Repenser au territoire :

Cybercriminalité et techniques d'enquête

Salomé Lannier

Doctorante, Université de Bordeaux, France (Centre de droit comparé du travail et de la sécurité sociale) et Université de Valencia, Espagne (Programme de doctorat en droits humains)

Le territoire est le fief ultime de la souveraineté de l'Etat. En droit pénal, il agit comme « *territoire-limite* »[1], déterminant les limites de son action, notamment l'encadrement géographique de ses pouvoirs d'enquête. Cependant, le numérique se joue du territoire national et la procédure pénale s'efforce tant bien que mal de s'adapter aux nouvelles réalités criminologiques.

Rapprocher « territoire » et « numérique » peut sembler un oxymore. Le territoire s'entend classiquement comme un espace qui définit les limites géographiques de la puissance, de la souveraineté des Etats[2]. L'un des éléments majeurs de cette souveraineté est le droit de punir[3], qui se matérialise en amont par les différentes étapes de la procédure pénale. Sur son territoire, l'Etat possède une « *exclusivité d'enquêter* »[4] en déterminant « *sans ingérence extérieure, les pouvoirs d'investigation, de poursuite et de sûreté confiés à ses agents* »[5]. Le revers de cette exclusivité réside en l'impossibilité d'étendre ses pouvoirs au-delà de son territoire. Se pose alors la question de cette limite dans l'espace numérique. Il a pu être argumenté que celui-ci ne possède pas de frontières, ou du moins, qu'il n'existe qu'une frontière entre celui-ci et l'espace matériel[6]. Cette dichotomie est cependant insoutenable considérant les

---

[1] H. Ruiz Fabri, « Immatériel, territorialité et État », *Archives de Philosophie du Droit*, Éditions Dalloz, 1999, vol. 43, p. 193

[2] O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1re éd., 1994, p. 53 ; J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2e éd., 2018, p. 2

[3] R. Roth, « Droit pénal transnational : un droit pénal sans Etat et son territoire », *in* C.-A. Morand (dir.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no 46, 2001, p. 140 ; M. Massé, « La souveraineté pénale », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 1999, p. 905 ; P. Beauvais, « Les mutations de la souveraineté pénale », *in* Collectif (dir.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 72

[4] M. Lasalle, « Souverainetés et responsabilités dans la collecte internationale de preuves - L'exemple de l'accès aux données bancaires en matière pénale », *in* Société française pour le droit international, M. Ubéda-Saillard (dir.), *La souveraineté pénale de l'État au XXIème siècle*, Éditions Pedone, 2018, p. 277

[5] P. Beauvais, « Les mutations de la souveraineté pénale », *op. cit.* note 3, p. 73

[6] D.R. Johnson, D. Post, « Law and Borders - The Rise of Law in Cyberspace », *Stanford Law Review*, mai 1996, vol. 48, no 5, p. 1379 ; A.L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York, N.Y, Century Foundation, 15 mai 2000, p. 31

impacts qu'un espace a sur l'autre et *vice versa*[7] : la frontière n'est pas à rechercher entre le virtuel et le réel[8]. Dès lors, le territoire comme limite aux actes d'enquête peut s'étendre au cyberespace : il s'agit d'une « *augmentation et [d']une extension numérique du territoire* »[9]. Se repose alors la question des frontières au sein de l'espace numérique. Des critères de rattachement liés aux Etats ont pu être énoncés : le suffixe aux noms de domaine (.fr), la géolocalisation de l'origine de la connexion, la langue[10], la localisation des serveurs[11], … D'autres critères de délimitation ont vu le jour, déconnectés des Etats[12] : par réseaux, par le « code »[13], par les différents espaces de commerce électronique[14], …

En l'absence de réponse, les auteurs d'infractions se jouent des territoires nationaux, qui pour eux, ne représentent qu'un trait sur une carte qui n'a pas d'équivalent dans le cyberespace[15]. Se développe donc le phénomène dénommé de « cyber criminalité », transnational par nature à l'image du numérique et accentué par son essor drastique en réponse à la crise de la COVID-19[16]. En ce sens, il s'agit de l'un des priorités de l'actuelle stratégie de l'Union Européenne visant à lutter contre la criminalité organisée[17]. Ce phénomène peut être défini « *comme toute action illégale dont l'objet est de perpétrer des infractions pénales sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunication* »[18]. Classiquement, il est divisé en deux catégories[19] : les infractions « aidées » par l'environnement numérique (comme moyen de l'infraction) ; et celles « centrées » sur l'environnement

---

[7] M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020, p. 289

[8] K.F. Aas, « Beyond 'the desert of the real': crime control in a virtual(ised) reality », *in* Y. Jewkes (dir.), *Crime online*, Willan, 2007, p. 167

[9] P. Musso, « Le Web : nouveau territoire et vieux concepts », *Annales des Mines - Réalités industrielles*, ESKA, novembre 2010, vol. 2010/4, nº 4, p. 75

[10] J.L. Goldsmith, T. Wu, *Who controls the Internet? Illusions of a borderless world*, Oxford University Press, 2006, p. 31-62

[11] M. Kettemann, *The normative order of the internet*, *op. cit.* note 7, p. 209

[12] D.G. Post, « Governing Cyberspace », *Wayne Law Review*, 1996, vol. 43, nº 1, p. 160

[13] L. Lessig, « The Zones of Cyberspace », *Stanford Law Review*, mai 1996, vol. 48, nº 5, p. 1406, 1409

[14] P. Musso, « Le Web : nouveau territoire et vieux concepts », *op. cit.* note 9, p. 76

[15] J. Perry Barlow, « Déclaration d'indépendance du cyberespace », *Libres enfants du savoir numérique*, Éd. de l'éclat, 2000, p. 47-54

[16] Europol, « Internet organised crime threat assessment », EU, 2020, p. 13 ; Europol, « Internet organised crime threat assessment », EU, 2021, p. 30 ; Europol, « European Union serious and organised crime threat assessment - A corrupting influence », EU, 2021, p. 38, 94

[17] European Commission, « Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 », EU, 14 avril 2021, p. 15, COM(2021) 170 final

[18] R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, Thesis, Université de Lorraine, 2016, p. 26-28. Actuellement, aucun texte international n'offre de définition harmonisé du phénomène.

[19] Au contraire, la convention de Budapest sur la cyber criminalité du 23 novembre 2001 divise restrictivement ce phénomène entre les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, les infractions informatiques et celles se rapportant au contenu.

numérique (comme objet de l'infraction)[20]. La seconde catégorie, la cyber criminalité au sens stricte, comprend les atteintes aux réseaux et à ses composants[21], par exemple, dans le langage courant, le *hacking*. La première catégorie, la cyber criminalité au sens large, recouvre tout type d'infraction dès lors qu'assistée, aidée, mise en œuvre *via* le cyberespace, qui n'est alors qu'un outil. Ainsi, la traite des êtres humains, qui criminalise le recrutement, le transport, l'hébergement de personnes à des fins d'exploitation[22], se développe naturellement dans l'espace numérique[23] : recrutement par des offres en ligne frauduleuse, organisation des trajets via des plateformes numériques, contrôle permanent des victimes par leur téléphone, …[24]

