LA CRIMINALITÉ INFORMATIQUE, FAÇONNÉE PAR LE DROIT DE L'UNION EUROPÉENNE ?

Paul Cazalbou
Maître de conférences à l'Université Toulouse I Capitole

Lorsqu'on se plonge dans la question de la criminalité informatique, plusieurs images viennent à l'esprit qui véhiculent leur lot d'idées reçues parfois franchement erronées.

La première de ces images est celle du « pirate » informatique[1] puisqu'il est difficile de trouver de la documentation relative à cette forme de criminalité qui n'emploie pas à l'envie le vocabulaire propre aux gens de fortune – flibustiers épris de liberté, écumant la toile, et ne se couchant devant personne ; sauf à devenir Corsaires lorsqu'ils sont engagés par un État pour faire la chasse aux pirates d'autres États. La seconde des images auxquelles on ne coupe pas est celle du cybercriminel exploitant les arcanes du réseau internet et les possibilités ouvertes par une technologie toujours plus pointue pour réaliser des infractions toujours plus délicates à appréhender. On n'est alors pas loin de voir en image subliminale, Néo, le personnage de la trilogie « Matrix » chassant le lapin blanc dans un univers *underground* où les seules lumières seraient celles des lignes de code apparaissant sur le fond noir d'un écran plat installé à l'arrière d'un garage ou dans les caves d'un immeuble.

Autant d'images récurrentes et pourtant loin de rendre compte de la réalité de la criminalité informatique[2].

1 - On a pu parler à leur égard de « formes de délinquances qui réinventent la piraterie » : E. Dreyer, Atteintes aux systèmes de traitement informatisés de données (Fraude informatique), *Lamy Droit pénal des affaires*, 2013, §727.

2 - Réalité qui est par ailleurs difficile à saisir comme le relevait le Groupe de travail interministériel sur la lutte contre la cybercriminalité dans un rapport de février 2014, p.15, en ces termes : « Jamais, un phénomène criminel n'a fait l'objet d'affirmations autant péremptoires quant à son importance et quant au préjudice qu'il induit, y compris de la part d'organisations internationales officielles. Pourtant, si l'ensemble des acteurs s'accordent sur cette importance et cette gravité, les sources d'information paraissent parcellaires et approximatives ».

Cette délinquance n'a bien souvent qu'un pur objet lucratif[3], les exemples de fraudes informatiques réalisées dans le but de dévoiler ce que, par exemple, les États cachent aux citoyens étant, malgré quelques affaires médiatiques, assez anecdotiques, et faisant l'objet d'une appréhension pénale sous des qualifications sans lien avec les fraudes informatiques[4].

La criminalité informatique n'impose pas non plus de connaissances techniques pointues. Il n'est ainsi pas nécessaire de savoir coder en langage machine pour réaliser l'infraction probablement la plus courante : l'arnaque dite « à la nigériane ». Arnaque qui consiste à adresser par centaine le même message à des inconnus leur réclamant de l'argent pour une cause louable et avec l'assurance d'un remboursement rapide voire même d'un bénéfice[5]. Aucune volonté de faire prévaloir la liberté ici, et pas de connaissance plus poussée de l'informatique que celle permettant d'envoyer un e-mail.

Pénalement, ce dernier comportement est très intéressant car, outre son qualificatif d'arnaque à la nigériane, il est parfois désigné comme « fraude 419 » ou « scam 419 »[6] de l'article du code pénal nigérian l'incriminant. Or la lecture de cet article ne fait pas apparaître un comportement spécifiquement lié à l'informatique ou aux réseaux : il s'agit simplement du texte incriminant en droit nigérian, et dans des termes d'ailleurs très proches du droit français, l'escroquerie[7].

---

3 - Le rapport 2013, dernier disponible en texte intégral, de l'Observatoire National de la Délinquance et des Réponses Pénales (ONRDP) est sans appel sur ce point. Les « escroqueries et infractions économiques et financières commises sur Internet » enregistrées pour l'année 2012 sont au nombre de 29.796 quand, sur la même période, les autres formes de délinquance informatique, atteintes aux systèmes, accès ou maintien frauduleux dans les systèmes ou encore la fourniture de moyen en vue de ces infractions, ne dépassent pas les 3000 occurrences enregistrées. V. p. 302 et 303 du rapport.

4 - Edward Snowden fait ainsi l'objet de poursuites sous les qualifications de divulgation non autorisée d'informations relatives à la défense nationale, de divulgation non autorisée de communications contenant des informations classifiées et de vol de biens appartenant au Gouvernement.

5 - Cette fraude a même les honneurs d'une page internet sur le site des ministères économiques et financiers : http://www.economie.gouv.fr/dgccrf/Fraude-nigeriane-843.

6 - L'expression est reprise, p. 161, dans le rapport 2013 de l'ONRDP sur la criminalité en France.

