ASSOCIATION INTERNATIONALE DE DROIT PENAL
XIXe Congrès International de Droit Pénal

"Société de l'information et Droit Pénal"

Colloque Préparatoire - Section 4

CYBERCRIMINALITE
ASPECTS DE DROIT PENAL INTERNATIONAL *

Rapport français
par Jacques FRANCILLON
Professeur agrégé des Facultés de droit
ancien professeur émérite de l'Université Paris-Sud 11

Présentation générale
(en rapport avec l'annexe 1 commun aux 4 sections)

Les concepts de cybercriminalité et de cyberdélinquance sont flous. Ils le sont d'autant plus que les textes ne les définissent pas. Une triple approche permet néanmoins d'apporter les éclaircissements nécessaires.

Approche sémantique. Celle-ci fournit une première indication. Elle fait apparaître le lien qui unit la criminalité (ou la délinquance) au cyberespace, c'est-à-dire à l'espace cybernétique, à la communication en ligne, à la communication par voie électronique, aux réseaux de télécommunication (le Web en l'occurrence). C'est dans cet espace, en apparence virtuel, immatériel, en tout cas sans frontières, mondialisé, universel,[1] que des infractions pénales sont susceptibles d'être commises et qu'elles le sont effectivement.[2] Ainsi est mis d'emblée en lumière l'un des aspects qui est au cœur de la problématique du droit pénal de l'internet : dans quelle mesure ce droit prend-il en compte à la fois l'ubiquité et l'immédiateté qui caractérisent les flux d'information sur le Web ?

Approche criminologique. Elle fournit plusieurs autres indications. Il en ressort : que de nouvelles formes de déviance sont apparues sur le web à côté de formes plus

[1] V. Le droit et l'immatériel, *in* Archives de philosophie du droit, t. 43, 1999, Dalloz/ Sirey, 1999, par divers auteurs, spéc. les études de W. Capeller et G. Vermelle p. 167 s. et 213 s., et Rapport du Conseil d'État 1998, cité *infra*.

[2] *ibid.* - *Adde* : C. Féral-Schuhl, Cyberdroit : le droit à l'épreuve de l'internet, Dalloz, 6è éd. 2011-2012 ; A. Lepage, Droit pénal et internet : la part de la tradition, l'œuvre de l'innovation, AJ Pénal 2005. 217 s. ; A. Huet, étude citée *infra*, cet auteur observant que « le phénomène criminel dans le "cyber-espace " comporte très fréquemment un élément d'extranéité et a donc un caractère international » (p. 165).

* 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.

traditionnelles ; qu'elles s'inscrivent toutes dans un ensemble multiple et hétérogène ; qu'elles sont facilitées et considérablement amplifiées par les nouvelles technologies de l'information et de la communication (NTIC) ; que les mobiles inspirant leurs auteurs sont très divers (l'argent, le sexe, le pouvoir). Il en ressort également qu'elles affectent le commerce électronique (délinquance « en col blanc »), mais aussi les activités non marchandes (*newsgroups* à visées racistes ou pédophiles) ; qu'elles peuvent notamment consister à pénétrer indûment dans les systèmes informatiques de grandes entreprises, à manipuler les citoyens par la propagande ou la désinformation, voire à déstabiliser les États eux-mêmes[3] ; qu'à cet égard les " déviations " du cyberespace sont multiples et lourdes de dangers. Il en ressort encore que le sentiment d'impunité qu'éprouvent les *hackers*, les *crackers*, les *crashers* et autres pirates ou « trafiquants du vide »,[4] est favorisé par les caractéristiques propres d'internet : volatilité des contenus, anonymat (cryptage), évolutions technologiques incessantes, caractère décentralisé et transnational du réseau. Dès lors, l'un des mérites d'une telle approche est de mettre en évidence un autre aspect de la problématique : le droit pénal est-il doté de moyens suffisamment efficaces pour répondre à la multiplicité et à la dangerosité des cybercrimes et délits ?

Approche juridique. Les infractions commises sur le web se rattachent à la criminalité informatique.[5] Celle-ci constitue elle-même une notion floue car elle

---

[3] Deux illustrations permettent d'en prendre la mesure. La première concerne un phénomène de grande ampleur : les piratages de créations intellectuelles sur le web. Un site internet figurant parmi les plus consultés en France (*Liberty Land),* et financé par d'importantes ressources publicitaires, donnait accès ces dernières années à des dizaines de milliers de liens vers des contenus contrefaisants. Sur plainte de la SACEM (organisme français chargé de protéger les droits d'auteur pour les œuvres musicales), la cellule de lutte contre la cybercriminalité de Rennes a procédé à une longue enquête. Ses recherches ont été difficiles car le site litigieux était hébergé au Canada et de nombreuses barrières avaient été mises en place pour préserver l'anonymat de ses administrateurs. Ceux-ci ont finalement été arrêtés et le site désactivé. Cette situation est à rapprocher d'un autre événement : la fermeture brutale du site MegaUpload en 2012 à l'initiative des autorités américaines, aussitôt suivie de représailles du collectif de pirates Anonymous. La seconde illustration est relative au plan américain de lutte contre les cyberattaques qui, on le sait, se multiplient à l'heure actuelle (virus espion *Stuxnet*. attaques dirigées contre *Sony* et *Nintendo,* attaques du site de la *CIA***,** etc..). Il s'inscrit dans une nouvelle stratégie destinée à renforcer la coopération internationale en matière d'internet, au besoin par des moyens militaires, afin notamment de faire face aux menaces cyberterroristes. Il a aussi pour but de promouvoir la liberté d'expression sur la toile tout en protégeant la vie privée des internautes. Quant au vent de panique qui a soufflé à Wall Street le 23 avril 2013 après le piratage du compte Twitter de l'agence Associated Press – une intrusion ayant fait perdre en trois minutes au Dow Jones l'équivalent de 105 millards d'Euros de capitalisation (Le Monde du 25 avril) - il permet de mesurer l'importance des enjeux économiques de ce type de délinquance.

[4] W. Capeller, étude citée *supra* p. 175.

[5] V. notre étude, Les crimes informatiques et autres crimes dans le domaine de la technologie informatique en France, Rapport national français au XVè Congrès de l'Association Internationale de Droit Pénal, *in* Information Technology Crime, RIDP 1993,

recouvre des réalités multiples. De manière schématique ces infractions peuvent être regroupées en deux catégories : les unes sont commises contre le réseau, tandis que les autres le sont grâce au réseau. Les premières sont dirigées contre les systèmes de traitement automatisés de données (STAD), qu'il s'agisse de l'accès non autorisé à ces systèmes ou des atteintes portées à l'intégrité des données ou à leur confidentialité. Les secondes sont des infractions classiques ; elles peuvent tout aussi bien être perpétrées en dehors du réseau. Il en résulte que la spécificité des infractions commises dans le cyberespace est toute relative.

La cyberdélinquance et la cybercriminalité soulèvent sur le plan juridique des questions d'autant plus difficiles à résoudre qu'elles affectent une société globalisée. Cette situation rend a priori la régulation illusoire à un niveau exclusivement national, territorial. Elle impose donc de mettre en place un cybercontrôle à l'échelle régionale, voire mondiale. Deux textes issus du Conseil de l'Europe mais ouverts à l'adhésion des États tiers répondent à cette exigence : la convention de Budapest sur la cybercriminalité du 23 novembre 2001 et son protocole additionnel du 28 janvier 2003.[6] Il ressort de ces instruments internationaux que les États sont (ou seront) tenus de prendre les « dispositions appropriées » de droit substantiel et de procédure en vue d'accroître l'efficacité de la lutte contre ce type de délinquance et de criminalité. Sont principalement visés les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données ainsi que leur usage frauduleux. S'y ajoutent, notamment, la piraterie dans le domaine du droit d'auteur et des droits voisins, ou encore les actes de nature raciste et xénophobe commis par voie électronique. Le renforcement, aux plans national et international, des pouvoirs de détection, d'investigation et de poursuite, de même que les mesures tendant à développer l'entraide répressive entre les États, sont également préconisés, sous réserve du respect par ces derniers des droits fondamentaux des personnes impliquées.[7] Sur ce dernier aspect, plusieurs textes issus de l'Union européenne, tels

---

n° 1 et 2, p. 291 s. ; La cybercriminalité, cybercrime, la cybercriminalidad, par divers auteurs, RIDP 2006, n° 4. - *Adde* sur les rapports entre cybercriminalité et criminalité informatique, les études citées *supra* et *infra*.

6 Décr. n° 2006-580 et 206-597 du 23 mai 2006, JO des 24 et 27 mai 2006, p. 7568 et 7937.

7 V. sur ces différents aspects les études de C. Latry-Bonnart, L'arsenal pénal juridique sur internet, Gaz. Pal. 1997, 2, p. 997, Y. Padova, Aperçu de la lutte contre la cybercriminalité en France, RSC 2002. 765, M. Chawki, Le droit pénal à l'épreuve de la cybercriminalité, Thèse, Lyon III, 2006, et F. Chopin, Cybercriminalité, Répertoire Pénal Dalloz, 2009, ainsi que les dossiers consacrés au sujet *in* RIDP 2006 n° 4, cité *supra* et AJ Pénal 2005 n° 6 (Internet : un nouvel espace de délinquance) et 2009 n° 3 (Cybercriminalité: morceaux choisis) ; V. également les ouvrages de C. Féral-Schuhl, cité *supra,* et M. Quéméner / J. Ferry, La cybercriminalité. Défi mondial, Economica, 2è éd. 2009, ainsi que le Rapport national français au XVIIIè Congrès international de droit comparé, par D. Chilstein, RIDC, 2010 n° 2, p. 553 s. *Adde* : L'internationalisation du droit pénal, Dr. pénal, sept. 2006, p. 1 s., par divers auteurs, spéc. la synthèse de V. Malabat, Étude 17.

que la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[8] ou ainsi que la proposition de directive portant sur le même sujet (actuellement en discussion au niveau du Parlement européen et du Conseil), révèle l'importance de ce dernier enjeu.

Les nouveaux défis auxquels les États doivent faire face sont dès lors clairement identifiés. Les difficultés que ces derniers s'efforcent de surmonter pour les relever le sont également. Il s'agit en effet de concilier le caractère spatio-temporel – délimité et stable – de la norme de droit pénal avec le caractère global de l'espace virtuel. A l'universalité des réseaux numériques, à l'ubiquité et à l'immédiateté des échanges sur le Web, aux pratiques d'externalisation des données (le *cloud computing* accroît le risque d'éparpillement d'informations parfois sensibles), répond un certain relativisme juridique.[9] Il en est particulièrement ainsi en matière pénale où les tendances souverainistes l'emportent aujourd'hui encore trop souvent sur les tendances universalistes, en dépit des évolutions en cours. Car la répression pénale demeure largement *« territorialisée »* : le droit pénal applicable aux cybercrimes et aux cyberdélits n'échappe pas à la règle en dépit de l'universalité du réseau internet auquel il se trouve confronté. Cette répression n'en est pas moins *« internationalisée »* : elle est en effet également confrontée au phénomène d'internationalisation qui, de manière plus générale, affecte l'ensemble du droit pénal contemporain.

Dans un rapport publié dès 1998, intitulé « Internet et les réseaux numériques », le Conseil d'État français avait déjà fait le constat suivant[10] : « Ce qui est nouveau, c'est d'une part, la plus grande facilité avec laquelle des infractions peuvent être commises et diffusées dans le monde du fait de la structure du réseau et de son mode de fonctionnement et, d'autre part, les difficultés rencontrées dans l'application des textes du fait de la fugacité extrême des contenus et de la dimension internationale d'Internet ». Aussi, à une « approche centralisée et verticale », était-il préconisé de substituer des « orientations transversales et décentralisées ». La nécessité d'adapter notre droit et de renforcer la coopération entre les États était également mise en évidence. Il apparaissait ainsi, en France, dès cette époque, que les initiatives purement nationales, pour aussi nécessaires qu'elles fussent, ne permettaient pas, à elles seules, de lutter avec toute l'efficacité souhaitable contre une forme de délinquance et de criminalité aussi envahissante. Cette observation se vérifie, tant en ce qui concerne les questions de compétence que les mécanismes d'entraide.

---

8 JO L 350, 30.12.2008, p 60.

9 M. Delmas-Marty, Les forces imaginantes du droit, t. 1, Le relatif et l'universel, éd. du Seuil, 2004, spéc. p. 336.

10 Rapport du Conseil d'État 1998, Internet et les réseaux numériques : étude adoptée par l'Assemblée générale le 2 juillet 1998, Section du rapport et des études, Collection Études du Conseil d'État, par J.-F. Théry et I. Falque Pierrotin, La Documentation française, 1998 [introduction de la 4è partie : « Lutter contre les contenus et comportements illicites »].

I. Questions de compétence

(points B et C du questionnaire)

Sur le plan interne, les critères de rattachement du droit commun en matière pénale (territorial, personnel, réel, universel), confrontés à l'universalité de l'internet, sont naturellement applicables aux cybercrimes et aux cyberdélits (A). Dès lors, la question se pose de savoir si, en dépit de la spécificité des NTIC et du Web, ces critères sont pertinents, ou si, à défaut, il conviendrait de les affiner, voire de leur en substituer d'autres (B).

A. Application des critères de rattachement du droit commun

A première vue, cette application ne soulève pas de problème particulier, du moins en ce qui concerne la loi applicable à l'action publique (1). Mais il s'agit plus d'une apparence que d'une réalité. De sérieuses difficultés résultent en effet de ce que la nature spécifique du Web n'est pas suffisamment prise en compte (2).

1° Apparente adaptation des critères de rattachement du droit commun

Les règles françaises attributives de la compétence législative et juridictionnelle en matière pénale répondent en apparence aux nécessités de la répression, le principe traditionnel étant celui de la solidarité de ces compétences.[11] Elles permettent en effet d'appréhender de manière relativement simple ce type de criminalité dans ses manifestations les plus diverses.

Il en est ainsi, plus particulièrement, en cas d'application du critère de compétence territorial, dès lors que l'infraction peut être localisée sur le territoire national, en totalité, ou en partie seulement, par application de la théorie dite de « l'ubiquité » ; il suffit, dans ce dernier cas, qu'un « fait constitutif » soit localisé sur ce territoire.[12] Or on sait qu'en France, comme d'ailleurs à l'étranger, la tendance jurisprudentielle dominante va dans le sens d'une extension de ce critère de compétence, au point que ses excès et son caractère « impérialiste » sont fréquemment dénoncés.[13] Toujours est-il que les exemples abondent et que les juges nationaux disposent ainsi d'un moyen efficace pour réprimer les crimes et délits de toutes natures localisés, au moins partiellement, parfois même de manière ténue, sur le territoire national.[14] Le domaine

---

[11] H. Donnedieu de Vabres, Les principes modernes du droit pénal international, Sirey, 1928, réédition par les Éditions Panthéon-Assas, 2004, avant-propos de J. Foyer ; C. Lombois, Droit pénal international, Dalloz, 2è éd. 1979 ; A. Huet et R. Koering-Joulin, Droit pénal international, collect. Thémis, PUF, 3è éd. 2005 ; D. Rebut, Droit pénal international, Précis Dalloz, 1ère éd. 2012.