En plus des autres avantages que leur offre le numérique (anonymat, rapidité, …), l'inadéquation entre l'espace numérique et les territoires nationaux offre un terrain propice à évincer les procédures pénales étatiques au profit de fins criminelles. Il s'agit d'un phénomène d'« a-territorialisation » permettant d'échapper aux contrôles étatiques et de développer des conduites criminelles sans craindre une enquête[25]. La prise en compte du cyberespace dans la régulation des techniques d'enquête est donc au cœur de la lutte contre la cyber criminalité[26]. Les réflexions initiales de ce colloque portaient, en réaction à ce premier phénomène, à réfléchir autour d'une « reterritorialisation » du droit. Ce phénomène a déjà pu être utilisé en matière de compétence juridictionnelle, notamment au niveau pénal, par l'extension du concept de

---

[20] S. Furnell, *Cybercrime: vandalizing the information society*, Addison-Wesley, A Pearson Education book, 1re éd., 2002, p. 22, cité dans K.-S. Choi, « Cyber-Routine Activities Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization », *in* K. Jaishankar (dir.), *Cyber criminology: exploring Internet crimes and criminal behavior*, Boca Raton, FL, CRC Press, 2011, p. 230. Néanmoins, cette division peut être considérée comme purement formelle, puisque, en pratique, les deux catégories peuvent se combiner, S. El Zein, « L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie », *in* M.-C. Piatti (dir.), *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, Presses universitaires de Lyon, 2001, p. 164

[21] Voir le chapitre du code pénal sur les atteintes aux systèmes de traitement automatisé de données, articles 323-1 à 323-8

[22] Article 225-4-1 du code pénal

[23] Cette modalité de traite s'inscrit dans les priorités de lutte au niveau de l'Union européenne, European Commission, « Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025 », EU, 14 avril 2021, p. 13-14, COM(2021) 171 final

[24] V. Greiman, C. Bain, « The Emergence of Cyber Activity as a Gateway to Human Trafficking », *International Journal of Cyber Warfare and Terrorism*, 2012, vol. 12, no 2, p. 41-49 ; S. Milivojević, « Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus », *in* M. Segrave, L. Vitis (dir.), *Gender, Technology and Violence*, Routledge, 2017, p. 28-44

[25] D.G. Post, « Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace », *Journal of Online Law*, 1995, § 39-40

[26] S. Howell, « Systemic Vulnerabilities on the Internet and the Exploitation of Women and Girls: Challenges and Prospects for Global Regulation », *in* H. Kury, S. Redo, E. Shea (dir.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, p. 582, DOI:10.1007/978-3-319-28424-8_22

territorialité[27]. Au contraire, les techniques d'enquête et notamment l'investigation numérique, définie comme un acte d'enquête visant à obtenir des données[28], « *mine d'or* »[29] de la preuve pénale, peinent à considérer le territoire. Le droit s'appuie sur des critères classiques, qui ne sont plus toujours adaptés aux réalités criminelles, pour définir le champ d'application des techniques d'enquête. De nouveaux critères pourraient établir une hiérarchie entre des techniques d'enquête plus ou moins invasives de la vie privée : plus que de re-territorialiser des actes qui peuvent difficilement l'être, le droit pourrait prendre en compte la diversité des territoires liée au cyberespace.

Dans quelle mesure le territoire délimite et pourrait re-délimiter le champ d'application des techniques d'enquête afin d'améliorer la lutte contre la cyber criminalité ?

La procédure pénale ne prend en compte en général qu'implicitement le critère de territoire. Pourtant, ce territoire, en tant qu'espace matériel et numérique, défini, limitativement ou extensivement, l'ampleur des techniques d'enquête (I). Cependant, cette prise en considération très partielle du territoire questionne les champs d'application matériel des techniques d'enquête, invitant à reconsidérer ces critères (II).

I. Cyberespace : entre limite et extension du territoire

Les techniques d'investigation numériques sont nombreuses au sein du code de procédure pénale et bénéficient de mises à jour et de développement très récurrents[30]. Ces réformes visent d'une part à faire évoluer les techniques d'enquête aux possibilités

[27] Article 113-2-1 du code pénal, D. Brach-Thiel, « Le nouvel article 113-13 du code pénal : contexte et analyse », *Actualité juridique Pénal*, Dalloz, 2013, p. 90 ; J. Alix, « Fallait-il étendre la compétence des juridictions pénales en matière terroriste ? (à propos de l'article 2 de la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme) », *Recueil Dalloz*, 2013, p. 518 ; T. Herran, « La nouvelle compétence française en matière de terrorisme - Réflexions sur l'article 113-13 du Code pénal », *Droit pénal*, avril 2013, n° 4, p. étude 10

[28] B. Roussel, *Les investigations numériques en procédure pénale*, Thesis, Université de Bordeaux, 7 juillet 2020, § 211

[29] R. Leary, J. Thomas, « How Complexity Theory is Changing the Role of Analysis in Law Enforcement and National Security », *in* B. Akhgar, S. Yates (dir.), *Intelligence Management*, Springer London, Advanced Information and Knowledge Processing, 2011, p. 65-66, DOI:10.1007/978-1-4471-2140-4_5

[30] Voir notamment : Loi n° 91-646 relative au secret des correspondances émises par la voie des télécommunications ; Loi n° 2003-239 pour la sécurité intérieure ; Loi n° 2004-204 portant adaptation de la justice aux évolutions de la criminalité ; Loi n° 2007-297 relative à la prévention de la délinquance ; Loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure ; Loi n° 2014-372 relative à la géolocalisation ; Loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme ; Loi n° 2016-731 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale ; Loi n° 2019-222 de programmation 2018-2022 et de réforme pour la justice ; Loi n° 2022-52 relative à la responsabilité pénale et à la sécurité intérieure

technologiques, notamment afin d'améliorer la répression de la cybercriminalité[31], et d'autre part à prendre en compte les exigences de la Cour européenne des droits de l'Homme (CrEDH) en matière de protection de la vie privée[32]. Cependant, ces évolutions prennent encore très peu en compte le territoire, qu'il soit matériel ou numérique. Bien qu'implicite, le premier vient pourtant limiter les actions géographiques des enquêteurs (A) ; tandis que le second ouvre, presque sans limite, leur champ d'action (B).

A. Un champ territorial limitant : une matérialité implicite

Plusieurs techniques d'enquête nécessitent l'utilisation de matériel ou de recourir à des opérateurs présents sur le territoire national. Dès lors, le territoire, même implicite, se présente comme une limite directe à la mise en œuvre des techniques d'enquête pouvant aider à enquêter sur des faits de cybercriminalité. Il peut aussi agir comme limite indirecte, au regard de l'évolution et de la structure du cyberespace.

