait le périmètre de notre étude et nous nous n'y attarderons pas[187].

La mesure est sujette au principe de spécialité, ce qui veut dire que les écoutes ne peuvent uniquement être utilisées que pour les infractions pour lesquelles elles étaient ordonnées[188]. Mais la jurisprudence accepte que si une nouvelle infraction est découverte par « hasard », on pourra valablement les déclarer et les écoutes pourront servir de base à une poursuite séparée[189], même si ces nouveaux faits concernent une infraction pour laquelle une mesure d'écoute n'est pas prévue par l'article 90ter, §§ 2-4 CIC[190]. Une disqualification ultérieure n'a aucun impact même si cette nouvelle qualification ne fait pas partie de la liste des infractions du § 2 de l'article 90ter CIC[191].

Comme pour la recherche de communications, l'on peut considérer que la violation du secret professionnel conduit à l'exclusion de la preuve ainsi obtenue[192]. Cependant, la Cour de Cassation considère que le juge peut légalement prendre connaissance du nom sous lequel le prévenu se présentait grâce à une retranscription de la conversation tenue avec le secrétariat d'un cabinet d'avocats afin de prendre un rendez-vous pour son frère, ce qui ne constituerait pas une violation du secret professionnel[193].

La Cour de Cassation a jugé que lorsque les preuves invoquées devant le juge du fond proviennent d'écoutes téléphoniques réalisées dans le cadre d'un dossier qui ne lui est pas soumis, la juridiction de jugement contrôle la légalité de la mesure sur la base de l'ordonnance et des pièces d'exécution produites régulièrement en copie aux débats; le juge ne saurait être tenu, en pareil cas, d'examiner en outre si l'instruction dont il n'est pas saisi confirme le bien-fondé des indices, faits et motifs repris à l'ordonnance[194]. Inutile de préciser que cette jurisprudence non nuancé est difficilement compatible avec la jurisprudence de la Cour E.D.H.[195].

(2) Les organismes d'application de la loi peuvent-ils avoir accès à / geler / rechercher/ saisir les systèmes d'information pour a) des données d'E-circulation; b) des données de contenu?

Le droit belge connaît différentes mesures qui permettent l'accès/ le gèle/ la recherche et la saisie de données. Il y a premièrement la perquisition (art. 87, 88, 89bis CIC) et la saisie classique (art. 89 CIC) qui permettent de saisir des appareils électroniques ou des données issues d'un système informatique. Puis, il y a l'accès à un système informatique et la recherche informatique qui s'apparente à une perquisition et la recherche informatique élargie qui concerne un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée (art. 88ter CIC). Ensuite, il y a la saisie de données, qui peut s'accompagner d'un gel de données (art. 39bis CIC). En matière de recherche, l'on pourra distinguer quelques spécificités concernant les données d'E-circulation. Dans les autres cas, il n'y aura, à notre sens, pas lieu de les distinguer. Nous traiterions simultanément les questions (a) et (b). Par contre, nous commencerons par l'analyse des règles en matière de perquisition et de recherche, pour ensuite nous tourner vers les saisies. Notons dès à présent que la matière manque cruellement de jurisprudence.

---

185 Voir concernant la motivation, les références citées ci—dessus concernant les conditions de forme; pour les autres voir Th. Freyne, *o.c.,* (2011), 312-14.

186 Cass. 14 octobre 2003, *RW* 2003-04, 67 avec les conclusions du procureur-général M. De Swaef et observations D. De Wolf, *RW* 2003-04, 1235-1239.

187 Voir parmi d'autres Ch. De Valkeneer, *o.c.,* (2006), 330; Th. Freyne, *l.c.,* (2008), p. 176-177.

188 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 678.

189 Voir Cass. 1 juin 2005, P.05.0725.F., *Pas.* 2005, n° 308; 25 février 2009, P.08.1818.F. et *in extenso* H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), p. 679-680.

190 Cass. 3 juin 2008, P.07.1517, *Pas.* 2008, n° 339.

191 M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),488, note 367.

192 Voir ci-dessus.

193 Cass. 14 octobre 2009, P.09.1279.F.

194 Cass. 25 février 2009, P.08.1818.F.

195 Voir parmi d'autres Comm.DEH Jespers c. Belgique,14 décembre 1982; Rowe et Davis c. Royaume-Uni 16 février 2000; Khan c. Royaume-Uni, 12 mai 2000; Matheron c. France, 29 mars 2005; sur la problématique de l'absence de pièces dans le dossier pénal en Belgique, voir D. De Wolf, *De rol van de rechter in de correctionele procedure bij de waarheidsvinding,* Heule/Brugge, UGA/Die Keure, 2010, 271-309.

2.1. L'accès et la recherche des systèmes d'informatiques

1. *Objet. La recherche informatique.* S'il s'agit d'appareils ou instruments électroniques, les pouvoirs de perquisition et de saisie classiques peuvent suffire (art. 87, 88 et 89bis CIC). Certains auteurs pensent que la prise de connaissance du contenu d'un GSM ou la lecture des e-mails sur un ordinateur consistent en une recherche dans un système informatique[196]. Si les données sont transmises sur un support classique (par exemple sur papier), les pouvoirs de perquisition et de saisie classiques pourront également suffire. Un e-mail qui sera imprimé pourra sans aucun problème être saisi pendant une perquisition, même si cet e-mail provient d'un système informatique. L'on peut dire de même au sujet de photos ou d'images téléchargées d'internet et puis imprimées sur papier.

Mais à partir du moment où il s'agit de chercher dans le système informatique même, on pourra sur un plan théorique être amené à distinguer, outre la perquisition, une nouvelle mesure, la recherche informatique. Des raisons d'ordre juridique et pratique peuvent conforter cette vision. Ces raisons sont les suivantes. Vu que d'une part le législateur a prévu que l'introduction dans un système informatique est punissable (art. 550bis CP)[197] et que les systèmes informatiques peuvent être considérés comme des données d'ordre privé qui tombent sous le coup de l'article 8 CEDH, l'accès et la recherche dans les systèmes informatiques doit être subordonnée à un pouvoir spécifique prévu par la loi. D'autre part, en matière de systèmes informatiques, il n'est pas fort aisé de prendre et de transporter physiquement tous les supports matériels, appareils et instruments à des fins de recherches dans les locaux de la police. Si ces systèmes servent au fonctionnement d'un organisme (par exemple un hôpital) ou d'une entreprise (par exemple une banque), il ne sera même pas souhaitable d'enlever tous les ordinateurs, serveurs et autres appareils électroniques[198]. Pour cette raison, le législateur a prévu que les autorités peuvent avoir accès à des systèmes informatiques et peuvent effectuer des recherches au sein de ces systèmes. Si nécessaire, les autorités pourront saisir les données en les copiant et même les geler (voir ci-dessus au point 2.2.).

Ceci relève en partie que de la théorie, puisque le législateur a bien introduit la notion de « recherche informatique » dans l'article 88ter CIC, mais étrangement ne règle pas le régime juridique[199] et semble entièrement l'assimiler à une perquisition[200]. Les travaux parlementaires[201] sont peu clairs sur ce point et peuvent à notre sens être interprété dans les deux sens, c'est-à-dire l'assimilation à la perquisition mais aussi à une visite de lieu public[202]. Plusieurs auteurs considèrent que les systèmes informatiques sont par de leur nature d'ordre privé[203] indépendamment s'ils sont utilisés dans des lieux publics (par exemples des gares) ou accessibles au public (par exemple dans un café) ou dans des endroits privés (par exemple une maison ou une entreprise). D'autres auteurs considèrent que l'utilisation d'une système informatique privé dans des lieux publics (ou accessibles aux public) ne relèvent pas des règles de la perquisition puisqu'une perquisition sera uniquement nécessaire pour la violation d'un domicile (art. 15 de la Constitution), alors que la violation de la vie privée (art. 8 CEDH) exige une loi expresse[204]. Cette discussion ressemble au statut des entreprises et des locaux professionnels qui ne tombent pas sous le coup de l'article 15 de la Constitution[205]. L'article 88ter stipule par contre clairement que le juge d'instruction ordonne une recherche dans un système informatique, ce qui semble plutôt indiquer qu'il s'agit là d'une perquisition au sens de l'article 87 et 88 du CIC ; mais il est vrai que la loi n'est pas très claire à ce sujet. D'autres auteurs encore pensent que les systèmes informatiques sont privés et nécessitent un pouvoir de perquisition, sauf pour l'accès à des systèmes informatiques dans des lieux publics (par exemples des cyber-cafés) ou même concernant des sites web sur l'internet[206]. En réaction à cette thèse, l'on a défendu qu'il fallait par contre distinguer selon que le système informatique public est vraiment public (par exemple un ordinateur dans une bibliothèque, mais nous pensons aussi au visionnage par un policier d'un site web accessible à tout le monde) ou si quelqu'un utilise un réseau public (nous pensons à une connexion à l'internet via un réseau public dans une bibliothèque, un cybercafé ou un hôtel ou une connexion « wifi » publique) pour accéder à un site privé protégé par un mot de passe[207]. Notons que dans ces cas, il ne pourra plus s'agir d'une recherche, mais d'une recherche élargie (voir ci-dessous) ou d'un recherche ou écoute de communications (voir ci-dessus la question 1). Les opinions divergentes des auteurs semblent se départager selon que l'on met l'accent sur la protection de la vie

[196] Voir P. De Hert et G. Lichtenstein, « Huiszoeking en beslag in geautomatiseerde omgevingen », *Custodes* 2003, afl. 4, (59) 74; Th. Incalza, « Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming », *Jura Falconis* 2010-2011, 357-358.
[197] Ch. De Valkeneer, *o.c.,* (2006), 393.
[198] Ch. De Valkeneer, *o.c.,* (2006), 428; P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 190.
[199] Ch. Meunier, l.c., (2001), 663; Th. Incalza, « Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming », *Jura Falconis* 2010-2011, 332 .
[200] Ch. Meunier, l.c., (2001), 663; R. Verstraeten, *o.c.,* (2005), n° 914; zie ook Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, 149, met noot.
[201] Projet de loi, travaux Parl. La Chambre 1999-2000, n°. 50-0214/001, p. 37.
[202] Voir Th. Incalza, *l.c.* (2010-2011), 333.
[203] Ch. De Valkeneer, *o.c.,* (2006), 393-394; R. Verstraeten, *o.c.,* (2005), n° 914.
[204] Th. Incalza, *l.c.* (2010-2011), 335-336.
[205] Voir D. De Wolf, « Het strafrechtelijk onderzoek naar het milieumisdrijf », dans A. De Nauw et autres (ed.), *Milieustraf- en Milieustrafprocesrecht. Actuele vraagstukken,* Brussel, Larcier, 2005, (183), 216-220.
[206] Ch. Meunier, l.c., (2001), 664, note 206.
[207] Th. Incalza, *l.c.* (2010-2011), 336-337.

privée, indépendamment du lieu, ou si l'on met l'accent sur le lieu (comparons la prise d'une photo d'une personne (célèbre) dénudée dans un lieu public à celle où cette même personne se trouve dans un lieu privé mais observable d'un lieu public).

Pour encore compliquer les choses, il faudra distinguer l'accès aux lieux où se trouvent les appareils ou instruments et l'accès à l'appareil ou l'instrument même. Concernant l'accès aux lieux où se trouvent les appareils ou instruments, un pouvoir de perquisition sera nécessaire si ces lieux ne sont pas publics ou accessibles au public[208]. Les cyber-cafés sont par exemple des lieux accessibles au public[209], mais une maison ou même une entreprise[210] ne le sont pas. Cependant, certains auteurs considèrent que si le système informatique se trouve dans un lieu privé, le mandat de perquisition pour ce lieu couvrira la recherche dans le système informatique même[211]. Il nous semble préférable de distinguer et de prévoir, éventuellement dans la même ordonnance, deux titres[212].

La recherche élargie/ en ligne / l'extension de la recherche. Si la recherche dans le système informatique se passe à partir d'un système informatique vers un autre qui se situe dans un autre lieu, on peut parler d'une recherche élargie. On parle aussi de recherche en ligne (en néerlandais « netwerkzoeking »)[213] ou de « l'extension de la recherche »[214] (la langue française semble être ici à court de mots). Dans la pratique, l'on avait constaté que dans de nombreux cas la personne avait accès au système informatique à partir d'un ordinateur dans un certain lieu où la perquisition donnait accès aux autorités, mais que les données elles-mêmes étaient stockées dans un autre lieu. On considérait que le mandat de perquisition ne permettait pas de rechercher dans cet autre lieu[215]. Si l'on devait identifier les lieux où les données se situent et puis obtenir un nouveau mandat de perquisition, l'on risquerait que les éléments de preuves auraient disparu[216]. En ces temps-là, il s'agissait d'ordinateurs connectées en ligne entre eux ou avec des serveurs. Aujourd'hui, il est d'usage de parler de stockage « in the cloud ».

Une certaine doctrine a désigné cette méthode de recherche, contrairement à la recherche dans un système informatique ou recherche uni-locale, comme la recherche multi-locale ou recherche en ligne (en néerlandais « netwerkzoeking »)[217]. C'est cette dernière hypothèse que le législateur a réglée dans l'article 88ter CIC. Le terme « système informatique » peut ici encore être compris dans le sens le plus large, afin de couvrir toutes les évolutions de la technologie[218]. Il peut donc s'agir d'ordinateurs, serveurs informatiques ou de systèmes de télécommunications. Dans ce sens, l'on a soutenu que deux GSM (du type « smartphone ») qui sont connectés en continu[219] ou d'une connexion avec un PDA[220], peuvent être examinés par le biais de la recherche élargie (en ligne). La recherche élargie est une recherche informatique et est donc généralement assimilée à une perquisition, à laquelle des conditions spécifiques s'ajoutent (voir ci-dessus au point 3).

Ici aussi, la doctrine se dispute sur la question – assez théorique – si la recherche élargie est une forme de perquisition ou non. L'on distingue d'une part, les partisans de la thèse de l'assimilation à la perquisition[221], d'autre part, les partisans qui estiment qu'il s'agit d'une méthode *sui generis*[222] et puis ceux qui considèrent qu'il s'agit d'une méthode *sui generis*, mais dont les limites de la recherche seront désignées par les règles de la perquisition[223]. S'il est correct de dire que la recherche

---

[208] Ch. De Valkeneer, *o.c.,* (2006), 394; concernant la distinction entre lieux privées et lieux publics ou accessible aux public voir par exemple D. De Wolf, « Het strafrechtelijk onderzoek naar het milieumisdrijf », dans A. De Nauw et autres (ed.), *Milieustraf- en Milieustrafprocesrecht. Actuele vraagstukken,* Brussel, Larcier, 2005, (183), 214-216; M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),303 et 454; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 392-394.

[209] Ch. De Valkeneer, *o.c.,* (2006), 394.

[210] Le statut des entreprises n'est pas très claire dans la jurisprudence, voir D. De Wolf, « Het strafrechtelijk onderzoek naar het milieumisdrijf », dans A. De Nauw et autres (ed.), *Milieustraf- en Milieustrafprocesrecht. Actuele vraagstukken,* Brussel, Larcier, 2005, (183), 216-220.

[211] R. Verstraeten, *o.c.,* (2005), n° 914.

[212] Allant dans le même sens Ch. De Valkeneer, *o.c.,* (2006), 394; Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 89. Nous pensons aussi à la jurisprudence de la Cour EDH Van Rossem et Ernst c. la Belgique.

[213] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 88.

[214] Ch. Meunier, l.c., (2001), 664.

[215] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 88; Ch. Meunier, l.c., (2001), 664; Ch. De Valkeneer, *o.c.,* (2006), 394.

[216] Ch. De Valkeneer, *o.c.,* (2006), 394.

[217] Th. Incalza, *l.c.* (2010-2011), 332.

[218] Th. Incalza, *l.c.* (2010-2011), 340.

[219] Th. Incalza, *l.c.* (2010-2011), 341.

[220] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 89.

[221] Ch. Meunier, l.c., (2001), 664; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 620; Y. Poullet, « A propos du projet de loi dit n° 21. La lutte de la criminalité dans le cyberspace à l'épreuve du principe de régularité des preuves », in X., *Liber amicorum Jean du Jardin,* Deurne, Kluwer, 2001, 12.

[222] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 89; P. De Hert et G. Lichtenstein, "De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht", *CBR Jaarboek* 2002-2003, 401; voir aussi Th. Incalza, *l.c.* (2010-2011), 339

[223] F. de Villenfagne et S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *AM* 2001, 60-81.

pourra se passer sans que les autorités ont été sur place[224], ceci pourrait être un argument en faveur de la deuxième thèse. Force est de constater que le législateur a consacré un article séparé à la recherche informatique et donc que dans l'esprit du législateur, il s'agit d'une chose à part entière. Enfin l'article 88ter, § 4 se réfère à l'article 89bis CIC, ce qui laisse penser que le législateur a cru que la recherche élargie ne s'assimile pas à une perquisition et donc qu'il fallait prévoir la délégation aux officiers de police judiciaire. Mais de là à dire que la méthode possède un caractère *sui generis* et n'a donc aucun lien avec la perquisition, conduit au constat que sur différents points le vide juridique existe, puisque les articles 87, 88 et 89bis CIC ne pourront plus être appliqués (voir ci-dessus les points 2 et 3). L'on pourrait peut-être dire de manière plus pragmatique que la recherche informatique est une forme spéciale de perquisition[225]?

La question se pose si une ordonnance concernant une recherche dans un système informatique suffit pour contenir une extension de recherche. Une certaine jurisprudence l'a accepté[226], mais la doctrine ne partage pas cette opinion. Il n'est pas aux enquêteurs de juger eux-mêmes de l'étendue des recherches et donc de l'étendue des pouvoirs qui leurs sont délégués par mandat[227]. Il semble que le juge d'instruction devrait pour la motivation de son ordonnance pouvoir disposer au préalable du type de système informatique que l'on pourrait rencontrer, sinon un nouveau mandat devra être délivré[228]. Les travaux parlementaires sont sur ce point de nouveau des plus flous[229]. Par contre, il n'est pas nécessaire de préciser les lieux où la recherche élargie devra s'effectuer, vu que la mesure tend à résoudre les problèmes d'identification des lieux ou les données se trouvent matériellement[230].