[12] V. en France : CP art. 113-2, al. 1 et 2, déclarant la loi pénale française applicable aux infractions commises ou *réputées* commises sur le territoire de la République.

[13] V. plusieurs des auteurs cités *supra* et *infra*.

[14] Parmi les décisions jurisprudentielles les plus remarquées : Crim., 12 févr. 1979,

de la cyberdélinquance et de la cybercriminalité est concerné de la même façon.[15] En outre, la jurisprudence française parvient à étendre ce critère de rattachement par le jeu de la connexité, et surtout de l'indivisibilité entre les infractions objet des poursuites. L'incrimination d'association de malfaiteurs, de même que la circonstance aggravante de bande organisée, se prêtent particulièrement bien à une telle extension.[16] *Mutatis mutandis*, les solutions retenues sont aisément transposables à la cybercriminalité. En effet, l'utilisation délictueuse des réseaux de communication électronique est souvent en relation avec la commission d'infractions graves se rattachant à la criminalité organisée (terrorisme, blanchiment, trafics de drogue, etc..) ; il importe peu, dès lors, que ces dernières soient entièrement localisées à l'étranger.

À cette jurisprudence extensive s'ajoutent les dispositions légales conférant une portée extraterritoriale à la loi pénale française.[17] Il en est ainsi lorsque la loi incrimine les sollicitations émanant de clients de prostitué(e)s mineur(e)s (CP art. 225-12-1 et s., résultant de la loi du 4 mars 2002 relative à l'autorité parentale). Dans ces situations dites de « tourisme sexuel », la compétence française peut en effet être retenue dès lors que les sollicitations litigieuses se font via internet, le cas échéant par e mail, depuis un ordinateur localisé à l'étranger, en direction de mineurs eux-mêmes situés à l'étranger. Car si le client est français, ou s'il a sa résidence habituelle en France, la compétence personnelle française n'est plus subordonnée à la condition de réciprocité d'incrimination ni à l'exigence d'une plainte préalable de la victime ou d'une dénonciation officielle des autorités compétentes étrangères (art. 225-12-3). C'est dire qu'en pareil cas, s'agissant de situations en rapport avec le tourisme sexuel,[18] le cyberdélinquant n'échappe pas au risque de poursuites pénales en France.[19] C'est une solution comparable qui a été retenue en matière de terrorisme par

---

Bull. crim. n° 60 (abus de confiance), 1er oct. 1986, *ibid.*, n° 262 (recel d'abus de confiance), 26 sept. 2007, *ibid.*, n° 224 (recel de vol).

15 V. à titre d'illustration : Crim., 11 sept. 2007, n° 07-82018, approuvant la condamnation pour recel de corruption de mineur d'un prévenu qui, après s'être connecté à internet, avait enregistré sur son ordinateur des images pédopornographiques provenant d'un site anglais hébergé par un serveur américain. - Rappr. : Crim., 4 févr. 2004, Bull. crim. n° 32, D. 2005. 621, note V. Malabat, Dr. Pénal 2004, comm. n° 80, note M. Véron, RSC 2004. 639, obs. Y. Mayaud, concernant un enregistrement d'images de même nature réalisé en Thaïlande ; l'arrêt admet, de manière il est vrai assez contestable, la compétence territoriale française en raison du fait qu'un contrat, non exécuté, avait été signé en France en vue de la diffusion de cet enregistrement ; V. not. pour les critiques, V. Malabat, note préc., et E. Dreyer, Étude citée *infra*, p. 277. *Adde* : CP art. 227-23, incriminant le fait de créer, de *transférer* ou d'*importer* des images à caractère pornographique représentant des mineurs ; et pour une application : Crim., 6 août 2008, n° 08-83490, inédit.

16 Crim., 23 avr. 1981, Bull. crim. n° 116, RSC 1982. 609, obs. A. Vitu ; 27 oct. 2004, Bull. crim. n° 263, RSC 2005. 294, note G. Vermelle, Dr. pénal 2005, comm. n° 16, obs. A. Maron, *ibid.*, comm. n° 32, obs. M. Véron.

17 CP art. 113-6 et s. ; CPP art. 689 et s. *Adde* : A. Huet, étude citée *infra*, spéc. p. 670 et 671.

18 V. déjà L. 17 juin 1998, et Chron. législ. *in* RSC 1998. 792, obs. J.-F. Seuvic.

19 *Adde* : L. 10 mars 2011 [LOPPSI 2], art. 4, et Cons. const., 10 mars 2011, n°

la loi du 21 décembre 2012 (CP art. 113-13, nouveau ; art. 421-2-4, nouveau).[20] Il en résulte que la compétence de la loi et des juridictions pénales françaises sera retenue si des français, ou des étrangers résidant habituellement en France, qui organisent des séjours terroristes à l'étranger (pex. au Pakistan), prennent contact via internet avec des tiers pour les inciter à commettre des actes de cette nature.

Certaines des solutions indiquées ci-dessus sont cependant moins satisfaisantes qu'il n'y paraît. Elles soulèvent, en réalité, de sérieuses difficultés.

2° Difficultés résultant de l'application des critères de rattachement du droit commun

Ces difficultés tiennent au fait que les règles de compétence du droit commun ne prennent pas en compte, en tout cas pas suffisamment, l'universalité d'internet. Il en résulte de fâcheuses incohérences et une réelle insécurité juridique.

Les incohérences concernent l'articulation entre les différents critères de compétence. Alors qu'il a longtemps été prétendu, à tort, que le Web avait créé un inquiétant vide juridique en raison du caractère insaisissable des flux transfrontaliers d'information, c'est plutôt d'un encombrant trop plein qu'il s'agit désormais, du fait précisément de l'ubiquité des échanges via les réseaux numériques et de l'externalisation des données dans le cadre du « *cloud computing* ». Tous les pays du monde sont en effet susceptibles de se déclarer compétents, ce qui revient à consacrer une compétence universelle – et non plus seulement territoriale, personnelle ou réelle – en faveur des juges pénaux nationaux, au risque de multiplier les conflits positifs de compétence.[21] L'incohérence est d'autant plus grande que l'harmonisation des législations nationales est encore trop souvent à l'état d'ébauche, qu'en règle générale la chose jugée à l'étranger ne paralyse pas la compétence territoriale française (et *vice-versa*), et que les condamnations pénales prononcées à l'étranger – quand elles le sont – ne peuvent en principe recevoir exécution dans le pays le plus intéressé par la répression du fait de l'absence d'exequatur en matière pénale.[22] Certes, la convention de Budapest du 23

2011-625 DC, pour le blocage par les FAI français de l'accès aux sites pédopornographiques, qu'ils soient situés en France ou à l'étranger.

[20] L. n° 2012-1432 du 21 déc. 2012 relative à la sécurité et à la lutte contre le terrorisme, art. 2 (JO du 22 déc. 2012 p. 20281) : « La loi pénale française s'applique aux crimes et délits qualifiés d'actes de terrorisme et réprimés par le titre II du livre IV (du CP) commis à l'étranger par un Français ou par une personne résidant habituellement sur le territoire français.» V. sur le premier de ces texte M.-H. Gozzi, Sécurité et lutte contre le terrorisme : l'arsenal juridique encore renforcé, D. 2013. 194 ; J. Alix, Fallait-il étendre la compétence des juridictions pénales en matière de terrorisme ? *Ibid.*. 518 ; D. Brach-Thiel, le nouvel article 13-13 du Code pénal : contexte et analyse, AJ Pénal 2013. 90. Rappr. CP art. 436-1, admettant également la compétence extraterritoriale française s'agissant du délit de participation à une activité de mercenaire.

[21] V. en ce sens M. Delmas-Marty, *op. cit.*, p. 342.

[22] V. not. sur ces aspects de droit pénal international : J.-F. Chassaing, L'internet et

novembre 2001 sur la cybercriminalité prévoit des règles de compétence communes ; elle n'en évacue pas moins le délicat problème de la litispendance internationale en s'en remettant à la « concertation » entre les Parties revendiquantes pour déterminer celle qui leur paraît la plus apte à exercer les poursuites, et encore seulement si cela est « opportun », ce qui, on le voit, n'est guère contraignant ![23]

Il s'y ajoute pour le justiciable le risque d'insécurité juridique. Il résulte en effet du principe de légalité criminelle que la loi pénale doit être accessible et prévisible pour tous.[24] Or tel n'est pas le cas si l'on considère, comme dans les situations envisagées, que tous les droits pénaux du monde sont applicables au contenu de la communication – quand bien même ils se contrediraient entre eux – et si l'on présume que tous les acteurs de celle-ci ont connaissance de toutes leurs prescriptions et sont par suite tenus de les respecter ![25] Outre qu'une telle exigence confine à l'absurde, elle conduit à rechercher d'autres voies, mieux adaptées que les précédentes aux spécificités d'internet et des NTIC ainsi qu'aux particularités des cybercrimes et cyberdélits.

B. Recherche de critères de rattachement adaptés aux spécificités du Web

Cette recherche risque de se révéler délicate, voire décevante. Il n'est pas simple, en effet, compte tenu de la diversité des infractions se rattachant à cette catégorie, elle-même difficile à circonscrire, de dégager des critères pertinents. Il est certes possible d'affiner les critères existants, *de lege lata* (1). Mais des changements plus profonds

---

le droit pénal, D. 1996. Chron. 329 s., spéc. p. 332 ; M. Vivant, Cybermonde : droit et droits des réseaux, JCP 1996. I. 3969, spéc. n° 19 ; A. Lepage, Libertés et droits fondamentaux à l'épreuve de l'internet, Litec, 2002, p. 85 et 86 ; A. Huet, Droit pénal international et internet, *in* Mélanges en l'honneur de Philippe Kahn, Litec, 2000. 663 s., et LPA, nov. 1999, n° 224, p. 39 ; E. Dreyer, L'internationalisation de la communication. Les lois applicables. Le droit pénal international, *in* Traité du droit de la presse et des médias, Litec, 2009, p. 1269 s. ; J. Huet et E. Dreyer, Droit de la communication numérique, LGDJ 2011, spéc. n° 207 et s. *Adde* les études, rapports et ouvrages cités *supra* et, pour une critique très argumentée de la théorie de l'ubiquité, D. Chilstein, Droit pénal international et lois de police. Essai sur l'application dans l'espace du droit pénal accessoire, collect. Nouvelle Bibliothèque de Thèses, Dalloz, 2003, préface de P. Mayer, spéc. n° 324 à 332).

[23] Conv. préc. du 8 nov. 2001, art. 22. Cette dernière disposition pourrait avoir été inspirée par la Convention du Conseil de l'Europe du 15 mai 1972 (non ratifiée par la France) sur la transmission des procédure répressives, art. 30.2 et 31 (STCE n° 073), qui laisse le règlement de la litispendance (ou son absence) au bon vouloir des États (V. A. Huet, *op. cit.*, p. 680 et 681, cet auteur proposant de résoudre ce problème en faisant application du critère de la priorité de la saisine).

[24] Sur l'exigence de « qualité de la loi » au sens de la Convention européenne des droits de l'homme et de la jurisprudence de la Cour de Strasbourg, V. not. CEDH, 15 nov. 1996, n° 17862/91, *Cantoni* c/ *France*, Rec. 1996-V, D. 1997. 202, obs. C. Henry, RSC 1997. 462, obs. R. Koering-Joulin, *ibid*. 646, obs. J.-P. Delmas Saint-Hilaire.

[25] V. not. M. Vivant, article préc., spéc. n° 19 ; A. Lepage, ouvrage préc., p. 85 et 86 ; E. Dreyer, étude préc., spéc. p. 1280 s.

peuvent également être envisagés, *de lege ferenda* (2).

1° Les affinements recherchés

Dès l'instant où de telles infractions sont commises en ligne, ou du moins impliquent un réseau électronique (communication à distance entre un émetteur et un récepteur), il est a priori rationnel de choisir, soit le lieu d'émission du message litigieux, soit son lieu de réception. Chacune de ces possibilités présente certes des avantages, mais elle comporte aussi des inconvénients : le choix en faveur du lieu d'origine conduit à encourager les fraudeurs à s'établir dans des pays à la législation bienveillante (« paradis informationnels ») ; quant au choix en faveur du lieu de réception, celui où le site étranger réalisant l'infraction est accessible à tous les internautes qui s'y connectent, depuis n'importe quel pays, il ne résout pas le problème des « chevauchements de compétence », de sorte que l'insécurité juridique subsiste.[26] A ceci près que ce dernier critère peut devenir pertinent si le message accessible en ligne a été préalablement « ciblé » en direction d'un pays bien déterminé.

La jurisprudence française a d'abord opté en faveur du critère de la réception, et, s'agissant d'internet, de celui de l'accessibilité au site. C'est ainsi que dans la célèbre affaire *Yahoo* concernant la mise en ligne d'objets nazis à partir d'un site américain de vente aux enchères, le lieu de réception a été retenu comme critère justifiant la compétence territoriale française.[27] La raison essentielle invoquée à l'appui de cette solution était que les agissements en cause entraient dans le cadre d'incriminations pénales françaises[28] et que leurs effets – le trouble à l'ordre public – s'étaient produits en France. En somme, il était fait application de la loi présentant les liens les plus étroits avec l'infraction, la loi dite de « l'enracinement social » du délit.[29] La même solution a été admise dans des affaires intéressant le droit de la presse, sa justification[30] étant que les messages litigieux diffusés à partir de l'étranger peuvent être localisés partout où ils ont été rendus publics.[31] Elle l'a été encore assez

---

[26] M. Vivant, *op. cit.*, *loc. cit.*, et Rapport sur la compétence, Conseil de l'Europe, Comité d'experts sur la criminalité dans le cyberespace, 1997.

[27] TGI Paris, réf., 22 mai et 20 nov. 2000, Comm. comm. électr. 2000, comm. n° 92 et 132, obs. J.-C. Galloux ; TGI Paris, 17è ch., 26 févr. 2002, Comm. comm. électr. 2002 n° 77, obs. A. Lepage ; Paris, 11è ch., 17 mars 2004, Comm. comm. électr. 2005, comm. n° 72, obs. A. Lepage.

[28] L. 29 juill. 1881, art. 24, al. 3, incriminant l'apologie de crimes de guerre ou de crimes contre l'humanité ; CP art. R. 645-1, visant l'exhibition en public d'insignes ou d'emblèmes nazis.

