PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

BANQUE DES MÉMOIRES

Master de Droit pénal et Procédure pénale
Dirigé par Philippe Conte et Didier Rebut
2023

La responsabilité pénale des intermédiaires d'Internet en cas de commission d'une cyber infraction par leurs utilisateurs

Tamaya LIMOUSIN OLIVEIRA

Sous la direction de Philippe Conte

La faculté n'entend donner aucune approbation, ni improbation aux opinions émises dans ce mémoire, ces opinions doivent être considérées comme propres à leur auteur.

La responsabilité pénale des intermédiaires d'Internet en cas de commission d'une cyber infraction par leurs utilisateurs

SOMMAIRE

REMERCIEMENTS

Je tiens à adresser mes remerciements les plus vifs à M. Brendan Rius, cofondateur de *MEE6 The Discord Bot*, sans lequel la réalisation de ce mémoire n'aurait tout bonnement pas été possible. En effet, à la complexité juridique du sujet s'est ajoutée une redoutable complexité technique ; me tourner vers M. Rius a en ce sens été salvateur. En classe de CM2, du haut de ses dix ans, M. Rius avait déjà écrit son premier code informatique. Il co-dirige aujourd'hui à vingt-six ans la plus grande société de gestion de serveurs Discord dans le monde. J'ai pour ma part commencé les recherches sans vraiment savoir ce qu'était une connexion Internet. Recueillir ses explications techniques, son ressenti, ses critiques, sa vision globale et relever le défi de ce mémoire m'ont permis de saisir tout le sens brut de la recherche : partir d'un chaos pour comprendre et créer.

Je le remercie donc infiniment de m'avoir insufflé une part infime de son savoir et d'avoir contribué à celle-ci.

Je remercie également ma grande sœur pour sa relecture aussi attentive que bienveillante.

À bien des égards, la tâche du critique est aisée. Nous ne risquons pas grand-chose, et pourtant, nous jouissons d'une position de supériorité par rapport à ceux qui se soumettent avec leur travail, à notre jugement. Nous nous épanouissons dans la critique négative plaisante à écrire et à lire. Mais l'amère vérité, qu'il nous faut bien regarder en face, c'est que dans le grand ordre des choses, le mets le plus médiocre a sans doute plus de valeur que la critique qui le dénonce comme tel.

— *Ratatouille*, Walt Disney (2007)

INTRODUCTION

1. Le droit et Internet. – « En 1995, le terme " numérique " n'avait pas encore le succès qu'on lui connaît de nos jours. On mentionnait plutôt le multimédia ou encore les nouvelles technologies qui, fin 2021, ne sont bien évidemment plus vraiment nouvelles. Le terme " électronique " était en vogue : le commerce électronique, la signature électronique, le courrier électronique... Même gloire pour le mot " information ", si usité pour désigner la société de l'information ou même les autoroutes de l'information. (...) Alors que, au son mystérieux du modem, les pages des sites de l'Internet se téléchargeaient lentement (et même très lentement) et que les adresses électroniques étaient composées d'une succession de chiffres, des juristes pionniers commençaient à s'intéresser à ces grands espaces de l'Internet qui n'étaient pas sans évoquer ceux d'un gigantesque Far West virtuel et mondial. C'était l'époque de l'Internet considéré comme étant une zone de non-droit et du fameux " vide juridique " des réseaux, propice à toutes les utopies. On soutenait qu'un site Internet était un " domicile virtuel " inviolable. (...) On se souvient ainsi de ces quelques étudiants malchanceux, premiers à avoir été condamnés en France pour contrefaçon en 1996. En effet, ils avaient innocemment reproduit sur le site Internet de leur école les paroles de chanson de Brel...(...) Vingt ans, vingt-cinq ans, c'est grosso modo une génération. Mais c'est aussi toute l'histoire du droit de l'Internet ! ». En signant *Fin de Siècle*,[1] l'auteur Christophe Caron rend compte avec exactitude de l'évolution fulgurante, presque monstrueuse, qu'eût Internet en seulement vingt-cinq ans, amorçant avec elle un tournant drastique pour nos sociétés. La collision d'Internet avec la matière juridique était alors à craindre, car si de nombreuses idées préconçues sur le droit sont souvent fausses, il y en est une qui porte une part de vérité : le droit n'est pas la science qui avance avec le plus de célérité. L'appréhension d'Internet par une matière qui mit plus de cent ans à dégager une théorie de la responsabilité délictuelle de l'article 1382 du Code civil ne semblait à ce titre pas si évidente. Qu'importe, l'ascension d'Internet s'accompagna d'un lot particulièrement dense de problèmes, et les juristes y furent confrontés. Au premier rang de ceux-ci, la criminalité d'Internet, ou cyber criminalité, explosa à l'aube des années 2000. Le droit pénal dut alors appréhender une criminalité dont la première des caractéristiques est

[1] C. Caron, Fin de siècle, Com. comm., électr n° 12, décembre 2021, n° 11.

qu'elle ne se laisse pas appréhender. Tenter de sanctionner les utilisateurs d'Internet à l'origine de celle-ci fut la première des réponses, ainsi que l'illustre la condamnation des faussaires de Jacques Brel. Partiellement satisfait, le droit pénal s'est ensuite intéressé aux acteurs d'Internet, les "intermédiaires", ceux qui en établissent la forme et parfois le fond. Pourquoi et dans quelle mesure ces derniers sont-ils saisis relativement à une criminalité qui transite par leurs services et infrastructures, mais dont ils ne constituent pas les auteurs directs ? C'est ce qui nous arrête ici. Avant de tenter de répondre à ces épineuses questions, il faut s'attacher à définir rigoureusement ce qu'est Internet, ce que sont ses intermédiaires et ses utilisateurs, et ce qu'est la responsabilité pénale, car nous nous apprêtons à analyser celle des intermédiaires d'Internet, les tarentules qui tissent la toile du *Web*.

2. Système et réseau d'Internet. – Le cadre de notre étude ne connaît ni frontières ni limites. Technique, complexe, aterritorial, fuyant, souvent anonyme, comment définir Internet ? Le terme « Internet » est une contraction de l'expression anglaise « interconnected networks », qui signifie « réseaux interconnectés ». L'expression fait référence à la structure même d'Internet, qui est un réseau de réseaux, c'est-à-dire un ensemble de réseaux informatiques interconnectés à travers le monde. Le terme a été utilisé pour la première fois en 1974 dans l'article de recherche « A Protocol for Packet Network Intercommunication »[2], écrit par Vint Cerf et Bob Kahn, les développeurs des premiers protocoles de communication qui ont permis la mise en place du système Internet tel que nous le connaissons. Aujourd'hui, on définit Internet comme un réseau global de communication qui connecte simultanément des utilisateurs en leur permettant d'accéder à une multitude de ressources, de contenus et de services en ligne. L'infrastructure d'Internet constitue indiscutablement le vecteur le plus important de la communication contemporaine, offrant aux individus, aux entreprises et aux gouvernements une gamme étendue de possibilités pour échanger des informations, collaborer, acheter et vendre des produits et des services, ainsi que pour se divertir. En bref, il est le réseau et le système sur lequel se loge l'intégralité du contenu dit contenu Internet. Une partie du contenu Internet se trouve sur « l'Internet de surface », *clean web* en anglais, la partie d'Internet accessible au grand public via les moteurs de recherche traditionnels. En revanche, certains contenus Internet se trouvent sur « l'Internet sombre », *Dark web* en anglais, la partie d'Internet qui n'est pas accessible par les moteurs de recherche traditionnels et nécessite l'utilisation de logiciels spécifiques ayant la particularité d'anonymiser l'utilisateur (V. 6). Ces mêmes logiciels peuvent être sollicités pour se connecter anonymement à des sites bien présents sur l'Internet de surface mais qui sont censurés dans l'État de l'utilisateur. Bien que certains États réfléchissent à criminaliser le fait de fournir une

[2] V.-G. Cerf, R.-E. Kahn, A Protocol for Packet Network Intercommunication, IEEE Transactions on Communications, 1974.

infrastructure technique aux opérateurs de plateformes existantes sur le *Dark Web,* comme les Länder Allemands, les deux utilisations d'Internet sont généralement libres et licites dans la grande majorité des États : seuls les agissements des utilisateurs et des intermédiaires d'Internet qui en résultent peuvent être générateurs de cybercriminalité. Qu'entend-t-on alors par les notions d'intermédiaire d'Internet et d'utilisateur ?

3. L'intermédiaire d'Internet et l'utilisateur. – Lorsque l'on parle d'intermédiaire d'Internet, il est en premier lieu fondamental de savoir de qui ou de quoi il est intermédiaire et donc à quoi il s'oppose : « l'utilisateur ». Plusieurs interprétations de celui-ci peuvent être admises : l'utilisateur peut renvoyer à l'utilisateur direct des services proposés par l'intermédiaire d'Internet, mais il peut également renvoyer à la notion d'utilisateur final, le destinataire de l'ensemble des services et contenus proposés par les prestataires de la société de l'information numérique, autrement dit l'internaute (également appelé utilisateur d'Internet). L'Union Européenne définit l'utilisateur final comme recouvrant « tous les types d'utilisation des services de la société de l'information, tant par les personnes qui fournissent l'information sur les réseaux ouverts tels que l'Internet que par celles qui recherchent des informations sur l'Internet pour des raisons privées ou professionnelles »[3]. Si les définitions semblent équivalentes il n'en est pourtant rien : l'utilisateur direct d'un intermédiaire d'Internet peut consister en un autre intermédiaire d'Internet, mais l'utilisateur final ne peut jamais être un intermédiaire dans la mesure où il se définit bien en creux de l'intermédiaire. Par exemple, les hébergeurs, des intermédiaires d'Internet, stockent le contenu de plateformes d'échanges multimédia, d'autres intermédiaires d'Internet qui ont pour utilisateurs des internautes ; ces derniers sont alors les destinataires finals de l'hébergeur tandis que la plateforme est son utilisateur direct. L'utilisateur final, l'internaute, n'est donc pas le seul destinataire des services des intermédiaires d'Internet et il n'est pas non plus le destinataire des seuls services et contenus proposés par les intermédiaires d'Internet puisqu'il est également le destinataire des services et du contenu proposé par les autres utilisateurs d'Internet, ceux-ci pouvant être des fournisseurs de contenu au sein de la société d'information. Toutefois, parfois par manque de rigueur ou pragmatisme, il est souvent entendu que la responsabilité de l'intermédiaire en cas de commission d'une cyber infraction par « l'utilisateur » englobe à la fois comme objet de responsabilité le concours apporté aux agissements de l'utilisateur final et le concours apporté à l'utilisateur direct des services de l'intermédiaire : dès lors, lorsque l'on examine la responsabilité de l'hébergeur ou d'un fournisseur d'accès à Internet au titre d'une cyber infraction commise par l'utilisateur, il

[3] Directive 2000/31/CE du 8 juin 2000 , dite « commerce électronique » PE et Cons. CE, dir. 2000/31/CE, 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, (20).

n'est pas impossible que l'utilisateur en question soit lui-même un intermédiaire qui sera considéré en l'espèce comme un utilisateur. Ainsi, malgré la distinction fondamentale de nature qui existe entre l'utilisateur direct de l'intermédiaire d'Internet et son utilisateur final, celle-ci est souvent gommée lorsque sont étudiés le statut et la responsabilité de l'intermédiaire, dont certains des services proposés ont pour destinataire tant des intermédiaires que des utilisateurs finals. Ainsi, afin de saisir correctement le droit positif des intermédiaires d'Internet, il est nécessaire de se conformer au raisonnement dominant dans la loi, la jurisprudence et la doctrine, autrement dit celui qui examine conjointement et sans distinction comme objet de leur responsabilité les utilisateurs finals d'Internet et les utilisateurs directs de leurs services. En pratique, un tel raisonnement n'est fort heureusement pas dénué de sens en ce qu'il permet d'être au plus proche de la réalité des intermédiaires. En effet, bien souvent, l'utilisateur direct des services de l'intermédiaire est également un utilisateur final, un internaute. En outre, les services fournis par les intermédiaires ne diffèrent pas selon que leur utilisateur direct soit un autre intermédiaire ou un utilisateur final, exception faite de leur rémunération. Il semblerait alors incohérent de distinguer là où il n'y a pas nécessairement lieu de distinguer. On l'aura donc compris, la définition de l'utilisateur possède une interprétation malléable, mais dès lors que c'est l'intermédiaire que l'on étudie, l'utilisateur doit être défini par rapport à la destination directe de ses services, qu'elle vise indifféremment un utilisateur final ou un autre intermédiaire. La notion d'intermédiaire d'Internet recouvre ainsi tout acteur qui permettrait à cet utilisateur d'accéder à Internet et son contenu ou de créer son propre contenu sur Internet. Dès l'an 2000, le Parlement Européen définit l'activité d'intermédiaire d'Internet comme étant « tout processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission ». Plus récemment, le Conseil de l'Europe a également proposé une définition de l'intermédiaire dans sa recommandation de 2018 sur le rôle et la responsabilité des intermédiaires d'Internet : « Une grande diversité d'acteurs, communément appelés " intermédiaires d'Internet " dont le nombre ne cesse de s'étendre, facilitent les interactions sur l'Internet entre les personnes physiques et entre les personnes physiques et morales en exerçant des fonctions diverses et en proposant des services variés »[4]. La recommandation mentionne certaines des ces fonctions et services comme la connexion à Internet, le traitement et le contrôle de données, leur stockage, l'agrégation et la recherche de données, l'accès direct aux contenus et services conçus où gérés par

[4] Recommandation CM/Rec(2018)2 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'Internet, §4.

des tiers, la vente et les transactions de toute nature[5]... Toutes ces fonctions convergent en ce qu'elles aident, directement ou indirectement, et de manières diverses, la mise en relation de l'utilisateur avec l'objet de sa visite sur Internet, qui n'est autre la création et/ou la consultation de contenu, éventuellement suivie d'interactions elles-même créatrices de contenu. Par exemple, si un internaute désire télécharger un contenu multimédia, les intermédiaires qu'il va nécessairement solliciter sont l'intermédiaire de connexion à Internet, le moteur de recherche, la plateforme autorisant le téléchargement et l'hébergeur de cette plateforme. Ainsi, lorsque l'utilisateur commet une infraction en relation avec Internet, une cyber infraction, l'intermédiaire qui jusque-là n'était qu'un intermédiaire d'Internet devient alors, *de facto*, un intermédiaire de cybercriminalité car il est bien celui qui, dans une certaine mesure, a rendu possible la commission de l'infraction, qu'il l'ait voulu ou non et qu'il le sache ou non. C'est cette relation entre l'infraction commise par l'utilisateur et l'intermédiaire d'Internet que l'on cherche donc à étudier ici sous le prisme de la responsabilité pénale. Toutefois, avant de s'y intéresser, il est nous est indispensable d'appréhender la notion d'intermédiaire d'Internet à travers une analyse purement technique dans l'objectif de comprendre quelles personnes et services la composent.