Là où les choses se compliquent vraiment est de faire la différence entre la recherche élargie (en ligne) d'une part et la recherche et l'écoute de communications d'autre part (art. 88bis et 90ter-quater CIC). Les données en phase de transmission tombent sous le coup de l'article 90ter CIC (voir ci-dessus) et la constatation de communications entre systèmes informatiques relève de la recherche de communications[231]. Les recherches dans un système informatique concernent des données stockées ou enregistrées sous un forme électronique et ont un caractère *ex tunc.* L'interception de télécommunications présente par contre un caractère ex nunc[232]. Dans la pratique, il ne sera pas chose aisée de savoir si la transmission est terminée - dans ce cas une ordonnance basé sur l'article 88ter CIC devra être prise - ou que la communication n'est pas encore terminée - dans ce cas une ordonnance sur base de l'article 90ter CIC devra être prise[233].

Ajoutons que les recherches dans un système informatique peuvent avoir trait à des « données d'e-traffic » ou de « contenu », alors que l'interception aura trait à des données de contenu.

Nous ne traiterons pas ici les problèmes liés à la transgression des frontières, les questions liées à la souveraineté d'états étrangers[234] et aux questions d'entraide judiciaire.

2. *Autorités.* Les perquisitions classiques sont de la compétence exclusive du juge d'instruction, sauf dans le cas de flagrant délit (art. 36 et 41 CIC), consentement exprès ou dans les cas prévus par les lois pénales spéciales (par exemple en matière de drogues) où le procureur du Roi ou les services de polices (s'il ont la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi, art. 49) ont des compétences[235]. Le juge d'instruction peut déléguer l'exécution d'une perquisition à un officier de police judiciaire (art. 89bis CIC). Notons aussi que les lois pénales spéciales ont attribué des moyens dits de contrôle exorbitants et notamment la recherche dans des endroits privées non associés à des habitations. Ces pouvoirs de contrôles administratifs ne peuvent cependant pas être utilisés à des fins de recherches pénales[236]. Certaines de ces lois signalent expressément la recherche dans des systèmes électroniques et la saisie de ceux-ci, par exemple le nouveau Code

---

224 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 90; contra Y. Poullet, *o.c.,* (2001), 15; D. Dewandeleer, "Misdrijven en strafonderzoek in de IT-context" in R. Verstraeten en F. Verbruggen (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 148; Th. Incalza, *l.c.* (2010-2011), 352-353; Ch. Meunier, l.c., (2001), 668.

225 Dans ce sens Ch. De Valkeneer, *o.c.,* (2006), 393-396 qui place la recherche informatique parmi « les visites domiciliaires » (voir sur la différence en terminologie entre « perquisition » et « visite domiciliaire », M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),452, note 184); O. Leroux, *l.c.,* (2012), 843.

226 Corr. Bruxelles 10 janvier 2008, *T. Strafr.* 2008, 149.

227 Bruxelles 26 juin 2008, réforme Corr. Bruxelles cité ci-avant, *T. Strafr.* 2008, 467, note; R. Verstraeten, *o.c.,* (2005), n° 916; D. Dewandeleer, "Misdrijven en strafonderzoek in de IT-context" in R. Verstraeten en F. Verbruggen (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 144-145; Th. Incalza, *l.c.* (2010-2011), 356.

228 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 90-94.

229 Voir le commentaire de R. Verstraeten, *o.c.,* (2005), n° 916.

230 Voir Ch. De Valkeneer, *o.c.,* (2006), 394.

231 Ch. De Valkeneer, *o.c.,* (2006), 394.

232 Ch. Meunier, l.c., (2001), 663.

233 Voir in extenso pour les différents cas de figures Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 91; voir aussi H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 620; Th. Freyne, *o.c.,* (2011), 308-309.

234 Fort critique sur ce point S. Evrard, « La loi du 28 novembre 2000 relative à la criminalité informatique », *JT* 2001, 244.

235 Voir par exemple M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),(2006),458 ; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 395-404.

236 Voir F. Deruyck en D. De Wolf, *Syllabus bijzondere strafwetten*, Brussel, VUB-uitgaven, ed. 2012.

Pénal Social[237], alors que d'autres lois demeurent muettes à ce sujet. La possibilité d'une mini-instruction est exclue par la loi (l'art 28septies CIC).

La recherche informatique (élargie ou non) est selon l'article 88ter CIC aussi du domaine exclusif du juge d'instruction. Si l'on assimile cette recherche à une perquisition, les mêmes règles s'appliqueront. Cette assimilation amène à considérer que la mini-instruction est exclue par l'article 28septies CIC[238]. Mais peut-être pourra-t-on défendre que le terme « perquisition » dans l'article 28septies CIC ne comprend pas les recherches informatiques (article 88ter CIC) vu que le législateur a cru nécessaire d'exclure le contrôle visuel discret (art. 89ter CIC) qui se trouve dans le même paragraphe que les perquisitions[239]? Les pouvoirs exceptionnels du procureur du Roi et des services de polices semblent être d'application[240]. Un auteur émet cependant une réserve concernant la recherche élargie, puisque l'article 88ter CIC ne réfère pas au procureur du Roi[241]. Les compétences en matière de consentement semblent aussi compromises dans ce cas, puisque certains auteurs sont d'avis que le consentement de la personne qui se connecte à un système informatique et y a accès n'est pas suffisant. Le consentement de la personne qui est propriétaire du serveur ou autre appareil qui héberge le système informatique serait nécessaire[242]. L'on pourrait peut-être dire que vu que la recherche élargie est limitée aux parties du système informatique auxquelles une personne a accès, le consentement de cette personne est suffisante et que le propriétaire du système informatique ou du lieu d'hébergement ne sont pas nécessaires (comparons avec la situation d'une perquisition chez un locataire sans le consentement du propriétaire du bâtiment, mais là aussi les opinions divergent).

Si par contre on refuse d'accepter cette assimilation (voir ci-dessus), les pouvoirs du procureur du Roi ou des services de polices en cas de flagrant délit ou de consentement semblent incertains (il faudra lire l'article 36 CIC extensivement)[243], une délégation est prévue (art. 88ter, § 4 *juncto* 89bis CIC) et une mini-instruction est possible[244]. Dans cette hypothèse, l'on peut se poser la question si cette législation vague et non précise satisfait aux exigences de l'article 8 CEDH. Refuser l'assimilation (partielle) au régime des perquisitions entraînera donc pas mal de problèmes.

3. *Conditions de la recherche élargie/en ligne*.

Comme signalé ci-dessus, la loi ne définit pas les conditions concernant la recherche dans un système informatique. Si l'on accepte l'assimilation avec le régime juridique d'une perquisition le problème sera résolu[245], sinon un problème se pose concernant la conformité avec l'article 8 CEDH.

En matière de recherche élargie la loi est plus précise et soumet la mesure à différentes conditions. La recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:

- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès (art. 88ter, §§ 1 et 2 CIC).

Trois conditions s'imposent donc[246]. *Premièrement,* la nécessité pour la manifestation de la vérité. Le but est donc de rassembler des preuves à charge ou à décharge concernant les faits qui font l'objet de l'instruction. Le juge devra rester dans sa saisine[247]. *Deuxièmement,* une condition de proportionnalité qui se traduit par le souci d'éviter des recherches importantes dans différents lieu et chez différentes personnes. On devra donc démontrer que d'autres mesures seraient disproportionnées[248]. *Troisièmement,* et de manière alternative avec la deuxième condition[249], l'existence d'un risque de

---

[237] K. Salomez, *Sociaal strafrecht,* dans *ICA Reeks*, n°10, Brugge, Die Keure, 2010, 93-96.
[238] Ch. Meunier, l.c., (2001), 664, note 208.
[239] Voir aussi Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 620; O. Leroux, *l.c.,* (2012), 843.
[240] R. Verstraeten, *o.c.,* (2005), n° 914; Ch. Meunier, l.c., (2001), 665; Ch. De Valkeneer, *o.c.,* (2006), 394.
[241] R. Verstraeten, *o.c.,* (2005), n° 658.
[242] Ch. Meunier, l.c., (2001), 665; Th. Incalza, *l.c.* (2010-2011), 355.
[243] Voir Th. Incalza, *l.c.* (2010-2011), 356, contra R. Verstraeten, *o.c.,* (2005), n° 658.
[244] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 89; Th. Incalza, *l.c.* (2010-2011), 355; I. Delbrouck, "Informaticacriminaliteit" in *Postal Memorialis* Antwerpen, Kluwer, 2007, (122) 147.
[245] Sur les formes d'une perquisition en droit belge voir Ch. De Valkeneer, *o.c.,* (2006), 361-392; M. Franchimont, A. Jacobs et A. Masset, o.c., (2006), 452-464; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 597-614.
[246] Voir aussi M. Franchimont, A. Jacobs et A. Masset, o.c., (2006), 490; R. Verstraeten, *o.c.,* (2005), n° 915.
[247] Ch. De Valkeneer, *o.c.,* (2006), 394; Ch. Meunier, l.c., (2001), 666 (concernant les faits non compris dans la saisine du juge d'instruction, mais découverts par hasard voir ci-dessus en matière d'écoutes).
[248] Ch. De Valkeneer, *o.c.,* (2006), 394.
[249] S. Evrard, *l.c.,* (2001), 244.

déperdition de preuves[250]. Une certaine doctrine a signalé, à juste titre, que ces conditions seront presque automatiquement réalisées[251].

En plus, on ne pourra pas dépasser l'autorisation d'accès dont la personne qui fait l'objet des mesures dispose dans le système informatique. Les autorités judiciaires ne peuvent pas avoir plus de droits que cette personne[252]. L'on ne pourra pas entamer des recherches tous azimuts[253]. Le « hacking » par la police ne serait pas possible[254], voir cependant ci-dessous les possibilités en matière de coopération concernant les mots de passes. L'on peut se demander si dans le cas où l'utilisateur initial a lui-même dépassé l'autorisation d'accès, les autorités judiciaires doivent limiter leur recherche ou non. On a soutenu que dans ce cas, une recherche uni-locale dans le système où l'utilisateur initial c'est introduit serait nécessaire. Comme le propriétaire du système informatique est lui-même la victime, il sera vraisemblablement disposé à consentir à la recherche[255]. En outre, la plupart des auteurs estiment qu'une recherche élargie ou en ligne à partir d'ordinateurs de la police ne serait pas autorisée[256]. Ce point de vue entraînera l'impossibilité de toute recherche discrète[257].

Ceci implique aussi qu'il existe un « lien permanent, stable et non purement occasionnel entres les systèmes informatiques »[258]. Étrangement, cette condition ce trouve uniquement dans les travaux parlementaires et non dans le texte de loi [259] . Cette condition entraînera beaucoup de problèmes d'appréciation dans la pratique et risque de limiter considérablement la mesure. On peut citer le cas d'un employé qui se connecte de temps en temps au serveur interne de son entreprise[260] ou une personne qui se rend de manière fortuite dans une bibliothèque publique pour visionner des images à caractère douteux. L'on a même soutenu que l'internet ne peut par définition pas faire l'objet d'une recherche élargie[261]. Dans la doctrine plusieurs critères ont été élaborés pour définir ce lien, comme le réseau normal[262] ou le domicile virtuel, ou tout endroit où la personne peut se dire chez elle comme un site bancaire ou une messagerie privée accessible par un site « web »[263]. Des sites sur internet qui présentent un caractère privé, comme des sites bancaires, des « webmails » ou de sites de stockages « in the cloud » relèveraient donc de la recherche élargie [264]. Il nous semble que tout cela complique inutilement les choses. Quand les sites sur internet sont accessibles à tout le monde, aucun pouvoir spécifique n'est nécessaire[265]. Pour le reste tout « système informatique » relève de la recherche élargie, indépendamment si ce système se situe sur internet ou sur un serveur ou sur des appareils ou des instruments de taille plus réduite comme des « smartphones » ou des PDA[266]. Cependant la condition de lien permanent, non occasionnel, est bel et bien une limitation qui sape l'utilité de cette mesure[267]. Si nous reprenons l'exemple de l'utilisateur d'un ordinateur dans une bibliothèque publique qui se connecte par un mot de passe à un site à caractère douteux, il semble que le législateur considère le système informatique avec lequel cette personne se connecte comme étant trop « éloigné » (voir aussi le critère du domicile virtuel) pour que l'on puisse y rechercher par le biais du système informatique initial. Il nous semble aussi trop simpliste de déduire de la possession d'un nom d'utilisateur et d'un mot de passe qu'il existe un lien permanent[268]. Il manque donc un pouvoir de recherche dans des systèmes informatiques sans qu'un lien permanent ne doive exister[269]. Par contre le mot de passe prouvera l'accès à ce système informatique.

Sauf dans le cas de flagrant délit ou de consentement, une ordonnance préalable[270] du juge d'instruction est nécessaire. Il nous semble, par analogie avec le mandat de perquisition, que cette ordonnance doit être motivée[271]. Dans cette motivation,

---

[250] Ch. De Valkeneer, *o.c.,* (2006), 393.
[251] Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 88.
[252] Th. Incalza, *l.c.* (2010-2011), 347.
[253] Ch. Meunier, l.c., (2001), 668.
[254] Ch. Meunier, l.c., (2001), 668; Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 90; Th. Incalza, *l.c.* (2010-2011), 3348; I. Delbrouck, "Informaticacriminaliteit" in *Postal Memorialis* Antwerpen, Kluwer, 2007, (122), 138; S. Evrard, *l.c.,* (2001), 244.
[255] Th. Incalza, *l.c.* (2010-2011), 348.
[256] Voir ci-dessus point 1.
[257] Voir Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 90-94.
[258] Ch. De Valkeneer, *o.c.,* (2006), 395.
[259] *Doc. Parl.,* Chambre, sess. n° 213/001, p. 23 .
[260] Voir Ch. Meunier, l.c., (2001), 668.
[261] Th. Incalza, *l.c.* (2010-2011), 349; mais cet auteur défend lui-même la thèse que l'internet est public et que donc les policiers y ont aussi accès (voir p. 351).
[262] Voir P. De Hert et G. Lichtenstein, « Huiszoeking en beslag in geautomatiseerde omgevingen », *Custodes* 2003, afl. 4, (59) 65.
[263] Y. Poullet, « A propos du projet de loi dit n° 21. La lutte de la criminalité dans le cyberspace à l'épreuve du principe de régularité des preuves », in X., *Liber amicorum Jean du Jardin,* Deurne, Kluwer, 2001, 14; F. de Villenfagne et S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *AM* 2001, 75.
[264] Th. Incalza, *l.c.* (2010-2011), 350.
[265] P. De Hert et G. Lichtenstein, « Huiszoeking en beslag in geautomatiseerde omgevingen », *Custodes* 2003, afl. 4, (59) 73.
[266] Voir Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 8; voir aussi H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 620.
[267] Contra Th. Incalza, *l.c.* (2010-2011), 351.
[268] Dans ce sens Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 88.
[269] Th. Freyne, *o.c.,* (2011), 316.
[270] Ch. De Valkeneer, *o.c.,* (2006), 395; contra Ch. Meunier, l.c., (2001), 667-668; Th. Incalza, *l.c.* (2010-2011), 357.

le juge prendra en compte des conditions d'application citées ci-dessus[272]. Si l'on accepte l'assimilation à une perquisition, le constat d'indices sérieux qu'une infraction a été commise ou est en train d'être commise devra aussi se retrouver dans l'ordonnance[273]. Une délégation de l'exécution du mandat est possible, mais les formes de l'article 89bis en matière de perquisitions devront être respectées (art. 88ter, § 4juncto 89bis CIC). Si les systèmes informatiques visités appartiennent à des personnes qui peuvent invoquer le secret professionnel, les règles d'usage en matière de perquisition chez cette catégorie de personnes s'imposent[274].

L'article 88ter, § 4 CIC stipule que le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées. Cette exigence s'avère dans la pratique assez difficile. Elle n'est cependant pas prescrite à peine de nullité et aucun délai n'est prévu[275].

4. Formes. Sanctions. Signalons qu'aucune des formes n'est prescrite à peine de nullité. En cas de violation, il n'y aura donc aucun effet [276] sauf si cela entraîne des doutes concernant la fiabilité des preuves ou en cas de violation du procès équitable[277].

2.2. Saisies et gel de données

Le régime des saisies de données et du gel de certaines données est moins compliqué. Si suite à une perquisition ou une recherche informatique ou une recherche élargie des données sont découvertes qui peuvent servir d'éléments de preuves, il sera nécessaire de les saisir soit afin de les analyser de manière plus approfondie pour les besoins de l'enquête (art. 35, § 1 CIC)[278], soit afin de les produire plus tard devant le tribunal comme moyen de preuve. Si ces données se trouvent sur des supports matériels ou sur des instruments ou appareils peu encombrants (par exemple GSM, PDA, CD-Rom ou DVD[279], clés USB[280], tablette, voire même des ordinateurs, …) on pourra les saisir selon les règles normales[281] des saisies en matière pénale (art. 35 CIC)[282].

Par contre, si l'on veut saisir les données mêmes, une forme particulière de saisie devra s'opérer puisque les données sont immatérielles et incorporelles[283]. En plus, comme il a déjà été signalé ci-avant, des raisons d'ordres pratiques peuvent mener à la conclusion que la saisie n'est pas souhaitable (continuité d'entreprises) ou difficilement réalisables (transport de serveurs volumineux installés dans une cave)[284]. Parfois, il ne sera même pas nécessaire de saisir le système informatique en entier. C'est pour cela que le législateur a prévu une forme particulière de saisie pour les données informatiques.