[29] V. *infra* 2°

[30] Depuis Crim., 30 avr. 1908, D. 1909. 1. 241, note G. Le Poittevin.

[31] V. not. pour des propos révisionnistes et diffamatoires diffusés sur internet depuis un site étranger : TGI Paris, 13 nov. 1998, Gaz. Pal. 2000. 1. doctr. 697 ; Limoges, 8 juin 2000, BICC 2001. 210. - *Adde* dans le même sens : Paris, 11è ch., 17 mars 2004, Comm. comm. électr. 2005, comm. n° 72, obs. A. Lepage. - V. égal. pour une étude d'ensemble de cette jurisprudence, E. Dreyer, *op. cit.*, *loc. cit.*, et les décisions citées.

récemment, par exemple dans une affaire de dénigrement de produits pharmaceutiques[32], ou en matière d'infraction à la réglementation française des jeux et paris en ligne.[33]

Cette dernière jurisprudence s'est ensuite infléchie et une nouvelle orientation semble avoir été prise, du moins en matière de contrefaçon de droit d'auteur et de droits voisins. On sait en effet que, selon une jurisprudence pénale constante – hors internet –, ce délit était localisé « au lieu de l'atteinte portée au droit d'auteur » (qui est le plus souvent celui du domicile du titulaire des droits), et pas seulement « au lieu de l'acte matériel de reproduction ».[34] Or, successivement dans deux arrêts de cassation, l'un du 9 septembre 2008[35], l'autre du 14 décembre 2010,[36] la Chambre criminelle de la Cour de cassation a jugé que la condition nécessaire pour que le délit soit considéré comme « perpétré » en France – élément constitutif de la contrefaçon – est qu'il soit « orienté vers le public français » (application de la théorie de la « focalisation »), ce qui, selon elle, n'avait pas été établi par les juges du fond en dépit des éléments de fait relevés en ce sens.[37] Désormais, la Chambre criminelle se montre par conséquent exigeante relativement au « faisceau d'indices » susceptible de rendre légitime l'admission de la compétence territoriale française en matière de contrefaçon de droit d'auteur.[38]

---

[32] Crim., 15 janv. 2008, Bull. crim. n° 5 : mise en ligne de faux rapports d'expertise sur des blogs à destination des publics français et espagnols ; l'arrêt retient la compétence du juge d'instruction français en raison de la possibilité offerte aux internautes d'accéder au site depuis le territoire français.

[33] Trib. corr. Nanterre, 15è ch., 15 mars 2007, RSC 2008. 101, obs. J. Francillon : site de poker localisé au Belize et accessible depuis la France via internet, cette accessibilité ayant constitué le facteur déterminant pour admettre la compétence française par application de l'art. 113-2, al. 1 et 2, CP. *Adde* : Ph. Aroyo, Applicabilité de la loi pénale française aux casinos en ligne : les sites « illégaux » le sont-ils réellement ? Dr. Pénal 2010. Étude 28.

[34] V. not. Crim., 2 févr. 1977, Bull. crim. n° 41 ; 6 juin 1991, Bull. crim. n° 240, D. 1993. 86, obs. C. Colombet, RSC 1992. 765, obs. P. Bouzat, RTD com. 1992. 484, obs. P. Bouzat.

[35] Crim., 9 sept. 2008, n° 07-87.281, D. 2009. 1992, obs. J. Larrieu, C. Le Stanc et P. Tréfigny, spéc. p. 2000 : article contrefaisant publié par un journal italien sur un site internet exclusivement rédigé en langue italienne et non destiné au public du territoire français.

[36] Crim., 14 déc. 2010, n° 10-80.088, D. 2011. 1055, obs. E. Dreyer, RTD com. 2011. 356, obs. F. Pollaud-Dulian, RPD pén. 2011, n° 1. 203, obs. D. Chilstein, RSC n° 3-2011, nos obs. à paraître : chansons d'un artiste français mises à disposition du public sous forme d'extraits musicaux sur un site internet hébergé en Allemagne et exploité par une société allemande.

[37] Faits constatés sur le territoire national, chansons appartenant au répertoire de la musique française, titres non traduits en allemand sur le site, icônes ne nécessitant pas la connaissance de l'allemand (Crim., 14 déc. 2010, préc.).

[38] Deux arrêts de la cour d'appel de Paris (26 avr. 2006 et 6 juin 2007, Legalis.net 19 juin 2007) avaient ouvert la voie. Soucieux de ne pas institutionnaliser le « *forum shopping* », qui offre à la victime la possibilité d'orienter son action vers les tribunaux du

Pour autant, ces solutions restrictives, qui rompent de manière « profonde » avec la jurisprudence *Yahoo* rappelée ci-dessus,[39] ne sont pas à l'abri de critiques : elles affaiblissent la répression dans un domaine sensible ; elles prennent encore, semble-t-il, quelques libertés avec le principe de légalité criminelle dans la mesure où le « faisceau d'indices » caractérisant le délit dépend des appréciations des juges ; elles imposent enfin de rechercher si le public français est bien le destinataire des messages litigieux, alors qu'il peut paraître plus logique – mais peut-être moins satisfaisant encore du point de l'efficacité répressive et de la protection des droits – de présumer que ce public ne l'est pas, donc de considérer qu'il est a priori exclu, sauf à rapporter la preuve contraire, c'est à dire à démontrer qu'il est réellement « ciblé ».[40] L'affinement réalisé n'est donc pas pleinement convaincant, d'autant plus que la jurisprudence demeure hésitante sur le choix du critère de rattachement en matière de contrefaçon de droit d'auteur[41] Aussi son extension à l'ensemble des cyberdélits

---

pays où la décision la plus favorable à ses intérêts est susceptible d'être rendue (V. Y. Kerbrat [Sous la direction de], Forum Shopping et concurrence des procédures contentieuses internationales, Bruylant, 2011), ils avaient subordonné la compétence territoriale française à l'existence d'un « lien suffisant, substantiel ou significatif entre faits ou actes et dommage allégué ». Ils se séparaient ainsi de la jurisprudence de la 1ère Chambre civile de la Cour de cassation qui, à la différence de la Chambre commerciale, se contente toujours du critère de l'accessibilité depuis la France au site internet étranger (Comp. : Civ. I, 9 déc. 2003, arrêt *Cristal*, et Com., 11 janv. 2005, arrêt *Hugo Boss*, cités *in* Panorama de droit International privé, févr. 2010-févr. 2011, par F. Jault-Seseke, D. 2011. 1381, Com., 9 mars 2010, Bull. civ. IV, n° 46, D. 2010.1183, note G. Lardeux, *ibid.*, 2323, note S. Bollée, spéc. 2331, JDI 2010. 870, note L. Usenier, et en dernier lieu Com. 29 mars 2011, arrêt *E. Bay c. Macéo*, Legalis.net 8 avr. 2011, Légipresse 2011, Act. Pan. n° 282-14, p. 2008, ce dernier arrêt, rendu en matière de contrefaçon de marque, subordonnant la compétence des juridictions françaises à la nécessité de viser le public de France et retenant quatre critères : caractère actif du site, langue, lieu de livraison, public). V. pour une synthèse de cet ensemble jurisprudentiel, S. Bollée, RLDI 2012. 2732, spéc. I.B, p. 123 et 124.

[39] D. Chilstein, obs. préc., *in fine*, et Rapport préc., p. 598 et 599.

[40] En ce sens E. Dreyer, note préc., II, *in fine*.

[41] Dans l'affaire ayant donné lieu à l'arrêt de cassation du 9 septembre 2008 (cité *supra*), la Chambre criminelle a ultérieurement adopté une position encore plus restrictive que précédemment. Saisie d'un pourvoi formé contre l'arrêt de renvoi qui avait écarté la compétence territoriale mais retenu la compétence personnelle passive des juridictions pénales françaises en raison de la nationalité française de la victime de la contrefaçon (CP art. 113-7), elle a de nouveau prononcé la cassation. Certes, elle l'a fait pour des motifs propres au droit d'auteur. Elle a en effet interprété la Convention de Berne du 9 sept. 1886 (art. 5 § 2) comme désignant la loi du lieu du fait générateur de l'atteinte, non celle du pays où le dommage est subi (donc s'agissant d'internet le lieu d'émission du message, non celui de sa réception (Crim. 29 nov. 2011, n° 09-88.250, JCP 2012. 248, note E. Dreyer ; J. Lasserre Capdeville, AJ Pénal 2012. 164 ; RSC 2012. 165, et les obs.). Une telle position est donc de nature à limiter, voire à neutraliser, du moins dans ce domaine particulier, l'étendue de la compétence (à la fois territoriale et personnelle passive) de la loi et des juridictions

apparaît-elle prématurée.[42]

Il est vrai que d'autres options sont concevables *de lege ferenda*. Elles reviendraient, si elles étaient retenues, à changer de paradigme s'agissant des règles de compétence applicables aux cybercrimes et aux cyberdélits.

2° Les changements de paradigme proposés

Ce sont des changements proposés en France par une doctrine autorisée. Une première option serait de transposer en matière pénale les méthodes du droit international privé. Elle se conçoit quand il s'agit de déterminer la loi compétente pour apprécier le bien-fondé de l'action civile exercée au pénal ; mais qu'en est-il s'agissant de l'action publique elle-même ? Ne devrait-on pas dissocier les compétences législative et juridictionnelle et admettre qu'un juge pénal français puisse appliquer une loi pénale étrangère ?[43] Si tel était le cas, il ne serait plus nécessaire de faire appel à la théorie de l'ubiquité pour justifier l'admission d'une compétence territoriale qui, en réalité, est aussi artificielle qu'arbitraire. Quant à la territorialité du droit pénal, elle pourrait alors se combiner de manière plus harmonieuse avec l'internationalité du Web. Certaines propositions doctrinales vont dans ce sens. Il a par exemple été préconisé d'appliquer la loi présentant les liens les plus étroits avec le délit, la loi dite de « l'enracinement social ». Selon cette thèse, la compétence judiciaire serait déterminée par le lieu du fait générateur (l'émission du message en l'occurrence), la compétence législative par le lieu de la survenance du résultat (la réception du message), lorsque du moins certaines conditions se trouvent réunies.[44] Il a encore été proposé, en prenant également pour modèle le droit international privé, de faire application en droit pénal de la méthode des lois de

---

pénales françaises. Elle est en outre inadaptée au « *cloud computing* » qui rend impossible techniquement la détermination du fait générateur du délit (V. M. Berguig, Le cloud : ombres et lumières sur l'informatique décentralisée », Comm. comm. électr. 2012. Étude 19).

[42] V. D. Chilstein, *op. cit.*, *loc. cit.* - A noter que les décisions récentes émanant de juges du fond et allant dans le sens de cette extension ne sont pas encore significatives. V. toutefois, s'agissant des jeux d'argent et de hasard en ligne, TGI Paris, ord. réf., 28 avr. 2011, Comm. comm. électr. 2011. comm. n° 78, obs. A. Debet, Legalis.net 5 mai 2011 : à l'argument des fournisseurs d'accès à internet (FAI) qui soutenaient que le site de paris sportifs et hippiques litigieux ne visait pas spécifiquement le public français mais pouvait être destiné au monde francophone, le tribunal rétorque que les offres de pari portant sur certains matchs de football se déroulant en France étaient « destinées, d'évidence, à attirer les internautes français » *Adde* : Paris, Pôle 1, ch. 3, 28 juin 2011, RSC 2011. 638, et nos obs., cet arrêt rejetant une question prioritaire de constitutionnalité (QPC) relative à une injonction de blocage de l'accès à un site de jeux d'argent et de hasard non agréé hébergé à l'étranger.

[43] V. not. A. Huet, Pour une application limitée de la loi pénale étrangère, JDI 1982, p. 623.

[44] R. Koering-Joulin, L'art. 693 du CPP et la localisation internationale de l'infraction, Thèse, Strasbourg, 1972, spéc. p. 348 s. ; D. Rebut, *op. cit.*, n° 53.

police, mais de la réserver au domaine du droit pénal accessoire[45]. Confrontées à la cyberdélinquance et à la cybercriminalité, ces thèses doctrinales pourraient ne pas être dépourvues d'intérêt dès lors qu'il s'agirait d'instaurer un droit pénal international spécifique à l'internet, ainsi que certains auteurs le souhaitent.[46]

Une seconde option serait moins ambitieuse mais plus réaliste. Elle consisterait à distinguer selon les catégories d'infractions susceptibles d'être commises dans le cyberespace. Les unes – évidemment les plus nombreuses – resteraient soumises à une territorialité de type classique. Le droit commun doit en effet logiquement conserver son emprise sur la masse des infractions contre les personnes ou contre les biens pour la perpétration desquelles l'utilisation du Web offre des facilités (terrorisme, agression sexuelle, corruption de mineur, blanchiment ou détournement d'argent, intrusions diverses, etc..). En revanche, s'agissant des infractions ayant un rapport direct, consubstantiel, avec le droit de diffuser et/ou de recevoir des informations (diffusion de propos diffamatoires ou apologétiques, transmission d'images pédophiles, téléchargement illégal d'œuvres protégées, connexion à un site non agréé de jeux d'argent ou de hasard situé à l'étranger, etc..), le critère de compétence territorial et le principe d'exclusivité des compétences nationales devraient être aménagés de telle manière que la spécificité du Web en tant que mode de communication soit réellement prise en compte. Dès lors en effet que l'intervention du droit pénal a pour objet de restreindre la liberté d'expression et de communication, il paraît logique de faire prévaloir un critère de rattachement et des règles procédurales adaptés aux particularités de la relation entre l'émetteur et le récepteur du message litigieux. Une telle solution aurait alors de meilleures chances de prospérer que l'extension de la théorie de la « focalisation », actuellement admise en matière de contrefaçon, à toutes les infractions commises via internet.[47]

Face à la mondialisation des risques, il n'est certes pas inconcevable d'imaginer une mondialisation de la réponse et d'instaurer une sorte de *lex paenalia electronica*. Mais on en est loin ! Quoi qu'il en soit, les normes destinées à encadrer les activités se déroulant dans le cyberespace sont perfectibles. Elles ne sont d'ailleurs pas seulement « territorialisées ». Elles sont aussi, de plus en plus, « internationalisées ». Cette tendance apparaît nettement en matière d'entraide répressive.

II. Coopération en matière pénale

(points D à F du questionnaire)

---

45 D. Chilstein, thèse citée *supra.*

46 A. Huet, étude préc. aux Mélanges Ph. Kahn, spéc. II, p. 675 s., cet auteur proposant d'abandonner en ce domaine les principes de territorialité et d'exclusivité des compétences nationales (V. égal. *infra*)

47 Rappr. D. Chilstein, ouvrage préc., spéc. n° 322, p. 166, cet auteur estimant à propos de la diffamation sur internet que « rien ne permet d'affirmer *a priori* que le champ de la répression des infractions commises sur la « toile » doit être unitaire, que les critères de localisation territoriale doivent s'interpréter de la même façon, quel que soit le délit commis ».