4. Catalogue des intermédiaires d'Internet. – Établissons alors un panorama peu ou prou complet des intermédiaires qui se dressent entre l'internaute et son clic. On évitera toutefois de pousser l'analyse technique à l'excès de sa complexité, au risque d'être contre-productif. Étudions alors successivement les intermédiaires qui permettent à l'utilisateur de se connecter et d'accéder au contenu d'Internet, les intermédiaires qui gèrent les structures offrant du contenu et/ou offrant la possibilité d'en créer et les intermédiaires qui hébergent ces structures et permettent ainsi leur existence sur le réseau Internet.

5. Fournisseur d'accès à Internet. –En premier lieu, la connexion à l'Internet est rendue possible par l'existence d'un réseau de câbles, parfois de satellites ou d'antennes cellulaires, présents sur toute la superficie du globe, des fonds océaniques jusqu'au domicile des utilisateurs d'Internet. L'entièreté du contenu existant sur Internet, quelle que soit sa forme et son fond, transite par cette infrastructure. Elle appartient à un fournisseur d'accès à Internet (FAI)[6], ou à un opérateur de communication électronique (OCE)[7] qui propose des services plus larges, comme la téléphonie mobile, et qui loue son infrastructure au fournisseur d'accès à Internet. Troisième possibilité, la plus commune, le FAI est aussi un OCE, c'est l'exemple de Free ou Orange. Le

[5] Ibid. §5.
[6] Art. L32 23° du Code des postes et communication électroniques.
[7] Art. L32 15° du Code des postes et communication électroniques.

fournisseur d'accès à Internet est donc l'entité qui fournit le service de la connexion à Internet : l'utilisateur, par un simple clic, envoie une demande de connexion à son fournisseur tandis que ce dernier achemine vers l'utilisateur le contenu objet de sa demande de connexion, de façon quasi-simultanée. Afin de protéger la sécurité des internautes et la confidentialité des données, un chiffrage mathématique, le Transport Layer Security (TLS) ou le Secure Sockets Layer (SSL), agit tel un cadenas inviolable et empêche le fournisseur de prendre connaissance du contenu qu'il fait simplement transiter vers l'internaute conformément à sa demande. Ce cadenas ne protège toutefois pas l'intégralité des données : lorsqu'il n'en est pas empêché par des technologies anonymisantes (V. 6), le FAI a accès à l'adresse Internet Protocol (IP) de l'utilisateur, le numéro d'identification qu'il a attribué à l'appareil connecté de l'utilisateur, et du site, ainsi que son nom. Pour métaphoriser, le fournisseur d'accès à Internet opère comme un facteur et la demande de connexion comme une lettre tamponnée : le facteur a connaissance de l'adresse de l'expéditeur et du destinataire, les adresses IP, et éventuellement de leur noms mais pas du contenu de la lettre. Cette connaissance n'est pas anodine dans la mesure où les fournisseurs d'accès à Internet peuvent soit filtrer toutes les demandes de connexion provenant d'une adresse IP en particulier, soit filtrer toutes les demandes de connexion dont l'objet est la consultation de certains sites en particulier, et, le cas échéant, les bloquer. La Corée du Nord ou plus récemment la Chine ne s'en sont par exemple pas privées : depuis 2011, par le biais d'un filtrage mis en place par les FAI chinois nommé « Grande Muraille numérique » ou « Great Firewall », Facebook ou Twitter ont été censurés dans le pays[8].

6. Connexion anonyme. – Courantes dans les États autoritaires, à l'heure où les États-Unis réfléchissent à censurer le géant chinois TikTok[9], les pratiques précitées de filtrages de données ont historiquement généré la création d'outils et technologies d'anonymisation de connexion afin d'y échapper, tels que le *Virtual Private Network* (VPN) ou les Proxy, le plus connu étant le routeur en oignon, *The Onion Router* (TOR). Des bénévoles poussés par leurs convictions philosophiques et des individus par des motivations pécuniaires gèrent en continu le maintien de leur programme. Au motif d'anonymisation originel, l'accès à la consultation de sites Internet censurés dans un pays, s'ajoute aujourd'hui un motif dérivé d'accès à des sites illicites qui ne sont pas indexé par des moteurs de recherches classiques, autrement dit n'existant que sur le *Dark Web*. Les outils et technologies d'anonymisation utilisés à ces fins sont généralement de source ouverte, *Open Source* en anglais, car ils sont mis à

[8] A. De La Grange, Comment la Chine contrôle Internet, Figaro international, Paris : 22 janvier 2010.

[9] V. Malingre et A. Leparmentier, TikTok, menacé d'interdiction aux États-Unis, veut jouer l'opinion contre les gouvernements occidentaux, Le Monde, Paris : 23 mars 2023., V. également : P. Escande, TikTok : Les États-Unis entendent faire tomber le rideau sur les appétits des marchands chinois, Le Monde, Paris : 16 mars 2023.

disposition gratuitement au public partout sur Internet. Ils permettent efficacement une double anonymisation : celle de l'utilisateur qui les sollicite et celle du site ou de la plateforme auquel il a voulu accéder pour consulter du contenu ou en créer.

7. L'Exemple TOR. – Par exemple, le logiciel TOR, installé sur l'ordinateur de l'utilisateur, fonctionne en enveloppant par plusieurs couches successives de chiffrage mathématique le noyau d'informations relatives à la destination de la connexion et en le camouflant ainsi. Le logiciel TOR envoie ensuite la demande de connexion sous cette forme, dite en oignon, au réseau TOR dont les serveurs appelés nœuds se chargent de peler les couches de chiffrage une à une, afin d'accéder au noyau de la demande de connexion et donc aux informations relatives à sa destination. La technologie TOR opère comme suit : le premier nœud pèle une couche de chiffrage qui lui est attitrée et transmet le reste de l'oignon, sans transmettre l'adresse IP de l'utilisateur, à un deuxième nœud qui pèle à son tour une couche de chiffrage lui étant attitrée et transmet le reste de l'oignon à un troisième nœud et ainsi de suite jusqu'au dernier nœud qui pèle la dernière couche de chiffrage. Celui-ci peut alors accéder au noyau d'informations relatives à la destination de la connexion et envoyer le contenu qui en est l'objet à l'utilisateur par la même manœuvre, en remontant la chaîne des nœuds, le tout sans avoir eu connaissance de l'adresse IP du requérant. Par conséquent, en vertu des caractéristiques de chaque outil anonymisant, leur connaissance des données de l'utilisateur et de la destination de sa connexion est donc limitée. Les fournisseurs d'accès à Internet permettent l'utilisation de TOR, des VPN et l'exécution de leur technologie, qui est généralement légale : la directive commerce électronique affirme par ailleurs en son considérant 14 qu'elle « ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet ». Les FAI sont alors matériellement empêchés dans l'identification du site auquel l'utilisateur a voulu se connecter car ils ne peuvent que constater la connexion de celui-ci à un outil anonymisant tel que TOR ou un VPN. En outre, la connaissance de l'adresse IP des nœuds TOR est d'autant plus stérile que chacun d'entre eux peuvent utiliser un FAI différent. Par ailleurs, lorsque des intermédiaires soupçonnent la commission d'une infraction sur leur plateforme par une adresse IP et en font part aux autorités, celles-ci demandent au FAI de communiquer l'identité derrière l'adresse IP. Or, si l'adresse en question est celle d'un VPN ou d'un dernier nœud TOR, le FAI ne peut matériellement connaître l'identité de l'utilisateur qui s'est connecté au VPN ou au Proxy TOR dont il détient l'adresse IP. En cela, ils constituent eux-même des intermédiaires d'Internet qui mettent anonymement en lien l'internaute et le contenu présent sur Internet ou offrent la possibilité d'en créer anonymement.

8. Moteurs de recherche. – Nonobstant, le cas particulier de la connexion anonyme vers des sites non indexés, une connexion Internet active implique classiquement l'utilisation d'un moteur de recherche, tel que Google ou Yahoo, autre intermédiaire d'Internet. Le moteur de recherche renvoie l'utilisateur vers du contenu adéquat à sa recherche en associant par des algorithmes mathématiques les mots qui la constituent à des sites Internet qui lui correspondent. Pour être précis, le moteur de recherche visite continuellement et automatiquement des milliards de liens de sites Internet, les enregistre et les tri afin de répondre adéquatement à la recherche de l'utilisateur ; cette chaîne de travail est baptisée scanner, *crawler* en anglais. Techniquement, le moteur de recherche prend connaissance du contenu présent sur l'intégralité des sites indexés ainsi que de l'adresse IP des utilisateurs et des sites Internet, bien qu'il s'agisse d'une connaissance purement mécanique et algorithmique. Logiquement, la connaissance par le moteur de recherche de l'identité et du contenu de certains sites est établie *a fortiori* s'il met systématiquement en avant leurs liens lorsqu'il répond à une recherche contre rémunération. Tout agissement de la part de l'utilisateur passé cette recherche est hors de la portée du moteur de recherche.

9. Liens hypertexte. – Autre outil de référencement de contenu, les liens hypertextes permettent aux utilisateurs de naviguer d'une page à l'autre en cliquant sur des liens textuels ou graphiques. Les liens hypertexte sont créés en utilisant le langage HyperText Markup Language (HTML), qui permet de définir la structure et le contenu des pages web. Ils peuvent être internes (pointant vers d'autres pages du même site) ou externes (pointant vers d'autres sites web). On l'aura compris, fournisseurs d'accès Internet, outils de connexion anonyme, moteurs de recherche et liens hypertexte permettent tous par leur différents services l'accès à un contenu, lequel est mis à disposition par des infrastructures ou créées par les utilisateurs de celles-ci.

10. Sites et applications accessibles par Internet. – Se trouve donc au sein de la chaîne des intermédiaires le cœur de l'activité de l'internaute : les sites Internet et les applications accessibles par Internet. Cette catégorie possède de nombreux noms en doctrine : éditeurs de contenus ou de services, fournisseurs de moyens ou de services, outils d'échange... Les qualifications suggérées par la doctrine pour distinguer les différents intermédiaires qui les composent sont éparses, souvent abstraites et amènent à une confusion générale puisqu'elles tentent de rassembler sous des termes parapluie des intermédiaires à l'activité bien distincte, en raison d'un objectif en apparence commun. Que l'on ne s'y trompe pas : s'il est intéressant de qualifier juridiquement des activités purement techniques et d'observer des rapprochement entre elles, on ne peut

gommer leurs caractéristiques bien distinctes pour tenter de les unir sous une même bannière. Il est alors plus sage pour nous d'étudier et de distinguer le fond de leurs activités. Deux types de services bien distincts sont proposés par les intermédiaires qui gèrent sites Internet et applications accessibles par Internet : d'une part la fourniture *stricto sensu* de contenus divers et variés suivant une ligne éditoriale bien définie et d'autre part la possibilité pour les utilisateurs d'échanger et de créer leur propre contenu de toute nature. La fourniture de contenu est proposée par des sites et applications dits non-participatifs tandis que la possibilité d'échanger et de créer est proposée par des sites et applications dits participatifs. Ils convergent néanmoins s'agissant de leur connaissance des données qui transitent par leur plateforme.

11. Sites et applications non-participatives. – Les sites et applications non-participatives fournissent directement du contenu selon une ligne éditoriale. Ils le transmettent également à l'utilisateur, ce qui fait d'eux non seulement des fournisseurs de contenus mais également des intermédiaires entre celui-ci et l'utilisateur. À titre d'exemple, on retrouve dans cette première catégorie les journaux en ligne ou les sites à but informatif, tels que le site officiel de la Cour de cassation, Médiapart, Le Monde ou le site officiel du Musée du Louvre. Si le contenu proposé est de nature commerciale on parlera plutôt de plateformes de commerce en ligne telles que Zalando, Livre de Poche ou Ikea, tandis que s'il consiste en des vidéos et des audios on parlera plutôt de plateformes multimédia, telles que MyCanal, Netflix et Disney +. La plupart des sites pornographiques en font également partie. Le dénominateur commun reste le même : celui d'une fourniture de contenu en vertu d'une ligne éditoriale propre à chacun de ces intermédiaires et l'absence de participation de l'internaute à l'activité du site, ce dernier étant limité à la simple visite ou à l'achat en ligne. Les sites et applications non-participatives sont à ce titre souvent qualifiés d'éditeurs en ligne.

12. Sites et applications participatives. – La seconde catégorie de service proposée sur Internet est apparue progressivement dans les années 2000 et prend aujourd'hui une place colossale dans l'utilisation d'Internet. Elle a transformé le web des années 1980 et 1990, aussi dit statique ou 1.0, en un web dit participatif et 2.0, par l'avènement de la participation directe de l'internaute à la création de contenu sur Internet. Ce sont des services de partage, proposés par des sites et applications généralement qualifiés de plateformes d'échange. Le contenu créé et partagé par l'internaute même sur la plateforme peut être de toute nature : commentaires, messages privés, photos, vidéos, audios, annonces de biens, de services ou de conseils pour ne citer qu'eux, à titre gratuit ou onéreux, à titre professionnel ou non. Au premier rang de ces plateformes se trouvent

traditionnellement les blogs, les forums, ainsi que les réseaux sociaux, auxquels se sont ajoutés plus récemment les sites d'achat et de vente/revente entre particuliers : Facebook, Wikipédia, Particuliers à Particuliers, Airbnb, Ebay, YouTube, Vinted ou encore Twitter en font partie. Ici, le dénominateur commun est la participation de l'utilisateur à l'activité du site, dont le service principal est de rendre possible et d'organiser cette participation. Une sous catégorie particulière des sites Internet participatifs est celle des boîtes mail : des plateformes telles que Hotmail ou Wanadoo permettent bien un échange entre utilisateurs d'une même boîte mail – et donc la création d'un contenu par l'internaute sous forme de message, l'e-mail – mais elles le permettent également avec des utilisateurs d'autres boîtes e-mail, spécificité que ne proposent par les autres systèmes de messageries (un utilisateur Messenger ne peut échanger avec un utilisateur Twitter tant dis qu'un utilisateur de Gmail peut échanger avec un utilisateur d'Hotmail). Généralement, l'ensemble des sites et applications accessibles par Internet ont la possibilité matérielle de prendre connaissance du contenu consulté par l'utilisateur, celui-ci n'étant pas chiffré pour ces intermédiaires, et de son identité numérique *via* son adresse IP, mais cette capacité n'est pas toujours mise en œuvre, volontairement. En outre, les intermédiaires qui permettent un partage de contenu par l'internaute et donc ne fournissent pas eux-mêmes de contenu peuvent délibérément intégrer le chiffrage des données comme modalité du service proposé, auquel cas la connaissance par l'intermédiaire du contenu échangé entre internautes devient techniquement impossible. Ce choix est rare mais pas inexistant : Whatsapp ou Telegram proposent un service de messagerie chiffré au contenu inaccessible par leur service, les rendant à ce titre attractifs aux yeux de nombreux utilisateurs. En tout état de cause, le contenu créé par l'utilisateur ou par les intermédiaires et mis à disposition par ceux-ci est nécessairement stocké, sans quoi il ne peut exister : c'est l'activité d'hébergement de données.