Premièrement, seront abordées trois techniques d'enquête de droit commun : les interceptions de communication[33], la géolocalisation[34] ainsi que les captation et les fixations d'images dans les lieux publics au moyen de dispositifs aéroportés, autrement appelés drones[35]. A celles-ci seront rajoutées deux techniques spéciales d'enquête du Titre XXV du Livre IV du code de procédure pénale : les sonorisations et des fixations d'images de certains lieux ou véhicules (privés ou publics)[36], ainsi que le recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques[37]. Ces techniques sont numériques dans le sens où elles permettent d'obtenir des données, mais ne portant pas à proprement parlé sur le cyberespace, entendu comme Internet. Elles reposent sur l'usage de dispositifs particuliers (comme une balise ou un drone), ou sur la collaboration avec

---

[31] Voir notamment M. Quéméner, « Les techniques spéciales d'enquête en matière de lutte contre la cybercriminalité », *Actualité juridique Pénal*, Dalloz, 2015, p. 403

[32] La France a notamment été condamnée un certain nombre de fois sur ces sujets, voir par exemple ECHR, *Huvig v. France*, 24 avril 1990, nº 11105/84 ; ECHR, *Kruslin v. France*, 24 avril 1990, nº 11801/85 ; ECHR, *Lambert v. France*, 24 août 1998, nº 88/1997/872/1084 ; ECHR, *Matheron v. France*, 29 mars 2005, nº 57752/00 ; ECHR, *Vetter v. France*, 31 mai 2005, nº 59842/00 ; ECHR, *Wisse v. France*, 20 décembre 2005, nº 71611/01 ; ECHR, *Ben Faiza v. France*, 8 février 2018, nº 31446/12

[33] Articles 100 à 100-8 du code de procédure pénale

[34] Articles 230-32 à 230-44 du code de procédure pénale

[35] Articles 230-47 à 230-53 du code de procédure pénale. Voir par exemple M. Bouchet, « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *Dalloz IP/IT*, Dalloz, 2022, p. 299

[36] Articles 706-96 à 706-98 du code de procédure pénale

[37] Article 706-95-20 du code de procédure pénale. Cette technique s'utilise notamment quand les données permettant une interception classique de communications ne sont pas disponibles (technique mise en œuvre grâce notamment à un *IMSI* (*International Mobile Subscriber Identity*) *catcher*)

des opérateurs nationaux de téléphonie (comme pour les interceptions de communications ou pour la géolocalisation sur la base des données de télécommunication[38]). Par application du principe de territorialité, la mise en œuvre des techniques d'enquête se limite au territoire matériel de l'Etat. Ainsi, bien que les articles régulant ces techniques d'enquête ne mentionnent pas de manière explicite le territoire, celui-ci fonctionne comme un critère limitatif, déterminant le champ d'application géographique. Si l'auteur présumé de l'infraction sort du territoire national, l'interception de communications devra prendre fin, ou encore, les données obtenues grâce à la balise posée sur son véhicule ne pourront pas constituer des preuves valables[39].

Deuxièmement, d'autres limites sont liées au territoire, bien qu'indirectement. Pour se faire, il convient de s'attarder à l'usage des réquisitions judiciaires [40], qui permettront de requérir à des opérateurs de service numérique des informations concernant ses usagers ou le contenu qu'il héberge. Cependant, le développement de l'espace numérique s'est principalement reposé sur des opérateurs étrangers, notamment américains. Dès lors, l'obtention de données suppose de recourir à la coopération internationale, processus lent et inadapté aux besoins des enquêtes en matière de cyber criminalité, notamment en raison de la haute volatilité des données[41]. Au-delà des réquisitions, la structure du cyberespace peut aussi supposer de demander la collaboration de ces acteurs étrangers : le chiffrement[42]. Celui-ci est un obstacle majeur à l'obtention de données utiles lors d'une interception de communications : si l'acte d'enquête peut prouver que l'auteur présumé se connecte à l'application WhatsApp, il est impossible d'obtenir les conversations qui s'y échangent (contrairement à des conversations téléphoniques classiques ou des échanges de SMS[43]). Les possibilités de déchiffrement sont

---

[38] J. Pronier, « Fascicule 20 : Géolocalisation - Articles 230-32 à 230-44 », *JurisClasseur Communication*, LexisNexis, 14 août 2021, § 4-5

[39] En effet, les communications doivent transiter par un opérateur français, Cour de Cassation, Chambre criminelle, 20 juin 2018, nº 17-86651 ; Cour de Cassation, Chambre criminelle, 20 juin 2018, nº 17-86657. Entre Etats-membres de l'Union européenne, une certaine extraterritorialité est néanmoins facilitée, voir l'article 100-8 du code de procédure pénale ; contrairement à la géolocalisation qui ne permet pas cette extension, M. Quéméner, « Fascicule 982 : Géolocalisation dans le cadre pénal - Articles 689 à 693 », *JurisClasseur Communication*, LexisNexis, 3 juillet 2019, § 55-60 ; Cour de Cassation, Chambre criminelle, 9 février 2016, 15-85.070 ; Cour de Cassation, Chambre criminelle, 10 avril 2018, nº 17-85607

[40] Articles 60-1 à 60-3, 77-1-1 à 77-1-3, 99-3 à 99-5 du code de procédure pénale

[41] Des négociations sont en cours pour un instrument entre les Etats-Unis et l'Union européenne, K. Propp, « Has the Time for an EU-U.S. Agreement on E-Evidence Come and Gone? », *Lawfare*, 2 juin 2022, en ligne https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone (consulté le 13 juin 2022) ; ainsi qu'un instrument au sein de l'Union européenne dédié aux preuves électroniques, proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, publié par la Commission européenne le 17 mai 2018

[42] M. Quéméner, « App. Art. 427 à 457 - Fasc. 20 : La preuve numérique dans un cadre pénal », *JurisClasseur Procédure pénale*, 25 avril 2022, § 87 et suivants

[43] Abréviation de *Short Message Service*

pour l'instant limitées au niveau national[44], supposant une nécessaire coopération d'opérateurs étrangers, dont la réponse n'est pour l'instant que volontaire ou dépendante de législations étrangères.

La lutte contre la cyber criminalité peut tout d'abord se reposer sur des techniques d'enquête mises en œuvre depuis longtemps, telles que les interceptions de communications, la géolocalisation, ou très récentes, comme l'usage de drones. Cependant, cette première catégorie d'actes ne prend en compte qu'implicitement le territoire, à raison : elles reposent sur des dispositifs matériels, sans forcément recourir au cyberespace, contrairement à d'autres techniques qui y seront dédiées.

B. Un champ territorial extensif : l'ouverture au numérique

D'autres techniques d'enquête vont permettre d'aller rechercher des preuves en particulier dans le cyberespace. Le territoire numérique n'est alors pas défini, concept implicite une nouvelle fois, mais il agit pour ces techniques comme un critère extensif du territoire géographique national. Cette extension ne repose sur aucune limite, malgré une, explicite, qui a tenté d'être imposée.

La cybercriminalité fait usage de l'ensemble des technologies disponibles qui pourraient faciliter la commission de faits infractionnels. Le cyberespace, grâce au chiffrement, à l'anonymat, à la rapidité et le caractère éphémère des échanges, offre un lieu idoine pour faciliter ou commettre directement des infractions. Ainsi, des techniques d'enquête ont été développées afin de permettre aux enquêteurs d'agir dans cet espace particulier. D'une part, des techniques classiques, telles les perquisitions, ont été étendues aux dispositifs électroniques trouvés sur place ou à la possibilité de réaliser des perquisitions dans des espaces numériques à