Quelques observations seront présentées à titre préliminaire. Elles concernent les fondements, la nature et l'évolution de l'entraide répressive entre États telle que celle-ci est envisagée en France (A). Cette évolution va dans le sens non seulement d'un renforcement de l'efficacité des procédures en matière pénale (B), mais également dans celui d'une protection plus étendue des libertés et des droits fondamentaux des personnes faisant l'objet d'investigations policières et/ou judiciaires (C).

A. Fondement, nature et évolution de l'entraide répressive (généralités)

L'entraide en matière pénale répond à la nécessité pour les États de lutter contre une criminalité qui leur est commune.[48] Qu'il s'agisse de l'entraide judiciaire ou de la coopération strictement policière, les actes qui en relèvent sont accomplis dans le cadre d'une relation directe entre les États concernés dont la souveraineté doit être respectée. Leur intérêt réciproque à se prêter assistance justifie donc que soient mis en place un certain nombre de dispositifs susceptibles de remédier aux insuffisances des moyens de lutte purement internes, notamment dans le domaine de la cyberdélinquance et de la cybercriminalité (1°). Mais, inversement, l'absence d'intérêt réciproque à cette assistance explique que, dans un certain nombre de cas, les États soient conduits à restreindre, voire à refuser, l'entraide sollicitée (2°). Aussi la question se pose-t-elle de savoir si, et dans quelle mesure, les spécificités de la technologie de l'information changent la nature de l'assistance mutuelle (3°).

1° Renforcement des dispositifs d'entraide

Il y a là une tendance qui est assez générale et à laquelle, évidemment, la France n'échappe pas. L'observation vaut plus particulièrement pour les États membres de l'Union européenne. Les efforts d'harmonisation des législations nationales ainsi que la reconnaissance mutuelle des décisions judiciaires au sein de l'Union ont en effet déjà permis d'obtenir des résultats significatifs dans la lutte contre la criminalité transfrontière. L'un des objectifs poursuivis est en effet de remédier aux insuffisances des droits internes préjudiciable à l'efficacité de la répression, donc aux disparités existantes entre les États dans l'application des règles relatives à l'entraide répressive. Les efforts tendant à harmoniser les législations pénales sont particulièrement sensibles au niveau européen (Conseil de l'Europe et Union européenne), ce dont témoignent des textes majeurs comme la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité (ratifiée aussi par des États tiers) et son protocole additionnel ou la décision-cadre du 18 décembre 2006, déjà citée, relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union. Il s'y ajoute bien évidemment la Convention d'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, faite à Bruxelles le 29 mai 2000. Cette convention, ouverte initialement à

[48] D. Rebut, Droit pénal international, Précis Dalloz, 1ère éd. 2012, n° 207, cet auteur parlant de criminalité "partagée" entre l'État requérant et l'État requis.

l'adhésion des seuls États membre de l'Union Européenne, a été étendue aux États membres du Conseil de l'Europe par son second protocole additionnel qui est désormais en vigueur en France49. Destinée à encourager et à faciliter l'entraide entre les autorités judiciaires, policières et douanières en matière pénale, elle améliore et complète la Convention du Conseil de l'Europe du 20 avril 1959 sur l'entraide judiciaire en matière pénale qui constitue le droit commun de cette entraide en droit pénal français. Tous ces textes engagent évidemment la France qui, pour sa part, met en œuvre les règles qu'ils prescrivent au regard de l'entraide.[50]

L'internationalisation de la lutte contre la criminalité transfrontières, notamment contre la cybercriminalité, se manifeste aussi par un rapprochement des juges. La reconnaissance mutuelle des décisions de justice en matière pénale constitue en effet l'un des apports essentiels de l'évolution récente du droit de l'Union européenne. Ce principe repose sur l'idée de confiance mutuelle entre États membres de l'Union (« degré de confiance élevé »). Il procède de la volonté de créer un espace judiciaire commun et conduit donc à un certain effacement des souverainetés. Il est évidemment applicable aux cybercrimes et aux cyberdélits. La décision cadre du 13 juin 2002 instituant le mandat d'arrêt européen (MAE) en fournit une illustration significative. Ce mécanisme de remise simplifiée du délinquant aux autorités du pays qui le réclame est en effet considéré comme la « pierre angulaire » de la coopération judiciaire au sein de l'Union. Ainsi la cybercriminalité est-elle incluse dans la liste des 32 catégories d'infractions considérées comme graves en raison de la peine encourue (emprisonnement égal ou supérieur à trois ans selon la loi de l'État membre d'émission) et pour lesquelles l'exigence du contrôle de double incrimination est écartée (en France : CPP art. 695-23). Il est clair que la volonté de renforcer l'efficacité de la coopération et de la lutte contre cette forme de criminalité est ici prédominante.[51]

L'évolution dans le même sens se poursuit d'ailleurs en France où un projet de loi visant à transposer le droit de l'Union européenne est actuellement en discussion au Parlement, notamment en ce qui concerne Eurojust.[52] Ce texte prévoit notamment que

---

[49] L. n° 2005-287 du 30 mars 2005, JO du 31 mars 2005 p. 5793 ; décret n° 2012-813 du 16 juin 2012, JO du 20 juin 2012 p. 10201

[50] V. not. *infra* pour la transposition de la décision cadre de 2006 en droit interne (CPP art. 695-9-31 à 695-9-49, créés par Ord. n° 2011-1069 du 8 sept. 2011, JO 9 sept. p.15200).

[51] La même observation peut être faite au sujet non seulement des transmissions de commissions rogatoires directement de juge à juge, mais également du dispositif instauré par la décision-cadre du 19 décembre 2008 relative au mandat européen d'obtention des preuves en vue de faciliter la communication des éléments probatoires (objets, documents, données informatiques) nécessaires à la manifestation de la vérité dans le cadre de procédures pénales. Cet outil peut donc se révéler particulièrement utile dans la lutte contre les infractions transfrontalières, notamment en matière de contrefaçon *via* internet.

[52] Projet de loi transposant en droit français la décision-cadre 2008/909/JAI du 27 nov. 2008 (doc. Sénat n° 250, 2011-2012, Étude d'impact).

cette unité de coopération judiciaire à laquelle participe la France – au même titre qu'à Europol et à Interpol s'agissant de la coopération policière – pourra désormais accéder, dans des conditions identiques à celles des autorités judiciaires, aux informations contenues dans les fichiers judiciaires, dans les fichiers de police judiciaire ou dans tout autre fichier contenant des informations nécessaires à l'accomplissement de ses missions. C'est dire que ce dispositif viendra compléter de manière opportune les mécanismes existants tels que le Réseau judiciaire européen,[53] les équipes communes d'enquête[54] ou les magistrats ou officiers de liaison.

La possibilité d'effectuer des enquêtes extraterritoriales renforce d'ailleurs l'efficacité de la lutte contre la criminalité organisée dont la cybercriminalité est l'une des manifestations. Des OPJ français (ou des agents étrangers) détachés auprès d'une équipe commune d'enquête peuvent ainsi être amenés à procéder à des infiltrations en territoire étranger (ou sur le territoire français) s'ils sont spécialement habilités à cet effet. Même en dehors de ce cadre, un droit d'observation ou même de poursuite transfrontières (au sens des art. 40 et 41 de la Convention de Schengen du 19 juin 1990) leur est reconnu. En France, ce droit a été validé par le Conseil constitutionnel qui a estimé qu'il n'y avait pas d'atteinte aux conditions essentielles d'exercice de la souveraineté nationale.[55] Il est vrai que ce droit est soumis à des conditions qui en rendent la reconnaissance légitime (parmi elles : l'autorisation préalable des autorités françaises et l'interdiction faite aux agents étrangers de procéder à des interpellation en territoire français). Cela étant, il est clair qu'une fois ces conditions réunies les agents concernés peuvent échanger, y compris par voie électronique, les informations qui leur paraîtront utile à l'enquête effectuée.[56]

2° Limites des dispositifs d'entraide

Ces limites sont traditionnelles, et elles sont de deux sortes. La première résulte de l'exigence de double incrimination. Il a été indiqué précédemment que cette exigence est écartée, s'agissant du mandat d'arrêt européen, pour des infractions entrant dans certaines catégories et présentant un niveau de gravité tel que la nécessité d'un contrôle judiciaire de cette condition ne s'impose plus. Cette dérogation à une règle classique du droit extraditionnel français repose sur l'idée de confiance mutuelle entre les États membres de l'union européenne. Or on verra plus loin qu'en pareil cas les échanges de données intéressant l'enquête sont possibles et qu'ils le sont sans qu'il soit nécessaire d'obtenir une autorisation judiciaire préalable. Dans les autres

---

53 Dispositif de coopération permettant aux autorités d'un État membre de disposer d'un point de contact sur le territoire de l'État auquel elles adressent une demande d'entraide et de coordonner l'exécution de plusieurs demandes adressées à un même État.

54 CPP art. 695-2 et 695-3, prévoyant la possibilité de les créer pour des infractions nécessitant la mobilisation d'importants moyens et une action "coordonnée et concertée" entre les États membres concernés.

55 Cons. const., 25 juill. 1991, Décision n° 91-294 DC (JO du 17 juill. 10001).

56 V. également *infra* B 1° et 3° les développements consacrés aux infiltrations ainsi qu'aux échanges de données.

situations, et bien que l'on se situe – si c'est le cas – en dehors du champ du droit extraditionnel, il est nécessaire qu'existe au moins un *intérêt réciproque* à se prêter assistance. A défaut, la demande d'échange d'informations au profit de l'État qui a subi seul le effets préjudiciables de la conduite qu'il criminalise ne pourra aboutir.

Quant aux refus d'entraide, il est logique qu'ils soient appliqués à tout type de recherche effectuée en matière pénale, sur internet ou ailleurs, dès lors que ces refus sont justifiés par des motifs généraux : préservation de la sécurité publique ou protection des libertés individuelles et des droits fondamentaux. En décider autrement serait évidemment contraire aux principes qui gouvernent la matière. Il en sera fourni ci-dessous plusieurs illustrations.

3° Nature de l'entraide (au regard de la spécificité des NTIC)

On se bornera à deux observations. La première est qu'en droit français les règles relatives à la coopération pénale internationale en matière de cybercriminalité ne sont pas regroupées dans un texte unique. La différence est donc nette avec la Convention de Budapest et son protocole additionnel qui sont des instruments internationaux portant exclusivement sur ce domaine. Certes, les mécanismes d'entraide entre États ne sont pas propres à ce type de délinquance et de criminalité, même s'ils ne sont pas dépourvus ici d'une certaine spécificité, particulièrement en ce qui concerne la coopération policière internationale et européenne. Le droit applicable en la matière est donc à rechercher soit dans des dispositions propres à certaines situations particulières, soit dans les réglementations de portée plus générale relatives à la coopération pénale internationale (pex. les règles relatives à l'extradition, au mandat d'arrêt européen ou aux échanges d'informations intéressant les enquêtes pénales) qui englobent, le cas échéant, le champ de la cybercriminalité.[57] En droit français, les particularités de celle-ci n'affectent donc pas, pour l'essentiel, les règles de droit commun applicables à l'entraide.

Selon nous, les nouvelles technologies de l'information et de la communication (NTIC) ne changent pas non plus fondamentalement la nature de l'assistance mutuelle. En effet, l'entraide en matière pénale repose traditionnellement sur la communication et l'échange d'informations utiles aux enquêtes. Aussi les nouveaux procédés de collecte, de transmission et de traitement des informations, comparées aux techniques traditionnelles de renseignement, introduisent-elles dans cette relation d'échange une différence qui est moins de nature que de degré. Leurs spécificités – rapidité, exhaustivité, fiabilité – ne font, en définitive, que faciliter les enquêtes, contribuant ainsi à renforcer l'efficacité de la lutte contre la cybercriminalité.

Pour autant, ces nouvelles technologies présentent des dangers au regard des libertés individuelles et des droits fondamentaux. Leurs spécificités sont en effet susceptibles de conférer un caractère très intrusif aux investigations policières et judiciaires

[57] V. en ce sens D. Chilstein, rapport préc., p. 595.

qu'elles permettent de mener. Par conséquent, elles ne doivent pouvoir être utilisées que dans les limites de ce qui est nécessaire au bon déroulement des enquêtes et au bon fonctionnement des mécanismes d'entraide mis en œuvre à cette fin.

Les règles procédurales applicables en France répondent à cette double préoccupation d'efficacité répressive (B) et de protection des libertés et des droits des personnes (C).

B. Renforcement de l'efficacité des procédures répressives

C'est surtout dans le cadre des procédures de mise en état des affaires pénales – enquête préliminaire/enquête de flagrance/instruction – que le recours aux NTIC se révèle particulièrement utile. Il est même devenu indispensable aux enquêteurs (souvent spécialisés) chargés de constater les infractions relevant de la cybercriminalité, d'en rassembler les preuves et d'en rechercher les auteurs (CPP art. 14, en ce qui concerne la police judiciaire). Il est également nécessaire que, dans un souci d'efficacité répressive, les informations ainsi obtenues puissent être transmises et exploitées dans le cadre de l'assistance mutuelle que s'accordent les États concernés. Les mesures coercitives, souvent très intrusives, admise en droit pénal français répondent à cette double préoccupation (1°). Il en est de même des règles concernant les échanges de données intéressant les enquêtes et de leur mise en œuvre (2°) ainsi que d'autres dispositifs d'assistance mutuelle plus spécifiques (3°).

1° Mesures coercitives et/ou intrusives

Ces mesures sont susceptibles de s'inscrire dans le cadre d'opérations d'entraide diligentées conformément aux procédures habituelles. Toutefois, certaines d'entre elles comportent des aspects spécifiques à cet égard, qu'il s'agisse de mesures d'investigation (a) ou d'injonction (b)

a) Mesures d'investigation

Elles ont pris une importance grandissante avec le développement des NTIC et celui, corrélatif, de la cybercriminalité. Il s'agit principalement des mesures suivantes : interception de télécommunication, captation de données informatiques à distance, perquisitions et saisies de données informatiques, infiltrations numériques. Leur efficacité procédurale est d'autant plus forte que la coopération entre les États concernés est la plus étroite possible.