13. Hébergeurs de données. – Les hébergeurs représentent le corps, la chair, la partie physique et tangible d'Internet. L'Internet tel qu'il existe aujourd'hui est dit centralisé en ce que la moindre donnée, le moindre site, qu'il soit indexé sur des moteurs de recherche classiques ou non (à l'inclusion du *Dark Web*) existe exclusivement grâce à son stockage sur des serveurs. Ce sont de grands ordinateurs sans écrans outre mesure puissants qui tournent vingt-quatre-heures sur vingt-quatre dans des centres de données, les *datacenters*. Leur mission est de stocker du contenu et de permettre par là même l'existence de ce contenu sur Internet ; autrement dit si les données d'un site ne sont pas hébergées il ne peut exister. Les sociétés d'hébergement, telles que OVH ou Scaleway, ne sont pas seules à réaliser une activité d'hébergement : des individus peuvent également exercer une activité d'hébergeur en gérant eux-même des serveurs. Toutes les données stockées proviennent

indifféremment de sites et d'applications de sociétés ou de particuliers. Lorsque les serveurs abritent des sites illicites et que les machines sont à ce titre volontairement cachées par l'hébergeur, le travail des autorités devient alors particulièrement difficile dans la mesure où l'unique moyen d'en cesser l'existence consiste en un débranchement physique du serveur introuvable. Des États comme la Suisse, le Panama, le Luxembourg et les Pays-Bas ont une régulation particulièrement protectrice de la confidentialité et de la sécurité des données, et sont souvent considérés comme des lieux où les ordinateurs-serveurs peuvent être cachés. Souvent les hébergeurs ne peuvent pas prendre connaissance du contenu qu'ils stockent, celui-ci étant volontairement chiffré, mais ce choix n'est pas systématique et la connaissance des données varie selon le service proposé par l'hébergeur. Typiquement, plus les données sont sensibles et plus la sécurité est de mise, plus les entreprises ou particuliers à l'origine des infrastructures qu'ils veulent stocker se tourneront vers des hébergeurs qui chiffrent les données et donc ne peuvent pas en prendre connaissance. L'échelon ultime de sécurité pour l'entreprise ou le particulier demeure l'internalisation du service d'hébergement ; par exemple, Facebook héberge ses propres données dans ses propres serveurs répartis dans le monde.

14. Réseau de distribution de contenu (CDN). – Enfin, s'agissant toujours du stockage, il est pertinent de présenter le réseau de distribution de contenu, Content Delivery Network (CDN). Celui-ci participe à la mise à disposition de contenu en le distribuant efficacement autour du monde. Les serveurs CDN stockent des copies du contenu du site web, telles que des images, des vidéos et des fichiers de script, et les distribuent aux utilisateurs en fonction de leur emplacement géographique. Ainsi, lorsque les utilisateurs demandent une page web, le serveur CDN le plus proche de leur emplacement répond à la requête, ce qui permet de réduire les temps de chargement et d'améliorer l'expérience utilisateur. Les CDN ont recours simultanément à du stockage permanent de contenu, à l'instar des hébergeurs, mais également de la mise en cache, un stockage temporaire portant sur les données les plus souvent demandées, afin d'améliorer les performances et de réduire la charge sur les serveurs d'origine. Si les CDN font de cette activité leur fond de commerce, de très nombreux hébergeurs la proposent également comme service additionnel, notamment à d'autres intermédiaires comme des plateformes désireuses d'être techniquement performantes.

15. Responsabilité pénale. – Ainsi, nous savons de qui nous allons étudier la responsabilité pénale. Si la responsabilité pénale des intermédiaires d'Internet peut être engagée à raison de multiples faits générateurs, l'étude menée ici est toutefois cantonnée à un objet de responsabilité spécifique, celui du concours apporté aux

cyber infractions commises *via* son service ou son infrastructure par l'utilisateur. À ce sujet, on entend par responsabilité pénale « l'obligation de répondre des infractions commises et de subir la peine prévue par le texte qui les réprime »[10]. L'article 121-1 du Code pénal précise que celle-ci doit demeurer personnelle. Autrement dit, le droit pénal interdit qu'une personne soit déclarée coupable et pénalement réprimée à raison de l'infraction d'autrui. Le principe de responsabilité personnelle a été également affirmé par le Conseil constitutionnel qui, en se fondant sur les articles 8 et 9 de la Déclarations des droits de l'homme a établi que « Nul n'est punissable que de son propre fait »[11]. Le principe est en vérité omniprésente dans la matière : « le principe de légalité énoncé par son article 5 s'adresse au citoyen doté de libre arbitre qui comprend les conséquences de sa liberté d'agir ; il en est de même de l'article 8, selon lequel les peines doivent être « strictement et évidemment nécessaires » pour dissuader les citoyens tentés de commettre des infractions et réprimer ceux qui s'en sont rendus coupables » rappelle l'auteur Jacques-Henri Robert[12]. La responsabilité pénale que l'on analyse ici semble alors ambiguë, en raison de son objet particulier, le concours des intermédiaires apporté aux agissements répréhensibles des utilisateurs. En effet, la question apparaît aux premiers abords être contre intuitive : en vertu du principe de responsabilité pénale personnelle, selon lequel *nul n'est responsable que de son propre fait*[13], retenir la responsabilité d'un intermédiaire Internet lorsqu'un fait pénalement sanctionné est commis par autrui ne serait-elle pas une solution *contra legem* ? En réalité, on verra qu'il s'agit bien non pas d'une responsabilité pénale « du fait de la commission d'une cyber infraction par l'utilisateur » mais bien « en cas de commission d'une cyber infraction par l'utilisateur » ; autrement dit, la commission de la cyber infraction ne constitue pas le fondement exclusif de la responsabilité de l'intermédiaire. En tout état de cause, figure au centre de cette responsabilité figure la commission d'une cyber infraction.

16. Définition de la cyber infraction. – L'appellation de cyber infraction renvoie à l'ensemble des infractions pénales commises via le réseau Internet. Elles représentent une constellation de comportements incriminés, tous distincts mais uniformément commis via Internet, qui représentent la cybercriminalité. L'Organisation des Nations Unies (ONU) définit la cybercriminalité à travers le comportement illégal des internautes, faisant intervenir des « opérations électroniques qui visent la sécurité des systèmes informatiques et

[10] G. Cornu, Vocabulaire juridique, 12ème édition, Association Henri Capitant, Presses Universitaires de France - P.U.F., p. 919.
[11] Cons. const., 16 juin 1999, n° 99-411 DC, cons. 7 : JurisData n° 1999-765189 ; D. 1999, jurispr. p. 589, note Y. Mayaud.
[12] J.-H. Robert, Principe de responsabilité personnelle, JurisClasseur Droit pénal, Fasc. 20, 24 août 2020.
[13] C. pén., art.121-1. ; Cons. const., 16 juin 1999, n° 99-411 DC, Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs.

des données qu'ils traitent » [14] tandis que l'Union Européenne vise l'infraction pénale commise « à l'aide de réseaux de communications électroniques et de systèmes d'information ou contre ces réseaux et systèmes »[15]. Les États la définissent également comme étant « l'intrusion illégale ou l'atteinte à l'intégrité d'un système informatique » s'agissant de la Chine, ou comme étant « l'accès non autorisé à un ordinateur, à un réseau ou à des fichiers à données électroniques en vue de commettre ou de faciliter la commission d'infractions »[16] s'agissant des États-Unis et de la Grande Bretagne. Les définitions se multiplient mais le point commun demeure, celui d'une nature particulière de l'infraction, une nature « cyber ». Mais, à quoi renvoie précisément le sens tant évolutif que méconnu du préfixe « cyber » ? Le terme originel, cybernétique, est inventé par André Ampère en 1848 et repris après la Seconde Guerre mondiale par un chercheur en mathématiques du Massachusetts Institute of Technology (MIT), Norbert Wiener, dans son ouvrage Cybernetics or Control and Communication in the Animal and the Machine[17]. Dans sa thèse, il désigne par ce terme la régulation d'un système vivant ou mécanique qui permettrait la poursuite d'un objectif[18]. La régulation du système permet d'éviter les obstacles qui se dressent devant la réalisation de l'objectif et se fait à travers la communication d'informations. Par exemple, l'optimisation d'un audimat de télévision est permise par l'analyse de celui-ci et la régulation des programmes télévisés qui découle de cette analyse. De ce fait, c'est tant la télévision qui nous regarde que nous qui regardons la télévision ; ici, la communication d'information est double et permet d'atteindre l'objectif souhaité. Le mathématicien transcende dans les années 1950 le sens purement technique de la cybernétique en l'investissant comme notion culturelle, philosophique et métaphysique[19] : la cybernétique renvoie dès lors à l'importance de la communication dans la hiérarchie des systèmes ainsi qu'au changement de paradigme entre l'ancien système de commande des hommes et l'actuel système d'échange informationnel, qui se retrouve désormais dans nos machines. Le préfixe cyber, redécouvert dans les années 1980, permet alors de désigner le nouveau processus d'échange informationnel numérique qu'est Internet, à la fois source d'intelligence collective et de contrôle de ses utilisateurs. Il est, selon le dictionnaire de la langue française Larousse, le préfixe servant à former tous les mots relatifs à l'utilisation du réseau Internet. L'origine même du terme cyber dont s'est inspiré le précurseur Wiener, *kubernân*, la gouvernance en grec ancien, fait sens avec sa

[14] M. Quéméner et J. Ferry, Cybercriminalité : défi mondial et réponses, Economica, 2007.
[15] Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité. §1.1. COM/2007/0267.
[16] S.-M. Cabon, L'influence du cyber espace sur la criminalité économique et financière, Dr. pénal 2018, no 3, Étude 5.
[17] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, The MIT Press, 1948.
[18] L. de Brabandere, Aux origines du mot « cyber », La tribune, Paris : 13 février 2017.
[19] N. Wiener, *The human use of human beings*, 1950, Eyre & Spottiswoode.

signification moderne : aujourd'hui, s'il y a bien une gouvernance palpable dans le système informationnel d'Internet, on ne sait plus exactement qui de l'utilisateur ou de l'intermédiaire gouverne et est gouverné. Ce point étymologique permet en tout état de cause de comprendre ce qu'il y a au fond de la notion de cybercriminalité et de cyber infraction : c'est le lien, la relation entre Internet et l'infraction qui est visée par cette dénomination. Le domaine des cyber infractions paraît à ce titre relativement dense et malléable et l'on peut alors tenter de les classifier pour y apporter de l'ordre.

17. Classification des cyber infractions. – La doctrine a notamment distingué certaines natures particulières de cyber infractions et proposé de les présenter en les catégorisant. Par exemple, l''auteur Frédérique Chopin distingue les cyber infractions en trois catégories, selon qu'un système et réseau numérique en soit l'objet, le support ou le moyen[20]. Dans le premier cas, un système ou réseau numérique constitue l'objet de l'infraction[21] : il s'agirait d'atteintes aux systèmes de traitement automatisé de données, telles que l'accès ou le maintien frauduleux de données dans un système de traitement automatisé[22], d'infractions relatives aux fichiers et traitements informatiques, telles que le détournement ou la divulgation des données personnelles[23], ou d'infractions relatives à la cryptologie. Dans le second cas, le système et le réseau numérique constituent le support de l'infraction[24]. Relèveraient de cette catégorie des infractions relatives à pédopornographie, des infractions de presse, des atteintes à la personne, comme le cyber harcèlement moral[25], ou des atteintes à la personnalité, notamment à la vie privée[26] ou au secret des correspondances[27]. Enfin, la dernière catégorie proposée vise les infractions commises au moyen d'un système et d'un réseau numérique[28]. On y retrouverait les infractions classiques commises contre les biens existant sur Internet, comme la fraude à la carte bancaire[29] ou plus classiquement l'escroquerie[30] et l'abus de confiance[31] commis *via* Internet, les atteintes à la propriété intellectuelle, telles que la contrefaçon[32] et les atteintes aux droits d'auteurs[33], ainsi que des infractions diverses de

[20] F. Chopin, Cybercriminalité, 2021 Répertoire de droit pénal et de procédure pénale, p. 20-203.
[21] Ibid., p.21.
[22] C. pén., art. 321-1.
[23] C. pén., art. 226-21.
[24] F. Chopin, op. cit., p. 60.
[25] C. pén., art. 222-33-2-2.
[26] C. pén., art. 226-1.
[27] C. pén., art. 226-15, C. pén., art. 432-9.
[28] F. Chopin, op. cit., p. 72.
[29] C. mon. fin., art L.163-3.
[30] C. pén., art. 313-1.
[31] C. pén., art. 314-1.
[32] F. Chopin, op. cit., p. 151.
[33] Ibid., p. 156.

publicité et de jeux. Analysons alors une telle classification des cyber infractions. En premier lieu, il est essentiel de nuancer et de constater qu'en réalité certaines de ces infractions ne sont pas des cyber infractions à proprement parler. Le terme de cyber infraction, on l'a vu, implique de façon *sine qua none* l'existence de tout ou partie de l'infraction dans le système et réseau d'Internet, sans quoi il n'existe aucune relation entre le cyber, Internet, et l'infraction (V. 16). Or, un système et réseau numérique, élément ici présenté comme déterminant des catégories de cybercriminalité, n'implique pas systématiquement l'utilisation du réseau Internet, qu'il soit objet, moyen ou support de l'infraction. La tentation de les confondre est là mais il n'y a strictement aucune réciproque entre l'utilisation d'un système et réseau numérique et l'utilisation d'Internet : si Internet peut lui-même être trivialement qualifié de système et réseau numérique connecté, tout système et réseau numérique n'est pour autant pas connecté et donc n'est pas pour autant le réceptacle d'Internet. Par exemple, l'accès frauduleux à des données dans un système de traitement automatisé (STAD)[34] peut parfaitement être commis sans utiliser Internet : un simple accès physique à un ordinateur à Internet et l'utilisation d'une clef *Universal Serial Bus* (USB) suffisent. Le traitement automatisé des données auquel l'auteur tente frauduleusement d'accéder peut également exister hors du réseau Internet : si les centrales nucléaires, les agences gouvernementales ou certaines entreprises stockent leurs données dans un système de traitement automatisé, celui-ci se trouve généralement sur des serveurs internes qui n'utilisent pas Internet, pour des raisons évidentes de sécurité. Ainsi, les infractions comprises dans les catégories doctrinales proposées ne peuvent être cyber qu'à la condition *sine qua none* que le système ou réseau numérique qui en est l'objet, le support ou le moyen soit connecté, utilise bien Internet. Autrement dit, pour que la classification proposée respecte la nature cyber des cyber infractions, l'objet de l'infraction doit bien exister sur Internet ou Internet doit être le support ou le moyen de l'infraction. C'est bien entendu une possibilité qui existe pour la plupart des infractions précitées : pour reprendre l'exemple de l'accès frauduleux à un STAD, celui-ci peut bien évidemment se commettre à l'encontre d'un STAD accessible en ligne, qui prend la forme d'un service *cloud*, d'une application en ligne ou d'une plateforme d'analyse des données. Cependant, certaines d'entres elles ne répondront jamais sérieusement à un tel critère : par exemple une infraction telle que le refus de remise d'une clef de chiffrement aux autorités judiciaires[35], qui relève de la première catégorie de cyber infraction dans cette proposition de classification, ne peut en réalité être une cyber infraction : le chiffrage – une méthode de protection des données tendant à les rendre illisibles pour autrui- ne nécessite aucunement un réseau Internet, pas plus que le refus de sa remise aux autorités judiciaires.

