Droit pénal et numérique : vers un nouveau paradigme ?

Vanessa FRANSSEN
Chargée de cours à l'ULiège, chercheuse affiliée à la KU Leuven, chargée de cours associée à l'Université du Luxembourg, membre du barreau de Bruxelles

INTRODUCTION

Mesdames, Messieurs, en vos titres et qualités,

Chers Collègues,

Chers Étudiants,

Chères Familles,

Chers Amis,

Je me souviens encore vivement de la remarque d'un de mes collègues, à la fin des leçons inaugurales du 16 octobre 2015 : « Bientôt, ce sera à toi de donner une leçon inaugurale, » et il poursuivait avec quelques conseils bienveillants. Je n'aurais pas pu croire que ce jour viendrait si vite… Depuis le moment où j'ai rejoint cette Faculté, en automne 2015, le temps semble s'être envolé. Un bon signe, n'est-ce pas ? D'un côté, cela suggère que j'ai eu de quoi m'occuper – mes proches savent à quel point c'est vrai. De l'autre, cela témoigne de l'accueil chaleureux que cette Faculté m'a donné, et je tiens à en remercier aujourd'hui très sincèrement l'ensemble du personnel et des étudiants de cette Faculté, et en particulier l'équipe du Service de droit pénal.

Le moment est donc venu de vous présenter ma leçon inaugurale – leçon que j'ai intitulée « Droit pénal et numérique : vers un nouveau paradigme ? ». Cette leçon a pour objectif de vous présenter l'un de mes domaines de recherche préférés, sur lequel j'enseigne également dans le programme du Master, et de vous illustrer les défis parfois inédits auxquels cette thématique nous confronte, en nous poussant à réfléchir à l'élaboration de nouveaux paradigmes.

Dans les (bientôt) seize minutes qu'il me reste, je vais vous emmener dans l'univers du numérique, des nouvelles technologies de l'information et de la communication (ci-après : les TIC) qui font partie, depuis un certain temps, de notre vie quotidienne à tous.

En effet, qui parmi vous aujourd'hui présents dans cette salle n'a pas de GSM dans sa poche ? Qui ne travaille pas sur un ordinateur ou n'achète jamais de produits en ligne ? Qui d'entre vous n'a encore jamais communiqué par *Skype* ou n'a pas de profil *Facebook* ? Et pour ceux qui viennent de plus loin et qui ne connaissent pas si bien le campus du Sart-Tilman, vous vous êtes peut-être servis d'un GPS ou d'une application de navigation comme *Waze* ?

Tous ces « outils » de l'information et de la communication sont devenus, en très peu de temps, tellement populaires et répandus qu'on ne se rend même plus compte à quel point ils ont changé la vie de tous les jours. Nous sommes presque constamment connectés et interconnectés, du matin jusqu'au soir, à la maison, au travail et en voyage. Pourtant, il n'y a pas si longtemps que ça, les GSM n'existaient pas, on écrivait des textes à la main ou sur une machine à écrire, il fallait consulter un atlas ou guide Michelin et bien préparer son chemin avant de se mettre en route.

Sans aucun doute, ces technologies nous facilitent énormément la vie. Néanmoins, elles soulèvent également bon nombre de défis sociétaux, qui méritent souvent une approche interdisciplinaire (juridique, criminologique, politique, sociologique, technologique…) et qui font partie des priorités de l'Unité de Recherche 'Cité' (ci-après : UR Cité), regroupant les trois départements de notre Faculté. Aujourd'hui, je vous présenterai quelques-uns de ces défis sous l'angle du droit pénal et de la procédure pénale, d'un point de vue national et international.

Mon analyse procédera en deux temps. Dans une première partie, j'aborderai une problématique spécifique au droit pénal. Le deuxième volet de mon exposé sera consacré à deux questions clés en matière de procédure pénale.

I. DROIT PÉNAL

En matière de droit pénal, l'une des questions qui pose beaucoup de problèmes est la question de l'application de la loi pénale dans le (cyber)espace.

Sous l'effet du numérique, il est devenu facile de commettre des infractions depuis n'importe où, à n'importe quel moment. Plus besoin d'être physiquement près des cibles ou des victimes de l'infraction ; il suffit d'être branché sur internet.