[44] Malgré les articles 230-1 à 230-5 du code de procédure pénale. Celui-ci a été utilisé dans l'affaire Encrochat, mais la légalité de ce déchiffrement massif de données demeure contestée, en raison de son caractère généralisé et indifférencié, J. Follorou, « Piratage d'EncroChat : les recours se multiplient contre la justice française », *Le Monde.fr*, 10 mars 2021, en ligne https://www.lemonde.fr/societe/article/2021/03/10/piratage-d-encrochat-les-recours-se-multiplient-contre-la-justice-francaise_6072569_3224.html (consulté le 29 avril 2021). Cependant, la protection des dispositifs de déchiffrement par le secret d'Etat a été validé par le Conseil Constitutionnel, Conseil constitutionnel, *M. Saïd Z.*, 8 avril 2022, 2022-987 QPC. Sur l'affaire Encrochat, voir aussi Europol, *IOCTA 2020*, *op. cit.* note 16, p. 21 ; Eurojust, « Annual report 2020 - Criminal justice across borders », EU, 2021, p. 29 ; *ibid.*. Des moyens de déchiffrement devraient être développés au niveau d'Europol, European Commission, *EU Strategy to tackle Organised Crime 2021-2025*, *op. cit.* note 17, p. 26 ; European Commission, « Communication To The European Parliament, The European Council And The Council - Eleventh progress report towards an effective and genuine Security Union », EU, 18 octobre 2017, p. 9-10, COM(2017) 608 final

distance, à travers les systèmes informatiques dans les locaux des forces de l'ordre[45]. D'autre part, des techniques dédiées à la criminalité organisée sont passées dans le droit commun, en particulier, l'enquête sous pseudonyme[46]. Celle-ci va permettre d'« infiltrer » un espace restreint d'Internet, afin de participer à des échanges et d'extraire des éléments de preuve. Enfin, le code a créé de nouvelles techniques spéciales d'enquête dans le cadre de la lutte contre la criminalité organisée. Sont particulièrement intéressantes l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique[47], permettant d'accéder à des échanges dans un espace restreint d'Internet, à l'insu de l'auteur présumé ; et la captation de données informatiques[48], qui est une forme légale d'hacking, permettant d'accéder aux données stockées, affichées sur un écran, introduites par saisies de caractères (tapées sur un clavier) ou transmises par des périphériques (caméra, microphone, …).

Les trois dernières techniques ne posent pas de limite territoriale à leur mise en œuvre. La limite numérique est néanmoins implicite en matière d'accès aux correspondances électroniques : les enquêteurs ne pourront accéder qu'aux espaces ouverts par les identifiants obtenus. Un doute persiste néanmoins : il est possible d'utiliser l'identifiant d'un espace pour se connecter à d'autres[49], questionnant donc la limite numérique de la mesure, dès lors fixé par le concept large de « correspondance »[50]. De même, la captation de données informatiques est limitée à ce qui est stockée sur le système, ou l'usage qu'en fait son utilisateur. Au contraire, l'enquête sous pseudonyme n'offre aucune limite quant aux espaces numériques au sein desquels pourront agir les enquêteurs (potentiellement, des sites en langue étrangère, ou de noms de domaine étrangers). Néanmoins, la technique souffre d'autres maux : le manque de

---

[45] Articles 56 et suivants, 76, 92 et suivants du code de procédure pénale. L'article 56 mentionne expressément la saisie de « *données informatiques* ». Pour les perquisitions à distance, voir l'article 57-1 al.2

[46] L'enquête sous pseudonyme a d'abord été limitée à des infractions spécifiques, article 706-35-1 du code de procédure pénale créé par la loi n° 2007-297 relative à la prévention de la délinquance ; avant d'être regroupée aux techniques spéciales d'enquête, article 706-87-1 créé par la loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme ; puis a été incluse dans les techniques de droit commun, article 230-46 du code de procédure pénale créé par la loi n° 2019-222 de programmation 2018-2022 et de réforme pour la justice

[47] Articles 706-95-1 à 706-95-3 du code de procédure pénale

[48] Articles 706-102-1 à 706-102-5 du code de procédure pénale

[49] Il est possible de se connecter à certains sites par un compte Google ou Facebook par exemple

[50] Si cela désignait classiquement « *le courrier échangé entre deux personnes, souvent sur une longue période* », P. Bonfils, « Secret des correspondances », *Répertoire de droit pénal et de procédure pénale*, Dalloz, juin 2022, § 1, le concept a été considérablement élargi à tout message écrit, « *quel qu'en soit le support, d'un ou de plusieurs auteurs déterminés ou déterminables à un ou plusieurs destinataires déterminés ou déterminables pour peu [qu'il ait] un caractère nominatif* », Y. Favier, « Correspondance – Messages électroniques », *Répertoire IP/IT et Communication*, Dalloz, octobre 2019, § 1. Ainsi, l'accès aux identifiants d'un compte Gmail peuvent aussi donner accès à un compte Google Drive, dans lequel un document partagé peut inclure des correspondances, des échanges de messages entre plusieurs personnes déterminées

personnel formé, habilité et hautement disponible[51] ; et de questionnement autour de la limite fine avec la provocation à l'infraction[52].

Au contraire, en matière de perquisitions numériques, sur place ou à distance, l'extension du territoire est *a priori* limitativement et explicitement déterminée. La technique est ouverte à tous les systèmes informatiques dès qu'accessibles à partir du système initial[53]. Il s'agit donc d'une ouverture particulièrement large, grâce à une sorte de « *droit de suite* »[54]. Cependant, s'il est avéré que les données sont stockées dans un « *système situé en dehors du territoire national* », les enquêteurs ne sont plus compétents et devront recourir à la coopération internationale. L'article pose donc le critère de la localisation des serveurs. Néanmoins, en pratique, le critère est permissif : faute de preuve des serveurs à l'étranger (ce qui est peu probable), les enquêteurs peuvent accéder aux données[55]. Une preuve qui vivra sous une épée de Damoclès s'il est prouvé que les données étaient stockées à l'étranger[56].

Les techniques d'enquête permettant de lutter contre la cyber criminalité, par l'obtention de multiples types de données, sont variées. Pour la plupart, l'espace géographique n'est pas déterminé, car se reposant sur le principe générique de territorialité. Cependant, ce territoire matériel est limité au niveau national, alors que les cybercriminels se jouent desdites frontières. D'autres techniques d'enquête ont donc vu le jour, afin de permettre aux forces de l'ordre d'obtenir des éléments de preuve directement dans le cyberespace. Celui-ci permet d'étendre le territoire national à un espace numérique, qui souffre d'absence de limites ou de critères inadaptés. Une fois cette relation entre cyberespace et territoire étudiée, il convient de vérifier

---

[51] Notamment en matière d'enquête sous pseudonyme, Inspection générale des affaires sociales, Inspection générale de l'administration, Inspection générale de la justice, « Evaluation de la loi du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées », France, décembre 2019, p. 9

[52] A. Bensoussan, A. Lepage, M. Quéméner, « Loyauté de la preuve et nouvelles technologies : entre exigences processuelles et efficacité répressive », *Les transformations de la justice pénale: cycle de conférences 2013 à la Cour de cassation*, 2014, p. 236 ; M. Quéméner, « Fascicule 1110 : Infiltrations numériques », *JurisClasseur Communication*, LexisNexis, 4 février 2015, § 39

[53] Article 57-1 du code de procédure pénale. Par exemple, accès à un ordinateur, puis au navigateur Internet, puis au compte Facebook si les identifiants de connexion ont été enregistrés automatiquement

[54] R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, *op. cit.* note 18, p. 308

[55] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 28, p. 98 ; Cour de Cassation, Chambre criminelle, 6 novembre 2013, nº 12-87130. Au contraire, en Belgique, la pratique consiste à mettre les équipements en mode avion afin de n'avoir accès qu'à ce qui est stocké sur le territoire national, à savoir, sur l'équipement, C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ? », *Revue du droit des technologies de l'information*, 2017, nº 66/67, p. 31

[56] Cour de Cassation, Chambre criminelle, 9 février 2016, *op. cit.* note 39 ; Cour de Cassation, Chambre criminelle, 10 avril 2018, *op. cit.* note 39

que les techniques d'enquête sont ouvertes largement, d'un point de vue matériel, à la lutte contre la cyber criminalité.