Interception de télécommunication. C'est depuis la loi n° 91-646 du 10 juillet 1991 que, par dérogation au principe du secret des correspondances, les interceptions de télécommunication sont admises en droit français. Elles étaient pratiquées auparavant de manière officieuse mais ne répondaient pas aux exigences européennes (Conv. EDH art. 8). Elles le sont désormais dans un cadre légal. Celui-ci,initialement destiné à réglementer les écoutes téléphonique, est également applicable aux échanges de messages électroniques sur internet (courriels) ou avec des appareils mobiles (portables). La loi distingue les interceptions administratives dites "de sécurité" (Ord.

n° 2012-351 du 12 mars 2012 ; CSI art. L. 241-2 et s.), et les interceptions judiciaires (CPP art. 100 à 100-7). Ces dernières sont permises en matière criminelle et en matière correctionnelle (si la peine encourue est supérieure ou égale à deux ans d'emprisonnement), mais seulement sur décision d'un juge d'instruction et lorsque les nécessités de l'information exigent que soient prescrits l'interception, l'enregistrement et la transcription des correspondances ainsi émises, sous réserve des exclusions ou restrictions prévues au profit de certaines personnes (parlementaires, magistrats, avocats, journalistes). Cette décision doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction visée ainsi que la durée de l'interception (4 mois maximum renouvelable). L'opération technique d'interception est réalisée sur réquisition du juge d'instruction ou de l'OPJ commis par lui. Cette réquisition peut être adressée à tout agent qualifié du service ou organisme public ou privé habilité à cet effet (opérateurs de communication électronique, exploitants de réseau, fournisseurs de services de télécommunications).

Le dispositif exposé ci-dessus est complété par celui applicable en matière de criminalité et de délinquance organisées (CPP art. 706-73 et 706-95 résultant de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, mod. L. n° 2011-267 du 14 mars 2011). En pareil cas, l'interception, l'enregistrement et la transcription des correspondances électroniques sont autorisés dès le stade de l'enquête de flagrance ou de l'enquête préliminaire, mais seulement sur décision d'un juge des libertés et de la détention (pour une durée d'un mois renouvelable une fois). Il s'agit donc d'un dispositif particulièrement dérogatoire au droit commun. Certes, les cybercrimes et les cyberdélits ne sont pas expressément mentionnés dans la liste des infractions graves visées par le premier de ces textes. Mais quand existent des raisons plausibles de soupçonner qu'une association de malfaiteurs (CP, art. 450-1 ; Conv. ONU contre la criminalité transnationale organisée, art. 5) a été formée en vue de préparer l'une de ces infractions, cette qualification est susceptible de justifier l'application d'un tel dispositif (CPP, art. 706-73, 15°). Le droit français répond donc pleinement aux exigences de la Convention de Budapest du 23 novembre 2001 (art. 21).[58] La France a déclaré qu'elle n'appliquerait les mesures prévues par cet article que si l'infraction poursuivie est punie d'une peine supérieure ou égale à deux ans d'emprisonnement (Déclaration concernant l'interception de données relatives au contenu).. Les dispositifs propres à la lutte antiterroriste sont également dérogatoires au droit commun (CPP, art. 706-16 à 706-25-2). Ainsi les réquisitions adressées par les enquêteurs de police et de gendarmerie spécialisés aux opérateurs de communication électronique le sont-elles indépendamment de toute autorisation d'un magistrat (CPCE, art. L. 34-1-1).

S'agissant de l'assistance judiciaire mutuelle en matière d'interception des télécommunications (Conv. Budapest 23 nov. 2001, préc., art. 34 : *"Entraide en matière d'interception de données relatives au contenu"*), le Code de procédure

[58] V. également *infra* B 1° et 3° les développements consacrés aux infiltrations ainsi qu'aux échanges de données.

pénale français ne contient pas de dispositions spécifiques. En revanche, la Convention d'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, faite à Bruxelles le 29 mai 2000, et étendue aux États membres du Conseil de l'Europe par son second protocole additionnel désormais en vigueur en France (V. *supra*), comporte de telles dispositions. L'une de ses particularités est de s'appliquer aux interceptions de communications téléphoniques échangées à l'aide de portables utilisés dans un autre État. L'économie générale du dispositif d'entraide est la suivante (art. 17 à 22). L'interception peut s'opérer (pex. en Italie) sur demande de l'autorité compétente d'un autre État membre (pex. la France). Elle est alors ordonnée par une autorité judiciaire ou une autorité administrative désignée par l'État membre concerné (l'Italie). Une fois interceptée, la télécommunication peut être soit transmise directement à l'État membre requérant (la France), soit enregistrée et transmise ultérieurement. L'interception peut également être effectuée sur le territoire d'un État membre où se trouve la station terrestre pour les communications par satellites (pex. en Italie). En pareil cas, si l'assistance technique de cet État n'est pas nécessaire, l'interception est réalisée par l'intermédiaire des fournisseurs de services ayant leur siège dans l'État requérant (pex. en France). Lorsque l'interception est autorisée par un État membre (dit "État interceptant", pex. la France) et lorsque la cible visée se déplace sur le territoire d'un autre État membre (dit "État notifié", pex. l'Italie) dont l'assistance technique n'est pas nécessaire pour effectuer cette interception, l'État membre interceptant est tenu d'informer l'État membre notifié de la réalisation de cette opération d'interception (art. 20). Le tout sans préjudice des arrangements bilatéraux ou multilatéraux conclus entre États membres pour ce type d'investigation (art. 22).

Captation de données informatiques à distance. Depuis la loi n° 2011-267 du 14 mars 2011 (dite « LOPPSI 2 » ; CPP art. 706-102-1 à 706-102-9), les « *captures d'écran* » sont autorisées afin, notamment, de repérer les pédophiles et les terroristes.[59]) Ces captations de données, opérées à l'insu des intéressés grâce à l'installation de dispositifs espions, ne doivent pas être confondues avec les perquisitions informatiques transfrontières dont la validité est subordonnée à des conditions distinctes (V. *infra*). Il en résulte qu'il est interdit aux enquêteurs de « *se promener et de fouiller* » dans l'ordinateur objet de leurs investigations à distance. Ce dispositif n'en a pas moins un caractère intrusif ; il constitue une variante des infiltrations numériques dans les réseaux criminels admises par ailleurs en droit français (V. *infra*). C'est pourquoi son champ d'application est restreint au domaine de la criminalité organisée (CPP art. 706-73). Sa mise en place est assurée par des OPJ agissant sur commission rogatoire d'un juge d'instruction. Ce dernier doit notamment préciser dans son ordonnance la localisation exacte des systèmes

[59] CPP art. 706-102-1, visant l'installation d'un "dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères".

informatiques concernés (qui pourraient le cas échéant être situés à l'étranger) ou décrire ces systèmes de manière détaillée. Afin de mettre en place ce dispositif, il peut autoriser sa transmission par un réseau de communications électroniques (y compris par conséquent en direction des autorités compétentes étrangères dont la participation pourrait être sollicitée). L'opération ne peut avoir un autre objet que la recherche et la constatation des infractions visées dans la décision du juge d'instruction, à peine de nullité. Toutefois, le fait qu'elle révèle une ou plusieurs infractions autres que celles visées dans la décision du juge ne constitue pas une cause de nullité des procédures incidentes.[60]

Encore deux observations. La première est qu'il n'existe pas dans les textes réglementant les captations de données informatiques à distance une disposition comparable à celle de l'article 57-1, al. 2, du Code de procédure pénale applicable aux perquisitions et saisies extraterritoriales de données informatiques (V. i*nfra*). Toutefois, l'article 706-102-1 indique que les enquêteurs commis sur commission rogatoire du juge d'instruction sont autorisés à mettre en place un dispositif "ayant pour objet (...) d'accéder, *en tous lieux*, à des données informatiques". C'est dire que celles-ci peuvent être obtenues, le cas échéant, directement du système informatique situé à l'étranger avec lequel la connexion est établie (pex. une base de données privée ou publique), et ce sans l'accord de son propriétaire ou de son exploitant. La seconde observation est que les informations obtenues grâce à l'utilisation de ce procédé d'investigation peuvent ensuite être communiquées aux autorités étrangères compétentes selon les procédures d'assistance mutuelle habituelles (V. *infra* 2° a).

Perquisitions et saisies de données informatiques. Les règles relatives aux perquisitions et saisies de données informatiques[61] ont été introduites dans le Code de procédure pénale par plusieurs lois successives (CPP art. 60-1, 77-1-1 et 99-3).[62] Elles prévoient qu'au cours d'une perquisition les enquêteurs peuvent procéder à la saisie des données informatiques nécessaires à la manifestation de la vérité. Il n'est fait aucune distinction selon le type de données informatiques. Sont donc concernées aussi bien les données relatives au trafic que les données relatives au contenu au sens de la Convention de Budapest du 23 novembre 2001 (art. 18 et 21). Les textes

---

60 V. cependant pour des analyses critiques de ce dispositif, S. Hennequin, obs. au D. 2011. 1358, et C. Ribeyre, obs. *in* Dr. pénal 2011. Étude 10, spéc. n° 33. *Adde* les craintes exprimés par A. Lepage, Un an de droit pénal des nouvelles technologies, Dr. pénal 2011. Étude 10, spéc. n° 13.

61 V. sur les difficultés soulevées par ces perquisitions, D. Bénichou, Cybercriminalité : jouer d'un nouvel espace sans frontière, AJ pénal 2005, p. 224, et F. Chopin, Les politiques publiques de lutte contre la cybercriminalité, préc., 2009. p. 101 et s., spéc. p. 104 et 105.

62 L. n° 2003-329 du 18 mars 2003 pour la sécurité intérieure (LSI), JO du 19 mars 2003, p. 4761, mod. L. n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (Perben II), JO du 10 mars 2004, p. 4637 et mod. L. n° 2001-1862 du 13 déc. 2001 relative à l'allègement de certaines procédures juridictionnelles, JO du 14 déc. 2011, p. 21105.

concernant l'enquête de flagrance et l'instruction apportent deux précisions importantes. En premier lieu, ils autorisent les enquêteurs à accéder non seulement au données intéressant l'enquête qui sont stockées dans le système informatique implanté sur les lieux où se déroule la perquisition (dénommé système initial), mais également aux données qui sont stockées dans un autre système informatique et qui sont "accessibles à partir du système initial ou disponibles pour le système initial" (CPP art. 57-1, al. 1). La fouille est donc susceptible de concerner tout un réseau d'ordinateurs. En second lieu, les enquêteurs sont autorisés à opérer cette fouille même lorsque le ou les autres systèmes informatiques auxquels ils accèdent sont "situé(s) en dehors du territoire national" (CPP art. 57-1, al. 2). C'est dire que leurs pouvoirs d'investigation sont alors très étendus,[63] sous réserve, précise encore le texte, que les conditions dans lesquelles les enquêteurs accèdent à un système informatique localisé à l'étranger (pex. une base de données publique ou privée) soient "prévues par les engagements internationaux en vigueur" (*ibid.*). Or la Convention de Budapest du 23 novembre 2001 est explicite en ce dernier sens (art. 19.2). Elle constitue donc juridiquement le fondement sur lequel repose le dispositif législatif français des perquisitions et saisies extraterritoriales de données informatiques.[64]

Infiltrations numériques. En droit français, les opérations d'infiltration sont autorisée dans les conditions précisées par le Code de procédure pénale. Elles concernent les infractions en rapport avec la criminalité et la délinquance organisées (CPP art. 706-73 et 706-81). Les enquêteurs habilités à les effectuer peuvent ainsi être amenés à utiliser les nouvelles technologies de communication afin d'obtenir des informations utiles à l'enquête. A cet effet, ils peuvent être conduits à fournir aux intéressés des moyens de télécommunication (CPP art. 06-82). Les opérations d'infiltration sont également autorisées lorsque certaines infractions prévues par le Code pénal ou des textes particuliers sont commises par un moyen de communication électronique (CPP art. 706-25-2, 706-35-1, 706-47-3 ; L. 12 mai 2010, art. 59).[65] Elles permettent

---

63 Il est vrai qu'avec le « *cloud computing* », le stockage des informations se trouvant déporté et étant situé en dehors des lieux où les enquêteurs sont habitués à intervenir, leur travail d'investigation pour récupérer les informations devient plus compliqué.

64 Ce dispositif est également proche des recommandations du Conseil de l'Europe. V. C. Féral-Schuhl, Cyberdroit, 6è éd. 2011-2012, n° 141-33, citant la recommandation du 11 septembre 1995 qui incite les États à prévoir une distinction entre l'entraide en matière d'accès aux données (art. 31 : demande adressée à un autre État membre pour qu'il perquisitionne et saisisse des données stockées dans un système informatique situé sur son territoire) et l'accès transfrontalier ne nécessitant pas l'entraide judiciaire (art. 32 : accès sans l'autorisation d'un autre État membre à des informations accessibles au public, quelle que soit leur localisation, et avec son autorisation dans les autres cas).

65 Ces infractions sont les suivantes : traite des êtres humains (CP art. 225-4-1 à 225-4-9), proxénétisme (CP art. 225-5 à 225-12), recours à la prostitution d'un mineur ou d'une personne vulnérable (CP art. 225-12-1 à 225-12-4), mise en péril d'un mineur (CP 227-18 à 227-24), provocation directe aux actes de terrorisme ou apologie de ces actes (L.

aux enquêteurs de participer sous un pseudonyme aux échanges électroniques (pex. à un forum de discussion), de prendre contact avec les auteurs potentiels d'infractions, d'acquérir et de conserver des contenus illicites, et de pouvoir ainsi constater ces infractions, en rassembler les preuves et en rechercher les auteurs. Des garanties sont toutefois prévues afin d'éviter les abus (V. *Infra* C 2° sur la question des provocations policières). La loi précise en effet qu'à peine de nullité ces actes ne doivent pas constituer une incitation à commettre de telles infractions. En outre, aucune condamnation ne peut être prononcée sur le seul fondement des déclarations faites par les OPJ ou agents infiltrés (CPP art. 706-87). Afin de renforcer l'efficacité de leurs interventions les enquêteurs peuvent être conduits à solliciter le concours des autorités compétentes étrangères. Le Code de procédure pénale ne comportant pas de dispositions spécifiques à cet égard ce sont les règles ordinaires en matière d'assistance mutuelle qui s'appliquent, dans le respect des engagements internationaux et du droit des États concernés.

b) Mesures d'injonction

Ces injonctions sont de natures différentes. Certaines se situent dans le cadre de procédures judiciaires et ont une finalité répressive. Elles sont destinées à permettre aux autorités judiciaires d'obtenir les informations nécessaires aux enquêtes pénales (enquêtes préliminaires, enquêtes de flagrance, instruction). Il s'agit des réquisitions informatiques proprement dites. D'autres sont de nature plus préventive que répressive. Elles ont pour but d'obtenir le blocage de l'accès aux sites qui véhiculent des messages contraires à l'ordre public. Les problèmes d'entraide ne se posent pas alors dans les mêmes termes et sont résolus différemment.