L'article 39bis, § 2 du CIC stipule que lorsque le procureur du Roi ou l'auditeur du travail découvrent dans un système informatique des données stockées qui sont utiles aux mêmes finalités que celles prévues pour la saisie[285], mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, seront copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles aux personnes autorisées à utiliser le système informatique. Le juge d'instruction est également compétent (art. 89 CIC)[286]. En ce qui concerne les données recueillies par

---

271 Dans le même sens Ch. De Valkeneer, *o.c.,* (2006), 395; O. Leroux, *l.c.,* (2012), 843.
272 Ch. Meunier, l.c., (2001), 666.
273 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 597.
274 Voir parmi d'autres H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 603 et seq.
275 Ph. Van Linthout et J. Kerkhofs, *l.c.,* (2008), p. 90.
276 Ch. De Valkeneer, *o.c.,* (2006), 394.
277 Cass. 14 octobre 2003, *RW* 2003-04, 67 avec les conclusions du procureur-général M. De Swaef et observations D. De Wolf, *RW* 2003-04, 1235-1239. .
278 O. Leroux, *l.c.,* (2012), 841.Ceci se limitera aux données trouver sur l'appareil ou l'instrument électronique. Si l'on voudra exploiter des e-mails qui se trouvent sur des serveurs il faudra appliquer d'autres mesures (au sujet de cette problématique voir ci-dessus la recherche informatique élargie et l'écoute de communications).
279 Ch. Meunier, l.c., (2001), 671.
280 O. Leroux, *l.c.,* (2012), 840.
281 Ch. De Valkeneer, *o.c.,* (2006), 428.
282 Voir parmi d'autres Ch. De Valkeneer, *o.c.,* (2006), 423-427; D. De Wolf, « Het strafrechtelijk onderzoek naar het milieumisdrijf », dans A. De Nauw et autres (ed.), *Milieustraf- en Milieustrafprocesrecht. Actuele vraagstukken,* Brussel, Larcier, 2005, (183), 224-229 et les références en notes; M. Franchimont, A. Jacobs et A. Masset, o.c., (2006),464-470 et les références en notes; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 407-455; J. De Peuter, « Het beslag in strafzaken », in R. Declercq, J. De Peuter, et A. Vandeplas, *Strafprocesrecht voor rechtspractici,* Leuven, Acco, 1996, 59-100; A. Viaene, *Huiszoeking en beslag in strafzaken*, dans APR, 1962, 287 p.; R. Verstraeten, « Beslag in strafzaken», dans X., *Commentaar strafrecht en strafvordering*, Anvers, Kluwer, 2003, 44 p.; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 407-455; F. Desterbeck, *De inbeslagneming en verbeurdverklaring in strafzaken in België,* Mechelen, Kluwer, 2007, 1-50; R. Declercq, *Eléments de procédure pénale,* Bruxelles, Bruylant, 2006, n°s 412 et 558.
283 Ch. De Valkeneer, *o.c.,* (2006), 428; voir aussi Ch. Meunier, l.c., (2001), 670.
284 Voir Ch. De Valkeneer, *o.c.,* (2006), 428; P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 190.
285 Ceci est une référence à l'article 35 CIC; par finalités, on comprend de saisir tout ce qui paraîtra constituer l'une des choses visées aux articles 42 et 43quater du Code pénal (la confiscation) et de tout ce qui pourra servir à la manifestation de la vérité (voir Ch. Meunier, l.c., (2001), 671).
286 Voir aussi Ch. Meunier, l.c., (2001), 671.

l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, l'article 88ter, § 3 CIC stipule que les règles prévues à l'article 39bis CIC s'appliquent.

La saisie s'effectuera en copiant les données stockées sur un système informatique. On effectuera cette copie en utilisant des supports des autorités ou exceptionnellement en cas d'urgence ou pour des raisons techniques sur des supports des utilisateurs du système informatique[287]. L'on pourra aussi copier les données nécessaire à la lecture de données[288]. Certains auteurs défendent la thèse que les saisies ne pourront être ordonnées que si le principe de proportionnalité a été respecté[289]. D'autres soulignent que la saisie des supports seront la règle et que la copie sera l'exception vu que celle-ci sera effectuée si la saisie matérielle n'est pas souhaitable[290]. L'on peut se poser la question si cette lecture stricte s'impose. Les autorités pourront à notre sens également préférer de copier les données si cela est plus pratique, sans devoir démontrer que la saisie du support n'est pas souhaitable.

Il est vrai que, contrairement aux mesures d'écoutes, on n'ait prévu de faire deux copies, une copie de travail et une en réserve que l'on déposera au greffe, ni la manière dont les policiers spécialisés devront faire rapport de leur travaux[291].

Afin d'éviter toute manipulation, une mesure de blocage, une sorte de scellés électroniques, sera opérée sur l'original et les copies[292]. On peut penser au blocage par un mot de passe ou par un moyen de cryptage[293]. L'article 39bis, § 3, al. 1 CIC stipule à cet effet : Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité. Le § 5 y ajoute en plus que le procureur du Roi ou l'auditeur du travail utilisent les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données. Des moyens techniques appropriés sont utilisés pour leur conservation au greffe. La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.

Le législateur n'a, de manière voulue, pas défini ce qu'il entendait par « moyens techniques appropriés », afin de prévoir les évolutions techniques futures. Une certaine doctrine craint que le manque de précision soit une source de débats concernant la manière dont les données saisies doivent être conservées[294].

Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité (art. 39bis, § 4 CIC) [295].

Le § 3, al. 2 permet ensuite de geler certaines données afin d'éviter toute diffusion de données. Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes moeurs (par exemples des images porno-pédophiles) ou constituent un danger pour l'intégrité des systèmes informatiques ou pour les données stockées, traitées ou transmises par le biais de tels systèmes (par exemples les « hackertools »), le procureur du Roi ou l'auditeur du travail utilisent tous les moyens techniques appropriés pour rendre ces données inaccessibles. En pratique, l'on effacera les données qui sont contraires à l'ordre public ou aux bonnes moeurs ou qui constituent un danger[296]. Certains auteurs lisent le texte de manière stricte. Le terme « objet de l'infraction » ne comportera donc pas « l'instrument de l'infraction » comme un virus informatique[297]. Il semble aussi possible d'ordonner aux opérateurs et fournisseurs de services qu'un site internet ne soit pas accessible aux utilisateurs belges[298].

Sauf les données ainsi gelées ; il peut cependant, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites (art. 39bis, § 3, al. 3 CIC). Ceci est une exception au droit commun[299].

Les règles du CIC relatives à la saisie, y compris l'article 28sexies (référé pénal et demande de levée des saisies), sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique (art. 39bis, § 1 CIC). Ici aussi il a été prévu que les autorités informent le responsable du système informatique

---

287 Ch. De Valkeneer, *o.c.,* (2006), 429.
288 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 190; Ch. Meunier, l.c., (2001), 672.
289 O. Leroux, *l.c.,* (2012), 841.
290 Ch. Meunier, l.c., (2001), 672.
291 Ch. Meunier, l.c., (2001), 673.
292 Ch. De Valkeneer, *o.c.,* (2006), 429.
293 Ch. Meunier, l.c., (2001), 675.
294 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 190.
295 Voir Ch. Meunier, l.c., (2001), 674.
296 Ch. Meunier, l.c., (2001), 675.
297 Ch. Meunier, l.c., (2001), 676.
298 O. Leroux, *l.c.,* (2012), 841, note 25, citant JI Malines 6 avril 2012 et Prés réf. Malines 19 juillet 2012, tous inédits.
299 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 190.

de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées (art. 39bis, § 5 CIC). Mais ici aussi, aucun délai n'a été prévu, ni aucune sanction[300].

(3) Les entreprises de télécommunications ou les fournisseurs de services peuvent-ils avoir l'obligation de partager des données avec les organismes d'application de la loi? En cas de refus, existe-t-il des mesures coercitives ou des sanctions?

Oui, opérateurs et fournisseurs de services doivent coopérer en cas de demande des autorités judiciaires. Le caractère obligatoire est conforté par une sanction pénale en cas de refus et par la diminution des honoraires en cas d'exécution déficiente. Au surplus, la divulgation d'information est pénalement réprimée.

Il existe de diverses obligations. Les opérateurs ou fournisseurs n'ont aucun droit de juger de l'opportunité des mesures[301].

1. L'article 88bis CIC stipule que chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication communique les informations qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications[302]. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les Télécommunications, est punie d'une amende de vingt-six euros à dix mille euros.

L'article 90quater, § 2 stipule que si la mesure comporte une opération sur un réseau de communication, l'opérateur de ce réseau ou le fournisseur du service de télécommunication est tenu de prêter son concours technique, quand le juge d'instruction le requiert. Le § 4 CIC y ajoute en ce même sens que le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues à y donner suite, dans la mesure de leurs moyens.

Le § 2 s'adresse uniquement aux opérateurs ou fournisseurs, alors que le champ d'action du § 4 est plus large[303]. Il semble dans tous les cas qu'il s'agit d'une obligation de moyens et non de résultats (voir ci-dessus la sanction pénale et plus loin concernant l'article 88quater CIC).

Celui qui refuse de fournir la collaboration ordonnée, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs (à lire comme euros en augmentant avec les décimes additionnels) ou d'une de ces peines seulement. On pourra cependant signaler le droit du suspect de ne pas collaborer à sa propre inculpation[304].

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal.

2. Les modalités de l'obligation de coopération sont fixées par arrêté royal[305]. Les opérateurs et fournisseurs ont l'obligation de créer ou de partager une Cellule de coordination de la Justice[306]. Concernant les recherches visées par l'article 88bis CIC, la Cellule de coordination de la Justice communique, en temps réel, sauf dispositions contraires dans la réquisition, au juge d'instruction ou, le cas échéant, au procureur du Roi, dès réception de la réquisition, les données d'appel et les données de localisation requises d'équipements terminaux à partir desquels ou vers lesquels des appels sont effectués en temps réel ou datant de moins de trente jours. Les données datant de plus de trente jours seront communiquées au plus tard le jour ouvrable suivant, à la même heure de la réception de la requête, sauf dispositions contraires dans la réquisition[307].

Pour l'application de l'article 90quater, § 2 du Code d'instruction criminelle, la Cellule de coordination de la Justice prend les mesures nécessaires pour faire écouter, prendre connaissance et enregistrer des communications ou des télécommunications privées, immédiatement, pendant leur transmission, dès réception de l'ordonnance visée à l'article 90ter,

---

[300] Ch. Meunier, l.c., (2001), 679.
[301] B. De Smet, *o.c.,* (2008), n° 34, p. 14.
[302] Voir arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, modifiés par l'AR du 8 février 2011 ; pour un commentaire de l'ancien AR voir F. Goossens, « Concretisering van de medewerkingsverplichting aan een telefoontap », TVW 2003, 167 et seq.
[303] Ch. Meunier, l.c., (2001), 688.
[304] H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* (2010), 676.
[305] Ch. De Valkeneer, *o.c.,* (2006), 323.
[306]Art. 2 AR 9 janvier 2003.
[307] Art. 4 AR du 9 janvier 2003.

§ 1er ou § 5, sauf dispositions contraires indiquées dans l'ordonnance. La communication interceptée est transmise en temps réel au service NTSU-CTIF [308].

La Cellule de coordination de la Justice communique les données requises selon les règles de l'art et avec les moyens techniques performants disponibles sur le marché. Elle communique ces données, en règle [309], par voie électronique sécurisée sous une forme aisément utilisable pour le requérant[310]. Les données doivent être précises à la seconde près et correspondre au fuseau horaire auquel appartient la Belgique[311].

Quand il s'agit de messages envoyés électroniquement, les autorités peuvent demander aux fournisseurs de services internet l'adresse IP (statique ou dynamique), le numéro d'appel utilisé pour la connexion, la localisation des connections internet, les dates et les moments précis où les communications ont eu lieu et la liste des communications reçues ou envoyées[312].

Les frais d'investissement, d'exploitation et d'entretien pour les moyens techniques utilisés par les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques sont à charge de ces opérateurs et de ces fournisseurs. La seule indemnité que les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques obtiennent en échange de leur collaboration conformément aux articles 3, 4 et 5 de l'arrêté royal du 9 janvier 2003 figure à l'annexe de cet arrêté royal. Les prestations qui ne figurent pas à l'annexe de cet arrêté royal sont uniquement rétribuées selon les coûts réels, sur présentation des pièces justificatives.

Après l'exécution de la mesure, le magistrat instructeur vérifiera premièrement si les postes des frais correspondent à la nomenclature. Ensuite, il jugera les frais et honoraires puisqu'ils forment des frais de justice[313]. Il peut les diminuer en cas d'exécution déficiente, de retard dans l'exécution ou de frais ou honoraires exagérés[314]. Ce système a été complété en 2004 par un contrôle *a priori* puisque surtout les frais de mesures d'écoutes sapent le budget du ministère de la justice. Le juge d'instruction ou le procureur du Roi devra soumettre sa décision au premier président de la Cour d'appel ou au Procureur général pour « avis » si le coût communiqué par l'opérateur requis du réseau de télécommunication ou le fournisseur du service de télécommunication est supérieur au montant fixé par le Roi[315]. Cette loi n'est cependant à ce jour pas en vigueur. On peut craindre que ce système *a priori* risquera de retarder considérablement l'exécution des mesures[316].

3. Nous avons déjà développé plus haut l'obligation de conservation des données pour les opérateurs et fournisseurs.

L'article 127 de la loi du 13 juin 2005 relative aux communications électroniques y ajoute que le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finaux, en vue de permettre :

1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence;
2° l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.
Le Roi fixe, après l'avis de l'Institut, la méthode de détermination de la contribution dans les frais d'investissement, d'exploitation et d'entretien de ces mesures qui est à la charge des opérateurs de réseaux et services de communications électroniques, ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.

---

[308] Art. 5 AR du 9 janvier 2003.

[309] Dans l'impossibilité, pour quelque raison que ce soit, de transmettre les données requises par voie électronique, les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques sont tenus de communiquer les informations requises à l'officier de police judiciaire désigné à cet effet par l'autorité judiciaire requérante.

[310] Le Ministre de la Justice et le ministre compétent pour les matières relatives aux communications électroniques, déterminent le format spécifique de présentation des données par les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques, ainsi que le mode de transmission de ces données (art. 10bis AR du 9 janvier 2003).

[311] Art. 8 AR du 9 janvier 2003.

[312] Voir B. De Smet, *o.c.,* (2008), n°. 71.

[313] Voir l'article 2 *(Tout retard injustifié dans l'exécution de la mission ou le dépôt du rapport entraîne une réduction des honoraires de l'expert. Le magistrat qui requiert un expert assigne à celui-ci, chaque fois que faire ce pourra, un délai dans lequel la mission doit être terminée et le rapport déposé)* et 78, al. 4 (*Si le magistrat estime ne pas pouvoir arrêter tels quels les mémoires dont question à l'alinéa précédent, ou si les opérations, par leur nature ou par exception, ne rentrent pas dans le barème prévu par l'article 1er, les mémoires sont taxés par le magistrat requérant qui, le cas échéant, peut en réduire le montant par ordonnance motivée***)** du Règlement général du 28 décembre 1950 sur les frais de justice en matière répressive.

[314] Th. Freyne, *o.c.,* (2011), 306.

[315] Art. 16, 4° de la loi du 27 décembre 2004 portant des dispositions diverses.

[316] M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale,* Bruxelles, Larcier, 2006, 482; H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 654; R. Verstraeten, *Handboek strafvordering,* Antwerpen, Maklu, 2005, n° 934.

Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées ci-dessus, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

Jusqu'à ce que les mesures visées ci-dessus entrent en vigueur, l'interdiction visée ci-dessus ne s'applique pas aux services de communications électroniques publics mobiles fournis sur base d'une carte prépayée.

Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les utilisateurs finaux qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finaux ne sont en aucune manière indemnisés pour la déconnection.

Si un opérateur ne déconnecte pas les utilisateurs finaux qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible. Chaque opérateur établit (…) une procédure interne permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

L'article 145 de cette loi punit d'une amende de 50 à 50 000 EUR, la personne qui enfreint l'article 127 et les arrêtés pris en exécution.

L'article 6 de l'arrêté royal du 9 janvier 2003 stipule que pour l'application de l'article 127, § 1er, alinéa 1er, 2° de la loi du 13 juin 2005, les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques, le cas échéant conjointement, doivent être techniquement en mesure de répondre, dans les conditions fixées par les articles 46bis, 88bis, 90ter et suivants du Code d'instruction criminelle, pour la communication des données demandées, aux exigences fonctionnelles suivantes :

1° transmettre tant les données d'appel et les données de localisation du service de communications électroniques surveillé que le contenu de la communication de manière à pouvoir en établir la corrélation avec précision, dans les conditions fixées par les articles 88bis et 90ter du Code d'instruction criminelle;

2° transmettre, en temps réel, la communication interceptée pour l'ensemble du territoire couvert par l'opérateur du réseau de communications électroniques ou le fournisseur du service de communications électroniques et pour toutes les connexions de, vers ou via le territoire belge, dans les conditions fixées par l'article 90ter du Code d'instruction criminelle;

3° transmettre l'information interceptée dans un format couramment disponible;

4° transmettre le contenu de la communication en clair si l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques a introduit un codage, une compression ou un cryptage de l'échange de communications électroniques, dans les conditions fixées par l'article 90ter du Code d'instruction criminelle;

5° les transmettre de manière sûre afin que les données ne puissent être interceptées par des tiers.

Les fournisseurs de services de communications électroniques, qui utilisent différentes technologies en même temps, doivent donner toutes les données d'appel et de localisation relatives aux différentes phases et aux services utilisés de la communication électronique telles qu'elles sont imposées aux diverses catégories d'opérateurs et de fournisseurs de services. La combinaison des données enregistrées doit permettre d'établir la relation entre l'origine de la communication et sa destination.