7 - L'incrimination est ainsi rédigée *: « Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years ».* On reconnaît ici les manœuvres frauduleuses, « *false pretence* », et la remise, « *obtains from any other person* », caractéristique de l'escroquerie.

C'est donc que la criminalité informatique ne serait non seulement pas spécifique en elle-même mais que juridiquement elle ne nécessiterait pas non plus de textes particuliers puisque pouvant être réprimée par des incriminations classiques[8]. Tout au plus l'outil informatique serait le moyen de commettre des infractions de droit commun, rendant inutile l'édiction de textes nouveaux et n'imposant que des règles de procédure particulière pour appréhender ce nouveau mode de commission des infractions[9].

La réalité du droit pénal informatique ou de la criminalité informatique n'est toutefois pas aussi simple en droit français contemporain et, selon une distinction très établie, il convient de la scinder selon que l'on vise, d'une part, les atteintes aux systèmes de traitement automatisé des données (STAD) eux-mêmes, d'autre part, les atteintes réalisées par le moyen de l'outil informatique[10].
Les premières font l'objet d'une division particulière du Livre III du code pénal consacré aux atteintes aux biens[11] tandis que les secondes font l'objet d'une appréhension à plusieurs titres. Il suffit ainsi bien souvent que les termes d'une incrimination ne mentionnent pas les moyens spécifiques mis en œuvre pour que, par hypothèse, l'outil informatique puisse y servir[12]. Dans d'autres cas, toutefois, le législateur est plus explicite et consacre l'usage de l'outil informatique comme une circonstance aggravante d'une infraction de droit commun[13]. Enfin, il lui arrive même de consacrer des passages entiers du code aux atteintes portées, par exemple,

8 - En ce sens : J. Devèze, La fraude informatique – Aspects juridiques, JCP 1987. I. 3289, §3 et 4.

9 - Notamment des règles de compétence comme l'assez tardif article 113-2-1 du code pénal, introduit par la loi n°2016-731 du 3 juin 2016, et selon lequel : « Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République ».

10 - Cette distinction formait le plan même d'un article de Raymond Gassin, Le droit pénal de l'informatique, D. 1986, chron. p. 35, qui distinguait « L'informatique, objet de délits » de « L'informatique, moyen de délits ». L'auteur ajoutait une autre distinction, « L'informatique, occasion de délits », qui, elle, n'a pas fait école.

11 – Art. 323-1 à 323-7 du code pénal.

12 - L'escroquerie de l'article 313-1 du code pénal en est l'exemple parfait.

13 - Ainsi de l'article 227-23 alinéa 3 du code pénal qui érige l'utilisation d'un « réseau de télécommunication » en circonstance aggravante de l'infraction de diffusion d'image à caractère pédopornographique.

aux données à caractère personnel par le moyen d'un système de traitement informatisé des données[14].
C'est au sein de ces diverses dispositions que doit s'évaluer l'influence du droit de l'Union Européenne.

Et s'interroger sur cette influence, sur le fait de savoir si le droit de l'Union européenne a façonné cette criminalité, se justifie d'autant plus que, depuis le traité de Lisbonne, l'Union européenne dispose au titre de l'article 83 du TFUE d'une compétence relative à la définition des infractions et à la détermination des sanctions pour les cas de criminalité particulièrement graves et transfrontalières. La criminalité informatique est donc tout naturellement visée au titre des domaines de compétence en matière pénale de l'Union européenne par le deuxième alinéa de l'article 83. Toutefois, le traité de Lisbonne est encore une œuvre assez récente et, il faut le dire, la plus grande partie de la législation française en matière de criminalité informatique est antérieure à son adoption.

L'influence du droit de l'Union européenne sera donc envisagée à l'aune de l'ensemble des instruments européens y compris lorsqu'ils auraient été adoptés bien avant que l'Union se dote expressément d'une compétence en matière pénale. Il faut également relever que l'article 83 renvoie expressément à la définition des infractions et des sanctions applicables. L'influence de la norme européenne doit donc être examinée à l'égard des deux constantes de la norme d'incrimination : la norme de comportement et la norme de pénalité. Il ne faut, par ailleurs, pas non plus occulter le fait que le développement du réseau internet et la multiplicité des intervenants, notamment des intervenants techniques, impliqués par exemple dans la transmission d'un simple mail ou dans la publication d'un commentaire sur un forum de discussion, emporte de délicates questions quant à la mise en œuvre éventuelle de la responsabilité pénale de chacun lorsqu'une infraction est commise au moyen du réseau et de l'outil informatique. Il se pourrait donc bien que la norme européenne ait une influence sur ces règles de responsabilité.

Nous envisagerons donc dans un premier temps l'influence du droit de l'Union européenne sur les incriminations informatiques (section I) et son influence sur les règles de responsabilité (section II).

14 – Art. 226-16 à 226-24 du code pénal.