[34] C. pén., art. 321-1.
[35] C. pén., art. 434-15-2.

D'autres auteurs opposent alors plus classiquement objet de la cyber infraction et moyen de sa commission pour les distinguer. L'exercice de classification de cyber infractions, aussi nombreuses que variées, s'avère donc particulièrement difficile et se complique pour la doctrine, en raison de la particulière technicité d'Internet qui apporte souvent de la confusion : on l'a vu, le numérique est trop souvent corrélé à l'Internet alors même que le premier ne nécessite pas toujours le second. En parallèle de la doctrine, les amateurs de l'Internet et des nouvelles technologies ont tendance à proposer une classification thématique et sectorielle des cyber infractions, en distinguant par exemple la cybercriminalité de propriété (atteintes aux biens), la cybercriminalité de personne (atteintes à la personne et à la personnalité) et la cybercriminalité de gouvernement (l'exemple du cyberterrorisme)[36], mais omettent régulièrement certaines cyber infractions plus isolées, par exemple celles relatives à la publicité. Quant à nous, proposons de distinguer les cyber infractions à raison de leur mode d'incrimination. La cyber infraction peut être incriminée en tant que telle, comme infraction *sui generis* ayant la particularité d'être cyber, ainsi qu'au titre d'une circonstance aggravante, accolée à une infraction de droit commun telle que la provocation à la commission d'actes terroristes[37], la contrefaçon[38] ou le harcèlement moral[39] commis en utilisant un « service de communication au public en ligne ». Les cyber infractions peuvent aussi être distinguées selon qu'Internet constitue le mode de commission ou l'élément constitutif de l'infraction, bien qu'il arrive que l'élément constitutif de l'infraction impliquant le réseau Internet relève aussi de son mode de commission (V. 24). Cette proposition rejoint en fait la première : lorsque l'utilisation du réseau Internet constitue le mode de commission, l'infraction de droit commun devient cyber infraction et celle-ci est généralement incriminée au titre d'une circonstance aggravante prévoyant un mode de commission particulier tandis que lorsque le système et réseau d'Internet constitue un élément constitutif de l'infraction, soit objet soit son support, c'est au titre d'une incrimination spéciale que la cyber infraction sera réprimée. Au fond, on découvre par ces deux classifications une dichotomie entre les cyber infractions par nature – celles dont les éléments constitutifs n'existent que sur Internet et qui par conséquent ne peuvent être incriminées qu' à ce titre – et les infractions qui peuvent exister tant bien dans que hors d'Internet mais qui sont aggravées lorsqu'elles sont commises sur Internet. En tout état de cause, les cyber infractions constituent toutes une source potentielle de responsabilité pour les intermédiaires d'Internet. Cependant, les réflexions et les régimes qui en

[36] Panda MediaCenter, Quels sont les différents types de cybercriminalité ? Rennes : janvier 2023.
[37] C. pén., art. 421-2-5 al. 2.
[38] CPI, art. L. 335-7.
[39] C. pén., art. 222-33-2-2 4°.

découlent pour l'intermédiaire ne sont pas les mêmes selon qu'elles soient commises par l'intermédiaire même ou par l'utilisateur.

18. Distinction avec d'autres régimes de responsabilité. – La responsabilité pénale des intermédiaires à raison de cyber infractions commises par les utilisateurs dénote avec d'autres responsabilités juridiques de l'intermédiaire d'Internet. En premier lieu, elle dénote naturellement avec leur responsabilité relevant du domaine du droit civil, commercial, social, fiscal, de la concurrence, de la consommation... S'agissant ensuite de la matière pénale, la responsabilité de l'intermédiaire d'Internet se décline selon deux types de faits générateurs : d'une part la responsabilité du fait d'une cyber infraction commise par un utilisateur, qui nous arrête ici, et d'autre part la responsabilité du fait d'une cyber infraction commise à titre personnel par l'intermédiaire. Il s'agit de deux régimes fondamentalement distincts qui doivent dès lors être analysés séparément. Intéressons nous alors un instant à la responsabilité du fait de la commission d'une cyber infraction par les intermédiaires d'Internet, celle dont on ne traitera pas et qu'il faut à ce titre identifier avant de l'écarter.

19. Convergence avec le régime de l'utilisateur. – Lorsque les agissements des intermédiaires s'avèrent être illicites car pénalement réprimés au titre d'une cyber infraction, c'est bien la responsabilité de l'intermédiaire en tant qu'auteur qui est logiquement retenue. Par exemple, une plateforme de commerce en ligne peut voir sa responsabilité engagée à titre personnel du fait d'une fraude à la carte bancaire qu'elle aurait commise à l'encontre de ses utilisateurs. C'est pourquoi, exception faite de la peine qui varie selon que l'auteur soit une personne morale ou physique, le régime de responsabilité de l'intermédiaire est identique à celui des utilisateurs lorsque la responsabilité pénale est engagée à raison de leur propre fait réalisé au moyen de leur service.

20. Divergence avec le régime de l'utilisateur. – Cependant, le régime de l'intermédiaire diffère de celui de l'utilisateur si l'intermédiaire en question est un service de communication au public par voie électronique au sens de la loi du 28 juillet 1982, modifiée par la loi du 9 mars 2004[40] – laquelle étend le régime prévu cent ans auparavant par la loi du 29 juillet 1881[41] pour les organes de presse et les organes de communication audiovisuelle – et si la cyber infraction en question est une infraction commise par voie électronique au moyen de ce service de communication au public. Les intermédiaires seront considérés comme gérant de tels services s'ils répondent aux critères posés par l'article 1.IV de la loi du 21 juin 2004, autrement dit

[40] Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, art 1.
[41] Loi du 29 juillet 1881 sur la liberté de la presse.

s'ils mettent à disposition du public un contenu composé « de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée »[42], par le biais d'une communication électronique. Les intermédiaires qui gèrent sites et applications proposant du contenu de toute nature à l'utilisateur répondent par exemple à ces critères. Au titre de ce régime spécial, les organes usant d'une communication électronique bénéficient de règles dérogatoires au droit commun sur de nombreux points. En premier lieu, s'agissant des règles de désignation des auteurs, le régime des infractions commises par voie électronique par un service de communication au public prévoit une responsabilité dite en cascade qui reprend celle de l'article 93-3 de la loi de 1982 pour la communication audiovisuelle : le directeur de publication est responsable mais, à défaut de pouvoir l'identifier, c'est l'auteur qui est responsable et, à défaut de pouvoir identifier ce dernier, c'est le producteur qui est responsable. Ensuite, le régime déroge aux règles classiques de procédures en ce que l'action publique se prescrit en un délai de trois mois[43]. En outre, s'agissant de la répression, les peines prévues et prononcées sont plus souples que celles du droit commun : la peine consistant en une publication de la décision prononcée[44] en est l'illustration. L'esprit du régime est relativement libéral, les règles étant conçues *in favorem* de l'organe de presse et de communication au public par voie électronique dans un but de protection du volet actif de la liberté d'expression pour ces organes ainsi que du volet passif de la liberté d'expression pour leurs utilisateurs. Le domaine d'application d'un tel régime relève de toutes les infractions commises par voie de presse, présentes dans le chapitre IV de la loi de 1881 et caractérisées par leur publicité systématique, comme la diffamation[45], et de certaines infractions de droit commun aussi applicables aux organes de presse et de communication électronique, telles que la provocation au suicide[46], l'atteinte à la vie privée[47], les messages violents ou pornographiques accessibles aux mineurs[48], la provocations des mineurs à la toxicomanie, à l'alcoolisme, à la délinquance, à la débauche ou à la pornographie[49], la provocation à la rébellion[50], la provocation à la consommation de stupéfiants ou à la participation au trafic de stupéfiants[51] ou encore les infractions d'apologie du terrorisme ou d'incitation au terrorisme[52].

[42] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 1.
[43] Loi du 29 juillet 1881 sur la liberté de la presse, art. 65.
[44] C. pén., art.131-5.
[45] Loi du 29 juillet 1881 sur la liberté de la presse, art. 30.
[46] C. pén., art. 223-15.
[47] C. pén., art. 226-2.
[48] C. pén., art.227-24.
[49] C. pén., art. 227-28.
[50] C. pén., art. 433-10.
[51] CSP., art L.3421-2.
[52] C. pén., art. 421-2-5.

21. Bilan de la responsabilité de l'intermédiaire. – La responsabilité pénale de l'intermédiaire se découpe donc en deux régimes principaux : un régime de droit commun de responsabilité à titre personnel du fait de la commission d'une cyber infraction et un régime de responsabilité en cas de commission d'une cyber infraction par un utilisateur sollicitant son service ou son infrastructure. Pour mener à bien notre étude, il est donc fondamental d'identifier et de distinguer le second du premier, dans la mesure où les différents faits générateurs qui en sont à l'origine font différer en tout point les conséquences sur le régime de responsabilité pénale applicable. C'est là l'un des enjeux majeurs de notre étude car un tel objet de responsabilité est aussi épineux à cerner que difficile à régir, et il ne suffit pas ici d'une simple extension d'un régime à un autre pour s'en défaire, comme a pu en bénéficier l'organe de communication au public par voie électronique. Ce pan particulier de responsabilité des intermédiaires d'Internet a en ce sens été abordé avec un lot solide de flottements et d'incertitudes.

22. Encadrement tâtonnant des intermédiaires. – Dès les années 1990 et l'arrivée d'Internet pour le grand public, des auteurs ont commencé à interroger l'encadrement juridique, notamment pénal, des intermédiaires techniques classiques, tels que les hébergeurs et les fournisseurs d'accès à Internet, et des médias électroniques[53], constatant l'insuffisance des infractions du droit commun pour réprimer les agissements numériques ou cyber et la nécessité pour la jurisprudence d'en étendre les supports dans tous les domaines, en témoigne le célèbre arrêt Bourquin[54]. Ces interrogations doctrinales arrivent à une époque où le Code pénal en vigueur, celui de 1810, était silencieux quant à la responsabilité des personnes morales, ce qui poussait la Cour de cassation a l'écarter systématiquement. Quelques premières tentatives législatives afin d'exonérer expressément certains intermédiaires de leur responsabilité pénale restèrent veines : l'amendement du projet de loi sur la réglementation des télécommunications proposant une exonération pour les fournisseurs d'accès Internet fut censurée en 1997 par le Conseil constitutionnel tandis que la proposition de loi Madelin relative à la liberté de communication sur Internet du 9 mars 1999 ne fut jamais concrétisée. Pour l'Union Européenne, l'encadrement du statut et de la responsabilité des intermédiaires remonte à l'année 2000 et à sa célèbre directive sur le commerce électronique[55] inspirée par le Digital Millenium Copyright Act (DMCA) américain de 1998, lui-même inspiré du rapport de 1995 de Bruce Lehman, secrétaire d'État de Bill Clinton. La seconde vitesse fut

[53] O. Itéanu et A. Livory, Intermédiaires techniques de l'Internet, quelles responsabilités ? 1992 R. GASSIN, Le droit pénal de l'informatique, D. 1986. Chron. 35.

[54] Cass. crim., 12 janv. 1989, n° 87-82.265 : JurisData n° 1989-700634 ; Bull. crim. 1989, n° 14, RSC 1990, p. 346 obs. Bouzat et p. 507, obs. M.-P. Lucas de Leyssac.

[55] Dir. n° 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, JOCE, no L 178, 17 juill.

passée en France à l'occasion de la loi dite Perben II[56], introduisant dans le Code pénal un nouvel article 121-2 permettant expressément l'engagement de la responsabilité pénale des personnes morales au titre de la commission d'une infraction. La loi LCEN[57] suivit quelques mois après pour établir enfin un véritable régime autonome de responsabilité des intermédiaires. Quelques récents et très attendus instruments de droit européens, dont certains ne rentreront en vigueur qu'à partir de l'année prochaine, ont ensuite été adoptés pour mettre à jour et renforcer le droit applicable. Autrement dit, le régime de responsabilité des intermédiaires d'Internet n'a jamais été celui qui a suscité le plus d'engouement législatif et le plus de production de textes. Les textes européens de 2000 et français de 2004, relativement peu changés depuis, régissent encore la matière, vingt ans après. Mais que représentent vingt années dans l'univers d'Internet ? Depuis 2004, Internet est passé d'une version 1.0 où les utilisateurs n'étaient à proprement parler que des visiteurs, à une version 2.0 les faisant directement interagir, et l'on parle aujourd'hui d'un web 3.0 qui, dans un futur proche, rendrait l'intégralité du réseau Internet décentralisé puisque le contenu existant sur Internet n'aurait plus besoin d'être stocké sur des serveurs et existerait simultanément sur tous les ordinateurs. Certains intermédiaires deviendraient alors obsolètes et les utilisateurs seraient par conséquent bien moins dépendants de ces entités centralisées. Bien qu'elle ne soit pour l'instant qu'une projection, une telle avancée a déjà été engagée par le réseau Bitcoin, lequel permet la création d'un système complètement décentralisé et sécurisé pour enregistrer des transactions. En outre, l'intelligence artificielle, qui a décollé pour le grand public en 2023, est en train de révolutionner l'utilisation d'Internet et sa cybercriminalité. Alors, si certains intermédiaires d'Internet – et ils sont rares – ont peu changé en vingt ans, il est assez paradoxale qu'une matière qui progresse et évolue à une vitesse prodigieuse soit encore régie par des dispositions qui datent de majoritairement de 2000 ou de 2004, alors même que d'autres matières, davantage statiques, bénéficient de plus d'attention de la part des législateurs (depuis 1980, une loi sur l'immigration est passée tous les 17 mois[58]). Pour rappel, au 1er janvier 2004, Google Chrome, Facebook et les applications mobiles n'existaient pas, le moteur de recherche Firefox comptabilisait 2 mois d'existence et aucune vidéo n'avait encore jamais été postée par un internaute. Est-il alors satisfaisant que les intermédiaires d'Internet voient encore leur statut et leur responsabilité être régie par des textes datant d'une époque où la majorité d'entre eux n'avaient encore jamais vu le jour ? À l'heure où la massification de l'échange et du commerce numérique a fait exploser certains contentieux cybercriminels, tel que celui de la contrefaçon ou des contenus haineux, la

[56] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[57] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[58] M. Harzoune, 1980-2022 : lois sur l'immigration, le mille-feuilles législatif, Musée de l'histoire de l'immigration, Paris : janvier 2023.

réponse ne peut qu'être négative : il semble y avoir un décalage dérangeant entre certains de ces textes et la réalité d'Internet, source d'impunité disent certains ou de sévérité soutiennent d'autres. Il est donc à identifier car, si certains mécanismes ont perduré par leur malléabilité et leur pertinence, des manquements et des silences regrettables de la loi se font manifestement sentir, on le verra. Lorsqu'Internet dépasse et surpasse la justice sur de nombreux points, arrivent les obstacles législatifs (comment régir la matière ?) ainsi que juridiques et procéduraux (comment rendre effectif les textes par une application et des moyens juridiques efficaces ?), notamment de réactivité de la justice.