Les spécifications techniques doivent répondre aux standards et rapports du « *European Telecommunications Standards Institute* », y compris les actualisations éventuelles[317]. Les options qui doivent être reprises dans ces standards seront

[317] Il s'agit des données : 1° TS 101-331 : "Lawful Interception (LI); Requirements of Law Enforcement Agencies"; 2° TS 101-671 : " Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic "; 3° TS 101-909-20-1: "AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services "; 4° TS 101-909-20-2 : " AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services"; 5° TR 101-943 : "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture"; 6° TR 101-944 : "Lawful Interception (LI); Issues on IP Interception"; 7° TR 102-053: "Lawful Interception (LI); Notes on ISDN LI functionality"; 8° TS 102-232: "Lawful Interception (LI); Handover Specification for IP Delivery"; 9° TS 102-233 : "Service-specific details for e-mail services"; 10° TS 102-234: "Lawful Interception (LI); Service-specific details for internet access services"; 11° TS 102-815: "Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception; 12° TS 133-106: Universal Mobile Telecommunication System (UMTS); "Lawful interception requirements (3GPP TS 33.106 version 5.1.0 Release 5) [3GPP SA3]"; 13° TS 133-107: Universal Mobile Telecommunication System (UMTS); 3 G security; "Lawful interception architecture and functions (3GPP TS 33.107 version 5.5.0 Release 5) [3GPP SA3]"; 14° TS 133-108: "Universal Mobile Telecommunications System (UMTS); 3G Security; Handover interface for Lawful interception (LI) (3GPP TS 33.108 version 5.4.0 Release 5) [3GPP SA3]"; 15° ES 201-158: " Lawful Interception (LI); Requirements for Network Functions"; 16° ES 201-671: "Lawful Interception (LI): Handover Interface for the Lawful Interception of Telecommunications Traffic"; 17° Digital cellular

déterminées par le Ministre de la Justice, après avis, dans les deux mois, de l'Institut belge des services postaux et des télécommunications.

Les articles 8, 10 et 10 bis de l'arrêté cités ci-dessus sont applicables.

4. L'article 88quater CIC stipule en outre que le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ou à l'auditeur du travail.

Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail qu'il y a délégué, peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

L'ordonnance visée ci-dessus ne peut être prise à l'égard de l'inculpé ni à l'égard des personnes visées à l'article 156 (§ 2).

Il s'agit d'une obligation d'information et d'intervention[318]. Dans la pratique, la mesure est assez peu utilisée, voir même inconnue[319]. Un des auteurs argumente sur base des travaux parlementaires que le juge d'instruction ne pourra ordonner la mesure qu'en cas de nécessité[320]. Notons que la loi ne stipule pas expressément cette condition, mais oblige le juge uniquement de signaler les circonstances propres à l'affaire justifiant la mesure. On peut estimer que le procureur du Roi a les mêmes compétences de réquisition que le juge d'instruction en cas de flagrant délit ou de consentement[321]. La personne à qui la réquisition s'adresse peut être une personne dont le juge présume qu'elle dispose d'une connaissance particulière ou toute personne appropriée. Ce sont des termes dont le sens est extrêmement étendu et qui laissent une large marge d'appréciation au juge[322]. Exception est faite pour le suspect, les proches et on peut y ajouter les personnes tenues par le secret professionnel[323]. Dans ce dernier cas, non seulement la personne qui y est tenue juge elle-même si elle doit garder ce secret[324], mais il nous semble que l'exemption ne sera pas totale, puisqu'elle se limitera au informations couvertes par le secret professionnel et donc pas à l'ensemble du système informatique.

Celui qui refuse de fournir la collaboration ordonnée ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs (à lire comme euros en augmentant avec les décimes additionnels) ou d'une de ces peines seulement. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal (§§ 3-4). De l'ensemble du § 2 et 3, il résulte qu'une obligation de moyens et non de résultats est demandée[325]. L'hypothèse de la personne qui fait obstacle vise le cas de la personne qui - entre autre – feint de ne pas pouvoir accéder aux fichiers ou même les effacera[326]. Notons que le droit belge ne connaît pas d'incrimination pour celui qui ne livre pas la clef électronique en cas d'encryptage de données[327].

L'État est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système (§ 5).

---

telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33 version 8.0.0 Release 1999) [TC SMG] TR 101 514; 18° Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (GSM 02.33 version 8.0.1 Release 1999) [TC SMG] TR 101 507; 19° Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (3GPP TS 43.033 version 5.0.0 Release 5) [3 GPP SA3] TR 143 033; 20° Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (3GPP TS 42.033 version 5.0.0 Release 5) [3GPP SA3] TR 142 033; 21° Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5) [3GPP SA3] TR 141 033; 22° Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception - Stage 2 (3GPP TS 03.33 version 8.1.0 Release 1999) [3GPP SA3] TS 101 509.

318 Ch. Meunier, l.c., (2001), 682.

319 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 199.

320 S. Evrard, *l.c.,* (2001), 245.

321 Ch. Meunier, l.c., (2001), 682.

322 Dans ce sens Ch. Meunier, l.c., (2001),684-685 ; S. Evrard, *l.c.,* (2001), 245.

323 Ch. Meunier, l.c., (2001), 685-686.

324 Ch. Meunier, l.c., (2001), 686.

325 Ch. Meunier, l.c., (2001),683.

326 Ch. Meunier, l.c., (2001),683.

327 P. Van Linthout en J. Kerkhofs, *l.c.,* (2010), 192.

(4) Les organismes d'application de la loi peuvent-ils faire de la surveillance vidéo? Peuvent-ils obliger les personnes physiques ou morales à coopérer?

Oui, les autorités ont le pouvoir de faire de la vidéo-surveillance dans des lieux publics ou non-publics (l'observation avec des moyens techniques) et même en installant des caméras dans une maison (contrôle visuel discret). L'utilisation d'images captées par des systèmes de vidéo-surveillance privées a été abordée par la jurisprudence. Par contre, les autorités n'ont pas de moyens de coercition sur les particuliers afin d'obtenir leur coopération, mais ils peuvent obliger les personnes privées à mettre les images captées à la disposition des autorités.

a. Vidéo-surveillance par les autorités en dehors ou sans vue sur un domicile

En droit belge, il faut d'abord préciser qu'une distinction est faite entre l'observation et l'observation systématique. Dans les deux cas, il s'agit d'une observation en dehors ou sans vue sur un domicile ou un lieu assimilé. L'observation n'est pas réglée[328] et peut être effectuée par tout agent ou officier de police[329], comme chaque citoyen. L'observation dans le CIC est une observation systématique et il s'agit d'une mesure particulière de recherche. L'observation dans le CIC est donc définie par l'article 47sexies CIC comme l'observation systématique par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés. La notion de fonctionnaire de police doit être comprise comme les membres de la police fédérale ou locale. Les fonctionnaires qui sont désignés comme officiers de la police judiciaire ne le sont pas et ne peuvent pas exécuter d'observation systématique[330].

Une observation est dite systématique quand elle a lieu pendant plus de cinq jours consécutifs ou plus de cinq jours non consécutifs répartis sur une période d'un mois, lorsqu'il s'agit d'une observation dans le cadre duquel des moyens techniques sont utilisés, d'une observation revêtant un caractère international ou d'une observation exécutée par des unités spécialisées de la police fédérale. Certains auteurs signalent que le caractère systématique implique un acte intentionnel et se passe toujours à l'insu de la personne observée. L'exemple est donné d'une patrouille de police qui passe plusieurs fois à un endroit et faits des constatations fortuites concernant des personnes ou le cas où un policier entre dans une maison avec l'accord de l'habitant et lors de cette visite fait des constatations[331]. Tout dépendra bien sûr du cas[332].

Un moyen technique au sens de l'article 47sexies CIC est une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90ter (l'écoute directe)[333]. L'on peut penser à des caméras vidéo, appareillage de localisation et de surveillance, systèmes GPS, etc. [334]. Il ne suffira cependant pas qu'un moyen technique soit utilisé, il sera encore nécessaire que l'observation soit effectuée par un fonctionnaire de police. L'utilisation d'informations obtenues par un moyen technique dont dispose un citoyen et que celui-ci met à la disposition des services de polices, n'est pas une observation avec des moyens techniques par un fonctionnaire de police pour laquelle une autorisation est requise[335]. L'exécution d'une mesure d'observation par des moyens techniques devra être faite par des unités spéciales de la police fédérale[336].

Un appareil utilisé pour la prise de photographies sans prises de vues dans un domicile ou un lieu assimilé, n'est pas considéré comme un moyen technique. Le législateur semble prendre en considération le lieu (non public), le degré de dissimulation (moyens techniques) et la capacité de recueillir des données privées[337]. Ceci explique – peut-être - l'exclusion d'appareils photos, même cachés et munis d'accessoires qui en augmentent la portée (téléobjectif). Il est correct d'observer qu'en droit belge la prises d'images, dans un endroit public ou non, n'est pas punissable pénalement[338].

L'observation en utilisant des caméras est de toute façon et dans tous les cas (moins de cinq jour, lieu public, sans dissimulation, …) une observation systématique. En outre, si l'observation par caméra devient une surveillance, on atteindra aussi le caractère systématique, la durée étant de plus de cinq jours. Cependant, l'utilisation de moyens techniques aura comme conséquence que des conditions plus strictes seront d'application. Vu le sujet de ce rapport nous n'analyserons que l'observation systématique par des moyens techniques. Des règles différentes seront applicables pour les observations dans ou avec vue sur un domicile ou des lieux assimilés, nous les traiterons dans un point séparé ci-dessous.

Notons d'emblée qu'aucune règle n'est prescrite à peine de nullité. Ceci veut dire que, sauf influence sur la fiabilité ou sur le procès équitable, aucune sanction n'est prévue en cas de violations des règles. Un des auteurs a écrit que ces règles

328 Chambre m. acc. Anvers 18 octobre 2007, *NC* 2009, 211, note L. Huybrechts.
329 A. De Nauw et F. Schuermans, *l.c.,* 937.
330 Cass. 2 septembre 2008, P.08.0483.N., *NC* 2009, 193 et *T. Strafr.* 2009, 304, note X.
331 Ch. De Valkeneer, *o.c.,* (2006), 259.
332 Voir Cass. 3 octobre 2006, P.06.0919.N.
333 Pour plus de détails voir Ch. De Valkeneer, *o.c.,* (2006), 261-262.
334 Ch. De Valkeneer, *o.c.,* (2006), 262; A. De Nauw et F. Schuermans, *l.c.,* 936.
335 Cass. 19 juin 2012, P.12.0362.N., *RABG* 2013, 46, note Y. Van Den Berge, « Quid met de gegevens voortkomende uit technische hulpmiddelen verstrekt door derden? ».
336 Ch. De Valkeneer, *o.c.,* (2006), 271.
337 Voir Ch. De Valkeneer, *o.c.,* (2006), 262-263; A. De Nauw et F. Schuermans, *l.c.,* 936.
338 Ch. De Valkeneer, *o.c.,* (2006), 264.

risqueront de souffrir d'une certaine érosion … [339]. La régularité peut cependant être contrôlée par la Chambre des mises en accusation qui prononce la nullité de l'acte qui en est entaché. Les pièces annulées sont retirées du dossier et déposées au greffe du tribunal de première instance, après l'expiration du délai de cassation (art. 235bis, § 6 CIC). Il n'est cependant pas aussi clair si la Chambre des mises en accusation doit à ce moment appliquer les critères en matière d'exclusion de la preuve obtenue illégalement ou pas. Dans le cas d'une réponse affirmative, les pièces ne peuvent être retirées du dossier que si la fiabilité ou le procès équitable sont entachés[340].

Autorité. Les mesures particulières de recherche sont de la compétence du procureur du Roi. Cependant le juge d'instruction pourra lors d'une instruction l'ordonner ou l'autoriser. Dans ce cas, le procureur du Roi est chargé de l'exécution des autorisations d'observation accordées par le juge d'instruction (art. 467sexies, § 7 CIC). Le fait que cette mesure peut être exécutée lors d'une information, signifie qu'une enquête proactive est aussi possible (voir aussi § 3, article 47sexies CIC)[341].

Conditions. L'article 47sexies, § 2 CIC stipule que le procureur du Roi peut, dans le cadre de l'information, autoriser une observation si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. Les conditions de nécessité ou de proportionnalité et de subsidiarité sont donc requises. La nécessité implique que des indices sérieux doivent exister (voir § 3, article 47sexies CIC)[342]. Une observation effectuée à l'aide de moyens techniques ne peut être autorisée que lorsqu'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. La condition de subsidiarité est similaire qu'en matière d'écoutes (voir ci-dessus)[343].

Il n'y a aucune condition de durée. Mais comme la mesure doit être nécessaire, on peut considérer que l'observation à l'infini n'est pas légale. Le § 3 de l'article 47sexies CIC atteste de cette vision en stipulant que la durée de la mesure sera indiquée dans l'autorisation. Puis le § 6 CIC du même article stipule que le procureur pourra prolonger la mesure, mais il pourra aussi à tout moment retirer son autorisation. Prolonger veut dire que le délai initial de la mesure sera prolongé[344]. Le calcul du délai mentionné dans l'autorisation doit être effectué selon les articles 52 à 54 du Code judiciaire[345]. Le dépassement rétrospectif de la limitation de la durée ou de la fréquence sans l'autorisation requise entraîne l'irrégularité de l'observation dans son intégralité et non en partie[346].

L'autorisation devra mentionner le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes observées, ainsi que des choses, des lieux ou des événements. Lorsque des indices existent démontrant que les faits poursuivis sont commis par plusieurs personnes non encore identifiées et dans un vaste territoire, la description générale des personnes observées, objets, lieux et événements n'enfreint pas la spécificité prescrite par l'article 47sexies, § 3, 3° CIC[347]. L'observation ne devra pas nécessairement concerner un suspect[348].

Rapportage. L'officier de police judiciaire fait rapport écrit de manière précise, complète et conforme à la vérité, au procureur du Roi sur chaque phase de l'exécution des observations qu'il dirige. Ces rapports confidentiels sont communiqués directement au procureur du Roi, qui les conserve dans un dossier séparé et confidentiel. Il est le seul à avoir accès à ce dossier, sans préjudice du droit de consultation du juge d'instruction et de la chambre des mises en accusation. Le contenu de ce dossier est couvert par le secret professionnel.

Par contre, les procès-verbaux ainsi que l'autorisation d'observation et les décisions de modification, d'extension ou de prolongation sont joints au dossier répressif au plus tard après qu'il a été mis fin à l'observation. L'officier de police judiciaire rédige le procès-verbal des différentes phases de l'exécution de l'observation, mais n'y mentionne aucun des éléments susceptibles de compromettre les moyens techniques et les techniques d'enquête policière utilisés ou la garantie de la sécurité et de l'anonymat de l'indicateur et des fonctionnaires de police chargés de l'exécution de l'observation. Ces éléments ne figurent que dans le rapport écrit (art. 47septies CIC).

Contrôle visuel discret. Afin d'installer dans le cadre d'une observation un moyen technique visé à l'article 47sexies, § 1, al. 3 CIC ou en cas de pénétration en utilisant des moyens techniques dans un lieu privé qui n'est pas un domicile ou un lieu

---

339 Ch. De Valkeneer, *o.c.,* (2006), 267.

340 Comparez Cass. 11 janvier 2006, P.05.1371.F, *Pas.* 2006, 118, *JT* 2006, 106, *JLMB* 2006, 588, *RDPC* 2006, 591, *NC* 2008, 273, *RW* 2006-07, 174, Vigiles 2006, 189 et Cass. 28 juin 2011, P.11.1120.N, *T. Strafr.* 2011, 431, note J. Van Gaever, « Het prima facie onderzoek van onregelmatige onderzoekshandelingen in het kader van de voorlopige hechtenis: de "antigoon"-test heeft ook hier zijn intrede gedaan ».

341 Ch. De Valkeneer, *o.c.,* (2006), 265.

342 Ch. De Valkeneer, *o.c.,* (2006), 265.

343 Cass. 28 octobre 2009, P.09.1280.F, *Pas.* 2009, 2458, *NC* 2010, 290, *RDPC* 2010, 502, note H.D. Bosly, « Méthode particulière de recherche et principe de subsidiarité »; Ch. De Valkeneer, *o.c.,* (2006), 248; A. De Nauw et F. Schuermans, *l.c.,* 923.

344 Cass. 7 juin 2011, *Pas.* 2011, 1628 et *T. Strafr*. 2012, 80, note Y. Van Den Berge.

345 Cass. 27 janvier 2010, P.09.1705.F.

346 Cass. 2 septembre 2008, P.08.0483.N., *NC* 2009, 193 et *T. Strafr.* 2009, 304.

347 Cass. 12 janvier 2010, P.09.1666.F.

348 A. De Nauw et F. Schuermans, « De Wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden », *RW* 2003-04, 937.

assimilé (voir ci-dessous), le procureur du Roi peut, par une décision écrite et motivée, autoriser les services de police à pénétrer à tout moment à l'insu du propriétaire ou de son ayant droit ou sans le consentement de ceux-ci, s'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont commis ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité (art. 46quinquies, §§ 1-2 et 4 CIC.

Le procureur du Roi ne peut décider d'un contrôle visuel discret que pour des lieux où, sur la base d'indications précises, l'on suppose que se trouvent les choses qui forment l'objet d'une infraction, qui ont servi ou qui sont destinées à en commettre une ou qui ont été produites par une infraction, des avantages patrimoniaux tirés directement de l'infraction, des biens et valeurs qui leur ont été substitués et des revenus de ces avantages investis ou que des preuves peuvent en être collectées ou dont on suppose qu'ils sont utilisés par des personnes suspectes (art. 46quinquies, § 3 CIC).

b. Vidéo-surveillance dans un domicile par les autorités

La vidéo-surveillance reste possible mais ici les conditions sont plus strictes.