À titre d'exemple (et l'exemple n'est peut-être pas tout à fait fictif), un hackeur qui se trouve en Russie pourrait prendre accès à un système informatique situé aux États-Unis, par exemple pour manipuler les résultats d'élections.

Ou encore, autre exemple tiré de l'actualité : en mai dernier, le « *ransomware* » *WannaCry* a affecté des dizaines de milliers d'ordinateurs utilisant un système d'exploitation Windows de chez Microsoft dans cent cinquante pays à travers le monde ; le logiciel malveillant (le « *malware* ») s'est diffusé extrêmement vite, en une poignée d'heures. Sur la base d'une analyse linguistique des messages envoyés par le logiciel malveillant, on a pu constater que les personnes derrière l'attaque maîtrisaient parfaitement le chinois et avait une bonne connaissance de l'anglais ; des entreprises spécialisées en cyber sécurité ainsi que le UK National Cyber Security Centre et le National Security Agency des États-Unis ont pointé du doigt la Corée du Nord comme pays d'où provenait l'attaque, mais la Corée du Nord nie toute implication(1).

Clairement, grâce à l'emploi des TIC, beaucoup de formes de criminalité ne connaissent plus de frontières. Certaines sont devenues par nature transfrontalières, à l'image de nos activités quotidiennes : on envoie un simple courriel depuis la Belgique à un destinataire en France, mais les données de cette communication seront stockées dans un centre de données en Irlande et le siège social du fournisseur du service Webmail que nous avons utilisé est situé aux États-Unis. Or, si ce courriel contenait une annexe comprenant des photos pédopornographiques, où l'infraction de pédopornographie (art. 383*bis*, §§ 1 et 2, C. pén.) serait-elle juridiquement commise ?

De manière générale, l'application de la loi pénale dans l'espace est régie par le principe de territorialité, tandis que l'application extraterritoriale fait l'exception. Mais comment rattacher une infraction au territoire d'un État ? En Belgique, par exemple, les cours et tribunaux appliquent à cet effet la théorie de l'ubiquité objective, suivant laquelle une infraction est considérée comme étant située sur le territoire belge à partir du moment où l'on peut localiser un élément constitutif ou aggravant matériel de l'infraction en Belgique(2). D'autres systèmes juridiques prennent parfois (également) en compte l'endroit de l'élément moral (théorie de l'ubiquité subjective) ou celui où les effets de l'infrac-

(1) Voy., entre autres, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack; https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack ; J. Kastrenakes, « The NSA reportedly believes North Korea was responsible for WannaCry ransomware attacks », *The Verge*, 14 juin 2017, https://www.theverge.com/2017/6/14/15805346/wannacry-north-korea-linked-by-nsa ; T.P. Bossert, « It's Official: North Korea Is Behind WannaCry », *Wall Street Journal*, 18 décembre 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 ; T. Fox-Brewster, « U.S. Blames North Korea for WannaCry – But Are Trump's Cybersleuths Wrong? », *Forbes*, 19 décembre 2017, https://www.forbes.com/sites/thomasbrewster/2017/12/19/north-korea-did-wannacry-says-trump-administration/#6bce739462ed.

(2) Voy., entre autres, Cass., 7 juin 2011, R.G. n° P.11.0172.N ; L. Dupont, *Beginselen van strafrecht*, t. 1, Louvain, Acco, 2003, p. 70 ; H. Fransen, « Loi pénale », in X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, Kluwer, mars 2017, L 32, pp. 56 à 58 ; F. Kuty, *Principes généraux du droit pénal belge*, t. 1, *La loi pénale*, Bruxelles, Larcier, 2009, pp. 365 à 369 ; T. Moreau et D. Vandermeersch, *Éléments de droit pénal*, Bruxelles, la Charte, 2017, p. 42.

tion (même ceux qui ne font pas partie des éléments constitutifs ou aggravants) se sont ressentis (théorie de l'effet)(3).