II. Champ d'application : la multi territorialité à reconsidérer

Le territoire et le cyberespace ont été étudiés comme champ « géographique » aux techniques d'enquête. Au-delà des espaces auxquels elles permettent d'accéder, il convient aussi de questionner le rôle du territoire dans la détermination de leur champ d'application matériel. Aujourd'hui, ce rôle est inexistant. D'une part, les champs actuels d'application des techniques d'enquête ne semblent pas s'adapter complètement aux besoins de la lutte contre la cyber criminalité (A). D'autre part, la notion centrale aux techniques centrales d'enquête, le critère de « bande organisée », fait face à de nombreux obstacles dans son application à ce phénomène : dès lors, la notion de (multi) territorialité pourrait permettre de construire une nouvelle hiérarchie dans la mise en œuvre des techniques d'enquête (B).

A. L'inadéquation partielle des champs d'application matériels

En matière de champ d'application matériel des techniques d'enquête numériques, celles-ci peuvent être divisées entre techniques de droit commun et techniques spéciales d'enquête, bien qu'au sein des catégories, les champs ne soient pas entièrement harmonisés.

En premier lieu, certaines techniques d'enquête de droit commun peuvent être mises en œuvre pour toute infraction, comme les perquisitions de données informatiques[57] ou les réquisitions[58]. D'autres ne peuvent être mises en œuvre de manière générale que pour des infractions d'une certaine gravité[59], à savoir, punies d'au moins trois ans d'emprisonnement, comme pour les réquisitions visant à obtenir de données techniques de connexion, ou de trafic

[57] Articles 56, notamment 57-1, 76, 76-3, 93, et 97-1 du code de procédure pénale, sous réserve des conditions particulières de régulation de l'acte

[58] Articles 60-1 à 60-3, 77-1-1 à 77-1-3, 99-3 à 99-5 du code de procédure pénale, sous réserve de l'article 60-1-2

[59] Notamment utilisé par la Cour de Justice de l'Union européenne (CJUE), voir notamment CJEU, *Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a. (C-594/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána and Ireland*, 8 avril 2014, C-293/12 and C-594/12, § 41 ; CJEU, *Ministerio Fiscal*, 2 octobre 2018, C-207/16, § 56-63 ; CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen,* 21 décembre 2016, C-203/15 and C-698/15, § 102 ; et la CrEDH, ECHR, *Klass and others v. Germany*, 6 septembre 1978, n° 5029/71, § 51 et voir notamment ECHR, *Roman Zakharov v. Russia*, 4 décembre 2015, n° 47143/06, § 244. Ce critère permet d'établir la proportionnalité entre l'ingérence au droit à la vie privée et les besoins de la poursuite des infractions pénales

et de localisation[60], les interceptions de communication[61], la géolocalisation[62] et l'usage de drones[63]. Ce seuil de gravité est réduit à un an lorsque l'infraction est commise par la voie des communications électroniques : en matière d'enquête sous pseudonyme[64], et d'interception de communications et de réquisitions de certaines données[65]. Ces seuils sont particulièrement bas, ce qui peut amener à critiquer leur utilité[66] et imprécision[67], et semblent établir des hiérarchisations ou des regroupements particulièrement critiquables : ne sont pas différenciées la géolocalisation en temps réel et différée ; les réquisitions visant des données de connexion sont limitées par seuil de gravité, tant que celles visant des données de contenu, a priori plus invasives de la vie privée, ne le sont pas, … Néanmoins, ces seuils permettent d'ouvrir l'ensemble de ces techniques à un grand nombre d'infractions, incluant la cybercriminalité tant au sens strict qu'au sens large. Cependant, au regard des limites territoriales et techniques mentionnées pour ces techniques de droit commun, celles-ci doivent être complétées par les techniques spéciales d'enquête.

En second lieu, les techniques spéciales d'enquête sont regroupées sous le Titre XXV du Livre IV du code de procédure pénale et inclus notamment des actes d'investigation numérique[68]. Ce Titre fait l'objet d'un manque d'harmonisation flagrant[69]. Ses trois premiers articles définissent son champ d'application[70]. Pourtant, chaque acte va définir son propre champ d'application[71], sans compter des articles hors du Titre qui vont étendre celui-ci[72]. En

---

[60] Article 60-1-2.1° du code de procédure pénale. Cela inclut « *les opérations de géolocalisation en temps réel ont pour objet la localisation d'un équipement terminal de communication électronique, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la victime de l'infraction sur laquelle porte l'enquête ou l'instruction ou la personne disparue […] dès lors que ces opérations ont pour objet de retrouver la victime, l'objet qui lui a été dérobé ou la personne disparue* », article 230-44

[61] Article 100 al.1 du code de procédure pénale

[62] Article 230-32.1° du code de procédure pénale

[63] Article 230-47.1° du code de procédure pénale. Subsidiairement, ces actes incluent d'autres critères d'application : les procédures d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition et les procédures de recherche d'une personne en fuite, articles 230-32.2° et 3° et 230.17.2° et 3°

[64] Article 230-46 al.1 du code de procédure pénale

[65] Sous certaines conditions : réquisitions afin d'obtenir des données de connexion, de trafic ou de localisation dès lors que cela vise à identifier l'auteur de l'infraction, ou concernant des équipements de la victime et à sa demande, article 60-1-2.2° et 3° du code de procédure pénale ; interceptions de communication sur la ligne de la victime à sa demande, article 100 al.3

[66] REFERENCE

[67] F. Molins, « De la nécessité de lutter plus activement contre les nouvelles formes de criminalités », *Actualité juridique Pénal*, Dalloz, 2004, p. 177

[68] Mais aussi des spécificités en matière de surveillance, d'infiltration, de garde à vue, de perquisitions, …

[69] M. Quéméner, « La preuve numérique dans un cadre pénal », *op. cit.* note 42, § 80. Il est possible de souligner que ce manque d'harmonisation conduit notamment à avoir plus de 30 procédures spéciales différentes au sein du Livre IV du code de procédure pénale

[70] Articles 706-73, 706-73-1 et 706-74 du code de procédure pénale

[71] Articles 706-95 à 706-95-3 et 706-95-11 du code de procédure pénale

[72] Articles 706-2-2, 706-1-1 et 706-1-2 du code de procédure pénale

matière d'accès à distance aux correspondances, la technique est ouverte à tout crime[73]. L'ensemble des techniques spéciales d'enquête numériques[74] sont ouvertes au champs d'application matériels définis aux articles 706-73 et 706-73-1 du code de procédure pénale. Ces articles définissent une liste d'infractions qui ne cessent d'augmenter[75] et dont certaines exclusions[76] semblent parfois critiquables. Ces infractions sont des crimes et délits, majoritairement limités à leur version aggravée commise en bande organisée ; ou autres circonstances aggravantes. Celles-ci peuvent inclure la facilitation de l'infraction par le cyberespace[77], mais ces mentions sont limitées dans les infractions qu'elles concernent et dans leur rédaction. La plupart des infractions incluses au champ d'application hors circonstances aggravantes sont bien souvent des infractions pouvant être vues comme « naturellement » commises en bande organisée[78]. En matière de cybercriminalité au sens strict, seules sont incluses les atteintes aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat commises en bande organisée[79].