S'il s'agit d'une observation, visée à l'article 47sexies, effectuée à l'aide de moyens techniques afin d'avoir une vue dans un domicile, ou dans une dépendance propre y enclose de ce domicile au sens des articles 479, 480 et 481 du Code pénal, ou dans un local utilisé à des fins professionnelles ou comme résidence par un avocat ou un médecin, seul le juge d'instruction pourra l'autoriser (56bis, al. 2 CIC). Au surplus et bien que prévu initialement, mais annulé par la Cour constitutionnelle[349], une mini-instruction n'est pas possible[350]. Le domicile au sens des articles 479, 480 et 481 du Code pénal (comme l'article 15 de la Constitution) est assez restrictif dans le sens que des lieux privés non habités ou même des bâtiments d'entreprise[351] ne tombent pas sous le coup cette notion[352].

En plus, l'autorisation sera uniquement possible s'il existe des indices sérieux que les faits punissables constituent ou constitueraient une infraction visée à l'article 90ter, §§ 2 à 4, ou sont ou seraient commis dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal (art. 56bis, al. 2 CIC; comparez en matière d'écoutes, voir ci-dessus)[353]. Analogue à la règlementation en matière d'écoutes, un procédure complémentaire est prévue pour les locaux utilisés à des fins professionnelles ou la résidence d'un avocat ou d'un médecin (voir art. 56bis, al. 3 et 4 CIC)[354].

Dans le cadre de l'exécution de la mesure prévue à l'article 46quinquies CIC, le contrôle visuel discret, et aux conditions qu'il énonce, seul le juge d'instruction peut autoriser les services de police à pénétrer à tout moment dans un domicile, ou dans une dépendance propre y enclose de ce domicile au sens des articles 479, 480 et 481 du Code pénal, ou dans un local utilisé à des fins professionnelles ou comme résidence par un avocat ou un médecin, à l'insu du propriétaire ou de son ayant droit, ou de l'occupant, ou sans le consentement de ceux-ci (art. 89ter, §§ 1-2 et 4 CIC).

Ici aussi, il est nécessaire qu'il existe des indices sérieux que les faits punissables constituent ou constitueraient un délit visé à l'article 90ter, §§ 2 à 4, ou sont commis ou seraient commis dans le cadre d'une organisation criminelle, telle que définie à l'article 324bis du Code pénal, et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité (art. 89ter, §§ 3 CIC).

c. Utilisation d'images provenant de vidéo-surveillances privés

Une autre cas de figure doit encore être examiné : il s'agit de l'utilisation comme preuve de délits d'images provenant de vidéo-surveillances privées, c'est-à-dire la vidéo-surveillance qui n'est pas effectué par les autorités judiciaires, mais par des personnes privées - ou même par des organismes publics en dehors des services de police – et installée afin de protéger des biens ou des vies de personnes. Nous pensons que la différence avec les mesures particulières de recherche, comme l'observation, ne se limite pas seulement au caractère secret[355], mais aussi et surtout par le fait qu'ils s'effectuent par les autorités eux-mêmes. Cela n'empêche pas la police d'effectuer de la vidéo-surveillance non secrète dans un but de contrôle. Nous l'avons vu précédemment (question C.1). Nous verrons que dans ce cas, les images des caméras posées par des particuliers ou par les autorités peuvent être utilisées à des fins de preuve de délits. Mais la plupart des questions se posent lorsqu'il s'agit de l'utilisation d'images provenant de vidéo-surveillances privées. Nous verrons que ces questions sont multiples. Nous examinerons d'abord l'utilisation par les autorités judiciaires d'images captées par des vidéo-surveillances privées, puis l'utilisation par des personnes privées dans un procès pénal. Nous terminerons par la présence de caméras de tiers lors d'une enquête policière.

---

[349] CC 21 décembre 2004, n° 202/2004.

[350] Ch. De Valkeneer, *o.c.,* (2006), 272.

[351] Cass. 21 octobre 1992, *Pas.* 1993, I, n° 679, avec les conclusions de l'avocat-général Janssens de Bisthoven, *RDPC* 1993, 445 et *JT* 1993, 161.

[352] Voir aussi Ch. De Valkeneer, *o.c.,* (2006), 273.

[353] Voir aussi Ch. De Valkeneer, *o.c.,* (2006), 272.

[354] Voir Ch. De Valkeneer, *o.c.,* (2006), 273.

[355] F. Schuermans, « Het gebruik van camera's in de (strafrechts-) handhaving: volatiele rechtspraak vraagt en krijgt meer duidelijkheid van de wetgever », *T. Strafr.* 2012, 315-316. On peut même penser q'une mesure n'est pas entièrement secrète et est partiellement visible.

1. La question se posait si la vidéo-surveillance était autorisée et plus précisément si les autorités peuvent utiliser des images prises par un système de vidéo-surveillance posé par des particuliers. La Cour d'appel de Gand a dans un premier temps décidé que des images de surveillance de la voie publique, captées par une banque, peuvent fournir une preuve d'un délit dont la banque n'est pas la victime, sans violer l'article 8 CEDH[356]. Dans le cas d'espèce, le système de surveillance de la banque n'était pas utilisé pour l'identification de personnes et ne filmait aucun lieu privé. C'est à la suite de la prise d'images, que les autorités ont pu identifier le suspect. La Cour soulignait que des garanties suffisantes concernant l'authenticité et la véracité des images doivent être présentes, ce qui devra être jugé sur le plan de l'appréciation de la preuve. Dans un autre arrêt, cette même Cour d'appel avait jugé que le placement d'une caméra dans un magasin afin de protéger la propriété privée était légitime vu qu'aucune surveillance de personnes n'était effectuée[357]. Dans l'arrêt du 17 mars 2010 la Cour de Cassation[358] a ensuite considéré que « *de la seule circonstance qu'une caméra de surveillance, installée visiblement sur la voie publique, permet de réunir des éléments de preuve des infractions qui s'y commettent, il ne saurait se déduire une ingérence dans l'exercice du droit au respect de la vie privée. L'arrêt considère que la caméra était visible et que, concernant le comportement du demandeur sur la voie publique, les scènes filmées et enregistrées ne mettent pas en cause son intimité. Par ces considérations, les juges d'appel ont légalement décidé que l'enregistrement contesté n'était pas prohibé par l'article 8 de la Convention (EDH)* ». Au moment des faits de la cause, aucune disposition légale ne réglementait l'usage d'une telle caméra installée dans un lieu public.

Depuis, la loi du 21 mars 2007 règle l'installation et l'utilisation de caméras de surveillance[359]. Une caméra de surveillance est définie par l'article 2, 4° de la loi comme tout système d'observation fixe ou mobile dont le but est de prévenir, de constater ou de déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou de maintenir l'ordre public, et qui, à cet effet, collecte, traite ou sauvegarde des images; est réputée mobile, la caméra de surveillance qui est déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions.

Cette loi stipule dans son article 9 que les personnes qui ont accès aux images sont soumises au devoir de discrétion en ce qui concerne les données personnelles fournies par les images, étant entendu que le responsable du traitement pour ce qui est des lieux fermés accessibles au public ou des lieux fermés non accessibles au public ou la personne agissant sous son autorité :

1° peut transmettre les images aux services de police ou aux autorités judiciaires s'il constate des faits pouvant être constitutifs d'infraction ou de nuisances et que les images peuvent contribuer à faire la preuve de ces faits ou à en identifier les auteurs;

2° doit transmettre gratuitement les images aux services de police si ceux-ci les réclament dans le cadre de leurs missions de police administrative ou judiciaire et si les images concernent l'infraction ou les nuisances constatées. S'il s'agit d'un lieu fermé non accessible au public, le responsable du traitement ou la personne agissant sous son autorité peut toutefois exiger la production d'un mandat judiciaire dans le cadre d'une information ou d'une instruction.

Sans préjudice de l'application des articles 47sexies et 47septies du Code d'Instruction criminelle, les services de la police fédérale et locale ont, dans le cadre de leurs missions de police judiciaire ou administrative, un accès en temps réel, libre et gratuit, aux images des caméras installées sur le réseau des sociétés publiques des transports en commun ou dans les sites nucléaires déterminés par arrêté royal délibéré en Conseil des ministres. Les conditions et modalités du libre accès aux images par les services de police sont déterminées par arrêté royal délibéré en Conseil des Ministres, après avis de la Commission de la protection de la vie privée[360].

Dans un arrêt du 5 octobre 2010, la Cour de Cassation s'est exprimé sur le cas où depuis un café des faits avait été filmés. Cette fois ci, la loi du 21 mars 2007 était entrée en vigueur. Le prévenu contestait que l'on pouvait utiliser des images d'un système de vidéo-surveillance pour prouver des faits de faux en écriture alors que ce système y était placé afin de prévenir des délits contres des biens ou personnes. La Cour de Cassation considère que si le but de l'installation ou de l'utilisation de caméras de surveillance ne peut être que de prévenir, de constater ou de déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou de maintenir l'ordre public, l'utilisation des images collectées, traitées ou sauvegardées par les caméras de surveillance n'est pas exclue si elle peut contribuer à apporter la preuve d'une infraction autre qu'un délit contre les personnes ou les biens tel que visé à l'article 2, 4°, de la loi du

---

[356] Gand 28 mars 2002, *NJW* 2003, p. 819 et *T. Strafr.,* 2002, 326, note P. De Hert p. 315—317, selon cet auteur, il aurait suffi de juger sur base de l'article 4 de la loi du 8 décembre 1992 que l'utilisation pour des fins répressives était raisonnablement prévisible, alors que les considération sur l'article 8 CEDH sont hasardeuses notamment par manque de base légale à cette époque; voir aussi R. De Corte, *« De achterkant van de privacy. Kan het beroep op privacy leiden tot straffeloosheid?* », *NJW 2003, 798*.

[357] Gand 21 mai 2002, *NJW* 2003, 822.

[358] Cass. 17 mars 2010, P.09.1691.F.

[359] P. De Hert et R. Saelens, « De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid », *T. Strafr.* 2007, 93-100.

[360] Pour un commentaire de cet article modifié par la loi du 3 août 2012, F. Schuermans, « Het gebruik van camera's in de (strafrechts-) handhaving: volatiele rechtspraak vraagt en krijgt meer duidelijkheid van de wetgever », *T. Strafr.* 2012, 317-319.

21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[361]. Autrement dit, la Cour fait une distinction entre la légalité du placement du système de vidéo-surveillance et l'utilisation de ces images par les autorités judiciaires à d'autres fins[362].

Dans un arrêt du 13 mai 2011, la Cour d'appel de Bruxelles a écarté des images vidéos provenant d'un système de vidéo-surveillance installé par une commune, pour les motifs que cette vidéo-surveillance n'avait qu'un but administratif et que l'utilisation des images prises résultait dans une observation au sens de l'article 47sexies CIC. Puisque selon la Cour le procès équitable aurait été violé, les preuves devaient être écartées. Le prévenu fut cependant condamné puisqu'il y avait assez de preuves d'une autre nature[363]. C'est arrêt est critiquable[364] dans la mesure où la loi du 21 mars 2007 n'interdit pas que le responsable du traitement qui installe la vidéo-surveillance soit un administration publique (art. 2, 5°). Les services de polices sont même seuls autorisés à utiliser des caméras mobiles (art. 7/1-7/2), ce qui confirme qu'ils peuvent aussi installer des caméras fixes. Cette vidéo-surveillance dans un lieu public a un but administratif ou judiciaire, puisque l'article 2, 4° de la loi stipule qu'il a le but de prévenir, de constater ou de déceler les délits. L'article 5, § 4, al. 3 stipule depuis 2009 en plus que l'enregistrement d'images n'est autorisé que dans le but de réunir la preuve de nuisances ou de faits constitutifs d'infraction ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes. Dans ce cas, il ne s'agit pas comme la Cour l'avait estimé d'un visionnage « real-time », mais bien d'images d'une période révolue. Il est donc invraisemblable que les autorités ne pourraient pas utiliser des images comme preuve dans un procès pénal d'un système de vidéo-surveillance installé par une administration publique et opéré par des policiers.

2. La question s'est aussi posée si des particuliers peuvent filmer des faits ou même vidéo-surveiller afin d'obtenir des preuves de délits. Il ne faut pas oublier que dans la procédure belge, la victime peut par la constitution de partie civile déclencher des poursuites pénales et que dans le procès pénal la partie civile peut elle-même produire des preuves afin de prouver les faits poursuivis. Dans une certaine affaire, une organisation de protection des animaux (GAIA) avait filmé certaines exactions contres de animaux dans des foires à bestiaux. La jurisprudence a réagi de façon assez différente. Le tribunal correctionnel de Bruxelles avait considéré qu'il s'agissait d'un traitement de données personnelles (loi du 8 décembre 1992). Comme les conditions de cette loi n'étaient pas respectées, le tribunal décidait que les montages vidéo étaient illégales[365]. Le tribunal correctionnel de Dinant excluait aussi les preuves par vidéo, puisqu'elles heurtent les principes fondamentaux du respect des droits de la défense, du procès équitable et de la vie privée[366]. La Cour d'appel de Liège avait jugé dans le sens contraire qu'il ne s'agissait pas d'un traitement de données personnelles au sens de la loi du 8 décembre 1992 et que l'article 8 CEDH n'était pas violé puisque la prise d'images dans un lieu accessible au public était proportionnel vu le but légitime[367].

Dans une affaire concernant une employée dans un magasin, la preuve de l'employeur, partie civile dans le procès pénal, reposait sur des enregistrements faits sur cassettes audio et vidéo au moyen d'une caméra secrète alors qu'elle était occupée dans le magasin de la partie civile. La Cour de Cassation avait décidé que (l'article 8 CEDH) n'empêche pas que, sur la base d'une présomption légitime de l'implication de son employé dans des infractions commises à son détriment, un employeur prenne des mesures afin de prévenir ou de constater de nouveaux faits punissables au moyen de vidéo-surveillance dans un espace accessible au public du magasin qu'il exploite. Pour autant qu'elle a pour objectif la dénonciation des faits aux autorités et, partant de cet objectif, qu'elle est adéquate, utile et non excessive, une telle mesure n'implique pas d'ingérence dans l'exercice de ce droit au sens de l'article 8, alinéa 2, de la Convention de sauvegarde des

---

361 Cass 5 octobre 2010, P.10.0703.N., *Pas.* 2010, 2483, RW 2011-2012, 1338, note P. De Hert et R. Saelens, « Filmen maar! Versoepeling van de camerawet door het Hof van Cassatie », *T. Strafr.* 2011, 66, note B. Meganck et Computerr. 2011, 81, B. Ooms, « Gebruik van camerabeelden als bewijs ».

362 F. Schuermans, « Cassatie bevestigt geldigheid camerabeelden voor bewijsvoering », commentaire sous Cass. 5 octobre 2010, dans *Juristenkrant* 2011, n° 221, 1.

363 Bruxelles 13 mai 2011, *JLMB* 2012, 461 et *T. Strafr.* 2012, 351.

364 Voir, F. Schuermans, « Het gebruik van camera's in de (strafrechts-) handhaving: volatiele rechtspraak vraagt en krijgt meer duidelijkheid van de wetgever », *T. Strafr.* 2012, 317-319.

365 Voir R. De Corte, « De spelregels gelden ook voor Gaia », commentaire sous Corr. Bruxelles 14 janvier 2002, *Juristenkrant* 2002, n° 42, p. 12.

366 Corr. Dinant 14 novembre 2002, *TBBR* 2003, 161, note O. Leroux et Y. Poullet, « En marge de l'affaire Gaia: de la recevabilité de la preuve pénale et du respect de la vie privée ». La Commission pour la vie privée semble aussi accepter qu'une vidéo-surveillance est un traitement de données personnelles. Avis du 13 décembre 1999, n° 34/1999 ; comparez avis du 7 juin 1995, n° 14/95 ; voir aussi directive 95/46/CE, du Parlement Européen en du Conseil du 24 octobre 1995, *PB* L n°381, du 23 novembre 1995 ; P. De Hert, « De waarde van de Wet van 8 december 1992 bij de bewijsbeoordeling in strafzaken », *T. Strafr.* 2002, (310), 314-315; P. De Hert, O. De Schutter et S. Gutwirth, « Pour un réglementation de la vidéosurveillance », *JT* 1996, 569-579.

367 Liège 27 juin 2003, *Journ. proc.* 2003, n°. 463, 20, note F. Glansdorff et *RDTI* 2004, 103, note M. Loncke.

droits de l'homme et des libertés fondamentales. Celle-ci n'implique pas que la mesure ainsi prise doit être préalablement annoncée[368].

Bien que nous ne pouvons dans le cadre de ce rapport entrer dans les règles concernant l'emploi de caméras sur le lieu de travail[369], signalons que la Cour de Cassation a, dans un affaire connue sous le nom chocolaterie Manon, dans un premier temps décidé sur base de l'article 9 de la convention collective de travail n° 68, du 16 juin 1998, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par l'arrêté royal du 20 septembre 1998, que l'employeur doit, préalablement et lors de la mise en œuvre de la surveillance par caméras sur le lieu du travail, informer les travailleurs de tous les aspects de cette surveillance et que l'absence d'information préalable entraîne l'illégalité du mode de preuve utilisé[370]. Par la suite, la Cour a jugé sur base de sa jurisprudence en matière de preuves obtenues illégalement que la violation par l'employeur de son obligation d'information préalable du travailleur du placement d'une surveillance par caméra sur le lieu du travail n'étant pas sanctionnée de nullité par la loi, il appartient au juge d'apprécier les conséquences, sur la recevabilité des moyens de preuve produits aux débats, de l'irrégularité ayant entaché leur obtention[371]. Les juges d'appels avaient dans la cause constaté que, à la suite d'une présomption légitime de l'implication de la demanderesse dans des infractions qu'elle pourrait avoir commises au préjudice de son employeur, ce dernier avait installé, dans le magasin accessible au public où elle travaillait, un dispositif de vidéosurveillance visant uniquement la caisse sur laquelle il lui appartenait d'enregistrer les achats des clients. Les juges avaient ensuite décidé que la mesure, limitée quant à son objet et destinée à permettre la constatation d'infractions dont la demanderesse était soupçonnée depuis plusieurs années, était adéquate et utile, ne portait pas atteinte à sa vie privée et n'entravait pas son droit de contredire librement devant les juridictions de jugement les éléments produits à sa charge. Notons que la loi du 21 mars 2007 n'est pas applicable sur le lieu du travail (art. 3).