Section I - L'influence relative du droit de l'Union européenne sur les incriminations en matière « informatique »

L'influence des normes européennes doit être relativisée eu égard à la forte concurrence des normes nationales et internationales en matière d'atteintes aux STAD (§ 1). En ce qui concerne les atteintes réalisées aux moyens des STAD, ce phénomène de concurrence des normes, tout aussi patent, se double même d'un effet perturbateur du fonctionnement des incriminations dû à l'instabilité de la norme européenne (§ 2).

§ 1 : La norme européenne concurrencée en matière d'atteintes aux STAD

En ce qui concerne les atteintes portées à l'outil informatique, il faut être assez clair : la France s'est dotée d'outils de répression de manière précoce puisque l'incrimination des atteintes portées aux systèmes de traitement automatisé des données remonte à une loi 88-19 du 5 janvier 1988, dite « Godfrain », et qui rassemblait au sein des articles 462-2 et suivants du code pénal un nombre déjà conséquent de comportements punissables. En effet, en à peine six articles le législateur venait incriminer pas moins de dix comportements allant de la simple introduction dans un STAD à la modification même minime des données qu'il était censé contenir[15]. La tentative de ces délits était également prévue de même que l'association de malfaiteurs en vue de leur commission[16]. Le périmètre de la répression était donc déjà impressionnant puisque ces atteintes aux STAD peuvent être considérées en elles même comme des infractions obstacles aux infractions qui pourraient être réalisées à travers l'exploitation frauduleuse du système piraté et que la tentative et l'association de malfaiteurs permettaient de rehausser le seuil d'intervention de la répression bien en amont de la réalisation effective de l'infraction. Ce périmètre était d'ailleurs d'autant plus large que le législateur avait fait preuve de concision dans la rédaction des textes et avait eu recours à des termes très généraux pour définir

15 - Comportements prévus, respectivement, par les articles 462-2 et 462-4 de l'ancien code pénal.

16 - Par les articles 462-7 et 8 de l'ancien code pénal.

les infractions en cause[17]. On voit donc assez mal quel espace le législateur français pouvait avoir laissé à l'Union européenne pour légiférer en la matière. On le voit d'ailleurs d'autant plus mal qu'en ce qui concerne les atteintes au fonctionnement des STAD l'Union européenne n'est encore intervenue que postérieurement à une convention du Conseil de l'Europe consacrée à la cybercriminalité de 2001[18] et entrée en vigueur en France en mai 2006.

De tous ces instruments, celui adopté par l'UE, une décision-cadre de 2005[19], est peut-être le moins complet puisque ne visant que l'accès illicite, l'atteinte à l'intégrité du système et celle portée aux données y compris la complicité et la tentative[20]. La France, pour sa part, réprime ces atteintes bien au-delà de la simple tentative au moyen de l'association de malfaiteurs tandis que la Convention du Conseil de l'Europe prévoyait la répression de l'usage ou de la détention d'outil ou de moyen, logiciel ou matériel, permettant de réaliser ces infractions[21]. Ce n'est d'ailleurs qu'assez récemment que l'Union européenne a adopté une nouvelle directive réformant la précédente et intégrant la répression de la fabrication de ces outils[22] . On voit donc ici la concurrence à laquelle est soumise la norme européenne qui évolue presque systématiquement à la suite d'autres normes, nationales et internationales, qui ont donc contribué à la façonner.

De ce point de vue, l'influence du droit européen sur les infractions réalisées au moyen des STAD a peut-être été plus précoce et décisive quoiqu'on puisse constater, ici encore, la concurrence d'autres normes nationales et internationales ainsi que certaines perturbations due à l'instabilité des normes européennes.

---

17 - Il n'est pas rare de trouver dans ces textes les expressions marquantes d'un champ accru de la répression telles que « en tout ou partie », art. 462-2, « directement ou indirectement », art. 462-4, ou encore « quelle que soit leur forme », art. 462-5. Sur la capacité d'adaptation des termes employés aux évolutions de la technologie et une approche critique : E. Dreyer, Atteintes aux systèmes de traitement informatisés de données (Fraude informatique), *Lamy Droit pénal des affaires*, 2013, §727.

18 - Convention, STE-185, sur la cybercriminalité du 23 novembre 2001.

19 - Décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information.

20 – Art. 2 à 5 de la décision-cadre 2005/222/JAI.

21 – Art. 6 de la convention de 2001 sur la cybercriminalité.

22 – Art. 7 de la directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

§ 2 : La norme européenne également perturbatrice en matière d'atteintes au moyen des STAD

Si l'on laisse de côté la question des seules atteintes aux systèmes de traitement des données pour s'intéresser dans un second temps aux atteintes réalisées au moyen des STAD, on peut évaluer l'influence de la législation de l'Union Européenne sur plusieurs incriminations françaises.