23. Enjeux juridiques. Ainsi, la responsabilité des intermédiaires Internet en cas de commission d'une cyber infraction par l'un de leurs utilisateurs reste une question controversée, sujette à de la politisation, du lobby et des opinions doctrinales divergentes. Elles résultent de la confrontation d'enjeux majeurs pour les utilisateurs d'Internet – notamment en matière de protection des libertés individuelles, de sécurité en ligne ou de respect de la vie privée – et de la répression de la cybercriminalité. D'un côté, alourdir la responsabilité pénale des intermédiaires Internet en imposant des obligations de prévention et de coopération et en engageant leur responsabilité sous certaines conditions peut permettre de lutter efficacement contre la cybercriminalité. D'un autre côté, une telle responsabilité peut être considérée comme une atteinte tant aux libertés fondamentales, limitant l'accès à l'information et instaurant une surveillance accrue des activités en ligne qu'à l'activité des intermédiaires, lesquels sont tenus responsables d'une cybercriminalité qui émane quoi qu'il en soit de leurs utilisateurs, nonobstant de leurs manque de diligence ou de leur inertie face à celle-ci. Dans ce contexte, l'objectif central de notre étude consiste à prendre connaissance des contours, de la substance et de la mise en œuvre de la responsabilité pénale des intermédiaires Internet en cas de commission d'une cyber infractions par leurs utilisateurs. Afin d'y parvenir, on devra s'attacher à répondre à plusieurs questions fondamentales : quel est le degré d'implication des intermédiaires d'Internet dans la commission des cyber infractions et comment module-t-il leur responsabilité pénale ? Sur quel modèle celle-ci a-t-elle été construite et quels en sont les éléments constitutifs ? Comment le régime choisi trouve-t-il à respecter simultanément le principe de responsabilité personnelle, la réalité complexe des intermédiaires d'Internet et la volonté du législateur de sanctionner et de lutter contre la cybercriminalité ? Quels écueils et prospectives la responsabilité pénale des intermédiaires en cas de commission d'une cyber infraction par leurs utilisateurs porte-t-elle en son sein ? Nous proposons d'y répondre en présentant en premier lieu la teneur du régime de responsabilité pénale des intermédiaires (PARTIE PREMIÈRE), afin de répondre aux questions du quoi et du pourquoi, et en second

lieu la mise en oeuvre complexe d'un tel régime (PARTIE SECONDE), afin de répondre aux questions du qui et du comment.

PARTIE PREMIÈRE

LE RÉGIME DE RESPONSABILITÉ PÉNALE DES INTERMÉDIAIRES D'INTERNET

Afin d'en appréhender l'articulation, le régime de responsabilité pénale des intermédiaires d'internet en cas de commission d'une cyber infraction par l'utilisateur doit être présenté en bonne et due forme. Pour ce faire, nous exposerons les raisons de son existence, celles qui ont poussé le législateur d'il y a vingt ans à construire des mécanismes de responsabilité auxquels sont soumis les intermédiaires (Chapitre 1). Elles nous conduiront à comprendre pourquoi un tel régime a été scindé en différents mécanismes applicables (Chapitre 2).

Chapitre 1

FONDEMENT DE LA RESPONSABILITÉ PÉNALE DES INTERMÉDIAIRES D'INTERNET

Pour bien saisir les raisons qui ont poussé le législateur à établir dans les années 2000 un régime de responsabilité des intermédiaires en cas de commission d'une cyber infraction par leurs utilisateurs, il est pertinent de faire appel à un concept platonicien datant de la fin de l'Antiquité, le *pharmakon*. Celui-ci nous permettra de comprendre toute la *ratio legis* qui se cache derrière la volonté de tenir pour responsables les intermédiaires d'internet des agissements de leurs utilisateurs (Section 1). Naturellement, cette volonté est limitée par d'autres

impératifs que désire également respecter le législateur et qui modulent inévitablement la construction du régime de responsabilité des intermédiaires (Section 2).

Section 1. **L'intermédiaire-*pharmakon***

Platon introduit au IV[ème] siècle avant Jésus-Christ le concept de *pharmakon*, poison en grec ancien, dans son dialogue *Phèdre*[59]. Servant à Platon de métaphore pour l'écriture alphabétique, il renvoie en réalité à un terme pharmacologique qui désigne le produit pouvant être à la fois un poison et un remède selon la dose administrée. Suivant les idées portées par le philosophe Jacques Derrida dans son commentaire de *Phèdre*[60], Bernard Stiegler conceptualise cette notion dans l'espace social afin de décrire tout élément qui possèderait une telle ambivalence, qui serait tantôt toxique tantôt thérapeutique. Il développe également la troisième fonction du *pharmakon* : celui-ci serait un bouc émissaire exutoire des incurieux qui ne sauraient en tirer un partie bénéfique et qui s'acharneraient par conséquent dessus. Il est souvent dit qu'Internet est un *pharmakon*[61] en ce qu'il permet, entre autres, tant le développement d'une intelligence collective que le contrôle de ses utilisateurs, tant la libération de la parole opprimée que la libération de la parole qui trouble l'ordre public. Qu'en est-il alors des intermédiaires qui en gèrent le fond et la forme ? Tel un *pharmakon*, ils génèrent du poison, la cybercriminalité, (§1) mais en constituent également le remède (§2). Ils sont par ailleurs pointés du doigt par la loi et le juge qui peinent à contenir le phénomène de la criminalité à l'endroit d'Internet et qui recherchent par défaut la responsabilité de l'intermédiaire (§3).

§1. **L'intermédiaire-poison : une participation de fait au processus cybercriminel**

24. La cyber infraction et Internet. – Si l'intermédiaire d'Internet est le poison de la cybercriminalité, c'est bien parce qu'il en est le géniteur, étant à la source matérielle de son existence. Pour comprendre en quoi les intermédiaires d'Internet participent *de facto* à la commission de cyber infractions, bien qu'ils le fassent à des

[59] Platon, *Phèdre*, 274e-275a.
[60] J. Derrida, *La pharmacie de Platon*, in La dissémination, Paris : Seuil, 1972. ; R. Brague, En marge de « La pharmacie de Platon » de J. Derrida, Revue Philosophique de Louvain, p. 271-277.
[61] X. De La Porte, Internet n'est pas neutre, c'est un pharmakon, Ce qui nous arrive sur la toile, Matins Matins de France Culture, Radio France, 14 janvier 2014.

degrés différents et sans nécessairement le vouloir, il faut s'attacher à comprendre quel est le lien qui unit les infractions et Internet, lien *sine qua none* de la qualification de cyber infraction. Il suppose logiquement qu'*a minima* une partie de l'infraction existe, se manifeste dans le système et réseau Internet ou qu'Internet existe dans l'incrimination de l'infraction, bien qu'il s'agisse en réalité d'une réciproque dans la majorité des cas. Typiquement, l'infraction existe sur le réseau Internet et/ou Internet existe dans l'incrimination de l'infraction lorsque son mode de commission sollicite l'utilisation d'Internet ou que ses éléments constitutifs incluent, de quelque manière que ce soit, le réseau Internet. Par exemple l'escroquerie[62] dont les manoeuvres auraient été commises sur Internet devient une cyber infraction en raison du mode de commission qui se fait *via* Internet tandis que la consultation habituelle de sites à caractère pédopornographique[63] prévoit en ses éléments constitutifs une consultation de contenu déterminé sur Internet (mais donc également un mode de commission qui use du réseau Internet).

25. La cyber infraction et l'intermédiaire d'Internet. – Ainsi, à raison d'une commission sur ou *via* Internet, selon qu'il en soit le support, l'objet ou le moyen (V. 17), les intermédiaires qui en gèrent le contenu, le stockage et l'accès voient leurs services *de facto* sollicités ou détournés pour la commission des infractions qui sont cyber. Dès lors, les intermédiaires peuvent être qualifiés d'outil de cybercriminalité, de plateforme de cybercriminalité, de support de cybercriminalité... Le constat reste le même : la nature cyber de l'infraction fait participer les intermédiaires d'Internet, que l'on pourrait aussi qualifier d'intermédiaires cyber, à la commission d'infraction. Tel est le point de départ de la réflexion portant sur l'engagement de leur responsabilité relativement à la cybercriminalité qui est générée aux moyens de leur service.

§2. **L'intermédiaire-remède : un allié cardinal dans la lutte contre la cybercriminalité**

26. Pouvoirs de l'intermédiaire. – Le Doyen Jean Carbonnier disait « Il faut réparer le mal, faire qu'il semble n'avoir été qu'un rêve » s'agissant du droit civil. L'intermédiaire d'Internet aurait-il selon le législateur le pouvoir de « réparer » la cybercriminalité, de faire en sorte qu'elle ne « semble n'avoir été qu'un rêve » et qui justifierait sa responsabilité à raison de la commission d'une cyber infraction par son utilisateur ? Les

[62] C. pén., art. 313-1.
[63] C. pén., art. 227-23.

intermédiaires d'Internet ont surtout, chacun à leur niveau, un pouvoir de connaissance et de contrôle des données qu'ils voient transiter par leurs services, pouvoir particulièrement précieux pour les autorités publiques qui tentent d'éradiquer la cybercriminalité là d'où elle vient, sur Internet même. Rappelons-le, s'agissant de la connaissance des données, les FAI détiennent les adresses IP des utilisateurs et intermédiaires qui utilisent leurs services – ou celle des outils d'anonymisation qui se connectent à la place des utilisateurs – et l'adresse IP des sites auxquels ils se connectent. Les sites et plateformes accessibles par Internet connaissent également l'adresse IP de leurs utilisateurs ou de leurs outils d'anonymisation ainsi que l'intégralité des données du contenu qui existe sur leur infrastructure, qu'il soit créé par le site ou l'application même ou par l'utilisateur, et peuvent par conséquent le supprimer. En outre, FAI, hébergeurs et plateformes commerciales connaissent *a priori* l'identité des personnes physiques et morales qui font appel à leurs services, *a minima* en raison des informations de paiement de ceux-ci. Les FAI ont également la capacité de filtrer l'accès à Internet, soit pour en bloquer l'accès pour un utilisateur en particulier, soit pour bloquer toute demande de connexion à un site en particulier tandis que les hébergeurs ont le pouvoir de mettre à mal l'existence même du contenu d'Internet : sans hébergement des sites et applications, ceux-ci ne peuvent exister sur le réseau Internet. En bref, les intermédiaires ont un pouvoir de contrôle sur Internet tiré de leurs modalités propres qui non seulement est indispensable à la répression des cyber infraction – la justice ne peut par exemple pas supprimer elle-même un contenu qu'elle aurait déclaré illicite, elle doit nécessairement ordonner à l'intermédiaire du site de le supprimer – mais qui, par surcroît, excède tout levier de manœuvre dont dispose la loi et le juge pour appréhender la cybercriminalité. À ce titre, le législateur a choisi de dépasser cette simple collaboration pour faire de l'utilisateur un allié cardinal de la lutte contre la cybercriminalité. Ce choix n'en est en revanche pas un pour l'intermédiaire, il est au contraire l'un des fondements de certains mécanismes de responsabilité au titre de la commission de cyber infraction par ses utilisateurs.

§3. **L'intermédiaire-bouc émissaire : un responsable expiatoire de cybercriminalité**

27. Responsables idéaux. – Dès l'avènement d'un Internet accessible au grand public, les intermédiaires d'Internet sont rapidement devenus les bouc émissaires du phénomène cybercriminel à l'époque nouveau. Tous

types de délits et d'affaires, en particulier celles de paparazzades constitutives d'atteintes à la vie privée[64], engagent alors la responsabilité pénale de l'intermédiaire qui les relaie, malgré le silence de la loi s'agissant de la responsabilité des intermédiaires d'Internet avant les années 2000. Les hébergeurs, notamment, sont attraits en justice en outre de l'auteur principal de la cyber infraction mais également à sa place[65]. La première tentative du législateur de régir la responsabilité tant civile que pénale des intermédiaires d'Internet[66] est par ailleurs censurée par le Conseil constitutionnel qui reproche alors un manque de conditions suffisamment précises pour l'engager[67]. S'en sont alors suivis de nombreux textes, tant européens que de droit interne, pour permettre la mise en œuvre d'une responsabilité pénale de l'intermédiaire d'Internet en cas de commission d'une cyber infraction par un utilisateur. Mais, dès lors que la cyber infraction en question a déjà un auteur principal, quelles sont les raisons qui ont poussé le droit européen ainsi que le législateur français à vouloir mettre en place un régime qui, en apparence du moins, s'apparente à une responsabilité pénale du fait d'autrui pourtant proscrite par l'article 121-1 ? Outre leur capacité à lutter contre le phénomène cybercriminel, plusieurs éléments notables font des intermédiaires d'Internet des responsables idéaux et expiatoires de cybercriminalité, sans qu'ils en soient nécessairement et directement des coupables : d'une part il n'y a aucune difficulté à les identifier, contrairement aux utilisateurs, d'autre part ils sont parfaitement solvables, ce qui n'est à nouveau pas toujours le cas des utilisateurs. Ensuite, la *ratio legis* favorable à la responsabilité de l'intermédiaire se place sur l'idée selon laquelle qui prend le risque en assume la responsabilité, le tout faisant de l'intermédiaire d'Internet le parfait bouc émissaire d'un incontrôlable phénomène de cybercriminalité. En plein, il s'agit de faire contribuer les intermédiaires à la responsabilité des auteurs à raison d'une cybercriminalité qu'ils aident à engendrer. En creux, on constate que c'est la difficulté évidente de sanctionner les auteurs principaux de cybercriminalité, les utilisateurs, qui est à l'origine de la sanction de ceux qui leur en donne les moyens, les intermédiaires par lesquels ils passent.