Dans un autre cas plus récent, les juges d'appels avaient constaté que des personnes avait illégalement installé une caméra cachée sur leur balcon afin de filmer leur voiture garée sur la voie publique et qui avait déjà à maintes reprises été endommagées par des inconnus. Les juges d'appels considéraient que l'infraction à la vie privée des passants était assez limitée et que la personne qui avait transpercé les pneus de la voiture n'était que brièvement filmée. Dans ce cas, les juges d'appels avait décidé que la preuve obtenue illégalement ne devait pas être écartées des débats. La Cour de Cassation[372] a approuvé cette décision sur base des critères de sa propre jurisprudence en matière de preuves obtenues illégalement[373]. Notons que la loi du 21 mars 2007 stipule en son article 8 que toute utilisation cachée de caméras de surveillance est interdite.

3. Dans un contexte différent, la Cour de Cassation a de manière assez surprenante décidé que les preuves recueillies devaient être exclues par la simple présence de caméras télévisées alors que les images ainsi filmées n'étaient même pas utilisées comme preuve. La cour a considéré que si la constatation, par des agents compétents de l'autorité, d'une infraction

---

[368] Cass. 27 février 2001, P.99.0706.N., *Juristenkrant,* 2001, n° 25, 1, commentaire R. De Corte, « Cassatie laat verborgen camera toe », *Vigiles* 2001, 153, noot P. De Hert et P. de Hert et S. Gutwirth, « Cassatie en geheime calmera's : meer gaten dan kaas », *Panopticon* 2001, 309-318.

[369] Voir parmi d'autres K. Rosier, « Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée », *RDTI* 2012, n° 48, 127-146; B. Marechal, « La convention collective de travail n° 68 en ce qui concerne la surveillance par caméras sur le lieu de travail » et B. Marechal, « Licéité de la preuve » et K. Rosier, « Réflexions sur les courriers électroniques et les pages web comme éléments de preuve dans la relation de travail », dans K. Rosier (ed.)., *Le droit du travail à l'ère du numérique. Les technologies de l'information et de la communication dans les relations de travail*, Limal, Anthemis, 2011, 455-466 et 467-482 et 483-498; F. Hendrickx, « Privacy op het werk en bewijs van onrechtmatig gedrag: (spookt) antigoon in het arbeidsrecht? », *TSR* 2006, 659-704; F. Hendrickx, *Elektronisch toezicht op het werk: internet en camera's*, dans *Sociale Praktijkstudies*, n° 21, Mechelen, Kluwer, 2005, 197 p. et -, *Surveillance électronique sur le lieu de travail: internet et caméras,* dans *Dossier social*, Bruxelles, Kluwer, 2001, 160 p.; D. Casaer en B. De Bie, « Controlerecht werkgever versus privacy werknemer bij fraude: een praktische benadering », *Or.* 2003, afl. 1, 1-14; P. Humblet, « Het gebruik van video-opnamen als bewijsmiddel: laat honderd bloemen bloeien », *RW* 2004-05, 1187-1189 et – « Geheime camera's en verborgen camera's », *RW* 2001-02, 1172-1173; K. Rosier, « Le cybercontrôle des travailleurs contrôlé par le juge », *Ors.* 2009, afl. 6, 22-26; O. Rijckaert, « Surveillance des travailleurs: nouveaux procédés, multiples contraintes », *Ors.* 2005, numéro spécial, 41-60; K. Rosier et L. Leonard, « La preuve en droit du travail », *Ors.* 2007, afl. 4, 1-17; T. Leonard et K. Rosier, « La jurisprudence 'antigoon' face à la protection des données: salvatrice ou dangereuse? », *RTDI* 2009, n° 36, 5-10; M. Lauvaux, V. Simon et D. Stas de Richelle, *Criminalité au travail. Détecter et contrôler les comportements frauduleux - sanctions et responsabilité du travailleur*, dans *Etudes pratiques de droit social*, n° 2007/1, Waterloo, Kluwer, 2007, 196 p. ; I. Verhelst, et N. Thoelen, « Over privacy, controle en (on)rechtmatig verkregen bewijs », *Or.* 2008, afl. 8, 197-208; S. Cockx, « Sociale media in de arbeidsrelatie: 'vriend' of vijand? », *Or.* 2012, afl. 1, 12-27; D. Dejonghe, « Controle van inhoud van e-mails: is de c.a.o. nr. 81 een maat voor niets? » *Soc.Kron.* 2006, afl. 3, 131-135; P. Culliford, « Telefoongesprekken vanuit de arbeidsplaats: mag de werkgever meeluisteren? », *Or.* 2005, afl. 1, 1-13 .

[370] Cass. 9 juin 2004, P.04.0603.F.; voir L. Delbrouck, « Camerabewaking in het licht van Antigoon », *RABG* 2004, 1083-1089.

[371] Cass. 2 mars 2005, *Pas.* 2005, 505, concl. D. Vandermeersch,, *JT* 2005, 211, *JLMB* 2005, 1086, note M. Beernaert, *RDPC* 2005, 668, note Ch. De Valkeneer, *Journ. proc.* 2005, n° 499, 23, note Ph. Toussaint, Computerr. 2005, 258, note B. Ooms et P. Van Eecke, *Juristenkrant* 2005, n° 112, 1, commentaire R. De Corte, *RABG* 2005, 1161, note S. Berneman, « Is het ontmaskeren van een dief een schending van de privacy waard? » et *Soc.Kron.* 2006, afl. 1, 10, note.

[372] Cass. 5 juin 2012, P.11.2100.N.

[373] Voir aussi Anvers 26 octobre 2005, 453P2005, www.juridat.be et 26 octobre 2005*, T. Strafr.* 2006, 31, note F. Verbruggen.

à la police de la circulation routière sur la voie publique est une ingérence dans l'exercice du droit au respect de la vie privée qui est autorisée par l'article 8, alinéa 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, ce droit est toutefois violé lorsque la constatation de l'infraction à la police de la circulation routière a été réalisée dans une voiture équipée de trois caméras et en présence de tiers incompétents qui font partie d'une maison de production de programmes télévisés et qui, depuis le début, suivaient en "live" tout mouvement, de sorte que la prérogative de la police est ainsi délibérément partagée avec des tiers qui, d'entrée de jeu, étaient impliqués d'une manière active dans la phase initiale de recherche[374]. L'on peut se poser la question si la Cour n'a pas voulu mettre un coup d'arrêt à une certaine « reality tv ». Notons quand même que dans ce cas, la preuve n'était pas obtenue illégalement, mais qu'une illégalité fut commise par un tiers concomitant avec l'obtention de la preuve ou au cours de la procédure avant la phase de l'audience. Dans ce cas, il semble nécessaire de prouver une influence sur les droits de la défense ou du procès équitable.

(5) Les organismes d'application de la loi peuvent-ils ou doivent-ils faire des enregistrements audio-visuels des interrogatoires (de suspects, de témoins)?

La Cour de Cassation avait déjà décidée[375] que les bandes vidéo peuvent être utilisées comme preuve dans un procès pénal[376] et que les auditions peuvent être enregistrées sur bande-son[377]. Pour une réglementation, il fallut attendre la loi du 2 août 2002, qui introduisait en même temps les auditions à distance par vidéo- et visio-conférence (voir ci-dessus partie F). Cette loi fut précédée en 2000 par un autre loi qui avait déjà introduit l'enregistrement d'auditions de mineurs entendus comme victime ou témoin. Récemment, une loi du 30 novembre 2011 a renforcé ce dispositif et est entrée en vigueur le premier janvier 2013.

L'enregistrement de l'audition d'une personne majeur est réglé par les articles 112ter, 158quater et 189 CIC, l'audition des mineurs par les articles 92 à 101 CIC. Nous ne traiterons pas ici de l'auditions des mineurs en détail, mais nous indiquerons les grandes différences par rapport à l'audition des adultes.

Notons que l'enregistrement des auditions d'adultes n'est pas un automatisme en Belgique, mais facultatif pour les adultes. L'on peut même constater que l'enregistrement est même peu appliqué. Les milieux policiers y sont majoritairement fort hostiles[378].

L'article 112ter, § 1 CIC dispose que sans préjudice des dispositions des articles 92 à 103, le procureur du Roi ou le juge d'instruction peut ordonner l'enregistrement audiovisuel ou audio d'une audition. La personne à entendre est préalablement mise au courant de cette décision.

Les enregistrements se font sur cassettes[379]. Juridiquement, il n'y a pas de raison de distinguer l'enregistrement d'audition et l'audition avec enregistrement et analyse des comportements[380].

Les cassettes pourront être entendues ou visionnées à l'audience. Ce qui équivaut à la lecture d'un procès-verbal contenant les déclarations du témoin ou du suspect (voir aussi l'article 191 CIC). Ceci ne remplace cependant pas l'audition du témoin ou l'interrogatoire du suspect à l'audience, bien que ceux-ci sont facultatifs (voir l'article 191 CIC[381]).

Autorités compétentes. Le procureur du Roi ou le juge d'instruction décide de faire enregistrer les auditions. Sur réquisition motivée, le tribunal de police ou correctionnel peut aussi l'ordonner[382]. Le juge n'a donc aucune compétence de l'ordonner de sa propre initiative[383]. L'idée est que cet enregistrement pourra être utilisé en appel. C'est pour cette raison, que le législateur ne l'a pas prévu pour la Cour d'Appel ou la Cour d'Assises[384]. La doctrine pense qu'il n'y a cependant aucune interdiction pour la Cour d'Appel de l'ordonner[385].

---

[374] Cass. 8 novembre 2005, P.05.1106.N.; dans un autre cas Bruxelles 31 juillet 2007, *Juristenkrant* 2007, n° 153, 8, avec le commentaire de F. Schuermans, « Bolletjesslikker ontspringt dans door aanwezigheid camera » ; dans l'autre sens Cass. 21 novembre 2006, P.06.0806.N et Corr. Termonde 29 mars 2006, *Juristenkrant* 2007, n° 141, 6, avec le commentaire de F. Schuermans, « Niet alle strafrechters hebben problemen met reality tv ».

[375] Voir D. Van Daele, « Het afnemen van verklaringen met behulp van audiovisuele media : een commentaar bij de wet van 2 augustus 2002 », *T. Strafr.* 2003, 46.

[376] Cass. 21 mai 1962, *Pas.* 196, I, 1073.

[377] Cass. 17 août 1979, *AC* 178-79, 1341 et *JT* 1980, 104, note S. Nudelhole.

[378] Voir F. Goossens, « De audiovisuele registratie van het verhoor van meerderjarigen tijdens het onderzoek in strafzaken : van een wettelijke mogelijkheid naar een wettelijke verplichting? » et la réaction de P. Van Santvliet, « Enkele bedenkingen » et dans le sens opposée R. Horselenberg, « Voorkom gerechtelijke dwalingen : neem verdachtenverhoor op video op », *Orde van de dag* 2009, n° 45, 5-15, 41-42 et 43-46.

[379] D. Van Daele, *l.c.,* 47; voir L. François, « Videoverhoren », *Postal Memorialis,* Mechelen, Kluwer, 2011, 26 p.

[380] D. Van Daele, *l.c.,* 48; comparez M. Bockstaele, « Verhoren: audiovisueel verhoren van volwassenen », *Comm. Sr. en Sv.,*Mechelen, Kluwer, 2008, 3.

[381] Voir D. De Wolf, *De rol van de rechter … , o.c.,* 210-211 et 230-233.

[382] D. Van Daele, *l.c.,* 47.

[383] D. De Wolf, *De rol van de rechter …. , o.c.,* 121-122.

[384] D. Van Daele, *l.c.,* 48. Notons qu'en Belgique il n'y a pas de possibilité d'appel contre les décisions des Cours d'Assises.

[385] D. Van Daele, *l.c.,* 48.

Conditions. Il n'y a aucune condition. Elle n'est pas subordonnée à une suspicion concernant des faits d'une certaine gravité ou à des circonstances exceptionnelles[386]. La personne auditionnée est avertie, mais son consentement n'est pas requis[387].

Objet de l'enregistrement. L'objet de l'enregistrement sont les auditions. Il peut aussi bien s'agir d'auditions de victimes ou de témoins et témoins anonymes, que de suspects[388].

Exécution de la mesure. L'article 112ter, § 2 CIC stipule que l'audition enregistrée est effectuée par le procureur du Roi ou le juge d'instruction, selon le cas, ou par un fonctionnaire de police nominativement désigné par lui.

Si l'audition est effectuée par un tribunal, ce rôle incombera au président de la juridiction[389].

Rapportage. L'article 112ter, § 3 CIC stipule que le procureur du Roi ou le juge d'instruction dresse un procès-verbal de l'audition, dans lequel il reprend, sans préjudice des droits prévus à l'article 47bis, les principaux éléments de l'entretien et éventuellement une retranscription des passages les plus significatifs. Il est également fait mention dans le procès-verbal des motifs pour lesquels l'enregistrement audiovisuel ou audio a été ordonné.

Au cas où une juridiction l'ordonne, cette formalité sera remplie par les inscriptions au procès-verbal d'audience[390].

Sans préjudice de l'application de l'article 47bis, il est procédé, à la demande du juge d'instruction, du procureur du Roi, de la personne entendue ou des parties au procès, à la retranscription intégrale et littérale des parties additionnelles de l'audition qu'ils désignent. Elle est versée au dossier dans les plus brefs délais (§ 4).

Cette transcription n'est donc pas automatiquement prévue. La raison pour cela est que la mesure est prévue pour l'observation du comportement de la personne auditionnée, ce qui est difficilement réalisable par écrit[391]. Il faudra cependant, même si le texte ne le prévoit pas explicitement, transcrire intégralement, ce qui comporte aussi les pauses et incidents. La surcharge de travail qu'impliquent les transcriptions font que dans la pratique l'application de la mesure s'en trouve refrénée[392].

L'enregistrement de l'audition est réalisé en deux exemplaires. Les deux cassettes ont le statut d'originaux et sont déposées au greffe à titre de pièces à conviction (§ 5). L'enregistrement ne peut être visionné ou écouté que par des personnes qui participent professionnellement à l'information, à l'instruction ou au jugement dans le cadre du dossier judiciaire, ainsi que par les parties au procès et par la personne entendue. L'inculpé non détenu et la partie civile peuvent introduire une demande en ce sens auprès du juge d'instruction conformément à l'article 61ter. Toutes les parties ont le droit de visionner ou, selon le cas, d'écouter l'enregistrement après que le procureur du Roi ait pris des réquisitions en vue du règlement de la procédure, conformément à l'article 127,§ 1 CIC.

Les cassettes sont tantôt considérées comme des pièces à convictions, tantôt comme des pièces du dossier, ce qui est attesté par la possibilité de demander une copie par le biais de la requête au sens de l'article 61ter CIC. La destruction des casettes n'est pas prévue, elles seront donc archivées comme des pièces d'un dossier pénal[393]. Bien que le visionnage des cassettes est prévu par l'article, le matériel pour ce faire manque dans beaucoup de greffes.

Pour l'application de l'article 341 (ancien) CIC, l'enregistrement de l'audition d'un témoin est assimilé à une déclaration écrite (§ 7).

Auditions des mineurs[394]. *Différences*. Pour certaines infractions, l'enregistrement est obligatoire, sauf décision contraire motivée prise par le procureur du Roi ou le juge d'instruction tenant compte des circonstances propres à l'affaire et dans l'intérêt du mineur. Pour d'autres infractions il est facultatif comme pour les adultes. Dans tous les cas, le consentement est nécessaire si le mineur a plus de 12 ans. Sauf pour certaines infractions (la liste ici est différente), des raisons de circonstances graves et exceptionnelles sont nécessaires pour pouvoir ordonner la mesure. Il s'agit d'auditions de mineurs comme victimes ou témoins. On prendra des mesures d'accompagnement pendant l'audition (voir article 94 et 95 CIC). Le procès-verbal de l'audition doit être rédigé dans les 48 heures. Ici l'audition ou le visionnage remplace l'audition du mineur à l'audience. Toutefois, lorsqu'elle estime la comparution du mineur nécessaire à la manifestation de la vérité, la juridiction de jugement peut l'ordonner par une décision motivée (art. 100 CIC). Les cassettes peuvent être détruites sur décision de la juridiction de jugement (art 101 CIC).

E. TIC et preuves.

Avant d'entamer ce chapitre, il nous semble opportun de tracer en grandes lignes les principes du droit belge de la preuve en matière pénale.

---

386 D. Van Daele, *l.c.,* 48.
387 D. Van Daele, *l.c.,* 48.
388 D. Van Daele, *l.c.,* 48.
389 D. Van Daele, *l.c.,* 49.
390 D. Van Daele, *l.c.,* 49.
391 Voir D. Van Daele, *l.c.,* 49.
392 Voir L. François, « Videoverhoren in de praktijk », *Orde van de dag* 2009, n° 45, (29), 31.
393 D. Van Daele, *l.c.,* 51.
394 Voir B. De Smet, « Verhoren : audiovisueel verhoor van minderjarigen », in Comm. Strafr en Sv., Mechelen, Kluwer, 2012, 8 p.

On peut aborder la matière par ordre thématique, comme la charge de la preuve, la liberté des preuves, les moyens de preuves[395], ou par différentes questions, comme qui doit prouver, quels moyens de preuves et quelle force à accorder aux preuves[396]. Pour les sujets traités dans ce rapport, nous nous bornerons ici à désigner les grands principes du droit belge de la preuve en matière pénale[397].