Cette influence peut s'apprécier, dans un premier temps, au regard des textes venant prévoir la répression de la pédopornographie et de sa diffusion par internet.
Sous l'empire de l'ancien code pénal la question de la pédopornographie était réprimée lorsqu'elle pouvait rentrer dans les incriminations assurant la répression des atteintes aux mœurs[23].
L'usage de ces textes, non spécifiques, pouvait toutefois s'avérer hasardeuse et le législateur a saisi l'occasion de l'entrée en vigueur du nouveau code pénal pour établir une incrimination spécifique à la pédopornographie réprimant « le fait de diffuser, par quelque moyen que ce soit » l'image d'un mineur lorsqu'elle présente un caractère pornographique[24].
En ce qui concerne l'Union européenne, c'est par une action commune, norme peu contraignante, du 24 février 1997 relative à la lutte contre l'exploitation sexuelle des enfants qu'elle vient prévoir l'incrimination de cette exploitation « aux fins de la production de spectacle ou de matériel à caractère pornographique »[25] et, notamment la répression de « la vente et de la distribution ou d'autres formes de trafic de matériel »[26] pédopornographiques, dont on imagine qu'elle pouvait donc être effectuée par tout moyen, y compris informatique. Le législateur français respectait donc déjà les dispositions européennes mais réagit toutefois à l'action commune par une loi n°98-468 du 17 juin 1998 en prévoyant une aggravation des sanctions lorsque la diffusion ou la représentation

23 - V. M.-L. Rassat, J. Cl. Pénal code, art. 227-23 et 227-24, Fasc. 20, §1 et s.

24 - Alinéa 2 de l'article 227-23 du code pénal en sa rédaction lors de son entrée en vigueur le 1cr mars 1994.

25 - Titre II, A, a), de l'action commune du 24 février 1997 adopté par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants.

26 - Titre I, A, ii), c) de l'action commune.

d'une image pédopornographique aura été réalisée au moyen d'un réseau de télécommunication et à destination d'un public non-déterminé[27]. Il semble donc bien, qu'ici encore, le législateur allait plus loin que ce que le droit de l'Union Européenne exigeait[28]. On ajoutera que la Convention, déjà citée, du Conseil de l'Europe sur la cybercriminalité comportait également des dispositions de même nature prévoyant la répression de la pédopornographie réalisée par système informatique[29]. Enfin, les développements récents de ces dispositions à l'échelle européenne confirment l'avance persistante de la législation nationale puisque la répression de la simple consultation de pédopornographie au moyen des technologies de l'information et de la communication, prévue par une directive du 13 décembre 2011[30], était incriminée en droit français depuis 2007. On remarquera d'ailleurs, concernant la norme de pénalité, que le législateur avait pris les devants en prévoyant pour ce comportement une peine de deux ans d'emprisonnement quand la directive n'imposait pour sa part qu'un an d'emprisonnement[31].

L'influence de la législation européenne est donc toute relative en matière de pédopornographie réalisée au moyen des STAD.

Nous allons voir qu'elle ne se fait pas plus sentir quant à la répression des atteintes aux données personnelles par l'usage de l'outil informatique et qu'elle se double même d'un effet perturbateur

27 - Est alors créé un alinéa 3 de l'article 227-23 ainsi rédigé : « Les peines sont portées à cinq ans d'emprisonnement et à 500 000 F d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications ». Cette loi était également l'occasion d'élargir encore un peu plus le champ de la répression en visant non plus seulement « l'image » du mineur mais également sa « représentation » sous quelque forme que ce soit. Les textes étaient de surcroît désormais applicables aux images ou représentation d'une « personne dont l'aspect physique est celui d'un mineur ».

28 - On pourrait même estimer qu'il a attiré l'attention de l'Union européenne sur l'utilisation des réseaux informatiques en la matière puisque la Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie est venu se substituer au texte de l'action commune en précisant dans son article 3 que ces divers comportements, y compris la diffusion et la détention, devaient être punis qu'ils aient impliqués ou non l'usage d'un système informatique.

29 - Art. 9 de la convention, STE-185, sur la cybercriminalité du 23 novembre 2001.

30 – Art. 5.1 de la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

31 - Article 5.1 de la directive 2011/92/UE.