Réquisitions informatiques. Ces réquisitions concernent toutes les phases de la procédure de mise en état des affaires pénales (CPP, art. 60-1 et 60-2, 77-1-1, 77-1-2, 99-3, 99-4 : enquête préliminaire, enquête de flagrance, instruction préparatoire). Elles sont adressées par le procureur de la République, l'OPJ ou le juge d'instruction à toute personne ou organisme privé ou public susceptible de détenir des documents intéressant cette procédure. S'agissant des données informatiques, que celles-ci soient ou non nominatives, les prestataires de services sont tenus, sous peine d'amende, à une double obligation de conservation (pour un an au plus) et de mise à disposition par voie électronique.[66] En vertu de la réquisition, le fournisseur d'accès ou

---

29 juill. 1881, art. 24, al. 6), infractions en matière de paris ou de jeux d'argent ou de hasard en ligne (L. 12 mai 2010, art. 59). V. M. Quéméner, Lutte contre la cybercriminalité : l'infiltration gagne du terrain, Comm. comm. électr. 2010, alerte 82 ; A. Lepage, Étude préc., Dr. pénal 2011. spéc. n° 10, *in fine*, cet auteur regrettant l'absence de réflexion d'ensemble de la part du législateur.

[66] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), art. 6-II, al. 1er, (JO 22 juin 2004, p. 11168) ; CPP art. R. 15-33-61 et s. (décr. n° 2007-1538 du 26 oct. 2007) ; décr. n° 2011-219 du 25 févr. 2011, pris en application de l'article 6-II LCEN et relatif à la conservation et à la mise à disposition de données d'identification. V. not. sur ce dernier texte W. Duhen, Réquisitions judiciaires et conservation des données de connexion en ligne, AJ Pénal 2011. 184).

l'hébergeur doit remettre ces données sans pouvoir opposer le secret professionnel. Il peut également être fait injonction aux opérateurs de télécommunication, sous peine d'amende, de prendre sans délai "toute mesure propre à assurer la préservation (pour un an au plus) du *contenu* des informations consultées par les personnes (internautes, usagers de téléphones fixes ou mobiles, etc..) utilisatrices des services fournis par (ces) opérateurs" (CPP art. 60-2, al. 2 à 5).[67] Hormis ce cas, les opérateurs de télécommunication doivent effacer ou rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sauf possibilité de différer cet effacement (pour un an au plus) afin de mettre des informations utiles aux enquêtes à la disposition de l'autorité judiciaire. Les données conservées et traitées sont celles qui portent sur l'identification des utilisateurs et les caractéristiques techniques des communications échangées, à l'exclusion de toute donnée concernant le contenu des correspondances échangées ou des informations consultées dans le cadre de ces communications (CPCE art. L. 32-3-1).) La réquisition est alors subordonnée à l'autorisation préalable d'un magistrat (le JLD). Enfin, au titre de la prévention du terrorisme, des réquisitions limitées à certaines données techniques (identification de numéros d'abonnement, date et durée de connexions, localisation d'équipements terminaux) peuvent être faites auprès des opérateurs de communication électronique à la seule initiative des policiers et des gendarmes spécialement habilités, donc sans autorisation préalable d'un magistrat (CPCE art. L.34-1-1).

Ces réquisitions informatiques sont naturellement susceptibles de s'inscrire dans le cadre de la coopération judiciaire internationale. Elles peuvent faire suite à une demande d'entraide présentée par les autorités étrangères compétentes. Inversement, la même demande peut émaner des autorités judiciaires françaises. Elle sera alors exécutée dans les conditions prévues par l'État requis, si du moins elle est compatible avec le droit interne et les engagements internationaux de ce dernier. Il en sera notamment ainsi lorsque, en cas d'urgence, et à titre conservatoire, cet État aura été sollicité de prendre une mesure de gel provisoire des données numériques stockées sur des serveurs situés sur son territoire (Conv. Budapest, 23 nov. 2001, art. 16. V. sur les décisions de gel et leur exécution D. Rebut, *op. cit.*, n° 410, et n° 552 et s.).

Injonctions de blocage. Il s'agit d'un autre type d'injonction. Celui-ci est révélateur des vicissitudes de l'entraide répressive internationale. En effet, la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI II) prend acte des limites de la coopération internationale lorsqu'un État tente d'obtenir la fermeture de sites véhiculant des messages contraires à la dignité humaine et hébergés par des serveurs situés dans certains pays étrangers (aux USA par exemple, spécialement pour les sites négationnistes). Aussi le législateur a-t-il mis en place un dispositif administratif de blocage des adresses électroniques donnant accès à des sites pédopornographiques. En imposant cette obligation aux fournisseurs d'accès à internet (FAI), la loi française est ainsi parvenue à contourner la difficulté. Le Conseil constitutionnel a validé ce dispositif au motif

---

[67] JO 15 mars, p. 4582. Ce texte comporte un chapitre consacré à la lutte contre la cybercriminalité. Il crée notamment un délit spécifique d'usurpation d'identité.

qu'il ne lui apparaissait pas manifestement inapproprié à l'objectif poursuivi ni disproportionné au regard d'autres principes constitutionnels (sauvegarde de l'ordre public et liberté de communication).[68]

De manière générale, en France, les prestataires techniques (hébergeurs ou fournisseurs d'accès) ne sont pas soumis à une obligation générale de surveillance et de filtrage des informations qu'ils transmettent ou stockent.69 Ils peuvent toutefois être contraints par l'autorité judiciaire d'effectuer une surveillance ciblée et temporaire (LCEN, art. 6-I-7, al. 2) et de communiquer les données permettant d'identifier quiconque a contribué à la création de contenus qu'ils ont par ailleurs pour obligation de détenir et de conserver (*ibid.*, art. 6-II). Ils sont notamment tenus d'apporter leur concours à la lutte contre certaines infractions de presse particulièrement dangereuses pour l'ordre social (apologie des crimes contre l'humanité, incitation à la haine raciale, pornographie enfantine). Aussi n'est-il pas surprenant que la Cour de cassation française ait approuvé une décision ayant enjoint aux fournisseurs d'accès de mettre en œuvre toute mesure propre à interrompre l'accès au site litigieux à partir du territoire français.70 C'est dire que les considérations territorialistes demeurent ici prédominantes car le concours des autorités publiques étrangères afin qu'elles ordonnent le retrait des messages illicites, le blocage de l'accès au site litigieux ou la fermeture définitive de celui-ci dépend trop souvent du "bon vouloir" de ces autorités.71 Il n'en va différemment que dans le cercle des États membres de l'Union européenne, voire désormais du Conseil de l'Europe, là où les règles gouvernant l'entraide sont les plus élaborées.

2° Échange de données concernant les enquêtes

Ces échanges relèvent à la fois de l'entraide policière et de l'entraide judiciaire. Les règles qui leur sont applicables (a) sont mises en œuvre dans un souci d'efficacité répressive (b).

a) Règles françaises

---

[68] Cons. const., 10 mars 2011, Décision n° 2011-625 DC (JO 15 mars 2011, p. 4630).

[69] V. en ce sens CJUE, 16 févr. 2012, et les commentaires auxquels cette importante décision a donné lieu : E. Derieux, Neutralité de l'internet. Fournisseurs d'hébergement. Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage, RLDI 2012/80, n° 2666 ; A. Neri, L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables, Comm comm. électr. 2012. Étude 3 ; M. Quéméner, La loi LOPPSI 2 au regard des nouvelles technologies, Comm comm. électr. 2011. Étude 9, spéc. n° 9.

[70] Civ. I, 19 juin 2008, Bull. civ. n° 178, cet arrêt ayant considéré qu'une telle mesure était adéquate et proportionnée, comme l'a également estimé plus tard le Conseil constitutionnel (V. égal. la jurisprudence citée *supra* I A 2°).

[71] en ce sens D. Chilstein, étude préc., p. 601.

Les unes sont applicables de manière générale aux relations que la France entretient avec des États auxquels elle est liée par des accord nationaux ou multilatéraux (dont on fournira ci-dessous une illustration récente) ; il s'agit en quelque sorte de règles de droit commun. D'autres sont propres aux relations de notre pays avec les États membres de l'Union européenne.

Dispositions de droit commun. Ce sont celles qui déterminent les conditions dans lesquelles s'effectuent les échanges de données intéressant l'enquête entre la France et les autres États, que ces échanges se situent dans le cadre de la coopération policière ou dans celui de l'entraide judiciaire.

Les échanges d'informations entre services nationaux de police font l'objet d'une réglementation qui, en France, figure logiquement dans le Code de la sécurité intérieure en raison de leur finalité préventive. Ainsi l'article L. 235-1 de ce code, issu de l'ordonnance du 12 mars 2012[72] et situé dans le Livre II relatif à la coopération internationale en matière d'accès aux traitements automatisés de données personnelles, comporte-t-il des dispositions concernant la coopération active et la coopération passive entre ces services (Livre II : ordre et sécurité publics). Il en ressort que les données personnelles contenues dans des systèmes de traitement de données gérés par les services de police et de gendarmerie nationales peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou à des services de police étrangers. Ces services communiquent donc directement entre eux. Toutefois des restrictions sont prévues. Il est nécessaire que les services destinataires de ces informations donnent des garanties jugées "suffisantes" aux yeux des autorités françaises quant au respect de la vie privée et des droits fondamentaux des personnes concernées par le traitement.[73] Tel est le cas du fichier automatisé d'empreintes digitales.[74] Ce fichier peut être consulté, en vue notamment de faire l'objet de rapprochements, par les agents spécialement habilités d'organismes de coopération internationale en matière de police judiciaire ou par les agents des services de police ou de justice d'États étrangers, sur demande préalable motivée de leur part (art. 9-1 à 9-3) et dans le respect des finalités et conditions prévues par les engagements internationaux de la France (parmi lesquels le Traité de Prüm du 27 mai 2005). Sont notamment visés les engagements liant notre pays à des organismes internationaux ou à des États étrangers assurant le niveau de protection suffisant indiqué ci-dessus (V. égal. i*nfra*).

---

72 Ord. n° 2012-351 du 12 mars 2012, JO du 13 mars 2012 p. 4533.

73 Le caractère suffisant du niveau de protection assuré s'apprécie en fonction de plusieurs critères : dispositions en vigueur dans l'État destinataire, mesures de sécurité qui y sont appliquées, finalité et durée du traitement, nature, origine et destination des données traitées, etc.. (art. L. 235-1, al. 1, *in fine ;* L. n° 68-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 68, al. 2).

74 Décr. n° 87-249 du 8 avr. 1987, mod. décr. n° 2011-157 du 7 févr. 2011 (JO du 9 févr. 2011, p. 2507).

Quant aux échanges d'informations s'inscrivant dans un autre cadre, celui de l'entraide judiciaire, l'article 695-10 du Code de procédure pénale les envisage de manière générale et indirecte. Il renvoie en effet aux dispositions du même code réglementant les modes ordinaires de transmission des demandes d'entraide. Il renvoie également à celles de ces dispositions qui concernent les cas d'urgence (transmission directe des demandes entre autorités judiciaires compétentes) ainsi que les équipes communes d'enquête (accomplissement d'actions coordonnées et concertées entre les États membres – telles que les infiltrations – qui impliquent communication directe à des autorités judiciaires étrangères d'informations issues de procédures pénales en cours). Enfin, il étend ces dispositions aux demandes d'entraide entre la France et les autres États qui sont parties "à toute Convention *comportant des dispositions similaires* à celles de la Convention du 29 mai 2000". Or cette Convention, qui réglemente l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, et qui est désormais applicable aux relations entre la France et les États membres du Conseil de l'Europe (V. *supra*), autorise les échanges spontanés d'informations (art. 7), sous réserve du respect des droits nationaux et des conditions d'utilisation éventuellement fixées par l'autorité ayant fourni ces informations à l'État destinataire (le premier imposant par exemple au second le respect de certaines des prescriptions de la loi informatique et libertés du 6 janvier 1978, celle notamment qui interdit de détourner le traitement de sa finalité). Il en résulte qu'en droit français il n'y a pas a priori d'obstacle pour admettre la possibilité de consultation directe – c'est à dire sans demande préalable – par des autorités compétentes étrangères des bases de données nationales ou internationales contenant des informations utiles aux enquêtes criminelles.

Dispositions propres à l'entraide entre la France et d'autres États membres de l'Union européenne. Insérées dans le Code de procédure pénale au titre le l'entraide judiciaire internationale (art. 695-9-31 à 695-9-49),[75] en application de la décision-cadre 2006/960/ JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne elles sont destinées à simplifier les procédures applicables à l'échange d'informations entre, d'une part, la police, la gendarmerie et les douanes françaises et, d'autre part, les services compétents d'un autre État membre de l'UE (et vice-versa), ceci pour répondre de la manière la plus efficace possible aux besoins des enquêtes judiciaires (investigations tendant à établir la preuve des infractions et recherche de leurs auteurs) et de la prévention des infractions. Ces services sont autorisés à échanger les informations qui sont à leur disposition, "soit qu'ils les détiennent, soit qu'ils puissent y accéder, notamment par consultation d'un traitement automatisé de données, sans qu'il soit nécessaire de prendre ou solliciter une réquisition ou toute autre mesure coercitive" (CPP art. 695-9-31, *in fine*). S'il existe des raisons de supposer qu'un État membre détient des informations utiles, la transmission peut en être sollicitée par les services compétents de l'État qui souhaite les obtenir. La demande de transmission doit exposer les raisons laissant supposer

75 Ord. n° 2011-1069 du 8 sept. 2011, JO 9 sept. p.15200.

que lesdites informations sont détenues par ces services, préciser à quelles fins elles sont demandées et indiquer le lien entre les fins recherchées et la ou les personnes visées (art. 695-9-32).

Il résulte de ce qui précède qu'il n'est pas permis aux autorités compétentes concernées d'accéder "en libre service" aux informations. En outre, une fois obtenues, celles-ci ne peuvent être utilisées à titre de preuve qu'avec l'accord de l'État membre qui les a transmises (art. 695-9-34). Quant à leur utilisation à d'autres fins que celles pour lesquelles elles ont été communiquées, elle est également subordonnée à l'accord de l'État membre qui les a transmises.[76] Enfin, pour pouvoir effectuer cette transmission, il est nécessaire d'obtenir l'autorisation d'un magistrat "chaque fois (qu'elle) est requise en France pour accéder à ces mêmes informations ou les transmettre à un service ou à une unité de police judiciaire" (art. 695-9-40, cet article visant donc des mesures telles que l'interception de télécommunications, la captation de données informatiques ou certaines réquisitions. V. s*upra*).