La charge de la preuve. Ceci concerne la désignation de la partie dans le procès pénal qui devra apporter et prouver les faits et les circonstances. Il s'agit ici de la charge de la preuve au sens formel. C'est en ce sens-là que l'on comprend la charge de la preuve en Belgique[398]. Suivant un principe général de droit, la charge de la preuve incombe à la partie poursuivante, c'est-à-dire le ministère public, la partie civile ou le cas échéant l'administration[399]. Il n'y a pas de répartition de la charge[400]. Le suspect ne doit rien prouver[401] et peut se cantonner dans un rôle purement passif[402]. Il faut prouver la culpabilité, non pas l'innocence[403]. En plus, le doute profite à l'accusé, ce qui se traduit par l'adage Latin, *in dubbio pro reo.* L'exception à ces règles, est la preuve des causes de justification. La jurisprudence constante exige que lorsqu'un prévenu invoque une cause de justification, qu'il rende son allégation non dépourvue de tout élément de nature à lui donner crédit. Il incombe ensuite à la partie poursuivante (ministère publique ou administration) ou, le cas échéant, à la partie civile, de prouver que cette allégation est inexacte[404]. Premièrement, il faut souligner que ces règles sont d'ordre public et ne peuvent pas faire l'objet d'un accord entre parties. Deuxièmement, il n'existe aucune règle de renversement de la charge de la preuve, bien que la preuve des causes de justification y font penser.

On peut discerner quelques atténuations concernant le principe de la charge de la preuve : le rôle actif du juge pénal, le risque de la preuve et les données d'expérience notoire. Certains auteurs signalent aussi des atténuations ou entorses au principe, notamment en matière du droit des douanes et accises, droit de la circulation routière et concernant certaines formes de confiscation des avoirs[405].

Concernant le rôle actif du juge, l'on pourra noter qu'en principe un rôle actif est attribué au juge pénal, mais que ce rôle n'a qu'un caractère facultatif. Dans la procédure correctionnelle - la procédure sans jurés – les pouvoirs du juge sont fort limités. Par exemple, un supplément d'information n'est pas possible, ni l'audition de témoins sans l'assistance et donc l'accord des parties[406].

L'appréciation de la valeur probante de la preuve. La valeur probante est la mesure dans laquelle la foi doit être accordée à un élément de preuve. Il s'agit de la mesure dans laquelle quelque chose apporte la preuve d'un fait[407].

La règle générale en droit belge est que l'appréciation de la preuve par le juge pénal est libre. C'est en fait un corollaire de la liberté de la preuve. Le juge n'est d'aucune manière lié par les éléments que les parties souhaiteraient lui soumettent[408]. Selon la Cour de Cassation, le juge est libre d'apprécier les éléments sur lesquels il se fonde pour fonder sa conviction[409], sauf si la loi prescrit certaines règles spécifiques[410]. Compte tenu que le tribunal jugera en fait, cette appréciation reste souveraine, à l'exception encore une fois des règles spécifiques prévues par la loi[411]. Il découle de ces principes, qu'il n'y a pas d'hiérarchie de la preuve, que le juge n'est pas obligé de préférer une preuve à une autre, qu'il est libre de faire une sélection parmi les éléments de preuve, que le juge peut accepter des éléments fournis par une partie civile, que le juge ne doit pas se montrer méfiant devant certaines preuves et que l'appréciation n'est pas soumise à certaines règles scientifiques. Cependant la liberté ne correspond pas à l'arbitraire[412].

Il existe quelques exceptions à la règle de la libre appréciation (de la force probante) de la preuve : les procès-verbaux ayant une force probante particulière, la condamnation reposant uniquement ou de manière décisive sur certains éléments de preuves (témoins anonymes, informations déclassifiées, Salduz), preuve par vidéo-conférence. Le § 6 de l'article 158bis du

---

395 Voir R. Declercq, *Eléments de procédure pénale,* Bruxelles, Bruylant, 2006, 801 et seq.
396 En ce sens H.D. Bosly, D. Vandermeersch en M.-A. Beernaert, *Droit de la procédure pénale,* Bruxelles, La Charte, 2010, 989 et seq.
397 Concernant le droit de la preuve en matière pénal voir Ch. Van den Wyngaert et H.D. Bosly, « La preuve. Belgique », *RIDP* 1992, 105-116; P.E. Trousse, « La preuve des infractions », *RDP* 1958-59, 731-766.
398 Voir Ph. Traest, *Het bewijs in strafzaken*, Gent, Mys & Breesch, 1992, n° 330.
399 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* 990 .
400 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* 989.
401 Ph. Traest, *o.c.,* n° 337; voir aussi Cass. 22 april 2008, P.08.0087.N.
402 H.D. Bosly, D. Vandermeersch et M.-A. Beernaert, *o.c.,* 990.
403 R. Declercq, *Beginselen van strafrechtspleging,* Mechelen, Kluwer, 2010, n° 1956.
404 Voir par exemple: Cass. 4 janvier 1994, *Pas.* 1994, 6; voir R. Declercq, *Eléments de procédure pénale, o.c.,* 811-815.
405 Voir H.D. Bosly, D. Vandermeersch en M.-A. Beernaert, *o.c.,* 994-998.
406 Voir in extenso D. De Wolf, *De rol van de rechter in de correctionele procedure bij de waarheidsvinding,* Heule/Brugge, UGA/Die Keure, 2010, 713.
407 Voir F. Deruyck, *Strafprocesrecht,* Brussel, VUB-Uitgaven, 2008, 187.
408 R. Declercq, *Beginselen van strafrechtspleging, o.c.,* n° 2000.
409 Cass. 6 mars 1973, *AC* 1973, 658; 5 novembre 1973, *AC* 1974, 261.
410 Cass. 6 septembre 1971, *Pas.* 1972, I, 12.
411 Cass. 20 décembre 2000, *AC* 2000, 713; 27 février 2002, P.02.0072.F; 31 octobre 2006, P.06.0927.N.
412 Voir D. De Wolf, *Syllabus bijzondere vraagstukken van het strafprocesrecht*, Brussel, VUB-Uitgaven, 2013, 167-169.

CIC stipule que sur réquisition motivée du procureur du Roi, le tribunal peut décider d'autoriser l'altération de l'image et de la voix. Dans ce cas, les déclarations faites par le biais d'une vidéoconférence ou d'un circuit de télévision fermé ne peuvent être prise en considération à titre de preuve que si elles sont corroborées dans une mesure déterminante par d'autres moyens de preuve.

Le juge obtient sa décision de condamnation par intime conviction. Aussi bien en matière correctionnelle, qu'en cour d'assises, l'intime conviction est raisonnée puisque le tribunal ou la cour doivent motiver leur décision[413].

Signalons qu'il existe une différence entre la valeur probante de la preuve et la foi due à l'acte. Ceci exprime le respect à l'égard de la chose écrite. Le juge fait mentir l'acte en cas de non-respect[414].

La liberté de la preuve. En Belgique, la preuve est libre. Sauf quelques exceptions, ceci veut dire que la preuve d'un crime ou délit peut être apportée par tout moyen légal. En d'autres termes, tous les éléments sont potentiellement des preuves d'un crime ou d'un délit. En outre, le juge n'est pas lié par certaines catégories formelles de la preuve comme les témoignages, les expertises, les aveux. Chaque élément de preuve peut livrer une preuve dans la mesure où le juge en obtient l'intime conviction. Pour cette raison, la liberté de la preuve est aussi liée au système de la conviction intime. Le juge n'est lié par aucune preuve. Il juge selon sa conviction intime[415]. Il en résulte par exemple que la preuve du taux d'alcoolémie peut être prouvé par tout élément et ne doit pas nécessairement être prouvé par une analyse de l'haleine ou un examen sanguin[416], même si ces mesures sont réglementées.

Ici aussi, il existe des exceptions, les incidents ou exceptions préjudicielles.

L'admissibilité de la preuve. On peut faire la distinction entre l'inadmissibilité propre (le témoignage d'un mineur de moins de 15 ans ou sous certains conditions par des proches), la preuve illégale (le non-respect des règles de contradiction devant le juge) et la preuve obtenue illégalement.

La preuve obtenue illégalement peut être définie par la preuve obtenue en violation du droit, ce qui est une définition fort large. Depuis 2003, la jurisprudence n'accepte que dans un nombre de cas limités l'exclusion de la preuve obtenue illégalement. La pratique est bien plus nuancée. Nous devons ici nous limiter aux règles générales. Comme nous l'avons déjà indiqué précédemment, la Cour de Cassation a jugé sur le point de la sanction de preuve obtenue illégalement, que la circonstance qu'un élément de preuve a été obtenu illicitement a en principe pour seule conséquence que le juge ne peut prendre ni directement ni indirectement cet élément en considération lorsqu'il forme sa conviction:

- soit lorsque le respect de certaines conditions de forme est prescrit à peine de nullité;

- soit lorsque l'irrégularité commise a entaché la crédibilité (fiabilité) de la preuve;

- soit lorsque l'usage de la preuve est contraire au droit à un procès équitable[417].

(1) Y a-t-il des règles en matière de preuve qui sont spécifiques aux TIC liées à l'information?

Non, en règle générale. La loi du 28 novembre 2000 n'a rien changé en matière de preuve. En plus, la jurisprudence ne connaît pas d'exceptions spécifiques pour la preuve « digitale » (« digital evidence »)[418]. La liberté de la preuve et la libre appréciation restent intactes. Les cassettes vidéos[419] ou les supports digitaux ou les images digitales seront acceptés sans aucun problème comme possible preuve. La Cour de Cassation jugeait ainsi que, puisque la loi sur la sécurité lors des matches de football, pour des faits punis par une sanction administrative, n'impose aucune preuve particulière, la preuve des faits peut être livrée par tous les moyens de preuve soumis à la contradiction des parties en dont le juge apprécie souverainement la valeur probante ; il ne peut pas être déduit du fait que les images d'une vidéo, qui peuvent fournir la preuve des actes punis, proviennent d'un site web, qu'il s'agit d'une preuve illégale, qui violerait le respect de la vie privée ou droits de la défense des personnes concernées[420].

Rappelons quand même la règle, assez surprenante, en matière d'auditions par vidéo-conférence et par circuit de télévision fermé, où la libre appréciation de la preuve par le juge se voit limitée en cas d'altération de l'image et de la voix. En cas de déclarations faites par le biais d'une conférence téléphonique cette règle s'applique même sans altération de la voix.

---

413 Voir Ph. Traest, "Hard bewijs: wanneer is een rechter overtuigd?", in BLUS, *Bewijs in strafzaken,* Dossiers RDP, Bruxelles, Die Keure, 2011, (59), 69.
414 Voir D. De Wolf, *Syllabus bijzondere vraagstukken van het strafprocesrecht*, Brussel, VUB-Uitgaven, 2013, 179.
415 R. Declercq, *Beginselen van strafrechtspleging, o.c.,* n° 2004, p. 886-887 et nos 2005-2007.
416 Cass. 19 juin 1990, *AC* 1989-90, n° 609; 26 novembre 2008, *AC* 2008, n° 672.
417 Cass. 14 octobre 2003, *RW* 2003-04, 67 avec les conclusions du procureur-général M. De Swaef et observations D. De Wolf, *RW* 2003-04, 1235-1239; voir aussi A. Masset, « Les preuves illégales et irrégulières en matière pénale : 8 ans d'application du test Antigone », dans UBLDP, *La preuve en droit pénal,* Dossiers RDPC, Brussel, La Charte, 2011, 1-35.
418 Ch. Meunier, l.c., (2001),651; Y. Poullet, « A propos du projet de loi dit n° 21. La lutte de la criminalité dans le cyberspace à l'épreuve du principe de régularité des preuves », in X., *Liber amicorum Jean du Jardin,* Deurne, Kluwer, 2001, 13.
419 En dehors des exemples cité dans la question D.4, on citera Gand 6 février 1992, *TGR* 1992, 65; Corr. Bruxelles 31 décembre 1996, *Journ. Proc*. 1997, n° 328, p. 30.
420 Cass. 4 novembre 2010, C.10.0078.F..

(2) Y a-t-il des règles sur l'intégrité (par exemple : falsification ou traitement inadéquat) et la sécurité (par exemple : le piratage) des TIC liées à la preuve?

Les règles en matière d'écoutes de communications comprennent des garanties contre la falsification (voir question D.1.b). Les obligations de opérateurs et fournisseurs ont parfois rapport à la conservation et la disponibilité des données sur des supports compatibles (voir question D.3.).

C'est surtout en matière d'image vidéo que certains juges se sont montrés fort réticents[421], craignant des possibilités de manipulation par les parties (jurisprudence en matière civile ou sociale[422]) ou jugeant que les images ne fournissaient pas de preuves convaincantes. Le tribunal correctionnel d'Anvers a par exemple jugé qu'un montage d'images de télévision prises par une caméra cachée ne garantit pas la véracité en n'a donc pas de force probante pour les infractions d'outrage aux mœurs, la tenue d'une maison de débauche et l'incitation à la débauche[423].

On peut penser qu'il s'agit de juges avec peu d'expérience en matière de TIC. On manque cruellement de jugements des tribunaux et cours publiés ou d'arrêts de la Cour de Cassation en cette matière. On pourra aussi se demander si le rôle actif du juge ne l'oblige pas à lever le doute avant d'exclure la preuve digitale. Nous avons indiqué ci-dessus que le rôle actif du juge n'est que facultatif. Si le juge pense qu'il pourrait y avoir une manipulation ou que les images sont trop floues, ne devrait-il dans ce cas pas ordonner une expertise pour vérifier d'un point de vue technique la véracité ou la manipulation des images ou pour faire améliorer la qualité des images ? (voir aussi question F.4).

Il n'existe pas de règles spécifiques concernant le piratage de preuves.

(3) Y a-t-il des règles sur la recevabilité (y compris le principe de la légalité procédurale) des éléments de preuve qui sont spécifiques aux TIC liés à l'information?

Non, les règles générales s'appliquent. Voir la partie D où sont repris nombre d'exemples. On notera que la jurisprudence belge semble apporter peu d'intérêt à la légalité de la preuve, puisque sauf les quelques règles prescrites à peine de nullité (on citera à nouveau les écoutes de télécommunications), la violation de la loi restera le plus souvent sans effet.

(4) Y a-t-il des règles spécifiques sur la découverte et la divulgation de la preuve liée aux TIC?

On pourrait dire que le législateur prend plus de soins à régler la collecte des preuves digitales, mais on est loin des preuves génétiques ou de l'analyse sanguine en matière de roulage. Si des règles existent, elles sont soit en rapport à la découverte ou à la conservation pour des raisons techniques, soit elles entourent de plus de garanties l'administration de la preuve vu l'impact sur la vie privée.

Concernant la divulgation, l'on pourra citer les règles à propos des possibilités pour les parties de prendre connaissance des bandes sons, supports ou vidéos originaux. La Cour d'appel d'Anvers a jugé que le fait que les bandes son d'un enregistrement sonore étaient déposées au greffe et transcrites dans un procès-verbal permettaient les parties d'exercer les droits de la défense[424]. La jurisprudence ne fait cependant aucune différence entre la présentation de la preuve digitale sur son support original, transcrite ou décrite ou non dans un procès-verbal ou des preuves sous forme de données imprimées. Signalons que le droit belge ne connaît pas de principe d'immédiateté de la preuve ni l'exclusion ou la limitation des preuves par ouï-dire.

(5) Y a-t-il des règles particulières d'évaluation (valeur probante) des preuves liées aux TIC?

Non, l'appréciation de la preuve reste intacte. Rappelons quand même les réticences de la jurisprudence en matière de preuves digitales pour des raisons de manipulation ou de mauvaise visibilité due à une mauvaise qualité d'images ou par l'angle de vue.

(F) Les TIC dans les étapes du procès

(1) Comment les preuves liées aux TIC peuvent-elles ou doivent-elles être introduites dans le procès?

Il n'y a aucune règle spécifique en la matière. Rappelons que la preuve peut être livrée par le support digital avec ou sans transcription dans un procès-verbal ou sous formes de données imprimées (voir question D.4).

(2) Peut-on faire des interrogatoires à distance (par exemple par liaison satellite)?

Oui, les interrogatoires et auditions à distance sont possibles. Par distance, il peut s'agir de quelqu'un qui se trouve dans une autre pièce voisine, dans un autre bâtiment dans le pays ou même quelqu'un qui se trouve dans un autre pays[425].

---

421 Voir M. Franchimont, A. Jacobs et A. Masset, *o.c.,*1016, note 91 et J. Simons, « Photographie, cinéma et télévision : l'avenir de la preuve par image », *JT* 1988, 613-617.

422 Dans le même sens M. Franchimont, A. Jacobs et A. Masset, *o.c.*, (2006),1016, note 91, in fine.

423 Corr. Antwerpen 25 oktober 2004, AM 2005, 170.

424 Anvers 26 octobre 2005, 453P2005, www.juridat.be.

425 Voir D. Van Daele, « Het afnemen van verklaringen met behulp van audiovisuele media : een commentaar bij de wet van 2 augustus 2002 », *T. Strafr.* 2003, 53; voir aussi M. Bockstaele, « Verhoren : video, telefoonconferentie en gesloten telivisiecircuit », *Comm. Sr. en Sv.,* Mechelen, Kluwer, 2010, 23 p.

L'audition ou l'interrogatoire à distance est possible par vidéoconférence, par circuit de télévision fermé ou par téléconférence.