lié à l'instabilité des normes à l'échelle européenne.
En la matière, la législation française est également ancienne. La réglementation du traitement des données par l'outil informatique, si elle n'a pas toujours figuré dans le code pénal faisait l'objet de dispositions pénales aux articles 41 et suivants de la loi n°78-17 du 6 janvier 1978 dite « Informatique et libertés ». Intégrées au code pénal au sein des articles 226-16 et suivants, ces dispositions fonctionnent dans une large mesure comme des incriminations par renvoi prévoyant la sanction d'une extrême variété de comportements. Certaines visent directement le non respect des règles posées par la loi de 1978 pour le traitement automatisé des données personnelles comme l'article 226-16 alinéa 2, tandis que d'autres sont autonomes telles que l'alinéa 1 du même article prévoyant la répression du fait « de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations »[32].
La législation française est donc déjà forte, au moins dans le code pénal, de sept textes incriminateurs répertoriant plusieurs comportements susceptibles de porter atteinte à l'intégrité des données personnelles au moyen de l'outil informatique au moment où l'Union européenne commence à s'intéresser au traitement des données personnelles, c'est-à-dire par une directive du 24 octobre 1995[33]. Directive qui intervient, encore une fois, alors qu'une convention internationale avait déjà été adoptée par le Conseil de l'Europe dès 1981[34] sur la question du traitement automatisé des données à caractère personnel. La comparaison entre la directive du 24 octobre 1995 et ce dernier texte est d'ailleurs édifiante. La définition des données à caractère personnel est identique et désigne « toute information concernant une personne physique identifiée ou identifiable »[35]. La définition du « maître du fichier » ou du « responsable du traitement », malgré le changement de dénomination, n'en est pas moins très proche

32 - Dont on peut se demander assez légitimement s'il est bien conforme au principe de la légalité criminelle tant les termes de l'incrimination sont vagues.

33 - Directive 95/46/CE du Parlement et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

34 - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE-108, du 28 janvier 1981 entrée en vigueur, en France, dès 1985.

35 - Art. 2.a de la convention et article 2 de la directive.

en ce qu'elle vise « celui qui détermine la finalité du traitement et ses modalités »[36]. On retrouve même dans la convention du Conseil de l'Europe des dispositions concernant le transfert de données à caractère personnel vers d'autres États qui peut être interdit dans des termes très proches de ceux employés par la directive de 1995 « si la réglementation du destinataire n'accorde pas une protection équivalente »[37]. Il s'agit ici du précurseur de la fameuse notion de « *safe harbor* » sur lequel la CJUE est revenue récemment.

L'impact de la transposition de la directive de 1995 par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel est donc forcément limité quant au périmètre de la répression[38] et se double *a posteriori* d'un effet perturbateur à l'égard de certaines incriminations bien particulières. En effet, cette transposition était l'occasion d'intégrer au code pénal un article 226-22-1 réprimant le fait « hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ». Ce texte pose l'incrimination de la transmission de données personnelles vers un État qui n'assurerait pas un degré équivalent de protection des données personnelles et marque par le double renvoi effectué. Renvoi, tout d'abord, aux mesures prises par la Commission européenne, dont on sait que relativement à l'échange de données avec les États Unis d'Amérique, elles ont précisément fait l'objet d'une annulation par la CJUE estimant que les conditions du transfert cet État ne permettaient pas de garantir un niveau de

36 - Art. 2.d de la convention et article 2.d de la directive.

37 - Art. 12.3.a de la convention.

38 - On a d'ailleurs pu dire que les dispositions de la directive de 1995 « confortent, pour l'essentiel, les principales règles de la loi de 1978 et la doctrine de la CNIL » : J. Frayssinet, J. Cl. Pénal code, art. 226-16 à 226-24, fasc. 20, §19. V. pour un aperçu exhaustif et critique de la dimension pénale de la LCEN : A. Lepage, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, Dt. Pénal 2005, étude n°5.

protection équivalent[39]. Renvoi, ensuite, aux mesures que la CNIL pourrait prendre au titre de l'article 70 de la loi de 1978 pour refuser un transfert dans l'attente d'une décision de la commission européenne. Le droit de l'Union européenne, s'il a été décisif dans l'édification de cette incrimination, a également, par son instabilité, contribué à sa paralysie. Quelle attitude adopter, en effet, à l'égard de tous les transferts de données effectués en application de l'accord « *Safe Harbor* » avant qu'il ne soit annulé ? Des auteurs ont pu estimer que, l'accord disparaissant rétroactivement, ces transferts avaient perdu toute assise légale et tombaient sous le coup de sanction pénale[40]. Le G29, pour sa part, préférait inviter les États européens à une certaine indulgence en n'envisageant de sanction que pour les éventuels transferts de données postérieurs à la décision de la Cour[41]. Pour notre part, nous nous demanderons comment des transferts de données antérieurs auraient pu être effectués en violation des mesures prises par la Commission, comportement réprimé par le texte incriminateur, quand ces mêmes mesures, du fait de leur annulation, sont réputées n'avoir jamais existé.
On le voit donc, il est difficile de trouver des domaines où le droit européen aurait réellement façonné les incriminations françaises en matière de criminalité informatique. Cette situation n'a toutefois rien de choquant. La législation européenne n'est pas exclusivement destinée à la France et d'autres États membres ont pu bénéficier de ces textes. Peut-être plus intéressante peut paraître l'influence du droit de l'Union sur les règles de responsabilité applicables aux différents intervenants sur le réseau informatique.