28. Identification de l'intermédiaire. – Sans surprises, au vu des nombreux outils disponibles de connexion anonyme (V. 6), l'utilisateur d'Internet qui commet une cyber infraction reste souvent difficilement

[64] aff. Estelle Hallyday, Paris, 14e ch. A, 10 févr. 1999, n° 1998/16424 : JurisData n° 1999-020187 ; Comm. com. électr. 1999, comm. 34, note R. Desgorces ; JCP E 1999, p. 953, obs. M. Vivant et Ch. Le Stanc ; D. 1999, p. 389, note N. Mallet-Poujol ; Gaz. Pal. 2000, 1, p. 637, note C. Caron.

[65] L. Marino, Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement, JurisClasseur Communication, Fasc. 670, 30 août 2015, p.2.

[66] Loi n° 2000-719 du 1 août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

[67] Décision n° 2000-433 DC du 27 juillet 2000, Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

identifiable. Lorsqu'il n'est pas identifiable par son adresse IP, seule une collaboration des outils de connexion anonyme pourrait permettre aux autorités de prendre connaissance de l'identité de l'intéressé, collaboration rendue matériellement impossible dès lors que les VPN font de l'absence de sauvegarde de données leur fond de commerce et un argument de leur attractivité. La collaboration du Proxy TOR (V. 7) est *a fortiori* impraticable : il faudrait que tous les nœuds de connexion de la technologie TOR collaborent pour transmettre l'adresse IP du nœud précédent jusqu'au premier nœud qui a connaissance de l'adresse IP de l'utilisateur, or une telle manœuvre n'est matériellement pas possible. Par ailleurs, le chiffrage de données, proposé par certaines plateformes, empêche la connaissance du contenu par l'intermédiaire. Ainsi, si la cyber infraction est commise au moyen du service Whatsapp, l'intermédiaire comme les autorités n'ont pas le moyen d'en prendre connaissance. L'on pourrait alors qualifier les cyber infractions commises au moyen de ces outils et services d'infractions dissimulées[68], en ce que l'auteur s'est employé à en empêcher la découverte par les autorités publiques.

29. Solvabilité de l'intermédiaire. – C'est également sans surprises que l'on constate que les utilisateurs d'Internet, lorsque l'on peut les identifier, ne sont pas des responsables aussi solvables que les intermédiaires d'Internet. Cela va de soit et, pour appuyer un propos relativement évident, on se contentera de partager quelques uns de leurs chiffres d'affaires annuel, publiés publiquement après audit pour les entreprises côtées en bourse : 28,64 milliards de dollars pour Meta, qui détient Facebook et Instagram, 56,86 milliards de dollars pour Microsoft ou 127,36 milliards de dollars pour Amazon en mars 2023. La solvabilité du responsable n'est pas pertinente pour la sanction de toutes les cyber infractions mais lorsqu'elle l'est, l'intermédiaire sera toujours un meilleur coupable que l'auteur principal de la cyber infraction, ce pourquoi le législateur a eu tout intérêt à mettre en place des mécanismes de responsabilité en ce sens.

30. Théorie du risque. – En 1921, l'essayiste Frank Knight, distinguait dans sa thèse d'économie[69] le risque assurable, un aléa dont la survenance répond à une probabilité connue, de l'incertitude, le risque dit d'entreprise dont l'occurrence est inconnue et qui génère un risque d'erreur plus important. Appliquée en France au droit civil par des auteurs tels que Raymond Saleilles, Louis Losserand, François Chabas ou Henri

[68] CPP, art. 9-3, V. également Cass. ass. plén., 7 nov. 2014, n° 14-83.739, Bull. ass. plén. n° 1 ; : Dr. pén. 2014, comm. 151, obs. Maron et Haas ; Procédures 2014, comm. 326, obs. A.-S. Chavent-Leclère), A. Lepage : JCP G 2015, étude 69, AJ pénal 2015, p. 36, note A. Darsonville ; Rev. sc. crim. 2014, p. 777, obs. Y. Mayaud.

[69] F.-H. Knight, D.-E. Jones, *Risk, Uncertainty and Profit,* Cornell University Library's print collections, 1921.

Mazeaud[70], la théorie du risque se décline en plusieurs variantes. Notamment, la théorie du risque-profit et du risque-créé veulent respectivement que celui qui profite du risque et que celui qui engendre ledit risque soient responsables. Si ces raisonnements apparaissent à première vue incompatibles avec le droit pénal, dont la fonction première est la répression de comportements constitutifs d'infractions et non la réparation de dommages générés par des risques, il n'en est rien : outre l'existence même de la notion de risque en droit pénal, au sein d'infractions telle que la mise en danger d'autrui[71] par exemple, l'établissement même d'une responsabilité des intermédiaires d'Internet au titre des cyber infractions commises par leurs utilisateurs fait écho avec ces théories. En effet, le risque créé par les intermédiaires d'Internet est bien celui de la cybercriminalité puisque ceux-ci offrent volontairement ou non, consciemment ou non, les moyens de commettre des cyber infractions (V. 25). Par conséquent, l'engagement de leur responsabilité peut être conçue comme une réponse juridique, pénale, à la création de ce risque et au profit parfois tiré de celui-ci et peut être justifié ainsi. C'est pourquoi, dès l'apparition de régimes relativement atténués de responsabilité, des auteurs ont incité les juges à les appliquer plus sévèrement « comme pour en limiter la nocivité ou à tirer parti des ressources de la théorie du risque pour que celui qui tire profit d'une activité à risques en assume la responsabilité »[72].

Certes, les intermédiaires participent à la cybercriminalité, en sont des responsables idéaux et constituent un outil très précieux de lutte contre celle-ci. Toutefois, la volonté législative d'établir leur responsabilité pénale à raison de la cybercriminalité émanant de leurs utilisateurs s'est heurtée à d'importantes limites, lesquelles constituent par ailleurs un objet récurrent de discussion et critiques doctrinales.

***

[70] F. Chabas, H. & L. Mazeaud, A. Tunc, Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, 6e éd., t. 1, Montchrestien, 1965.
[71] C. pén., art. 223-1.
[72] T. Azzi, La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ?, in Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le WEB 2.0 : LexisNexis, coll. IRPI, 2009, p. 59 s.

Section 2. **Limites du fondement**

Au fond de ces limites, on retrouve d'autres enjeux juridiques avec lesquels le législateur a dû composer, et qu'il a choisi de ne pas mettre à mal par une responsabilité extensive des intermédiaires (§1). Ces enjeux ont par conséquent eu une incidence indéniable sur la construction du régime de responsabilité pénale des intermédiaires en cas de commission d'une cyber infraction par leurs utilisateurs (§2).

§1. **Libéralisme économique et liberté d'expression**

31. Libéralisme économique. – La volonté de réprimer les acteurs d'Internet – et à l'époque il ne s'agissait que des intermédiaires d'Internet et non des utilisateurs puisque l'Internet de l'époque était statique – émerge dans les années 1990 et au début des années 2000 au même moment que la volonté de faire d'Internet un espace libre, régulé par le marché et où la rigueur du juridique y est absente. Au temps où la cybercriminalité était balbutiante et où le droit européen, anciennement communautaire, se concentrait exclusivement sur l'économie libérale européenne, Internet arrive avant tout en tant qu'un élément économique majeur dans la sphère marchande du numérique[73]. L'intitulé de la toute première directive cherchant à définir et régir l'activité et la responsabilité des intermédiaires d'Internet en est le parfait exemple[74] : il s'agissait pour le droit communautaire de réguler le « commerce électronique » au sein du « marché intérieur », la zone économique du commerce et des échanges intracommunautaires. C'est donc bien à travers le prisme commercial qu'Internet est perçu à l'époque, celui-ci justifiant la volonté de limiter les contraintes qui pourraient peser sur les nouveaux acteurs du marché numérique. La Bulle Internet, qui a eu pour conséquence de faire grimper en mars 2000 la spéculation de toutes les innovations et technologies relatives à Internet et de faire investir des milliards de toutes les devises du monde dans celles-ci avant de s'effondrer (- 27 % à la bourse de New York les deux dernière semaines d'avril 2000), illustre parfaitement l'ampleur des considérations économiques prodigieuses auxquelles ont dû faire face les États et le droit communautaire dans leur réflexion s'agissant de la régulation économique et juridique des acteurs d'Internet. Le mot d'ordre a donc été, *ab initio*, la volonté d'établir – si régulation et

[73] L. Marino., op. cit, p.2.

[74] Directive 2000/31/CE du 8 juin 2000 , dite « commerce électronique » PE et Cons. CE, dir. 2000/31/CE, 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

responsabilité des intermédiaires il y avait – les règles les plus respectueuses possibles du libéralisme économique dans lequel est né Internet et donc les moins constitutives d'entraves à leurs activités. C'est pourquoi il est souvent dit des intermédiaires d'Internet qu'ils bénéficient depuis toujours d'une impunité voire même d'une immunité[75]. Ce raisonnement tient purement d'une politique plus économique que juridique et, ainsi que l'auteur Laure Marino le souligne « dès lors que la règle juridique est l'habillage d'un choix économique et politique, on peut toujours en défendre une autre »[76].

32. Liberté d'expression. – Si l'utilisateur, en avide consommateur d'Internet qu'il est, a toujours bénéficié de l'argument du libéralisme économique en fond de toile de mécanismes visant à alléger la responsabilité des intermédiaires d'Internet, c'est plus récemment de la liberté d'expression dont il bénéficie également au titre de ce régime atténué. En effet, depuis l'avènement d'un Internet 2.0 aussi appelé Internet social ou participatif, l'exercice de la liberté d'expression sur le réseau d'Internet a été offert aux utilisateurs d'Internet en outre des intermédiaires distribuant du contenu sur Internet. Internet a en conséquence été considéré comme l'outil permettant « de renouer avec la promesse démocratique des origines »[77]. Dès lors, un régime juridique qui serait particulièrement lourd pour les intermédiaires, qu'il s'agisse en amont de filtrer le contenu ou en aval d'être facilement tenu responsable de toutes cyber infractions commises par les utilisateurs, porterait doublement atteinte à la liberté d'expression de ceux qui en usent sur Internet : d'une part les obligations de filtrer le contenu reviendrait à octroyer aux entreprises privées le pouvoir de conditionner l'exercice de cette liberté en la censurant sans intervention d'un juge, d'autre part une responsabilité de l'intermédiaire trop aisément engagée rendrait leur activité nettement moins attractive et, sur le très long terme, conduirait à un amoindrissement de l'offre de plateformes sur lesquelles s'exerce la liberté d'expression dans son volet actif et passif. Si cette dernière hypothèse paraît lointaine à l'heure actuelle, les difficultés techniques que peuvent rencontrer certaines plateformes d'échange telle que Twitter, conduisant parfois à leur indisponibilité pendant quelques heures, plongent certaines zones du monde dans un silence et une privation d'informations qui ne laissent pas les populations indifférentes. Le constat est d'autant plus vrai que l'information et l'échange sur Internet est concentrée autour d'une poignée de géants de la communication tels que Facebook ou Google. Un manque d'attractivité économique conduisant à leur fin serait en ce sens particulièrement impactant pour la

[75] J. Bossan, Le droit pénal confronté à la diversité des intermédiaires d'internet, Revue de droit pénal et sciences criminelles n° 2, 2013, p. 296.
[76] L. Marino., op. cit., p.2.
[77] E. Plenel, *Le droit de savoir,* Don Quichotte éd., coll. « Points 3207 », 2013, p.49., V. également P. Riché, Internet a rendu concrète la liberté d'expression, gare au retour en arrière !, in *Justice et liberté d'expression*, PULIM, coll. « D'Aguesseau », 2014, p.151.

liberté d'expression, les sociétés contemporaines ayant jeté leur dévolu sur leurs services pour l'exercer en masse. En marge de la liberté d'expression, la vie privée des utilisateurs est également menacée par des mécanismes de responsabilité pénale construites sur un modèle obligeant les intermédiaires à contrôler systématiquement les données, sous peine de l'engager. C'est pourquoi la responsabilité pénale des intermédiaires doit être appréhendée avec lucidité et réserve.

33. Limite à la limite. – Bien entendu, les libertés des utilisateurs et des intermédiaires et la vie privée des utilisateurs n'ont jamais eu non plus pour vocation de neutraliser la présence de tout mécanisme de responsabilité pour l'intermédiaire d'Internet. Si un tel argument fut un temps porté à l'avènement du réseau Internet, il s'est très vite essoufflé face à l'ampleur du phénomène. Même les adeptes les plus convaincus d'un « Internet libre »[78] ne peuvent soutenir l'absence absolue de tous les régimes juridiques de responsabilité, en particulier lorsqu'il s'agit d'une responsabilité pénale en principe étrangère aux considérations d'ordre purement privé. Ainsi que l'auteur Emmanuel Dérieux le rappelle : « La liberté ne peut pas être l'absence de règles et de sanction de leur violation. La règle de droit, démocratiquement établie, et le contrôle de son application, assuré par les juges, constituent la seule et vraie garantie de l'équilibre des droits et des libertés. Les " lois " du marché et la raison du plus fort, du plus puissant ou du plus habile dans l'usage des techniques sont une atteinte aux libertés. » et, citant Lacordaire, « Entre le faible et le fort, c'est la liberté qui opprime et la loi qui libère »[79].

§2. **Incidences sur la construction du régime de l'intermédiaire**

34. Respect des libertés. – En conséquence de la nécessité de respecter la liberté d'expression, la vie privée et le libéralisme économique dont bénéficient les intermédiaires d'internet et leurs utilisateurs, le régime de responsabilité pénale des intermédiaires doit être adapté et dosé. La loi Avia, visant à lutter contre les contenus haineux sur internet[80] fit en ce sens l'erreur de prévoir un régime de responsabilité pénale des intermédiaires particulièrement lourd lorsqu'étaient en cause des contenus haineux : à des obligations de retrait de contenus haineux sous peine d'engager des sanctions pénales s'ajoutaient des obligations de diligences démesurées afin que l'intermédiaire détecte et apprécie discrétionnairement le contenu haineux dont il est

[78] E. Derieux, Neutralité et responsabilité des intermédiaires de l'Internet. Mythe ou réalité ? La semaine de la doctrine, La semaine juridique - édition générale, n°13, 26 mars 2012, p. 621.
[79] Ibid. p. 627.
[80] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

question, dans un délai excessivement bref. En ce que ses dispositions portaient une atteinte à la liberté d'expression et de communication considérée comme n'étant pas adaptée, nécessaire et proportionnée au but poursuivi, la loi Avia a été majoritairement censurée par le Conseil constitutionnel[81]. Les mécanismes de responsabilité pénale des intermédiaires ne peuvent donc résulter en de la suppression de masse de contenus par l'intermédiaire, arbitraire et sous peine de sanctions lourdes, ou des obligations de diligences trop sévères : la solution inverse aurait des conséquences lourdes sur l'exercice des libertés fondamentales dont jouissent intermédiaires et utilisateurs.