Cependant, dans le cyberespace, les éléments ou critères potentiels qui permettent de rattacher une infraction au territoire d'un État sont multiples : la présence de l'auteur de l'infraction, la localisation du système informatique ou le simple accès à un site Web, l'endroit (ou les endroits) de stockage des données (qui peut, en plus, varier dans le temps), les effets de l'infraction, le siège social du fournisseur de services, etc. Cette multiplicité de critères permet aux États de définir leur territoire de manière expansive, engendrant, d'un côté, de nombreux conflits de lois et, de l'autre, de l'insécurité juridique pour les citoyens qui, potentiellement, peuvent être poursuivis dans plusieurs pays, même pour des faits qui ne sont pas incriminés dans l'État de résidence de l'auteur(4).

À présent, aucune convention internationale ne définit de manière limitative les critères de territorialité, ni ne met en avant une priorité de l'un ou l'autre critère. Par exemple, la Convention sur la cybercriminalité du Conseil de l'Europe de 2001 ne détermine pas quels critères permettent à un État d'établir sa compétence à l'égard des infractions commises « sur son territoire »(5). Or, pour reprendre l'une des résolutions de l'Association internationale de droit pénal (ci-après : l'AIDP) adoptées lors du dernier congrès mondial, consacré à la « Société de l'information et droit pénal »,

> « [m]ême si le principe de territorialité reste le principe fondamental de compétence également dans le cyberespace, il produit des effets adverses lorsqu'il est appliqué à des infractions dans le cyberespace, en ce sens que *de facto* il permet aux États de localiser l'infraction sur leur territoire sur une base quasi universelle (…) »(6).

Si l'AIDP a mis en avant quelques principes utiles en 2014, les conflits de compétence sont toujours loin d'être résolus tant que la communauté internationale ne se met pas d'accord sur une hiérarchie de critères et sur des principes contraignants pour régler de tels conflits. En conséquence, il est grand temps de

---

(3) Voy., entre autres, C. Van den Wyngaert et S. Vandromme, *Strafrecht en strafprocesrecht in hoofdlijnen*, d. 1, *Strafrecht*, Anvers-Apeldoorn, Maklu, 2009, pp. 149 à 150 ; T. Leus, « De situering van het misdrijf in de ruimte. Een vergelijkende studie tussen België en Frankrijk », *N. C.*, 2015 (Dossier), pp. 92 à 95.

(4) Pour une analyse approfondie voy. S.W. Brenner et B.J. Koops, « Approaches to Cybercrime Jurisdiction », *J. High Tech. L.*, 2004, pp. 1 à 46 ; S.W. Brenner, « Cybercrime Jurisdiction », *Crime Law Soc. Change*, 2006, pp. 189 à 206 ; E.S. Podgor, « Cybercrime : Discretionary Jurisdiction », *U. Louisville L. Rev.*, 2008, pp. 727 à 738.

(5) Art. 22, § 1er, a), Convention sur la cybercriminalité, ETS nº 185, Budapest, 23 novembre 2001.

(6) AIDP, « Société de l'information et droit pénal », XIXe Congrès international de droit pénal (Rio de Janeiro, Brésil, 31 août-6 septembre 2014), Section IV – Droit pénal international, Résolution nº 3. Nous soulignons.

réfléchir à un nouveau cadre théorique qui permet de mieux définir la compétence territoriale et l'exercice de la souveraineté des États.

II. PROCÉDURE PÉNALE

En procédure pénale, les défis créés par le numérique sont encore bien plus importants, puisqu'ils concernent directement les droits fondamentaux des citoyens. Il convient de souligner d'emblée que ces défis dépassent le seul champ de la cybercriminalité, même au sens large, et concernent de nos jours en fait n'importe quelle infraction, pourvu qu'à un moment donné un système informatique (par exemple, un GPS, un smartphone, un ordinateur, une carte bancaire, l'internet, etc.) ait été utilisé, que ce soit par l'auteur ou par la victime.

Compte tenu des contraintes de temps, je me confine à vous exposer deux de ces défis : d'une part, la nécessité de créer un cadre législatif qui permet aux autorités policières et judiciaires de combattre de manière adéquate la criminalité dans une société de l'information tout en respectant les droits fondamentaux des citoyens et, d'autre part, le besoin croissant de la collaboration des fournisseurs de services pour mener à bien les enquêtes pénales.

A. Des mesures d'enquête adéquates respectant les droits fondamentaux

Ce n'est pas un secret que la procédure pénale ait du mal à suivre les nombreuses et rapides évolutions technologiques de notre société numérique. Beaucoup de législateurs, en Europe et ailleurs, réfléchissent en ce moment à une modernisation de la procédure pénale.