Section II - L'influence plus décisive du droit de l'Union européenne sur les règles de responsabilité en matière informatique

Le constat s'impose ici de l'influence décisive du droit européen sur les règles de responsabilité pénale en matière informatique. Le législateur s'est ainsi contenté dans une large

39 - CJUE, 6 octobre 2015, Schrems c/ Data protection commissioner, C-362/14.

40 - C. Théard-Jallu, J.-M. Job et S. Mintz, Invalidation de l'accord *safe harbor* par la CJUE : portée, impacts et premiers éléments de solution, Dalloz IP/IT, n°1, janviers 2016, p. 26, spéc. p. 28 et s.

41 - Communiqué du G29 du 16 octobre 2015 relatif au jugement Schrems.

mesure de transposer les règles européennes de responsabilité en matière informatique (§ 1) sans, semble-t-il, se préoccuper de l'articulation des textes ainsi intégrés à notre droit avec les règles de responsabilité classique (§ 2).

§ 1 : La transposition « telle-quelle » des règles européennes de responsabilité informatique

Les règles relatives à la responsabilité pénale sont essentiellement contenues dans la partie générale du code pénal et permettent de définir les conditions de répression des différents participants à l'infraction qu'il s'agisse de l'auteur, personne physique ou morale, ou du complice. Ces règles s'accompagnent de règles de responsabilité plus générales telle que l'article 121-1 prévoyant que « nul n'est responsable que de son propre fait » ou de règle plus spécifiques telles que celles applicables aux mineurs en vertu de l'article 122-8. Cela n'empêche pas le législateur de prévoir parfois des régimes spéciaux et dérogatoires comme avec le mécanisme de responsabilité en cascade prévu par l'article 42 de la loi sur la liberté de la Presse et la jurisprudence d'en établir parfois de plus spécifiques comme pour le chef d'entreprise[42]. Ces régimes visent les individus dont on estime qu'ils méritent de subir la répression à raison du lien particulier qu'ils entretiennent avec l'auteur matériel ou avec la commission de l'infraction : le complice parce qu'il aide ou provoque ; la personne morale parce qu'elle a été l'instrument ou parce qu'elle a tiré, d'une manière ou d'une autre profit, de l'infraction ; le directeur de la publication parce qu'il a ouvert ses colonnes à un propos pénalement répréhensible ; le chef d'entreprise parce qu'il a un devoir de surveillance. Il y a en fait toujours une bonne raison d'appréhender les individus qui gravitent autour de la commission d'une infraction afin de leur faire également

42 - Il est ainsi acquis depuis longtemps que « Si, en principe, nul n'est passible de peines qu'à raison de son fait personnel, la responsabilité pénale peut cependant naître du fait d'autrui dans les cas exceptionnels ou certaines obligations légales imposent le devoir d'exercer une action directe sur les faits d'un auxiliaire ou d'un préposé ; il en est ainsi notamment, dans les industries ou commerces réglementés, ou la responsabilité remonte aux chefs d'entreprises, à qui sont personnellement imposés les conditions et le mode d'exploitation de leur industrie ou commerce » : cass. crim. 30 décembre 1892, S. 1894. 1. 201.

subir la sanction pénale[43]. Cette étude est l'occasion de constater que la criminalité informatique multiplie ces individus sans lesquels l'infraction ne peut être commise[44]. Leurs dénominations sont désormais connues en droit français, il s'agit du fournisseur d'accès, du fournisseur d'hébergement ou encore de l'opérateur.

Pour autant la définition des régimes de responsabilité propre aux intermédiaires informatiques ne peut pas réellement être mise au compte du législateur français qui a tergiversé à leur sujet vers la fin des années 1990[45]. C'est à la directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur que l'on doit l'existence de ces régimes de responsabilité. La directive vient ainsi définir plusieurs catégories de prestataires de service de la société de l'information dit « intermédiaires ». Ceux dont le rôle consiste à transmettre sur le réseau de communication les informations fournies par le destinataire du service ou à lui fournir l'accès au réseau, on y reconnaîtra les fournisseurs d'accès[46]. Ceux dont le rôle consiste à stocker les informations fournies par le destinataire du service, on y reconnaîtra les hébergeurs[47]. Enfin, une catégorie d'individus qui fournissent un service qualifié de « *caching* » permettant de stocker des portions d'informations sur des serveurs relais afin d'accélérer la consultation de données qui seraient contenues sur un serveur éloigné[48]. La directive est globalement assez claire sur les obligations pesant sur ces intermédiaires : les États ne peuvent pas leur imposer une obligation générale de surveillance des informations qu'ils transmettent ou stockent, pas plus qu'ils ne peuvent leur imposer de rechercher activement des faits ou des circonstances révélant

43 - V. sur ces questions de criminalité dépendante et d'appréhension des participants à l'infraction notre thèse : Étude de la catégorie des infractions de conséquence, 2016, t. 63, LGDJ, Bibl. sc. crim.

44 - V. sur la question de leur responsabilité : F. Terré, Être ou ne pas être ... responsable. - A propos des prestataires de service par internet, JCP G 2011, doctr. 1175.