35. Respect du principe de responsabilité personnelle. – En outre, la responsabilité de l'intermédiaire d'internet ne peut constituer en une substitution de la responsabilité des utilisateurs et donc en une responsabilité du fait d'autrui, laquelle est prohibée par l'article 121-1 du Code pénal, en raison du seul fait qu'il participe *de facto* à la cybercriminalité de ses utilisateurs qui transite par ses services et infrastructure. En effet, la théorie du risque demeure une théorie civile : au titre du droit commun en matière pénale, la responsabilité pénale ne peut être engagée qu'après l'examen d'un élément matériel et moral qui démontre la commission ou le concours à la commission d'une cyber infraction. La responsabilité pénale des intermédiaires d'Internet doit respecter les mécanismes de droit pénal établis et ne pas tomber dans une responsabilité du fait d'autrui, laquelle est prohibée par l'article 121-1 du Code pénal. On cherche donc ici à sanctionner un comportement de l'intermédiaire et non le comportement exclusif de son utilisateur.

Le régime de responsabilité pénale des intermédiaires a dû se construire autour des nombreux impératifs antagonistes que l'on vient de présenter. Entre volonté de réprimer la cybercriminalité et respect des utilisateurs, entre attractivité économique libérale et contribution à la responsabilité de l'utilisateur auteur de la cyber infraction, le régime de l'intermédiaire a dû se forger en trouvant un équilibre respectueux et pragmatique par rapport à la réalité complexe des intermédiaires. La solution trouvée par le législateur a donc été de scinder le régime de responsabilité pénale de l'intermédiaire en plusieurs mécanismes de responsabilité dont il peut relever.

***

[81] Cons. const., 18 juin 2020, n° 2020-801 DC, relative à la loi visant à lutter contre les contenus haineux sur internet, §18.

Chapitre 2

SCISSION DE LA RESPONSABILITÉ PÉNALE

DES INTERMÉDIAIRES D'INTERNET

Avant d'étudier la teneur de cette scission, il nous paraît indispensable d'avoir une vision globale des droits qui peuvent s'appliquer à l'intermédiaire dans le cadre de cette responsabilité, autrement dit ce à quoi l'intermédiaire peut être potentiellement soumis (Section préliminaire). Ensuite, nous découvrirons que le régime de responsabilité de l'intermédiaire a été scindé comme suit : d'une part l'intermédiaire d'Internet est soumis à un régime dit de responsabilisation pénale (Section 1), d'autre part il est soumis à un régime de responsabilité pénale de droit commun (Section 2).

Section préliminaire. **Le droit applicable**

La question du droit applicable, et notamment celle de l'applicabilité du droit pénal, doit bien entendu être analysée *ratione materiae* (§1) et *ratione loci* (2).

§1. **Le droit substantiellement applicable**

36. Spécialité du droit pénal. – Naturellement, la commission d'une cyber infraction étant l'élément déclencheur de la responsabilité pénale des intermédiaires, le droit pénal vient à s'appliquer substantiellement. Son applicabilité aux intermédiaires d'Internet provoque la question d'un droit spécifique exclusivement applicable dans l'espace d'Internet et donc l'idée d'un droit autonome de l'Internet. En effet « Internet obéit-il aux mécanismes généraux ou est-il forgé au regard de l'activité sur laquelle il porte »[82] ? Lorsqu'on évoque la

[82] J. Bossan, op. cit., p. 296.

relation particulière entre Internet, ses acteurs et le droit pénal, la réflexion souffre d'un présupposé selon lequel le droit pénal n'aurait pas sa place dans l'espace cyber lorsque son objectif est d'en punir les intermédiaires pour une cybercriminalité provenant des utilisateurs. Du côté du juge pénal, il serait étranger au monde des intermédiaires d'Internet qu'il ne maîtrise pas et du côté des acteurs d'Internet le droit pénal aurait un effet pervers antiéconomique et castrateur. Les mécanismes de responsabilité dont on s'apprête à prendre connaissance démontrent toutefois que le droit pénal peut parfaitement se montrer réaliste en se spécialisant et en s'adaptant aux activités des intermédiaires sans pour autant délaisser des mécanismes généraux de la matière. En effet, bien que le droit pénal pénal soit une matière *per se*, il est simultanément l'accessoire de tous les autres droits et de tous les domaines, à l'inclusion d'Internet : il a alors tout naturellement vocation à s'appliquer lorsque l'intermédiaire d'Internet démontre un degré d'implication dans la commission d'une cyber infraction par son utilisateur, qu'elle soit passive ou active. Ainsi, le droit pénal est applicable aux intermédiaires dans toutes ses facettes : droit pénal général, tel que les mécanismes établis de responsabilité pénale, mais aussi droit pénal spécial applicable à certaines infractions *ratione materiae*, comme les infractions dite de presse. Ainsi, bien qu'il n'y est pas de droit pénal « pleinement abouti qui s'applique à Internet »[83], il existe bien un droit pénal spécifique relatif aux intermédiaires d'Internet. Ou plutôt, il existe des droits pénaux applicables aux intermédiaires d'Internet, ceux-ci étant soumis *ratione loci* à la compétence législative de plusieurs lois pénales.

§2. **Le droit territorialement applicable**

37. Applicabilité territoriale du droit pénal aux intermédiaires. – C'est en vertu des règles de compétence territoriale de la loi pénale française à l'endroit de la cybercriminalité que doit être analysé le droit territorialement applicable aux intermédiaires. En effet, dans la mesure où c'est à raison d'une cyber infraction commise par un utilisateur que le législateur a introduit des mécanismes de responsabilité de l'intermédiaire, la loi pénale territorialement applicable à son régime de responsabilité n'est autre que celle compétente pour réprimer ces cyber infractions, ce pourquoi nous devons nous attacher à la découvrir. On le verra, celle-ci est particulièrement souple, à l'instar de nombreux autres États. C'est pourquoi la coopération étatique en la matière, engagée dès les années 2000 par l'Union Européenne malgré une effectivité parfois relative, est plus que nécessaire à la cohérence du régime de responsabilité de l'intermédiaire d'Internet.

[83] Ibid.

38. Applicabilité de la loi pénale dans l'espace. – Rappelons-le, selon une jurisprudence internationale bien établie[84] tout État est libre de fixer la sphère de compétence territoriale de sa loi pénale en vertu de sa souveraineté nationale. La compétence législative de la loi pénale française n'y fait pas défaut ; elle est souverainement régie par un principe de territorialité ainsi qu'une application extraterritoriale exceptionnelle et subsidiaire. La compétence est territoriale si l'infraction est commise sur le territoire de la République[85]. En revanche elle est extraterritoriale si l'infraction commise à l'étranger par un Français relève du Titre I du Livre IV du Code pénal[86], si elle est commise à l'étranger sur des Français[87] ou par des Français[88] selon certaines conditions, si elle est consécutive à un refus d'extradition ou de remise[89], ou bien si la compétence est universelle en vertu de conventions internationales telles que la Convention sur la lutte contre la corruption d'agents publics étrangers[90], ou à raison de la commission d'un crime de droit international[91].

39. Applicabilité de la loi pénale dans l'espace cyber. – À première vue, Internet existant simultanément hors et dans les frontières du territoire de la République, le principe de territorialité de la loi pénale semble être difficilement applicable ; l'obstacle tient de la nature atteritoriale d'Internet. Au sens de cette compétence territoriale, il a toujours été entendu que l'infraction devait avoir, à défaut d'une commission intégrale, une commission réputée sur le territoire de la République ou ayant généré des effets sur celui-ci. Il a en premier lieu été simplement exigé par la jurisprudence que la victime soit *a minima* un résident français ou une personne morale dont le siège se trouve en France pour que soit exercée la compétence territoriale de la loi pénale française dans le cadre de la cybercriminalité[92]. C'est ensuite par le biais d'une commission réputée sur le territoire que la compétence territoriale de la loi pénale française a été originellement établie en étant considérée comme applicable à la seule raison d'une émission ou d'une réception du contenu illicite, à l'occasion d'une affaire Yahoo[93]. Ainsi que le relève à juste titre l'auteur Mireille Delmas Marty, cette compétence était dès lors

[84] Affaire du « Lotus » du 4 septembre 1927 (France c. Turquie), arrêt, C.P. J.I., Recueil (1927) série A - n° 70.
[85] C. pén., art. 113-1 ; C. pén., art. 113-2.
[86] C. pén., art 113-10 ; C. pén., art 113-13.
[87] C. pén., art 113-6.
[88] C. pén., art 113-7.
[89] C. pén., art. 113-8-2.
[90] Convention de l'Organisation européenne de coopération économique sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, 21 novembre 1997, art. 4.
[91] CPP., art 689-11.
[92] Cour d'appel de Limoges, 8 juin 2000 n° 00-431, Sté Porcelaine Carpenet.
[93] T. corr. Paris, 26 févr. 2002, Comm. com. électr. 2002, comm. 77, obs. A. Lepage ; TGI Paris, 13 nov. 1998, Gaz. Pal. 2000. 1. Doctr. 697, obs. M. Manseur-Rivet ; CA Paris, 17 mars 2004, Comm. com. élect. 2005, comm. 72, obs. A. Lepage.

« quasi-universelle »[94] : dans l'affaire précitée, la société américaine a été condamnée en France pour apologie du nazisme et négationnisme en raison de l'existence d'une page organisant la vente aux enchères d'objets nazis sur son moteur de recherche. Internet est par définition un réseau mondial interconnecté dont la substance ne subit aucune limite territoriale. La réception du contenu sur le territoire français, ancien critère d'applicabilité de la loi pénale française à l'endroit d'Internet, pouvait ainsi engager la responsabilité de l'intégralité des intermédiaires d'Internet au titre d'une cyber infraction commise par l'utilisateur, dans la mesure où l'entièreté du contenu présent sur le réseau d'Internet peut être réceptionné en France. À ce titre, la jurisprudence française a tempéré dès 2010 sa solution en exigeant que le site soit orienté vers le public français[95], de manière non exclusive. La solution de 2010 ne s'écarte en réalité que timidement de la précédente étant donné qu'une majorité des sites et applications sont destinées au public européen et français. L'illustration par excellence d'une absence de destination au public d'Internet a néanmoins été donnée par un contentieux en contrefaçon opposant la société Buttress à la filiale de l'Oréal Paris, Lancôme : « la société Lancôme exploite un site Internet sur lequel elle présente l'ensemble des produits de sa gamme destinés à l'Europe, l'Amérique et l'Asie, que le masque de beauté portant la dénomination " Nutri-Riche " et présenté sur ce site sous la rubrique " autres pays ", n'est pas offert à la vente, ni disponible, en France » ; « du reste, la partie du site destinée à la France, différenciée des pages destinées à la clientèle francophone, ne présente aucun produit sous la dénomination " Nutri-Riche " mais sous celle de " Nutri-Intense " »[96]. En 2016, le législateur vient codifier la solution selon laquelle l'infraction est réputée commise sur le territoire français lorsque la victime réside ou a son siège social en France et que l'infraction est commise au moyen d'un réseau de communication électronique[97] et neutralise ainsi définitivement l'exigence d'une destination au public français dès lors que la compétence personnelle passive s'exerce. La jurisprudence maintient toutefois le critère de la destination au public français à défaut de la commission au préjudice d'une victime française. Dans une affaire où étaient en cause des propos visant des personnes japonaises et des événement survenus au Japon, la Cour de cassation a en effet retenu que « la seule

[94] M. Delmas-Marty, Le relatif et l'universel. Les forces imaginantes du droit, T. 1, Seuil, coll. La couleur des idées, 2004, p. 342.

[95] T. corr. Paris, 13 novembre 1998 : Droit et patrimoine, sept. 1999, p. 111, obs. E. Caprioli ; Gaz. Pal. 2000, 1, doctr. p. 697, obs. M. Manseur-Rivet.

[96]. Cass. com., 10 juill. 2007, n° 05-18.571, Sté Buttress BV et a. c/ Sté l'Oréal et a. : Rev. crit. DIP 2008, p. 322, note E. Treppoz ; JCP G 2007, II, 10161, note C. Chabert ; JCP E 2007, 2269, note J. Passa ; Comm. com. électr. 2007, comm. 119, obs. C. Caron ; déjà en ce sens, Cass. com., 11 janv. 2005, n° 02-18.381, Hugo Boss : JurisData n° 2005-026462 ; D. 2005, p. 428, note C. Manara ; JCP E 2005, 571, note C. Castets-Renard ; JCP G 2006, I, 103, § 21, obs. C. Caron ; JCP E 2006, n° 1195, obs. M. Vivant ; Propr. intell. 2005, n° 15, p. 203, obs. X. Buffet-Delmas ; RLDI 2005, 27, n° 57, obs. Costes ; Légipresse 2005, n° 221, III, p. 77, note J. Passa ; Comm. com. électr. 2005, comm. 35, note C. Caron.

[97] C. pén., art 113-2-1.

accessibilité d'un site Internet sur le territoire français n'est pas suffisante pour retenir la compétence des juridictions françaises, prises comme celles du lieu du dommage allégué, sans rechercher si les annonces litigieuses étaient destinées au public de France »[98].

40. Conséquences d'une compétence territoriale souple. – Ainsi, la loi pénale française bénéficie d'une compétence à l'endroit d'Internet très souple, permise par la souplesse de son applicabilité territoriale, que les intermédiaires mis en cause soient français, implantés à l'étrangers ou purement étrangers. Dès lors, le respect du droit du lieu où le contenu est généré devient insuffisant pour l'intermédiaire qui doit désormais respecter tous les droits pénaux du monde, selon la formule de l'auteur Agathe Lepage[99], notamment lorsque d'autres États s'octroient souverainement une compétence également sinon plus large. S'agissant par exemple des États-Unis, le rapport d'information sur l'extraterritorialité de la législation américaine présenté en 2016 par le Parlement[100] fait non seulement part d'une compétence territoriale qui englobe certains éléments relevant en France de la compétence extraterritoriale et d'un manque de justification lorsqu'est exercée une compétence mais également de critères outre mesure extensifs : dans une affaire mettant en cause des dirigeants hongrois pour des faits de corruption en Macédoine et au Monténégro, et le critère de compétence « d'émetteur sur les marchés financiers américains » ne pouvant être utilisé, c'est à raison de mails échangés entre les auteurs ayant transité par des serveurs aux États-Unis que le lien de territorialité a été déterminé et la compétence territoriale exercée. La justification sous-jacente faisait ici appel à la dimension mondiale du réseau Internet, qui aurait dû pousser les intéressés à se douter que leurs mails allaient transiter dans le monde et notamment par le sol américain[101]. *In fine,* la difficulté pour les intermédiaires comme pour les utilisateurs – tous deux responsables selon différents régimes des cyber infractions commises par les utilisateurs – consiste à déterminer les législations pénales dont elles relèvent et de toutes les respecter. Une uniformité de celles-ci ne serait-elle pas en ce sens souhaitable ?