Il est vrai qu'un régime particulier est établi s'agissant des infractions – parmi lesquelles celles qui se rattachent à la cybercriminalité (V. *supra*) – incluses dans la liste des 32 catégories d'infractions considérées comme graves (la peine encourue en France étant au moins égale à trois ans d'emprisonnement) et pour lesquelles l'exigence du contrôle de la double incrimination est écarté. En effet, les informations mentionnées à l'article 695-9-31 qui sont détenue par les services de police, de gendarmerie ou des douanes français relativement à ces infractions peuvent être transmises *sans autorisation préalable* s'il apparaît utile de les communiquer aux autorités compétentes étrangères pour leur permettre, soit de prévenir la commission de telles infractions, soit de conduire les investigations tendant à en établir la preuve ou à en rechercher les auteurs (art. 695-9-38). Dans les autres cas, en revanche, c'est à dire en dehors des prévisions des articles 695-23 et 695-9-38, cette autorisation préalable est nécessaire ainsi qu'il a été indiqué ci-dessus. Il en est de même en cas de communication ultérieure de l'information à un autre État que le destinataire initial (art. 695-9-39).

Quoiqu'il en soit, dans toutes les hypothèses où la transmission est permise, les informations obtenues par les services étrangers compétents peuvent être utilisées par eux "à titre de preuve", sauf indication contraire lors de la transmission (art. 695-9-45). Le service compétent indique au service destinataire leurs conditions d'utilisation et peut demander à ce dernier, chaque fois qu'il l'estime utile, de l'informer de l'utilisation ultérieure de l'information transmise. Le même service est compétent pour juger de l'opportunité d'autoriser, à la demande de l'État destinataire, la retransmission de cette information à un État tiers ou sa nouvelle utilisation, et, le cas échéant, d'en fixer les conditions. Enfin, et en tout état de cause, les informations ou

---

[76] Sauf s'il s'agit de prévenir un danger grave pour la sécurité publique, et sans préjudice du contrôle exercé sur le plan interne par les autorités judiciaires (CPP art 12 et 13) et d'autres autorités compétentes (L. 6 janv. 1978, art. 11 et s. relatif aux pouvoirs de la CNIL).

données échangées doivent rester confidentielles (art. 695-9-32, qui précise que "les modalités de leur transmission et de leur conservation garantissent le respect de ce principe", et ce "sans préjudice des dispositions de l'article 11 [du Code de procédure pénale français] relatives au secret de l'enquête et de l'instruction").

Quant aux refus de transmission, ils sont strictement limités aux cas prévus par la loi : risque d'atteinte aux intérêts fondamentaux relevant de la sécurité nationale ; communication de nature à nuire au déroulement des enquêtes pénales ; risque d'atteinte à la sécurité des personnes ; disproportion manifeste de cette transmission au regard des finalités de la demande (art. 695-9-41). Il s'y ajoute la marge d'appréciation offerte aux services compétents lorsque l'infraction est de faible gravité (inférieure ou égale à un an d'emprisonnement). En pareil cas, ces derniers peuvent refuser la transmission sollicitée s'ils estiment qu'elle ne revêt pas un "intérêt suffisant" au regard des contraintes qu'elle implique (art. 695-9-42).

En définitive, le dispositif mis en place au sein de l'Union européenne est allégé et relativement souple par rapport aux procédures classiques d'entraide. Il est donc de nature à renforcer l'efficacité de la lutte contre la cybercriminalité. Il serait dès lors souhaitable de l'étendre – lorsque ce n'est pas déjà le cas – à la coopération entre la France et les États auxquels notre pays est liés en vertu d'accords bilatéraux ou multilatéraux, comme cela est prévu vis-à-vis des unités EUROJUST et EUROPOL et des États non membres de l'Union européenne associés à l'acquis de Schengen (art. 695-9-48).

Dispositions relatives aux échanges de données figurant dans des conventions bilatérales. Illustration. Les accords dans le domaine de la coopération policière et de la sécurité intérieure – qui se sont multipliés depuis une vingtaine d'années s'agissant de la France – comportent en effet des dispositions ayant entre autre pour objet de déterminer les conditions dans lesquelles les transmissions d'informations entre les services compétents des parties contractantes sont assurées. Le principe général posé par ces accords est celui du respect de la législation nationale. Le rappel de ce principe concernant plus spécialement les attributions de l'autorité judiciaire, les règles applicables aux traitement des données confidentielles et des données à caractère personnel ainsi que les motifs de rejet des demandes de coopération. Des dispositions spécifiques relatives à la coopération en matière de lutte contre la criminalité transnationale organisée et le terrorisme sont également insérées dans ces accords.

A titre d'illustration, il sera fait état ci-dessous de l'accord portant sur la coopération policière conclu entre la France et la Serbie (État n'appartenant pas à l'Union européenne).77 Cet accord a pour objet de promouvoir, notamment à travers des échanges d'information, la coopération bilatérale policière entre les Parties en matière

---

77 A noter que dans un rapport récent la Commission européenne a recommandé l'ouverture de négociations d'adhésion avec la Serbie (Bruxelles, 22 avr. 2013 JOIN (2013) 7 final.), signé à Paris le 18 nov. 2009, dont l'approbation a été autorisée par la loi n° 2013-326 du 19 avril 2013 (JO 20 avr. 2013, p. 6944 ; décret non encore publié au JO à ce jour).

de prévention et de détection des actes criminels (art. 1er, al. 1 ; art. 3, b). Le crime organisé, le terrorisme et la cybercriminalité sont inclus dans le domaine de cette coopération (art. 2 a, b, e). Outre le rappel du principe selon lequel cette dernière doit être menée dans le strict respect des législations nationales des deux Parties et de leurs engagements internationaux (art. 1er, al. 2), l'accord comporte des dispositions consacrées à la protection des données et à leur communication aux tiers (Titre IV, art. 11). La Partie bénéficiaire ne peut utiliser ces données que pour les besoins définis lors de la demande et aux conditions fixées par la Partie émettrice, leur utilisation à d'autres fins étant subordonnée à l'autorisation préalable de cette Partie. Elle doit rendre compte de l'utilisation des informations fournies ainsi que des résultats obtenus et garantir un niveau de confidentialité et de protection contre tout accès, modification et diffusion non autorisé équivalent à celui qu'accordent les autorités compétentes de la Partie émettrice. Ces informations ne peuvent être transmises à d'autres autorités et États tiers sans l'accord préalable de la Partie émettrice. Les personnes dont les données à caractère personnel ont fait l'objet de transmission peuvent, sur leur demande, connaître le contenu de celles-ci ainsi que l'utilisation qui en a été faite. La divulgation des informations requiert une autorisation écrite préalable de la Partie émettrice et s'effectue en accord avec la législation nationale de la Partie requérante.

b) Mise en œuvre de l'échange des données

Afin de mettre en œuvre les règles relatives à l'échange des données qui viennent d'être exposées et de les rendre les plus efficaces possibles, il était nécessaire de prévoir des dispositifs centralisés et des réseaux de transmission adaptés aux nécessités répressives. Tel a été l'un des objectifs poursuivis par les rédacteurs de la Convention de Budapest du 23 novembre 2001 (art. 35) et de la Décision-cadre du Conseil de l'Union européenne du 18 décembre 2006. Pour répondre à cette exigence, un point de contact joignable 24 heures sur 24, sept jours sur sept, a été mis en place en France. Il s'agit de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) rattaché à la Direction Centrale de la Police Judiciaire (DCPJ) et situé à Nanterre. Cet organisme, dont les compétences opérationnelles et techniques s'exercent dans le domaine de la cybercriminalité, est habilité à recevoir les demandes d'informations provenant de services compétents étrangers, notamment des services d'enquête des États membres de l'Union européenne. En outre, il accueille deux plateformes accessibles au public : la plateforme PHAROS, qui exploite les signalements de contenus illicites circulant sur internet formulés sur le site officiel du gouvernement (www.internet-signalement.gouv.fr) ; la plateforme Info-Escroqueries, qui oriente et conseille les victimes d'escroqueries (0811.02.02.17). S'agissant des demandes d'informations émanant de services d'enquête étrangers, deux points de contact sont, plus précisément, habilités à les recevoir et à les traiter : la section centrale de coopération opérationnelle de police (PCC/SCCOPOL), gérée par la division des relations internationales (DRI) de la direction centrale de la police judiciaire ; le bureau de la communication et des relations extérieures (BCRE), intégré à la direction nationale

du renseignement et des enquêtes douanières.78 En outre, au sein de la DRI, un service est en charge des actions de coopération européenne et internationale (SCACEI).). La plateforme commune (PCC/SCCOPOL) regroupe les trois canaux institutionnels de la coopération opérationnelle policière internationale auxquels la France participe, à savoir INTERPOL, SCHENGEN et EUROPOL (V. CPP, art. D. 8-2). Elle centralise les demandes nationales de coopération qui sont à destination de l'étranger, vérifie la légalité de la demande, fait les premiers recoupements et choisit le canal de coopération le mieux adapté aux particularités des demandes des enquêteurs. Les services en charge de la coopération policière internationale en France se situent désormais dans un contexte interministériel regroupant Police nationale, Gendarmerie nationale, Douane et Justice. Cette dernière y participe par le biais de la mission justice du Bureau de l'Entraide Pénale Internationale (BEPI). On notera que la Commission nationale de informatique et des libertés (CNIL) et l'OCLCTIC sont désormais étroitement associés "dans un souci d'efficacité de l'action publique en matière de lutte contre la cybercriminalité".[79]

3° Autres dispositifs d'assistance mutuelle

Accords « Passenger Name Record » (PNR). Le nouvel accord UE-États-Unis dit "PNR" a été adopté le 19 avril 2012 par le Parlement européen et le 26 avril 2012 par le Conseil de l'Union européenne (doc. 17434/11). Il remplace l'accord appliqué à titre provisoire depuis 2007. La date d'entrée en vigueur prévue était le 1er juin 2012. Il vise à mettre en place un cadre juridique régissant le transfert des données des dossiers passagers (données PNR) par les transporteurs assurant des services de transport de passagers entre l'Union européenne et les États-Unis au ministère américain de la sécurité intérieure (DHS) et l'utilisation qui en sera faite par celui-ci. Il s'agit de prévenir et de détecter les infractions terroristes, les infractions pénales qui leur sont liées ainsi que d'autres formes graves de criminalité transnationale, afin de pouvoir effectuer des enquêtes et engager des poursuites contre les auteurs présumés de ces infractions.

La conclusion de cet accord a donné lieu, on le sait, à de vives controverses, celles-ci étant en rapport avec la protection des droits fondamentaux des personnes concernées (durée de conservation des données collectées, utilisation et garanties de protection de ces données, recours administratifs et judiciaires, etc..)80). Quoiqu'il en soit, la

---

78 V. en ce qui concerne les demandes émanant des services d'enquête des États membres de l'Union européenne : CPP art. 695-9-47 ; Arrêté du 27 septembre 2012 désignant les points de contact habilités).

79 Convention de partenariat, 11 janvier 2013, Préambule, § 8. V. spéc. art. 1er relatif à l'orientation des usagers et aux échanges d'informations concernant plus particulièrement l'état d'avancement des dossiers, les signalements reçus et les résultats des actions entreprises.

80 V. not. Proposition de Résolution européenne sur l'accord PNR avec les États-

collecte des données personnelles transmises en application de cet accord est désormais réglementée en France par les dispositions du Code de la sécurité intérieure (CSI art. L. 232-1 à L. 232-6 résultant de l'ordonnance du 12 mars 2012, préc.).[81] En vertu de ces textes, les compagnies ferroviaires, aériennes et maritimes sont tenues, sous peine d'amende (50.000 Euros au plus pour chaque voyage), de transmettre aux services du ministère de l'intérieur un certain nombre de données relatives aux passagers enregistrées dans les systèmes de réservation et de contrôle des départs. Ces données à caractère personnel peuvent être comparées avec le fichier des personnes recherchées (FPR) et leur traitement peut faire l'objet d'une interconnexion avec le fichier des personnes recherchées et le système d'information Schengen (SIS). Les transporteurs ont l'obligation d'informer les personnes concernées par la mise en œuvre du traitement conformément aux dispositions de la loi Informatique et libertés du 6 janvier 1978 (préc.).

Auditions à l'étranger par vidéoconférence et/ou téléconférence. L'utilisation des nouvelles technologies de la communication peut se révéler utile pour accomplir divers actes de procédure. Elle peut l'être notamment pour faciliter l'audition de témoins, experts, victimes ou accusés en cours d'enquête ou d'instruction, voire dans la phase de jugement lors d'une audience. Cette possibilité est offerte en France en vertu des dispositions du Code de procédure pénale relatives à l'utilisation de moyens de télécommunications au cours de la procédure (art. 706-71). En effet, lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne ainsi que les confrontations peuvent être effectués en plusieurs points du territoire national reliés par des moyens de télécommunications, pourvu que cette la confidentialité de la transmission soit assurée. Elles peuvent faire l'objet d'un enregistrement audiovisuel ou sonore. L'utilisation d'un moyen de télécommunication audiovisuelle est également possible devant la juridiction de jugement pour l'audition des témoins, des parties civiles et des experts ainsi que pour la comparution du prévenu devant le tribunal correctionnel si celui-ci est détenu (sous réserve dans ce dernier cas de l'accord du procureur de la République et de l'ensemble des parties).

Qu'en est-il pour les auditions et interrogatoires à distance par-delà les frontières ? Elles sont prévues, mais seulement de manière explicite entre États membres de l'Union européenne (Convention de Bruxelles du 29 mai 2000 relative à l'entraide judiciaire, préc., art. 10 et 11) et du Conseil de l'Europe (Protocole additionnel n° 2 à cette Convention, préc., désormais en vigueur en France). La France a toutefois écarté la possibilité de procéder à une telle audition dans le cadre d'une demande l'entraide judiciaire, donc d'auditionner par vidéoconférence ou conférence téléphonique les prévenus ou accusés comparaissant devant la juridiction de

---

Unis, doc. Sénat 2011-2012 n° 178, soulignant à l'époque que les conditions dans lesquelles les données seraient susceptibles d'être transmises à des États tiers n'offraient pas des garanties suffisantes.

[81] Dispositions substituées à celles que prévoyait déjà l'art. 7 de la loi préc. du 23 janv. 2006 relative à la lutte contre le terrorisme.

jugement, et ce alors même que cette audition serait admise par l'État étranger concerné. Cette position restrictive se situe d'ailleurs dans le ligne fixée par la jurisprudence de la Cour européenne des droits de l'homme selon laquelle la comparution d'un accusé par vidéoconférence n'est admissible qu'à la condition de poursuivre un but légitime et selon des modalités de déroulement compatibles avec les droits de la défense au sens de l'article 6 de la Convention.[82]

C. Extension de la protection des libertés individuelles et des droits fondamentaux

La nécessité d'assurer une protection renforcée de ces droits et libertés, notamment de la vie privée et des données à caractère personnel, s'impose en matière pénale comme en tout autre domaine. Il s'agit en France d'une préoccupation constante du législateur et des tribunaux (1°). Mais la protection de la personne va au delà. Elle s'étend au procès pénal lui-même en raison des principes qui le gouvernent : celui du droit à un procès équitable et, de façon plus spécifique, celui de loyauté des preuves (2°).