45 - Seule la responsabilité du fournisseur d'accès avait fait l'objet d'un traitement spécifique par la loi n°2000-719 du 1er août 2000 mais rapidement modifiée par la transposition de la directive 200/31/CE.

46 - Article 12 de la directive.

47 - Article 14 de la directive.

48 - Article 13 de la directive.

des activités illicites[49]. Sans viser directement la responsabilité pénale, mais en induisant donc qu'elle soit comprise, la directive prévoit même expressément que les États veillent à ce que ces intermédiaires ne soient pas responsables pour le stockage ou la transmission des données qu'ils manipulent[50]. C'est donc un principe d'irresponsabilité qui est posé et qui ne peut être renversé que dans certaines hypothèses bien délimitées et propres à chaque type de prestataire. Le fournisseur d'accès ne doit pas modifier l'information transmise, en sélectionner des portions, en choisir le destinataire ou être l'émetteur lui-même, tous comportements qui lui ôteraient sa neutralité dans le traitement de l'information[51]. L'hébergeur ne doit pas avoir connaissance du contenu des informations hébergées et, si c'est le cas, déférer promptement aux injonctions de suppression qui pourraient lui être adressées pour leur suppression[52]. Enfin, l'intermédiaire « cacheur », peut voir sa responsabilité mise en cause dans cinq hypothèses assez techniques d'intervention qu'il pourrait effectuer sur les informations mais surtout dans l'hypothèse où il modifie l'information stockée[53].

Cette directive a été transposée dans le droit français par la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui a largement repris les modèles européens alors que le droit français était presque totalement silencieux sur ces questions jusque-là. En ce qui concerne les fournisseurs d'accès et les intermédiaires procédant au stockage de type « *caching* » : la transposition opérée est un pur « copier-coller » des dispositions de la directive. Le même principe d'irresponsabilité, sauf exceptions, est repris et intégré dans les dispositions les articles L.32-3-3 et L.32-3-4 code des Postes et des communications électroniques. Pour ce qui est des hébergeurs, là encore la transposition se fait à la lettre quoique directement dans le texte de la loi relative à la confiance dans l'économie numérique en son article 6. Article qui reprend d'ailleurs, en son I. 7°, la dispense d'obligation générale de surveillance du

49 - Article 15.1 de la directive. En revanche des obligations ponctuelles sont envisageables et la France a mis en œuvre cette possibilité notamment en matière d'apologie de crime contre l'humanité et de pornographie enfantine. V. art. 6, I, 7° de la LCEN.

50 - Cette formulation est reprise en tête des articles 12, 13 et 14 de la directive.

51 - Art. 12.1, a, b et c de la directive.

52 - Art. 14.1, a et b de la directive.

53 - Art. 13.1, a, b, c, d et e de la directive.

contenu transmis ou stocké. C'est donc bien le droit de l'Union Européenne qui a façonné ici, plus que la criminalité informatique, la responsabilité pour criminalité informatique mais il faut encore relever que c'est la France qui a fait le choix de la pénalisation puisque la directive n'a jamais imposé un régime de sanction pénale pour ces intervenants[54]. À être tatillon, on pourrait relever que le législateur français n'a pas été totalement passif face aux développements des nouvelles technologies. On pourrait ainsi rappeler l'existence même fugace d'un article 43-8 de la loi du 30 septembre 1986 relative à la liberté de communication qui, créé par la loi n°2000-719 du 1er août 2000 et abrogé par la LCEN, venait poser la responsabilité pénale du fournisseur d'accès « qui n'aurait pas déféré promptement à une demande de retrait de contenu illicite »[55]. Plus pertinent paraît-il de rappeler qu'il existe d'autres systèmes de responsabilité propres aux infractions commises par internet et notamment en ce qui concerne les infractions de presse commises par les réseaux informatiques. On retrouve ainsi à l'article 93-3 de la loi sur la communication audiovisuelle un mécanisme inspiré de la responsabilité en cascade de l'article 42 de la loi sur la liberté de la presse de 1881 mais pourvu de quelques subtilités. Les qualités d'individus visés ne sont ainsi pas les mêmes. Le système nous intéresse plus particulièrement puisqu'il établit que la responsabilité du directeur de la publication ne pourra être mise en cause si le message diffusé n'a pas fait l'objet d'une fixation préalable ou, lorsque étant publié dans un espace dédié aux contributions personnelles, il est démontré qu'il n'en avait pas effectivement connaissance ou qu'il n'a pas pris les mesures de suppression après signalement. On voit ici resurgir un schéma de responsabilité envisagé par la directive : celui de l'hébergeur qui peut être sanctionné s'il avait connaissance de la nature illicite des données manipulées ou s'il n'a pas déféré à une injonction de retrait. On peut donc trouver, si l'on cherche bien, des mécanismes assez proches de ceux employés par la directive de 2000 mais cette recherche n'aboutirait pas beaucoup plus loin qu'une simple dispute sur la paternité de telle ou telle approche de la responsabilité

54 - Elle se contente d'appeler, en son article 20 et selon une expression consacrée, à des sanctions « effectives, proportionnées et dissuasives ».