Ainsi, les techniques de droit commun sont largement ouvertes à un grand nombre d'infractions, facilitant leur mise en œuvre dans la lutte contre la cybercriminalité. Cependant, leurs résultats ne sont pas toujours à la hauteur des besoins de telles enquêtes. Au contraire, les techniques spéciales d'enquête ne sont donc restrictivement applicables qu'à de rares faits de cyber criminalité au sens strict ; du reste, il convient d'établir si le critère de « bande organisée » est suffisant pour les étendre aux autres infractions listées, dès lors que facilitées par le numérique.

---

[73] Articles 706-95-1 et 706-95-2 du code de procédure pénale. Une telle extension a tenté d'être mise en œuvre pour les autres techniques spéciales d'enquête regroupées sous la section 6, article 706-95-11 du code de procédure pénale, mais celle-ci fut déclarée inconstitutionnelle, Conseil constitutionnel, *Loi de programmation 2018-2022 et de réforme pour la justice*, 21 mars 2019, 2019-778 DC, § 161-165. Cette différence de traitement semble difficilement justifiable

[74] Interception de communications étendue, article 706-95 du code de procédure pénale ; accès à distance aux correspondances, articles 706-95-1 à 706-95-3 ; recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électronique, sonorisations et fixations d'images de certains lieux ou véhicules et captation des données informatiques, articles 706-95-11 à 706-102-5

[75] L'article 706-73 du code de procédure pénale a connu 18 versions ; l'article 706-73-1 en a connu six

[76] Ainsi, la traite des êtres humains est incluse, ainsi qu'une des finalités d'exploitation, le proxénétisme. Cependant, les autres modalités d'exploitation de la traite ne sont pas présentes : agression ou atteintes sexuelles, réduction en esclavage, soumission à du travail ou à des services forcés, réduction en servitude, prélèvement de l'un de ses organes, exploitation de la mendicité, conditions de travail ou d'hébergement contraires à sa dignité, contraindre la victime à commettre tout crime ou délit, article 225-4-1 du code pénal

[77] Traite des êtres humains, article 225-4-2.I. 3° du code pénal ; proxénétisme, article 225-7.10°

[78] Trafic de stupéfiants, terrorisme, association de malfaiteurs, trafic de bien culturel notamment

[79] Article 323-4-1 du code pénal

B. Face à la « bande organisée » : repenser à la « multi territorialité »

La notion de « bande organisée » souffre de nombreux maux : ses contours demeurent flous au niveau juridique, tandis que ses critères peinent à s'adapter à certains nouveaux phénomènes de cyber criminalité. Face à ces limites, repenser au territoire, ou plutôt, à la multiplicité des territoires impliqués, permettrait de redéfinir une échelle dans les champs d'application des techniques d'enquête numériques.

Malgré des définitions supranationales relativement harmonisées[80], la définition de « bande organisée » est relativement large : « *tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions* »[81]. A la différence des textes internationaux, cette définition ne contient aucune information quant au nombre de personnes impliquées, à la base temporelle du groupe et à la nature des infractions qui seront commises. Dès lors, il s'agit d'un concept hautement critiqué par la doctrine[82]. Comme la Cour de cassation n'a pas fourni de définition plus détaillée, les juridictions se sont appuyées sur différents critères, tels qu'une pluralité d'individus se regroupant afin de commettre une infraction, des actes préparatoires coordonnés ou une organisation structurée[83]. En raison de l'absence de critères fixes, l'existence ou l'absence de la circonstance est laissée à la discrétion du procureur[84], et n'est majoritairement pas contrôlée par la Cour de Cassation[85].

De plus, la notion de « bande organisée » pourrait peiner à s'appliquer avec le développement de certains phénomènes criminologiques en lien avec la cyber criminalité.

---

[80] Voir notamment l'article 2.a de la Convention des Nations Unies contre la criminalité transnationale organisée ; au sein de l'Union européenne, l'article 1.1 de la décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée ; et au sein du Conseil de l'Europe, Committee of Ministers, « Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime », Council of Europe, 19 septembre 2001

[81] Article 132-71 du code pénal

[82] C. Lazerges, « La dérive de la procédure pénale », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2003, p. 644 ; E. Vergès, « La notion de criminalité organisée après la loi du 9 mai 2004 », *Actualité juridique Pénal*, Dalloz, 2004, p. 181 ; T. Godefroy, « The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference », *in* C. Fijnaut, L. Paoli (dir.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime n° 4, 1re éd., 2006, p. 763 ; C. Guerrier, « « Loppsi 2 » et l'utilisation des nouvelles technologies », *Revue Le Lamy Droit de l'immatériel*, 1 octobre 2010, n° 64 ; C. Lazerges, « Le déclin du droit pénal : l'émergence d'une politique criminelle de l'ennemi », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 649

[83] E. Vergès, « La notion de criminalité organisée après la loi du 9 mai 2004 », *op. cit.* note 82, p. 181

[84] C. Guerrier, « « Loppsi 2 » et l'utilisation des nouvelles technologies », *op. cit.* note 82

[85] E. Vergès, « La notion de criminalité organisée après la loi du 9 mai 2004 », *op. cit.* note 82, p. 181. However, in 2016, the court seemed to consider two criteria for the notion, that "*presupposes the premeditation of the offences and a structured organization of its members*," Cour de Cassation, Chambre criminelle, 22 juin 2016, n° 16-81834

Notamment, se multiplient les cas de « *crime as a service* »[86] (ou « *criminal experts* »)[87] : des « autoentrepreneurs », notamment des cybercriminels, vont offrir des solutions afin de faciliter ou de permettre à d'autres individus de commettre une infraction (par exemple, vente de logiciels permettant de commettre une atteinte à un système automatisé de traitement de données, ou une usurpation d'identité)[88]. D'autre part, le numérique permet à des micro-réseaux ou des personnes individuelles de commettre des infractions de grande ampleur[89]. De manière générale, les réseaux criminels semblent moins « coordonnés », basées plus sur le recours à une expertise ou à des considérations pratiques temporaires, plus qu'à une réelle « entente ». Ainsi, en 2021, Europol considère que 60% des réseaux criminels sont des structures fluides[90].

Par conséquent, si la notion de « bande organisée » ne permet plus d'inclure les techniques d'enquête nécessaire à lutter contre la cybercriminalité, dont les dommages peuvent s'étendre considérablement de par la rapidité des échanges et l'ubiquité du cyberespace, une meilleure harmonisation des champs d'application matériels et de nombreux critères de hiérarchisation devraient être repensés. En ce sens, le territoire, plus qu'une délimitation du champ géographique des techniques d'enquête, pourrait émerger comme un critère de leur champ d'application matériel. Plus que le territoire au sens limitatif, l'implication de multiples territoires liées à une infraction (IP étrangère, serveurs ou société mère dans des pays classés « à risque », dommages produits sur de multiples territoires, …) pourrait permettre la mise en œuvre de techniques d'enquête plus invasives de la vie privée. Ce critère pourrait s'appliquer tant à la cyber criminalité qu'à la criminalité organisée[91]. Afin de justifier l'ingérence au droit à la vie privée, la CrEDH accepte les termes généraux pour définir le champ d'application matériel, dès lors qu'ils sont définis[92]. Le défi à relever sera alors de redéfinir le territoire ou les territoires en prenant en compte les espaces numériques.