1. Protection de la vie privée et des données personnelles

Plusieurs illustrations en ont déjà été fournies ci-dessus. Ainsi rappellera-t-on qu'en France, depuis la loi « LOPPSI 2 » du 14 mars 2011, les « *captures d'écran* » sont autorisées afin, notamment, de repérer des pédophiles ; en revanche, comme on l'a indiqué, il est interdit aux enquêteurs de « *se promener et de fouiller* » dans l'ordinateur objet de leurs investigations à distance. En effet, ces captations de données, opérées grâce à l'installation de dispositifs espions, ne doivent être confondues avec les perquisitions informatiques transfrontières, dont la validité est subordonnée à des conditions distinctes. D'autres garanties sont également prévues ; mais elles sont parfois jugées insuffisantes du point de vue des libertés individuelles.[83] Quant à la jurisprudence, on se bornera à signaler un arrêt de la Chambre criminelle de la Cour de cassation du 16 juin 2011 rendu dans une espèce où, la preuve de pratiques anticoncurrentielles ayant été rapportée grâce à l'utilisation d'une technique de saisie sélective de messages échangés par voie électronique, la question était de savoir s'il avait été porté atteinte à la confidentialité des correspondances entre un avocat et son client.[84] Cet arrêt a le mérite de mettre en évidence la nécessité, mais aussi la difficulté, de concilier les exigences de la répression avec le besoin de protection, observation dont la portée est évidemment

---

82 CEDH, 5 oct. 2006, *Viola c. Italie*, Req. n° 45106/04, § 67.

83 V. not. sur ces critiques S. Hennequin, C. Ribeyre et A. Lepage, préc. *Adde* sur les difficultés soulevées par les perquisitions transfrontières, V. D. Bénichou et F. Chopin, préc.

84 Cass. crim., 16 juin 2011, n° 11-80.345, Bull. crim. n° 135, cassant un arrêt de la Cour d'appel de Paris du 4 janv. 2011 au motif « qu'il lui appartenait de vérifier concrètement (…) la régularité [des opérations] et d'ordonner, le cas échéant, la restitution des documents qu'il estimait appréhendés irrégulièrement ou en violation des droits de la défense ».

générale.

Le Conseil constitutionnel a eu pour sa part l'occasion de se prononcer sur la conformité aux normes constitutionnelles des dispositions législatives applicables dans le cadre d'enquêtes criminelles utilisant les nouvelles technologies de l'information et de la communication. La position qu'il adopte est plutôt nuancée dans la mesure où il prend assez largement en compte les préoccupations répressives du législateur contemporain. Il a ainsi estimé que celui-ci "peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières" (...). Selon le juge constitutionnel, en effet, "la criminalité organisée justifie la mise en place de dispositifs [spécifiques] (...) dès lors que l'autorisation de les utiliser émane de l'autorité judiciaire, gardienne de la liberté individuelle (Const. 4 oct. 1958, art. 66), et que sont prévues des garanties procédurales appropriées".[85] Aussi certains auteurs soulignent-ils les risques de dérive qu'une telle position est susceptible d'entraîner. "La logique policière, écrit l'un d'eux, qui contamine progressivement l'ensemble des dispositifs de lutte contre les formes graves de criminalité, apparaît inquiétante du point de vue de la préservation des libertés fondamentales".[86]

Quoi qu'il en soit, il convient de rappeler l'existence en France d'un texte très protecteur des données personnelles et de la vie privée : la loi "Informatique et libertés" du 6 janvier 1978 qui s'applique à tout traitement de données quelle que soit sa finalité.[87] Ce texte – cité précédemment à plusieurs reprises – comporte des dispositions applicables, on l'a vu, à la collecte, au traitement et à l'échange d'informations intéressant les enquêtes pénales. De telles opérations nécessitent de faire appel aux nouvelles technologies de l'information et de la communication. Certes, elles doivent être effectuées dans le respect d'un certain nombre d'obligations imposées par la loi aux responsables des traitements,[88] et elles le sont sous le contrôle

---

85 Cons. const., 2 mars 2004, Décision n° 2004-492 DC relative à la loi portant adaptation de la Justice aux évolutions de la criminalité (Loi n° 2004-204 du 9 mars 2004 [Perben II], JO 10 mars 2004, p. 4637).

86 D. Chilstein, rapport préc., p. 595.

87 Loi du 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, mod. L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (JO du 7 août 2004, p. 14063) et mod. L. n° 2011-334 du 29 mars 2011 relative au Défenseur des droits (JO du 30 mars 2011 p. 5504).

88 Les données sur lesquelles porte le traitement doivent être collectées et traitées "de manière loyale et licite" et pour des "finalités déterminées, explicites et légitimes", être "adéquates, pertinentes et non excessives" au regard de ces finalités, de même qu'elles doivent être "exactes, complètes, mises à jour si nécessaire" et, à défaut, "effacées ou rectifiées" ; enfin elles ne peuvent pas être conservées pour une durée excédant ce qui est nécessaire aux finalités du traitement. Il s'y ajoute l'interdiction de collecter et de traiter des données de nature sensible (au sens de l'art. 8-I : données relatives notamment aux origines raciales et ethniques des personnes ou à leurs opinions politiques, philosophiques ou

d'une autorité administrative indépendante (la CNIL) ainsi naturellement que de l'autorité judiciaire. Mais des dérogations spécifiques sont prévues pour certaines de ces obligations (art. 8-II et IV, 26, 32 V et VI, 38, 41 et 42, 45, 68, 69) ainsi que pour les droits reconnus aux personnes qui font l'objet de ces traitements (art. 32 et 38 à 43 : information, accès, rectification, opposition). A titre d'illustration on rappellera que si la loi "Informatique et libertés" autorise les traitements de données à caractère personnel "mis en œuvre pour le compte de l'État (et ayant) pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté" (art. 26), elle impose en revanche, afin de pouvoir transférer ces données vers un État n'appartenant pas à l'Union européenne, que les services destinataires de ces informations "assurent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet".[89] Certes, à défaut de cette garantie le transfert reste encore possible. Mais il est alors nécessaire, soit que la personne concernée y ait expressément consenti, soit que ce transfert s'impose pour des motifs qui sont limitativement déterminées par la loi telles que la sauvegarde de l'intérêt public ou de la vie d'une personne (L. 6 janv. 1978, art. 69 et art. 8-II). Le transfert est également autorisé, en dépit de l'absence d'un niveau suffisant de protection, lorsqu'il a lieu afin de permettre la "consultation (...) d'un registre public destiné à l'information du public et ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime" (art. 69, 4°).

Le régime applicable aux opérations de traitement des données à caractère personnel a donc été adapté aux exigences spécifiques de la lutte contre la criminalité. Dès lors, s'agissant de la coopération policière et judiciaire en matière pénale au sein de l'Union européenne, le fait que la France dispose, grâce à la loi "Informatique et libertés" ainsi qu'aux dispositions introduites dans le Code de procédure pénale aux articles 695-9-31 à 695-9-49 (V. *supra*), d'un niveau de protection adéquat au sens de la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à cette coopération, explique que ce dernier texte n'ait donné lieu à aucune mesure de transposition particulière dans notre droit. Certes, le cadre juridique existant est susceptible d'évoluer à l'avenir dans le sens d'un renforcement du droit de chaque personne physique au respect de sa vie privée et à la protection des données personnelles la concernant.[90] L'objectif est de remédier aux importantes disparités actuelles entre les législations nationales couvrant ce domaine et de répondre ainsi pleinement aux exigences de la Charte des droits fondamentaux de l'Union

---

religieuses) ainsi que des obligations relatives à l'information des personnes concernées (art. 32), à la durée de conservation des données (art. 6), à la préservation de leur sécurité (art. 34).

[89] CSI art. L. 235-1, al. 1, *in fine*, et L. n° 78-17 du 6 janv. 1978, art. 68, al. 2, cités *supra*.

[90] V. *supra* les propositions de nouveau Règlement et de nouvelle Directive non encore finalisées à ce jour et qui suscitent encore de sérieuses réticences en France. V. la Proposition de Résolution européenne sur la protection des données personnelles présentée par le Sénat le 7 févr. 2013, doc. Sénat n° 343.

européenne (art. 7 et 8) et du Traité de Lisbonne (TFUE art. 16).[91] Certes, à la différence de la Convention de Budapest du 23 novembre 2001, les textes précédemment cités n'appréhendent pas la cyberdélinquance et la cybercriminalité de manière spécifique. Ils n'en établissent pas moins des règles protectrices auxquelles les États sont tenus de se conformer et qui sont applicables aussi bien dans ce domaine particulier que dans n'importe quel autre. Cette dernière observation s'impose d'autant plus que la Convention de Budapest est décevante car hormis son préambule, et à la différence de la Convention de Bruxelles du 29 mai 2000 (art. 23), elle ne fournit guère d'indications sur l'exigence de garanties appropriées, particulièrement en matière de confidentialité. Celles-ci mériteraient pourtant d'être précisées en raison des particularités de cette forme de criminalité et de la spécificité des techniques d'investigation utilisées pour la combattre.

2° Respect du principe de loyauté des preuves et du droit à un procès équitable

La loyauté dans la recherche des preuves et le respect du droit à un procès équitable figurent parmi les principes directeurs du procès pénal qui s'imposent aux enquêteurs, que ces derniers soient ou non spécialisés dans la lutte contre la criminalité informatique. Il est vrai que la preuve de la commission de cybercrimes et délits se révèle souvent difficile à rapporter en raison du caractère immatériel, « virtuel » et « transfrontières » de l'espace et des modes de transmission utilisés. Mais, en dépit de l'anonymat recherché, et d'une virtuosité de plus en plus fréquente dans le maniement des outils existants (notamment des techniques de contournement des dispositifs de sécurité), l'informatique laisse des traces. Des enquêteurs avertis ont les moyens de les déceler ; ils peuvent toutefois être tentés de le faire en utilisant des méthodes d'infiltration déloyales. Or les principes rappelés ci-dessus s'opposent à ce que des preuves obtenues à la suite de provocations policières puissent servir de base à une condamnation.

La question envisagée ici comporte des aspects de droit international. Cela s'explique par le fait que les autorités nationales de police entretiennent d'étroites et intenses relations dans la lutte contre la criminalité organisée (terrorisme, infractions à caractère raciste, pédophilie, etc.). Deux arrêts de la chambre criminelle rendus dans une même affaire, l'un le 7 février 2007, l'autre le 4 juin 2008, en fournissent une illustration. En l'espèce, les autorités de police américaines avaient créé un site internet destiné à attirer des pédophiles. Grâce à cette technique de « harponnage » elles avaient pu transmettre à la police française des renseignements concernant l'un des individus piégés. La chambre criminelle a considéré qu'il convenait d'écarter les preuves ainsi obtenues et a invalidé l'ensemble de la procédure suivie contre le pédophile ayant fait l'objet de poursuites pénales en France. Elle a déclaré – à deux reprises dans cette affaire – qu'un tel procédé était déloyal et qu'il en résultait une

[91] V. déjà en ce sens le Préambule de Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008, § 48.

atteinte au droit à un procès équitable.[92]

Outre que la compétence territoriale française a été logiquement retenue,[93] ces deux arrêts de principe, rendus au visa de l'article 6.1 de la Convention européenne des droits de l'Homme et de l'article préliminaire du Code de procédure pénale, sont conformes à la jurisprudence de la Cour de Strasbourg.[94] Ils présentent surtout un grand intérêt, à la fois théorique et pratique. Sur le premier plan, il a été noté en doctrine que la norme de droit pénal interne se trouvait ainsi « *internationalisée* » au profit du justiciable, qu'elle constituait désormais un « *outil transnational* » de sa protection.[95] Sur le second, il est clair que les enquêteurs devront se montrer particulièrement vigilants, non seulement pour parvenir à déceler les infractions commises sur le web et à identifier leurs auteurs, mais également afin d'éviter que leurs techniques d'investigation – qui sont très intrusives – ne dépassent les limites admissibles.[96] De manière plus générale, d'ailleurs, les autorités nationales, voire internationales, chargées de la lutte contre ce type de criminalité sont tenues de respecter les droits et libertés individuelles des usagers du web.

---

92 Cass. crim., 7 févr. 2007, Bull. crim., n° 37 ; D. 2007. 1079, préc., D. 2007. 2012, note J.-R. Demarchi ; RSC 2008. 663, obs. J. Buisson ; AJ pénal 2007. 233 ; RSC 2007. 331, obs. R. Finielz, préc., RSC 2007. 560, obs. J. Francillon ; Dr. pénal 2007, chron. 29, obs. A. Lepage ; Procédures 2007, comm. 147, obs. J. Buisson ; Cass. crim., 4 juin 2008, Bull. crim., n° 141 ; D. 2008, AJ, p. 1766, note S. Lavric ; D. 2008, Pan. p. 2716, obs. J.-D. Bretzner ; RSC 2008, p. 621, obs. J. Francillon ; AJ pénal 2008. 425, obs. S. Lavric ; Dr. pénal 2008, chron. 10, obs. A. Lepage, préc. ; Dr. pénal 2009, chron. 1, obs. D. Guérin. *Adde* : M. Quéméner, Réponses pénales face à la cyberpornographie, AJ pénal 2009, p. 107 et s.).

93 V. *supra*, I, B.

94 CEDH, 9 juin 1998, *Teixeira de Castro c/ Portugal*, Rec. 1998-IV, JCP 1999, I, n° 105, n° 38, obs. F. Sudre, RSC 1999, p. 401, obs. R. Koering-Joulin. *Adde* dans le même sens : CEDH, 22 juill. 2003, *Edward et lewis c/ Royaume-Uni*, nos 33647/98 et 40461/98, non publiée, § 49, solution confirmée par la Grande Chambre dans la même affaire : CEDH, Gde Ch., 27 oct. 2004, Rec. 2004-X, § 48. V. sur cette jurisprudence J.-F. Renucci, Traité de droit européen des droits de l'Homme, LGDJ, 2007, n° 340, et les références à la jurisprudence et à la doctrine françaises.

95 J.-R. Finielz R. et Demarchi, obs. et note préc.

96 V. en ce sens D. Chilstein, Rapport préc., p. 553 et s., spéc. p. 605, cet auteur observant à juste titre que la logique policière, qui nécessite de lutter « à armes égales » contre les cybercriminels, ne doit pas conduire « à sacrifier systématiquement les garanties de l'État de droit ». À noter, s'agissant des opérations d'infiltration, que si les cyberenquêteurs sont autorisés à participer sous un pseudonyme aux échanges électroniques, il leur est en revanche interdit, à peine de nullité de la procédure, d'accomplir des actes constituant une incitation à commettre des infractions (V. *supra*).