En attendant la mise en place d'un cadre législatif modernisé, les autorités policières et judiciaires cherchent à se débrouiller, exploitant parfois les zones grises du cadre législatif existant. En même temps, les cours et tribunaux sont régulièrement amenés à se prononcer sur des questions fondamentales, qui devraient être tranchées par le législateur, de préférence en concertation avec ses collègues européens et ses partenaires internationaux privilégiés pour éviter des écarts trop importants qui compliquent ensuite la coopération internationale.

Les enjeux d'une « procédure pénale 2.0 » ne sont pas anodins et nous concernent tous. Par exemple, si les autorités policières et judiciaires veulent procéder à une recherche dans un système informatique – prenons un simple smartphone –, faut-il alors encadrer cette recherche des mêmes garanties procédurales qu'une perquisition classique, ou suffit-il au contraire de simplement saisir le support matériel pour accéder au contenu intégral du système informatique ?

Aux États-Unis, la Cour suprême a jugé en 2014 dans l'affaire *Riley c. la Californie* que l'exploitation d'un smartphone requiert, en principe, l'autorisa-

tion d'un juge, même s'il est saisi lors d'une arrestation, étant donné que, de nos jours, un smartphone contient souvent bien plus d'informations privées que le domicile du suspect, ou pour reprendre la motivation de la Cour :

> « *a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form unless the phone is* »(7).

Aux Pays-Bas et en Allemagne, les cours ont rendu des jugements comparables. Par contre, en Belgique, la Cour de cassation a adopté une position bien plus favorable aux autorités policières et judiciaires. Dans un arrêt du 11 février 2015, la Cour avait conclu que :

> « [l']exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme de sms, est une mesure découlant de la saisie [de ce téléphone], laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête »(8).

Cet arrêt a subi beaucoup de critiques dans la doctrine, mettant en évidence qu'une telle recherche constitue une importante intrusion dans la vie privée, qui s'apparente effectivement à une perquisition, et qu'une telle intrusion nécessite non pas seulement une base légale explicite, mais également l'autorisation préalable d'un juge d'instruction(9). Malgré ces critiques bien légitimes, le législateur belge a entre-temps codifié cette jurisprudence dans le nouvel article 39*bis*, § 2, alinéa 1er, du C.i.cr. Sur la base de cette disposition légale, un officier de police peut désormais décider de procéder à l'exploitation d'un système informatique qui se trouve sur un support matériel saisi (par exemple

(7) U.S. Supreme Court, *Riley c. Californie*, 573 U.S. (2014), pp. 20 à 21.

(8) Cass., 11 février 2015, *Rev. dr. pén.*, 2015, concl. D. Vandermeersch, p. 581, § 3, *R.W.*, 2015-2016, note C. Conings, *Vigiles*, 2015, note P. Vanwalleghem, p. 132, *T. Strafr.*, 2015, note G.S., p. 140.

(9) C. Conings, « Het uitlezen van een gsm of ander privaat IT-systeem : This is not America », note sous Cass., 11 février 2015, *R.W.*, 2015-2016, pp. 622 à 626 ; C. Forget, « La collecte de preuves informatiques en matière pénale », in J.-Fr. Henrotte et F. Jongen (réd.), *Pas de droit sans technologie*, coll. CUP, vol. 158, Bruxelles, Larcier, 2015, pp. 254 à 260. En revanche, d'autres auteurs se réjouissent de l'interprétation donnée par la Cour de cassation, soulignant que, grâce à cet arrêt, la portée de l'article 88*ter* du C.i.cr. est ramenée à ses justes proportions. Voy. G.S., note sous Cass., 11 février 2015, *T. Strafr.*, 2015, pp. 141 à 142. D'autres donnaient d'ailleurs déjà une telle interprétation au pouvoir de saisie du support matériel, par analogie avec la jurisprudence de la Cour de cassation concernant la prise de connaissance du contenu de la cassette du répondeur automatique, saisie lors d'une perquisition régulière. Voy. D. Dewandeleer, « Misdrijven en strafonderzoek in de IT-context », in R. Verstraeten et F. Verbruggen (réd.), *Straf- en strafprocesrecht*, coll. Themis, Bruges, die Keure, 2009-2010, p. 139, avec référence à Cass., 27 octobre 1999, *A.C.*, 1999, 1346.