Le procureur du Roi ou le juge d'instruction peut décider d'entendre par le biais d'une *vidéoconférence* un témoin menacé (voir article 102 CIC), à qui la Commission de protection des témoins a octroyé une mesure de protection, ou un témoin, un expert ou une personne soupçonnée résidant à l'étranger lorsque la réciprocité en la matière est garantie, avec son accord, s'il n'est pas souhaitable ou possible que la personne à entendre comparaisse en personne (art. 112, § 1 CIC). En cas de réquisition du parquet, cette mesure peut aussi être ordonnée par le tribunal de police, le tribunal correctionnel, la Cour d'Appel ou la Cour d'Assises (art. 158bis, § 1, 189, 211, 317quater (ancien) CIC). Mais par cette mesure, il n'est pas possible d'interroger un suspect[426]. La force probante reste la même que dans le cadre d'un témoignage classique[427]. Notons cependant que la libre appréciation de la preuve par le juge se voit limitée en cas d'altération de l'image et de la voix (art. 189 CIC). Cette mesure ne permet pas l'audition d'un témoin anonyme complet, mais l'article 86ter CIC permet l'audition par télécommunication spécifique.

Le procureur du Roi ou le juge d'instruction peut décider d'entendre par le biais d'un *circuit de télévision fermé* un témoin menacé, à qui la Commission de protection des témoins a octroyé une mesure de protection, avec son accord, s'il n'est pas souhaitable ou possible que la personne à entendre comparaisse en personne (art. 112, § 2 CIC). Par le caractère technique de cette mesure elle n'est pas applicable pour des personnes qui se trouvent à l'étranger. Pour le reste, les mêmes règles s'appliquent qu'en vidéoconférence.

Le procureur du Roi ou le juge d'instruction peut décider d'entendre par le biais d'une *conférence téléphonique* un témoin menacé, à qui la Commission de protection des témoins a octroyé une mesure de protection, ou un témoin ou un expert résidant à l'étranger lorsque la réciprocité en la matière est garantie, avec son accord, s'il n'est pas souhaitable ou possible que la personne à entendre comparaisse en personne ou qu'elle soit entendue par le biais d'une vidéoconférence ou d'un circuit de télévision fermé (art. 112bis, § 1 CIC).

La juridiction de jugement ne peut prendre en considération à titre de preuve les déclarations faites par le biais d'une conférence téléphonique que si elles sont corroborées dans une mesure déterminante par d'autres moyens de preuve (art. 112bis, § 6 CIC). Par ailleurs, les mêmes règles s'appliques qu'en vidéoconférence.

Près de la personne à entendre se trouve un officier de police judiciaire ou un fonctionnaire de police, nominativement désigné par le procureur du Roi ou le juge d'instruction, ou, lorsque la personne à entendre se trouve à l'étranger, une autorité judiciaire étrangère. Cette personne vérifie l'identité de la personne à entendre et en dresse un procès-verbal qui est signé par la personne à entendre.

Le procureur du Roi ou le juge d'instruction dresse un procès-verbal de l'audition, dans lequel il reprend, sans préjudice des droits prévus à l'article 47bis, les principaux éléments de l'entretien et éventuellement une retranscription des passages les plus significatifs. Il est également fait mention dans le procès-verbal des motifs pour lesquels il a été décidé d'entendre l'intéressé à distance.

L'audition fait toujours l'objet d'un enregistrement audio au sens de l'article 112ter.

(3) Peut-on utiliser des techniques numériques et virtuelles pour la reconstitution d'événements (meurtres, accidents de la circulation)?

Oui, des logiciels existent en la matière. Les experts judiciaires ou des parties peuvent les utiliser et les incorporer dans leur rapport d'expertise.

(4) Peut-on utiliser les techniques audio-visuelles pour présenter des preuves lors du procès (dans sa forme la plus simple: images et sons)?

Oui, la liberté de la preuve le permet. L'article 191 CIC stipule d'ailleurs que les pièces à convictions peuvent être montrées aux parties et aux témoins. Une application de ce principe est que le tribunal correctionnel peut visionner un film (la reconstruction d'un meurtre) à l'audience, ou si besoin est, dans une salle équipée, pourvu que les règles en matière de publicité de l'audience soient respectées[428].

Signalons aussi que la Cour de Cassation a jugé que le juge qui, même en présence de procès-verbaux qui décrivaient des cassettes pornographiques, acquitte un prévenu sous prétexte que les parties n'avaient pas livré d'appareils pour visionner ces cassettes, manque à son obligation d'information. Quand les éléments de preuves ne permettent pas d'arriver à une décision justifiable, le juge a vu son rôle actif l'obligation d'utiliser son droit d'initiative[429]. Notons que dans d'autres arrêts, la Cour n'est plus allée aussi loin. Dans l'état actuel, l'on ne pourra donc parler que d'un rôle actif facultatif, mais il restera que le juge ne pourra pas se cacher derrière l'absence de matériel quand il juge que le visionnage des preuves s'impose.

---

[426] D. Van Daele, *l.c.,* 54.
[427] D. Van Daele, *l.c.,* 54-55.
[428] Cass. 21 mai 1962, *Pas.* 1962, I, 1073.
[429] Cass. 23 novembre 1993, *AC* 1993, 981et *RW* 1993-94, 1053.

(5) Les casiers judiciaires sur papier peuvent-ils être remplacés par des casiers judiciaires électroniques? Y a-t-il une évolution vers l'informatisation du déroulement du procès?

a) Le casier judiciaire

L'article 589 CIC stipule que le Casier judiciaire central est un système de traitement automatisé tenu sous l'autorité du Ministre de la Justice, qui assure, conformément aux dispositions du présent chapitre, l'enregistrement, la conservation et la modification des données concernant les décisions rendues en matière pénale et de défense sociale.

La finalité du Casier judiciaire est la communication des renseignements qui y sont enregistrés :

1° aux autorités chargées de l'exécution des missions judiciaires en matière pénale;

2° aux autorités administratives afin d'appliquer des dispositions nécessitant la connaissance du passé judiciaire des personnes concernées par des mesures administratives;

3° aux particuliers lorsqu'ils doivent produire un extrait de Casier judiciaire;

4° aux autorités étrangères dans les cas prévus par des conventions internationales.

L'enregistrement des informations est effectué par les greffes des cours et tribunaux ou par le service du Casier judiciaire du Ministère de la Justice.

En application de l'article 8, § 1er de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ces informations peuvent servir de base à des statistiques établies et diffusées à l'initiative du Ministère de la Justice.

L'article 590 CIC y ajoute que pour chaque personne, le Casier judiciaire enregistre les peines et mesures imposées ainsi que les cas de réhabilitation, de libération conditionnelle, les arrêtés de grâce, les décisions d'amnistie, les arrêts d'annulation et décisions de rétractation. Les greffiers transmettent au Casier judiciaire ces décisions dans les trois jours qui suivent celui où celles-ci sont passées en force de chose jugée. Ils sont responsables de la conformité des informations transmises aux décisions rendues par les juridictions (art. 592 CIC). Aujourd'hui l'encodage des données se fait toujours en partie manuellement. D'autres données peuvent être transférées par voie électronique[430]. L'interconnection avec le « casier » communal et les données des tribunaux de polices est assez problématique pour des raisons techniques. En plus, le SFJustice accuse d'importants retards dans l'encodage[431] (voir aussi l'article 10 de la loi du 31 juillet modifié par la loi du 31 décembre 2012).

L'accès au Casier par les utilisateurs est graduel selon l'appartenance à une des trois catégories de personnes suivantes. Par ordre décroissant, l'accès sera plus limité pour les magistrats et policiers, autorités publiques et particuliers. Ces limitations se traduisent par le non-accès à certaines données[432]. L'article 593 CIC règle l'accès des magistrats, policiers et certains fonctionnaires au casier, sauf en ce qui concerne les faits amnistiés ou qui ont rapport à des incriminations supprimées, des décisions annulées ou rétractées. Ces personnes ainsi que les greffiers ont pour cette finalité également accès au Registre National. Ces autorités sont autorisées à utiliser le numéro d'identification au Registre national des personnes physiques à seule fin d'identification des personnes inscrites dans le Casier judiciaire (art. 591 CIC).

Les autorités publiques peuvent par arrêté Royal avoir accès au Casier, mais la liste des décisions qui sont exclues est plus longue (art. 594 CIC). Cette disposition a été annulée par la Cour Constitutionnelle[433].

Les articles 595 et 596 CIC règlent l'obtention d'un extrait par les simples citoyens. Cette législation a connu de sérieux déboires que nous ne détaillerons pas ici[434]. Les renseignements enregistrés dans le Casier judiciaire au sujet de personnes décédées sont transmis une fois par an aux Archives générales du Royaume (art. 598 CIC).

Les informations communiquées par le Casier judiciaire ne constituent pas la preuve des décisions judiciaires ou administratives auxquelles elles se rapportent (art. 600 CIC)[435].

b) L'informatisation de la justice – du déroulement de la procédure pénale

La loi du 10 juillet 2006 relative à la procédure par voie électronique règle cette question. Voulue comme le volet législatif du projet dit « Phenix », le but était d'introduire les TIC dans la procédure civile et pénale en fonction de l'avancement du projet[436]. Comme signalé ci-dessus – voir question B.2. – ce projet n'a pas abouti. De plus, cette loi du 10 juillet 2006 est

[430] Voir S. De Decker, « Art. 592 », dans M. De Busscher, J. Meese, D. Van Der Kelen, J. Verbist (ed.), *Larcier Wet & Duiding Strafprocesrecht*, Brussel, Larcier, 2013, 548.
[431] S. De Decker, « Art. 590-596 », *o.c.,* 547 et 551.
[432] Voir S. De Decker, « Art. 593-596 », *o.c.,* 548-552.
[433] CC 22 août 2011, n° 137/2011.
[434] P. Dhaeyer, « La saga du casier judiciaire », *JT* 2006, 398-399 ; V. Seron, « La fin du certificat de bonnes conduite, vie et mœurs : chronique d'une mort annoncée », *RDPC* 2007, 634-652.
[435] Voir Cass. 19 octobre 2005, P.05.1041.F., avec les conclusions de l'avocat-général D. Vandermeersch.
[436] Doc. Parl., Chambre 2004-2005, n° 51-1701/001, p. 5.

une des plus curieuses. Pour le volet pénal, le principe est le « tout papier ou tout électronique »[437]. L'inventaire sera cependant toujours électronique (art. 29, § 1), ce qui permet des changement faciles ... La pièce électronique équivaut à la pièce sur papier. Ce qui veut dire que l'option de base est soit de décider pour une procédure sur support électronique, soit d'opter pour une procédure sur papier. L'on ne pourra pas avoir de dossier sur papier avec quelque pièces électroniques, ni– et ceci est fort dangereux dans une première phase d'introduction des TIC – un dossier électronique avec une copie sur papier. Ceci évitera les problèmes selon le législateur en matière pénale ...

C'est le procureur du Roi - ou autres magistrats du parquet - qui « dans la phase transitoire » décidera de la voie électronique ou pas (art. 30) [438] … Mais dans le cas d'une enquête, le juge d'instruction pourra en décider autrement. Dans ce cas, le dossier sur papier devra être transféré sur support électronique ou vice versa[439]. De plus, les parties qui ne disposent pas d'un ordinateur pourront toujours recevoir un extrait sur papier (art. 4). Selon le législateur, le principe « tout papier ou tout électronique » n'est pas incompatible avec cela[440] ….

Dans le cas d'une procédure par voie électronique, la logique du législateur nous laisse parfois perplexe, puisque les avantages du TIC ne sont même pas utilisés. L'introduction des TIC est défendue par l'argument que son introduction contribuera à rendre la communication plus rapide, que certains acteurs de la justice, comme les avocats, ne devront plus se déplacer. Ceci diminuera les coûts procéduraux. Il est aussi question de l'augmentation de la vitesse de circulation des informations, la disponibilité permanente des dossiers, la réduction de l'espace nécessaire à l'archivage, une rédaction plus aisée et plus rapide[441]. En matière pénale, le législateur ne semble pas suivre ses propres idées. Par exemple, l'avocat qui voudra consulter un dossier pénal électronique devra se déplacer au greffe pour visionner les pièces du dossier sur un écran d'ordinateur[442]. Mais ce greffe ne sera pas le greffe du tribunal qui traite le dossier, mais le greffe où est sis le bureau de l'avocat[443]. La loi ne stipule pas si cette obligation est à peine de non-recevoir. On imagine aisément les problèmes que l'on pourrait rencontrer avec certains greffiers pointilleux… On suppose ici l'idée que l'avocat d'un autre arrondissement judiciaire ne devra plus se déplacer dans un autre arrondissement judiciaire (sorte de futur pôle régional de justice ou « Court Center », avec la réduction des arrondissements judicaires). Ceci implique que le dossier pénal ne sera pas stocké sur un support électronique lié aux ordinateurs du greffe, mais que les ordinateurs des greffes du Royaume seront connectés par une liaison électronique « on line » avec un serveur central. Le législateur signale qu'il faudra investir massivement pour équiper les greffes d'ordinateurs. On doutera que les budgets nécessaires seront présents … Notons que les locaux du greffe prévus pour la consultation des dossier papiers ne sont déjà aujourd'hui pas équipés pour une consultation de qualité.

On pourra alors se demander pourquoi l'avocat ne pourra pas consulter le dossier au bureau par le biais d'un portail électronique sur le « web »… Bouquet final, le législateur prévoit que la consultation pourra prendre place dans d'autres lieux selon l'avancement de la technologie. La règle de la loi est la règle sauf toute autre exception, … Ceci n'est donc pas une règle ….

En dehors de la phase de l'information ou de l'enquête – on se demande déjà pourquoi – la consultation pourra se faire par délivrance d'une copie électronique du dossier envoyé par voie électronique. Mais vu que cette lecture de la copie (en Néerlandais « inzage »), permet aussi le copiage et l'impression (en Néerlandais « kopiename ») et que cette dernière est assujettie à une taxe, donc d'ordre fiscale, l'on devra payer pour chaque consultation du dossier. Ce qui était gratuit devient donc payant. L'on pourra peut-être encore se déplacer au greffe pour consulter gratuitement le dossier, mais ceci n'est pas très clair.

Autre entorse ou principe « tout électronique ». Si par exemple le huissier de justice veut signifier un acte en personne, cette personne devra en principe toujours signer pour reçu. Le législateur a prévu que dans ce cas le huissier imprime la feuille correspondante, le justiciable signera la feuille de papier et ensuite le huissier – que l'on note qu'il est bien équipé au niveau des TIC – scannera la feuille papier et enverra électroniquement le document aux autorités judiciaires … La même règle s'applique en matière de signature des procès-verbaux des auditions et la délivrance d'une copie de ce procès-verbal (art. 34)[444]. On voit mal le progrès.

Il est clair qu'avec l'échec du projet « Phenix », le législateur devra aussi réviser sa copie. De toute façon, la loi du 10 juillet 2006 n'est pas en vigueur et la Ministre de la Justice actuelle prévoit l'introduction des TIC au premier janvier 2015. On peut déjà craindre que l'introduction des TIC à cette date ne sera pas réalisable. Notons quand même que depuis le 1er janvier 2013 certains articles de la procédure civile ont été mis en vigueur (voir les lois du 31 décembre 2012). Le nouvel article 32 du Code Judicaire introduit par la loi du 5 août 2006 mais qui n'étaient pas en vigueur à ce jour – applicable en matière pénale – stipule qu'une signification pourra aussi se passer par courrier électronique à l'adresse judiciaire électronique de la

[437] *Ibid.,* p. 5 et seq. et p. 44-53.
[438] *Ibid.,* p. 54.
[439] *Ibid.,* p. 55.
[440] *Ibid.,* p. 53.
[441] *Ibid.,* p. 5.
[442] *Ibid.,* p. 58.
[443] *Ibid.,* p. 59.
[444] *Ibid.,* p. 53.

personne[445]. Là encore, peu semble être réglé du point de vue pratique, ce qui laisse à supposer que l'application dans la pratique devra encore attendre.

Plus haut nous avons déjà signalé qu'entre temps d'une part un projet pour un portail Justice unique est en train d'être élaboré et que d'autre part le projet JustScan veut élaborer un système adéquat pour l'introduction d'un dossier répressif électronique. Il est clair que beaucoup de travail reste encore à faire.

G. Conclusions

Le droit belge s'est déjà fort bien adapté à l'ère numérique. Sans surprise, c'est au niveau de la phase avant l'audience (enquête ou information) que la règlementation est la plus complète. Les obligations des tiers à coopérer sont également bien développés. Ceci n'empêche pas les nombreux problèmes d'applications dans la pratique (différence entre les mesures de recherches, application de la vidéo-surveillance). Le virtuel ne va pas toujours de pair avec le réel. Par contre, la théorie de la preuve s'est peu développée suite au principe de la liberté de la preuve, la libre appréciation de la preuve et du principe de l'intime conviction. Du moment où l'on entre dans le vaste domaine des échanges d'informations en dehors du procès pénal tout devient encore plus flou. En outre, un sérieux retard existe au niveau de l'introduction des TIC dans le déroulement du procès pénal (auditions, procédure, dossier pénal, casiers judiciaires), quelquefois suite à une législation peu adaptée (procès pénal). On notera une certaine spécialisation parmi les autorités judiciaires (parquet, police, parfois les juges d'instructions), mais souvent rien de bien structuré ou même l'absence d'expérience au niveau du siège (vidéo-surveillance). Enfin, les règles protectrices de la vie privée sont parfois peu claires. L'appréciation presque libre de la sanction de la preuve obtenue illégalement vide en plus les garanties procédurales existantes de leur contenu (clairement en matière de vidéo-surveillance et les méthodes particulières de recherche). Bien que la règle de la légalité de l'article 8 CEDH est souvent respectée par l'élaboration récente de règles formelles, l'efficacité de ces garanties semble compromise par la liberté du juge à sanctionner les transgressions sérieuses. Il en résulte que les autorités sont relativement (il existe encore en théorie des sanctions pénales ou disciplinaires voire même civiles) libres de les appliquer ou non. Il s'agit ici du problème central du droit de la procédure pénale, c'est-à-dire trouver le juste équilibre entre les droits de l'individu d'une part et l'intérêt de la société à la répression des infractions d'autre part. Le virtuel rejoint ici le réel.

Bruxelles, avril 2013.

[445] *Ibid.,* voir p. 32-34.