---

[86] Europol, *SOCTA 2021*, *op. cit.* note 16, p. 20
[87] Europol, « European Union serious and organised crime threat assessment - Crime in the age of technology », EU, 2017, p. 13
[88] Europol, *IOCTA 2021*, *op. cit.* note 16, p. 17
[89] Europol, *SOCTA 2017*, *op. cit.* note 87, p. 14
[90] Europol, *SOCTA 2021*, *op. cit.* note 16, p. 18, notamment présents sur le Dark Web, Europol, *IOCTA 2021*, *op. cit.* note 16, p. 36
[91] Ainsi, parmi les réseaux criminels étudiés par Europol en 2021, sept sur dix étaient actifs dans plus de trois pays, Europol, *SOCTA 2021*, *op. cit.* note 16, p. 18
[92] ECHR, *Big Brother Watch and others v. the United Kingdom (2)*, 25 mai 2021, 58170/13, 62322/14 and 24960/15, § 368-371

Annexe 1 : Champs d'application matériel du Titre XXV quant à la procédure applicable à la criminalité et à la délinquance organisées et aux crimes

Article 706-73

Articles du code pénal	Infractions	Qualification
221-4 8°.4	Meurtre	Bande organisée
222-4	Tortures et actes de barbarie	Bande organisée
222-34 à 222-40	Trafic de stupéfiants	/
224-5-2	Enlèvement et de séquestration	Bande organisée
225-4-2 à 225-4-7	Traite des êtres humains	Formes aggravées
225-7 à 225-12	Proxénétisme	Formes aggravées
311-9	Vol	Bande organisée
312-6 et 312-7	Extorsion	Formes aggravées
322-8	Destruction, dégradation et détérioration d'un bien	Bande organisée
442-1 et 442-2	Crimes en matière de fausse monnaie	/
421-1 à 421-6	Actes de terrorisme	/
Titre Ier du livre IV	Atteinte aux intérêts fondamentaux de la nation	/
222-52 à 222-54, 222-56 à 222-59, 322-6-1 et 322-11-1	Délits en matière d'armes et de produits explosifs	/
L. 823-1 et L. 823-2 du code de l'entrée et du séjour des étrangers et du droit d'asile	Délits d'aide à l'entrée, à la circulation et au séjour irréguliers	Bande organisée
324-1 et 324-2	Blanchiment des infractions ci-dessus	/
321-1 et 321-2	Recel des infractions ci-dessus	/
224-6-1	Détournement d'aéronef, de navire ou de tout autre moyen de transport	Bande organisée
450-1	Association de malfaiteurs pour les infractions ci-dessus	/
321-6-1	Non-justification de ressources pour les infractions ci-dessus	/
L. 512-2 du code minier	Exploitation d'une mine ou de disposition d'une substance concessible sans titre d'exploitation ou autorisation, accompagné d'atteintes à l'environnement connexe aux infractions ci-dessus	Bande organisée
706-167 du code de procédure pénale	Crimes et délits contribuant à la prolifération des armes de destruction massive et de leurs vecteurs	Punis de dix ans d'emprisonnement

Article 706-73-1 (article 706-88 inapplicable en matière de garde à vue)

Articles du code pénal	Infractions	Qualification
313-2	Escroquerie	Bande organisée
323-4-1	Atteinte aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat[93]	Bande organisée
434-30	Evasion	Bande organisée

[93] Doublon avec l'article 706-72 du code de procédure pénale, ce dernier étant plus restrictif : « *Les articles 706-80 à 706-87, 706-95 à 706-103 et 706-105 du présent code sont applicables à l'enquête, à la poursuite, à l'instruction et au jugement des délits prévus à l'article 323-4-1 du code pénal*. »

L. 8221-1 1° et 3°, L. 8221-3, L. 8221-5, L. 8224-1, L. 8224-2, L. 8231-1, L. 8234-1, L. 8234-2, L. 8241-1, L. 8243-1, L. 8243-2, L. 8251-1 et L. 8256-2 du code du travail	Dissimulation d'activités ou de salariés, recours aux services d'une personne exerçant un travail dissimulé, marchandage de main-d'œuvre, prêt illicite de main-d'œuvre ou d'emploi d'étranger sans titre de travail	Bande organisée
324-1 et 324-2	Blanchiment des infractions ci-dessus	/
321-1 et 321-2	Recel des infractions ci-dessus	/
450-1	Association de malfaiteurs pour les infractions ci-dessus	/
324-2	Blanchiment (autres que ceux précédemment mentionnés)	Bande organisée ou habituel
321-6-1	Non-justification de ressources pour les infractions ci-dessus	/
322-3-2	Importation, exportation, transit, transport, détention, vente, acquisition ou échange d'un bien culturel	/
L. 415-6 du code de l'environnement	Atteintes au patrimoine naturel	Bande organisée
L. 253-17-1 3°, L. 253-15.II, L. 253-16.II et L. 254-12.III du code rural et de la pêche maritime	Trafic de produits phytopharmaceutiques	Bande organisée
L. 541-46.VII du code de l'environnement	Délits relatifs aux déchets	Bande organisée
L. 324-1 du code de la sécurité intérieure	Participation à la tenue d'une maison de jeux d'argent et de hasard	Bande organisée
L. 324-4 du code de la sécurité intérieure	Importation, fabrication, détention, mise à disposition de tiers, installation et exploitation d'appareil de jeux d'argent et de hasard ou d'adresse	Bande organisée
411-5,411-7 et 411-8, 412-2 §1 et 2, 413-1 et 413-13 §3	Atteinte aux intérêts fondamentaux de la nation	/

Article 706-74

Articles du code pénal	Infractions	Qualification
/	Crimes (autres)	Bande organisée
/	Délits (autres)	Bande organisée
450-1	Association de malfaiteurs pour les infractions ci-dessus	Pour des crimes et délits punis de dix ans d'emprisonnement

En matière d'atteintes à l'environnement, voir aussi l'article 706-2-2 du code de procédure pénale :

« *Les articles 706-80 à 706-87 et 706-95 à 706-103 sont applicables à l'enquête, à la poursuite, à l'instruction et au jugement :*

1° Des délits prévus aux articles L. 5421-2, L. 5421-13, L. 5426-1, L. 5432-1, L. 5432-2, L. 5432-3, L. 5438-4, L. 5438-6, L. 5439-1, L. 5439-2, L. 5442-10, L. 5442-14, L. 5461-3 et L. 5462-3 du code de la santé publique, lorsqu'ils sont punis d'une peine d'emprisonnement d'une durée supérieure à cinq ans [Formes aggravées uniquement] ;

2° Des délits prévus aux articles L. 451-2 [1° Si la substance falsifiée ou corrompue est nuisible à la santé humaine ou animale ; 2° Si les faits ont été commis en bande organisée] et L. 454-3 du code de la consommation [1° A eu pour conséquence de rendre l'utilisation de la marchandise dangereuse pour la santé de l'homme ou de l'animal ; 2° A été commis en bande organisée.].
Les articles 706-80 à 706-87 et 706-95 à 706-103 du présent code sont également applicables à l'enquête, à la poursuite, à l'instruction et au jugement du blanchiment des délits mentionnés aux 1° et 2° du présent article. »