un smartphone, un GPS ou un ordinateur). À l'image de la saisie de ce support (basée sur les articles 35 et s. du C.i.cr.), une intervention du procureur du Roi n'est même pas requise, sauf si le support est verrouillé. L'argument qu'un tel support contient souvent un grand nombre d'éléments intimement liés à la vie privée (actuelle *et* passée) de la personne concernée, n'a donc reçu aucun écho dans la nouvelle législation. Le souci d'augmenter l'« efficacité de la recherche » et d'adapter la procédure pénale belge « aux besoins d'une lutte effective contre la criminalité dans la société d'information » a indiscutablement pris le dessus(10). En conséquence, la vie privée du justiciable belge semble nettement moins bien protégée que celle de beaucoup de ses concitoyens européens et américains(11). Cette approche pourra-t-elle passer le test de l'article 8 de la Convention européenne des droits de l'homme ? À voir.

Des questions analogues se présentent pour la recherche d'un système informatique à distance, le cas échéant localisé à l'étranger (pensons, par exemple, à la boîte de réception du suspect dont les données sont stockées dans le « *cloud* »), ou encore par rapport aux possibilités pour les autorités de « cracker » le mot de passe d'un système informatique et de décrypter les données stockées, traitées ou transmises par le système informatique afin de les rendre compréhensibles. En Belgique, ces questions sont aujourd'hui réglées par les nouvelles dispositions insérées par la loi du 25 décembre 2016(12). Reste néanmoins la question cruciale de savoir si le juste équilibre entre les besoins de la recherche des autorités, d'un côté, et le droit à de la vie privée des citoyens, de l'autre, a été atteint… Le souci principal du législateur était clairement de renforcer les outils d'enquête des autorités policières et judiciaires. Le fait que les évolutions technologiques aient également modifié, et même de manière assez profonde, les attentes légitimes des citoyens concernant le respect du droit à la vie privée (comment protéger, par exemple, notre domicile « virtuel » ?) semble malheureusement avoir reçu beaucoup moins d'attention de la part du législateur.

(10) Exposé des motifs, Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/1, p. 7.

(11) Pour une analyse comparée ponctuelle avec les Pays-Bas, l'Allemagne et les États-Unis, voy. C. CONINGS, « Het uitlezen van een gsm of ander privaat IT-systeem : This is not America », note sous Cass., 11 février 2015, *R.W.*, 2015-2016, p. 625, § 12. Pour une analyse de la jurisprudence récente aux Pays-Bas, voy. J.J. OERLEMANS, note sous Cour Arnhem-Leeuwarden, 22 avril 2015, *Computerr.*, 2015, n° d'article 2015/127.

(12) Loi du 25 septembre 2016 portant modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017.

B. La collaboration indispensable des fournisseurs de services

Une deuxième problématique clé en procédure pénale concerne la collaboration d'entreprises privées dans le cadre des enquêtes pénales.

En effet, afin de rendre la lutte contre la criminalité dans la société numérique effective, les autorités policières et judiciaires ont de plus en plus besoin de la collaboration de personnes ayant une expertise spécifique ou une connaissance particulière d'un système informatique ainsi que des entreprises privées qui stockent, traitent ou transmettent des données par un système informatique. Pensons par exemple à *Dropbox*, *eBay* ou *Rakuten* (entreprise japonaise qui est propriétaire d'entre autres *Viber*). Sans cette expertise et l'accès à ces données, il serait aujourd'hui presque impossible de mener à bien beaucoup d'enquêtes pénales. L'accès aux traces digitales laissées par les suspects est en effet souvent indispensable pour l'action publique, tant à charge qu'à décharge.

Cependant, face aux évolutions technologiques, le champ d'application de ces obligations de collaboration suscite depuis quelques années de vives discussions, pas uniquement en Belgique, mais partout en Europe et aux États-Unis.