55 - L'article a toutefois, malgré sa disparition rapide, suscité de la jurisprudence : V. L. Grynbaum, Immunité confirmée des hébergeurs et immunité menacée des préposés, commentaire sous TGI Marseille, 11 juin 2003, Revue Communication Commerce électronique 2003, comm. 85.

des intervenants sur internet.
Le problème ne nous parait toutefois pas être là : mais plutôt dans l'articulation de ces régimes de responsabilité avec les règles de responsabilité classique existant en droit français.

§ 2 : L'articulation hasardeuse des règles transposées et des régimes de responsabilité classiques

En effet, à reprendre les dispositions transposées, on se rend compte que le législateur a simplement prévu des situations dans lesquelles la responsabilité pénale de ces intervenants peut être recherchée. Reste donc en suspens, la question du fondement de cette responsabilité, sur laquelle le législateur ne s'est pas prononcé. À ce titre, il ne faut pas oublier que ces activités, d'hébergement, de « *caching* » ou encore de fourniture d'accès, sont essentiellement assurées par des personnes morales. Dès lors, et conformément à l'article 121-2 du code pénal, leur responsabilité ne pourra être engagée qu'à condition d'établir qu'un de leurs organes ou représentant a commis une infraction en relation avec les données manipulées et pour leur compte. L'articulation de ces règles transposées avec le régime plus classique de responsabilité des personnes morales s'avère alors délicate.
S'agit-il de vérifier, dans un premier temps, que la personne morale peut être responsable parce qu'elle aurait manipulé les données en question ou aurait connu leur caractère illicite et, dans un second temps, qu'un de ses organes ou représentant a commis une infraction précise pour son compte ? S'agit-il au contraire, de vérifier dans, un premier temps, que la personne morale est potentiellement responsable au sens de l'article 121-2 avant d'établir, dans un second temps, qu'elle ne remplit pas les conditions issues de la directive pour être pénalement responsable ? L'ordre dans lequel ces questions doivent être posées pourrait toutefois être de peu d'importance puisqu'on y reconnaît un mécanisme de responsabilité pénale, les règles de l'article 121-2 du code pénal, et un mécanisme d'irresponsabilité pénale, la règle transposée. Dès lors, si les conditions de l'irresponsabilité s'avèrent remplies il n'est, en tout état de cause, pas utile de s'interroger sur l'éventuelle responsabilité de la personne morale.
Cet ordre est d'ailleurs d'autant moins intéressant que ces questions reviennent en fait au même. En effet, s'interroger sur le fait de

savoir si une personne morale a, ou non, eu connaissance des données qu'elle manipulait ou qu'elle modifiait, reviendra toujours à s'interroger sur le fait de savoir si, en son sein, des individus disposant de responsabilités, ont eu cette connaissance ou ont opéré cette modification. Ce qui reviendra, de fait, à se demander si les organes ou représentants de cette personne morale ont commis une infraction puisque la modification d'informations ou le transfert en connaissance de cause de matériaux illicites peuvent être appréhendés pénalement à bien plus d'un titre[56]. Ce qui revient à établir, ou pas, au sens de l'article 121-2 du code pénal, la responsabilité pénale de la personne morale. Ces deux questions, celle posée par l'article 121-2 et celle posée par les dispositions transposées, sont donc dans une large mesure redondantes ce qui n'est pas sans amener d'interrogations sur l'utilité de ces dernières dispositions qui, plus que d'éclairer la matière, viennent brouiller les pistes[57].

Allant plus loin, on pourrait finalement s'interroger sur l'utilité même de ces dispositions transposées au cas d'infractions commises par une personne physique assurant des fonctions d'hébergeur ou de fournisseur d'accès. Exiger d'une telle personne qu'elle ait eu une connaissance du contenu manipulé ou modifié ne revient à rien d'autre qu'à établir, dans le premier cas, l'élément intentionnel de son comportement, dans le second, l'élément matériel de certaines infractions informatiques.

Là encore on ne peut que constater la redondance du droit européen avec des règles déjà bien établies en droit interne ...

56 - V. l'ensemble des incriminations examinées en première partie.

57 - On remarquera, au surplus, qu'en matière de responsabilité des personnes morales les dispositions transposées contiennent d'autres redondances. Ainsi de ces 1° et 2° du VI de l'article 6 de la LCEN qui persistent à prévoir expressément, en dépit de la disparition du principe de spécialité, la possibilité de déclarer pénalement responsable les personnes morales, « dans les conditions prévues à l'article 121-2 du code pénal », pour les incriminations qu'ils établissent.