En matière économique et financière, voir aussi les articles 706-1, 706-1-1 et 706-1-2 du code de procédure pénale :
Article 706-1
« *Les articles 706-80 à 706-87 sont applicables à l'enquête relative aux délits prévus par les articles L. 335-2, L. 335-3, L. 335-4, L. 343-4, L. 521-10, L. 615-14, L. 716-9 et L. 716-10 du code de la propriété intellectuelle lorsqu'ils sont commis en bande organisée.* »
Article 706-1-1
« *Les articles 706-80 à 706-87 [Rédaction conforme au dernier alinéa de l'article 1er de la décision du Conseil constitutionnel n° 2013-679 DC du 4 décembre 2013], 706-95 à 706-103, 706-105 et 706-106 sont applicables à l'enquête, à la poursuite, à l'instruction et au jugement des délits prévus :*
1° Aux articles 432-11 [corruption passive et du trafic d'influence commis par des personnes exerçant une fonction publique], 432-15 [soustraction et du détournement de biens], 433-1, 433-2 [corruption active et du trafic d'influence commis par les particuliers], 434-9, 434-9-1 [corruption active et passive entravant l'exercice de la justice], 435-1 à 435-4 [corruption et du trafic d'influence passifs et actifs portant atteinte à l'administration publique] et 435-7 à 435-10 [corruption et du trafic d'influence passifs et actifs portant atteinte à l'action de la justice] du code pénal ;
2° Aux articles 1741 et 1743 [infractions de fraude à l'impôt] du code général des impôts, lorsqu'ils sont commis en bande organisée ou lorsqu'il existe des présomptions caractérisées que ces infractions résultent d'un des comportements mentionnés aux 1° à 5° du II de l'article L. 228 du livre des procédures fiscales [1° Soit de l'utilisation, aux fins de se soustraire à l'impôt, de comptes ouverts ou de contrats souscrits auprès d'organismes établis à l'étranger ; 2° Soit de l'interposition de personnes physiques ou morales ou de tout organisme, fiducie ou institution comparable établis à l'étranger ; 3° Soit de l'usage d'une fausse identité ou de faux documents au sens de l'article 441-1 du code pénal, ou de toute autre falsification ; 4° Soit d'une domiciliation fiscale fictive ou artificielle à l'étranger ; 5° Soit de toute autre manœuvre destinée à égarer l'administration.] ;
3° Au dernier alinéa de l'article 414 [contrebande ainsi que tout fait d'importation ou d'exportation sans déclaration lorsque ces infractions se rapportent à des marchandises de la catégorie de celles qui sont prohibées au sens du présent code ou aux produits du tabac manufacturé soit lorsque les faits de contrebande, d'importation ou d'exportation portent sur des marchandises dangereuses pour la santé, la moralité ou la sécurité publiques, dont la liste est fixée par arrêté du ministre chargé des douanes, soit lorsqu'ils sont commis en bande organisée] et à l'article 415 [opération financière entre la France et l'étranger portant sur des fonds qu'ils savaient provenir, directement ou indirectement, d'un délit prévu au présent code ou portant atteinte aux intérêts financiers de l'Union européenne, ou d'une infraction à la législation sur les substances ou plantes vénéneuses classées comme stupéfiants] du code des douanes, lorsqu'ils sont punis d'une peine d'emprisonnement d'une durée supérieure à cinq ans ;

4° Aux articles L. 465-1 à L. 465-3-3 [Atteintes à la transparence des marchés] du code monétaire et financier lorsqu'ils sont commis en bande organisée.
Les articles mentionnés au premier alinéa du présent article sont également applicables à l'enquête, à la poursuite, à l'instruction et au jugement du blanchiment des délits mentionnés aux 1° à 3°. »
Article 706-1-2
« *Les articles 706-80 à 706-87, 706-95 à 706-103 et 706-105 sont applicables à l'enquête, à la poursuite, à l'instruction et au jugement des délits prévus au dernier alinéa des articles L. 241-3 [infraction concernant les sociétés à responsabilité limitée punie par 5 ans d'emprisonnement] et L. 242-6 [infraction relatives à la direction et à l'administration des sociétés anonymes punie par 5 ans d'emprisonnement] du code de commerce*. »

Annexe 2 : Champs d'application matériel des techniques d'enquête étudiées

Articles du code de procédure pénale	Technique d'enquête	Champ d'application matériel
Techniques d'enquête de droit commun		
56 et suivants, 76, 92 et suivants	Perquisition	Toute infraction
60-1 à 60-3, 77-1-1 à 77-1-3, 99-3 à 99-5 (hors 60-1-2)	Réquisition	Toute infraction
60-1-2	Réquisitions portant sur les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux	• Crime ou délit puni d'au moins trois ans d'emprisonnement • Délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques, pour identifier l'auteur de l'infraction • Délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques, si concerne les équipements de la victime et à sa demande • Recherche des causes de la disparition prévue aux articles 74-1 et 80-4 • Procédure pour les crimes sériels ou non élucidés prévue à l'article 706-106-1
100 à 100-8	Interception de communications	• Crime ou délit si la peine encourue est égale ou supérieure à trois ans d'emprisonnement • Délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques, si interception sur la ligne de la victime à sa demande
230-32 à 230-43	Géolocalisation	• Crime ou délit puni d'au moins trois ans d'emprisonnement • Recherche des causes de la mort ou de la disparition prévue aux articles 74, 74-1 et 80-4 • Recherche d'une personne en fuite prévue à l'article 74-2
230-44 et t 60-1, 60-2, 77-1-1, 77-1-2, 99-3 ou 99-4	Géolocalisation en temps réel pour la localisation d'un équipement terminal de communication électronique, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la victime de l'infraction ou la	Toute infraction

	personne disparue, pour retrouver la victime, l'objet ou la personne disparue	
230-46	Enquête sous pseudonyme	Crime ou délit punis d'une peine d'emprisonnement commis par la voie des communications électroniques
230-1 à 230-5	Mise au clair des données chiffrées	Toute infraction
230-47 à 230-53	Captations et fixations d'images dans les lieux publics au moyen de dispositifs aéroportés	• Crime ou délit puni d'au moins trois ans d'emprisonnement • Recherche des causes de la mort ou de la disparition prévue aux articles 74, 74-1 et 80-4 • Recherche d'une personne en fuite prévue à l'article 74-2
Techniques spéciales d'enquête		
706-95	Interception de communications	Articles 706-73 et 706-73-1 ; articles 706-2-2, 706-1-1 et 706-1-2
706-95-1 à 706-95-3	Accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique	Crime ou l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 ; articles 706-2-2, 706-1-1 et 706-1-2
706-95-11 à 706-95-19 et 706-95-20	Recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques	Articles 706-73 et 706-73-1 ; articles 706-2-2, 706-1-1 et 706-1-2
706-95-11 à 706-95-19 et 706-96 à 706-98	Sonorisations et des fixations d'images de certains lieux ou véhicules	Articles 706-73 et 706-73-1 ; articles 706-2-2, 706-1-1 et 706-1-2
706-95-11 à 706-95-19 et 706-102-1 à 706-102-5	Captation des données informatiques	Articles 706-73 et 706-73-1 ; articles 706-2-2, 706-1-1 et 706-1-2