Un premier point de discussion relève du champ d'application personnel de ces obligations de collaboration. Quels acteurs privés sont obligés de collaborer avec les autorités policières et judiciaires ? Uniquement les opérateurs de réseaux de télécommunications (ou de communications électroniques) et les fournisseurs de tels services de communication ? Ou également les entreprises technologiques qui mettent à la disposition de leurs clients des logiciels qui permettent de communiquer via internet, que ce soit un logiciel permettant la communication orale (comme par exemple *Skype*) ou une plateforme pour publier et diffuser des informations sur internet (comme *Facebook*, *Instagram* ou *Twitter*) ? Contrairement aux opérateurs et fournisseurs classiques, ces entreprises technologiques n'ont pas forcément d'infrastructure physique sur le territoire des autorités en question. Certaines de ces entreprises sont des acteurs économiques mondiaux, qui opèrent dans les quatre coins de monde (comme les géants du Web ou « GAFAM » – *Google*, *Apple*, *Facebook*, *Amazon*, *Microsoft*).

Si les obligations de collaboration s'étendent à de telles entreprises technologiques mondiales, cela crée de nouveaux problèmes, notamment en ce qui concerne le champ d'application territorial de ces obligations. Peut-on obliger des entreprises étrangères, fournisseurs de services, à collaborer avec les autorités nationales ? Comment contraindre une personne qui n'est pas physiquement présente sur le territoire ? Ou suffit-il que cette entreprise offre des services ciblés sur le territoire en question, comme la Cour de cassation belge a décidé dans l'affaire *Yahoo*[13] ?

(13) Cass., 1er décembre 2015, R.G. nº P.13.2082.N.

Traditionnellement, pour remédier à une telle situation, on devrait recourir à la coopération internationale. Cependant, les règles en matière d'entraide judiciaire ne sont plus considérées comme adéquates, surtout en raison de la lenteur de la procédure. D'où l'intérêt croissant pour la coopération directe avec les fournisseurs de services étrangers.

Cette coopération directe (également proposée par la Convention sur la cybercriminalité, mais uniquement pour les injonctions de produire des données d'identification, autres que les données relatives au trafic ou au contenu) a entre-temps reçu une base légale explicite en droit belge(14). Cependant, alors que cette solution semble très séduisante, du moins du point de vue des autorités policières et judiciaires, elle témoigne d'une approche unilatérale qui risque de mettre les entreprises en question dans une situation difficile, voire impossible. En effet, si tous les pays adoptaient cette approche, ces entreprises devraient *de facto* collaborer avec toutes les autorités policières et judiciaires du monde, même lorsque la loi du pays où l'entreprise est établie lui interdit de passer des données personnelles à des autorités étrangères, ou que les données sont stockées sur un autre territoire. Ces questions sont en ce moment débattues devant les cours et tribunaux belges dans l'affaire *Skype* et devant la Cour suprême des États-Unis dans l'affaire *Microsoft-Irlande*, alors que la Commission européenne travaille sur une proposition législative qui devrait remédier à une partie de ce problème(15). De mon côté, je dirige un projet de recherche de droit comparé qui porte précisément sur les multiples questions liées aux obligations de collaboration des entreprises technologiques(16).

CONCLUSION

Mesdames et Messieurs, j'en arrive à la fin de mon exposé. J'espère que ces quelques illustrations vous ont permis d'avoir une meilleure idée du contenu de ma recherche et de son importance sociétale.

Faut-il élaborer de nouveaux paradigmes pour affronter les défis exposés ? Pour certains défis, cela me semble en effet indispensable. Je me réjouis donc de continuer mes recherches dans ce domaine dans les années à venir, de préférence en étroite collaboration avec mes collègues de l'UR Cité.

(14) Pour une analyse du nouveau cadre législatif belge, voy. V. FRANSSEN et S. TOSZA, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », in V. FRANSSEN et A. MASSET (dir.), *Les droits du justiciable face à la justice pénale*, coll. CUP, vol. 171, Limal, Anthemis, 2017, pp. 244 à 248.

(15) Pour une analyse plus étoffée voy. V. FRANSSEN, « The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level », *European Data Protection Law Review*, 2017, pp. 538 à 542.

(16) Financé par le Fonds de la recherche scientifique – FNRS (CDR J.0293.17) et par l'ULiège (Crédits Sectoriels de Recherche en Sciences Humaines).