41. Nécessité d'uniformiser les législations nationales. – Ainsi que le souligne l'auteur Jérôme Bossan, il est bien vital que l'ensemble des droits nationaux applicables à l'endroit d'Internet selon leurs critères souverainement déterminés, fassent preuve de convergence et d'uniformité sinon d'unicité en matière de

[98] Cass. Crim., 12 juill. 2016, pourvoi n° 15-86645.
[99] A. Lepage, Libertés et droits fondamentaux à l'épreuve de l'Internet, Litec, 2003, p. 86 et M. Vivant, « Cybermonde : Droit et droits des réseaux », JCP G. 1996, I, 3969, n° 23, spéc. note 52.
[100] Rapport sur l'extraterritorialité de la législation américaine, n°4082, Assemblée nationale, 5 octobre 2016.
[101] R. Bismuth, Pour une appréhension nuancée de l'extraterritorialité du droit américain – Quelques réflexions autour des procédures et sanctions visant Alstom et BNP Paribas, Annuaire français de droit international, 2015, pp. 785-807

cybercriminalité, auquel cas l'intermédiaire ne pourra réalistiquement s'y conformer[102]. La coopération des États et une approche transfrontalière paraissent fondamentales à cet égard[103], tant sur la question de la poursuite et de la répression de la cybercriminalité que sur les règles de mise en œuvre de la responsabilité pénale des intermédiaires à raison de cette cybercriminalité émanant de leur utilisateurs.

42. Uniformisation des législations relatives à la cybercriminalité. – L'Union Européenne s'est mise à sa table de travail dès 2001 afin d'apporter un cadre de règles relatives à la répression de la cybercriminalité en adoptant une Convention sur la cybercriminalité[104], dont les objectifs sont, entres autres, l'adaptation du « temps procédural » au « temps numérique »[105] et l'harmonisation des législations nationales relatives à la cybercriminalité[106]. En réalité, elle consiste avant tout à définir le phénomène à l'époque nouveau de la cybercriminalité et à enjoindre les États à le réprimer. Les efforts des États ont été relativement limités en la matière depuis, ainsi que le relève la Résolution sur la lutte contre la cybercriminalité du Parlement Européen de 2017[107] : de nombreux actes de cybercriminalité bénéficient encore d'une impunité en ne faisant l'objet d'aucune poursuite et les concours de compétences liés à la nature transfrontalière de la cybercriminalité demeurent[108]. La réticence de l'Union Européenne à régir les droits pénaux de ses États membres n'est pas nouvelle, ceux-ci représentant généralement l'émanation la plus directe de la volonté souveraine de chacun des États[109] que les régulations européennes s'efforcent de respecter.

43. Uniformisation des législations relatives aux Intermédiaires d'Internet. – L'Union Européenne se saisit également de la question du régime de responsabilité, de ses conditions et de sa mise en œuvre ainsi que des obligations de l'intermédiaire d'Internet pour plus d'uniformité avec notamment des directives relatives au commerce électronique de 2000[110], que l'on connaît, à la vie privée et aux communications électroniques de

[102] J. Bossan, op. cit., p. 298

[103] E. Dreyer, in Traité de droit de la presse et des médias, dir. B. Beigner, B. de Lamy et E. Dreyer, LexisNexis, coll. Traités, 2009, n° 2282

[104]Convention du Conseil de l'Europe sur la cybercriminalité, Série des traités européens - n° 185, Budapest : 23 décembre 2001

[105] Y. Padova, Un aperçu de la lutte contre la cybercriminalité en France, RSC 2002. 765.

[106]F. Chopin, op. cit., p. 18.

[107]Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI)).

[108] Ibid. §M.

[109] Art. 34 de la Constitution française prévoyant la légalité criminelle et délictuelle en son volet formel.

[110] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique) Journal officiel n° L 178 du 17/07/2000 p. 0001 - 0016.

2002[111], et au droit d'auteur[112]. L'Europe met également en place un Code des communications électroniques européen adopté par règlement[113] ainsi que le très attendu règlement sur les services numériques, le Digital Service Act[114], qui entrera en vigueur en 2024. En outre, la responsabilité des intermédiaires fait indirectement ou directement l'objet de nombreux actes de droit souple européen tel que des recommandations et des lignes directrices[115]. De par la nature des instruments principaux en la matière (directives devant être obligatoirement transposées et règlements faisant force de loi dans les États membres[116]) l'harmonisation des législations nationales est nettement plus satisfaisante s'agissant des règles relatives à l'engagement de la responsabilité des intermédiaires que des règles de fond et de formes régissant la poursuite et la répression de la cybercriminalité dont ils sont responsables.

⁂

Section 1. **Régime de responsabilisation pénale**

La « responsabilisation » n'est définitivement pas un terme dont on a l'habitude en sciences pénales, lesquelles sont systématiquement tournées vers la responsabilité pénale *stricto sensu* des auteurs. Il désigne pourtant l'un des deux mécanismes pouvant s'appliquer aux intermédiaires d'Internet. Il possède la double particularité de prévoir une exonération de responsabilité pénale (§1) dont les intermédiaires jouissent en échange du respect de quelques obligations mises à leur charge au titre de ce régime (§2).

[111] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) Journal officiel n° L 201 du 31/07/2002 p. 0037 - 0047.

[112] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

[113] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte).

[114] Règlement (UE) 2022/2065, op. cit.

[115] Recommandation CM/Rec(2018)2 op. cit. §12.

[116] Traité sur le fonctionnement de l'Union Européenne, art. 288.

§1. **Un régime exonératoire de responsabilité pénale**

44. Introduction d'un régime par contraste. – Le régime communément qualifié par l'ensemble de la doctrine de « responsabilisation pénale », renvoie à une série d'obligations pesant sur les intermédiaires, lesquelles engagent leur responsabilité au titre de manquements à ces obligations. En contrepartie, les intermédiaires « responsabilisés » jouissent d'une irresponsabilité pénale s'agissant des cyber infractions commises par leurs utilisateurs au moyen de leurs services. Un tel régime détonne alors drastiquement avec la potentielle complicité de l'intermédiaire des cyber infractions commises par ses utilisateurs, établie en vertu du régime de droit commun de la responsabilité pénale (V.53). C'est pourquoi il est dit que les deux régimes s'appliquent par contraste : les intermédiaires ne relèvent jamais simultanément du même régime, ils répondent soit des manquements aux obligations prévues par le régime de responsabilisation, soit du concours apporté à la commission de cyber infraction et puni au titre de la responsabilité pénale de droit commun. Ainsi, certains intermédiaires, spécialement nommés par la loi en vertu de leurs caractéristiques particulières, bénéficient du régime de responsabilisation pénale, qui prévoit leur irresponsabilité pénale, tandis que les autres relèvent du régime de responsabilité pénale de droit commun. Toutefois, lorsque les intermédiaires ne satisfont plus aux conditions d'exonération de responsabilité pénale prévue par leur régime de responsabilisation, ils ne sont plus soumis à celui-ci mais au droit commun de la responsabilité pénale. En cela, le régime de responsabilisation pénale est un régime exonératoire de responsabilité pénale. Comment justifier la distinction de régimes entre les intermédiaires pénalement responsables et les intermédiaires pénalement irresponsables mais pénalement responsabilisés ? Au centre de la *ratio legis*, on constate que c'est avant tout la volonté de soumettre certains intermédiaires à une interdiction de surveillance générale et proactive d'Internet qui explique la scission de régime car c'est en contrepartie de celle-ci qu'ils sont tenus pénalement irresponsables du contenu qu'ils n'ont pas le droit de surveiller et, en échange, répondent de certaines obligations. L'irresponsabilité pénale de ces intermédiaires, nous découvrirons lesquels, se fonde alors intégralement sur cette interdiction : *a contrario,* dès lors que l'intermédiaire n'y est pas soumis et est autorisé à exercer une telle surveillance, on retiendra sa responsabilité pénale. Il faut donc s'attacher à découvrir en premier lieu quelle est la substance d'une telle obligation.

45. Interdiction de la surveillance générale proactive d'Internet. – Dès la directive commerce électronique, l'Union Européenne a souhaité conserver le libéralisme économique et la liberté d'expression qui

font d'Internet une « zone neutre » en limitant d'une part les contraintes de responsabilité juridique à l'encontre des intermédiaires et d'autre part les atteintes aux droits des utilisateurs portées par le contrôle des intermédiaires sur leurs données et contenus. À ce titre, l'article 15 de la directive commerce électronique prohibe les États d'imposer toute « obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites », et nomme expressement les intermédiaires qui y sont soumis (V. 73). La même interdiction est reprise par la législation française en l'article 6.I-7 de la loi LCEN. Ainsi, en substance, aucune surveillance ou contrôle des données, exercé *a priori* d'un signalement, d'une demande ou d'une décision de justice, pour en différer le traitement n'est donc autorisé pour les intermédiaires concernés : c'est là le principe de « neutralité » qui leur est légalement imposé. L'interdiction ne semble agir que verticalement mais elle possède en réalité deux destinataires : d'une part elle s'adresse aux États qui ne peuvent obliger à une telle surveillance, d'autre part elle s'adresse aux intermédiaires, lesquels ne peuvent délibérément et arbitrairement l'exercer. La protection des utilisateurs agit bien ici tant horizontalement que verticalement. La Cour s'oppose donc « à une injonction faite à un fournisseur d'accès à Internet de mettre en place un système de filtrage de toutes les communications électroniques transitant par ses services » et qui « s'applique indistinctement à l'égard de toute sa clientèle, à titre préventif, à ses frais exclusifs et sans limitation de durée »[117]. Autrement dit, si la mise en place de filtrages généraux des données est systématiquement condamnée, l'Union Européenne laisse pour les États la possibilité d'enjoindre à des intermédiaires comme le fournisseur d'accès à Internet la mise en œuvre de filtrages plus ciblés et moins attentatoires[118]. L'absence de surveillance résultant de cette interdiction ne pourra donc logiquement engager la responsabilité des intermédiaires à raison d'une cyber infraction qui aurait été empêchée ou découverte par cette surveillance.

46. Libéralité du régime de responsabilisation. – Ainsi, le régime de responsabilisation est assurément plus libéral, et il faut comprendre par là léger pour son titulaire, qu'un régime de responsabilité pénale de droit commun exercé à l'encontre du complice : non seulement les obligations qui relèvent de ce régime, et dont on découvrira la substance (V. 47), ne brillent en effet pas par leur sévérité mais elles sont en outre prévues en creux de l'irresponsabilité pénale de l'intermédiaire concerné. Notons toutefois que lorsque l'on parle

[117] CJUE 24 novembre 2011, Affaire C-70/10, Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) ; CJUE 16 février 2012, Affaire C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contre Netlog NV.
[118] E. Derieux, op. cit., p. 626.

d'irresponsabilité pénale de l'intermédiaire au titre du régime de responsabilisation pénale, il n'est nullement question de présomption irréfragable d'irresponsabilité ou d'irresponsabilité pénale inconditionnelle : celle-ci possède assurément des limites (V. 64) qui, si elles sont franchies, engageront la responsabilité pénale de l'intermédiaire. Ainsi, les conditions d'engagement de leur responsabilité pénale diffèrent nettement selon que l'intermédiaire relève du régime de responsabilisation pénale ou du régime de responsabilité pénale de droit commun. C'est pourquoi, en raison d'une irresponsabilité tout de même plafonnée et des quelques obligations pesant en échange sur les intermédiaires responsabilisés, le titre de « responsabilité pénale atténué » ou « responsabilité pénale allégée » est parfois préféré en doctrine à celui de de responsabilisation pénale. Ces intitulés collent tous à la réalité du régime : la responsabilisation pénale est un régime exonératoire de responsabilité pénale duquel l'intermédiaire est exclu lorsqu'il ne remplit plus les conditions d'exonération, ce qui le fait alors tomber dans le régime de responsabilité pénale de droit commun. À ce titre, le régime de responsabilisation, s'appliquant par subsidiarité du régime de responsabilité pénale de droit commun, est convoité en raison de sa particulière libéralité, en particulier par les intermédiaires dont l'activité n'a pas été expressément nommée comme relevant d'un tel régime.

§2. **Un régime d'obligations incombant à l'intermédiaire**

47. Obligations à charge des intermédiaires irresponsables. – Appuyons-nous sur la présentation tripartite de l'auteur Frédérique Chopin afin de découvrir quelles obligations incombent à l'intermédiaire qui bénéficie d'un régime de responsabilisation pénale. La loi LCEN en prévoit trois à titre principal : le dispositif de signalement étendu, celui de filtrage du contenu et le dispositif de retrait, blocage et déréférencement de sites Internet. Sources de responsabilité pénale au titre de leurs manquements, elles font toutes de l'intermédiaire un allié dans la lutte contre la cybercriminalité des utilisateurs et interviennent en parallèle de leur indispensable collaboration à l'œuvre de la justice contre la cybercriminalité.

48. Le dispositif de signalement. – En premier lieu, l'intermédiaire responsabilisé a l'obligation de concourir à la lutte contre la « diffusion des infractions visées à l'article 24, alinéas 5, 7 et 8, de la loi du 29 juillet 1881 et aux articles 222-33, 225-4-1, 225-5, 225-6, 227-23, 227-24 et 421-2-5 du code pénal » prévoit l'article 6.I-7 alinéa 3 de la loi LCEN tandis que l'alinéa 5 étend son champ d'application à la répression des activités

illégales de jeux d'argent. Au titre de cette obligation, l'intermédiaire doit mettre en place un « dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données » précise l'alinéa 4. La justification d'une telle obligation réside dans la protection renforcée de l'intérêt général attaché à la répression des infractions précitées, telles que l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes en raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap, de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine. Ainsi, il a par exemple été ordonné à Twitter « de mettre en place dans le cadre de la plateforme française du service Twitter, un dispositif facilement accessible et visible permettant à toute personne de porter à sa connaissance des contenus illicites, tombant notamment sous le coup de l'apologie de crime contre l'humanité et de l'incitation à la haine raciale »[119]. Les intermédiaires ont également l'obligation d'informer promptement les autorités publiques (police et parquet) de l'existence de ces sites suite aux signalements reçus.

49. Le dispositif de filtrage. – En second lieu, conformément à l'article 6-I-1 de la LCEN, les intermédiaires responsabilisés ont l'obligation de mettre à disposition de leurs utilisateurs un moyen leur permettant de restreindre l'accès à certains services ou de les sélectionner et de les informer de l'existence de ces solutions techniques. Une telle obligation vise à leur garantir un niveau de contrôle sur les contenus et services accessibles par les mineurs, par le biais du filtrage de contenu. Les États doivent cependant rester vigilant à ne pas imposer la mise en place d'un dispositif qui s'apparenterait à de la surveillance générale proactive, car ceux-ci sont systématiquement mis en cause par la Cour de justice européenne : « l'exploitant d'un réseau social en ligne ne peut être contraint de mettre en place un système de filtrage général visant tous ses utilisateurs, pour prévenir le chargement illicite d'œuvres musicales et audiovisuelles » disait-elle à propos de Netlog [120]. Les critères permettant de distinguer le filtrage spécifique constitutif d'une obligation du filtrage général constitutif d'une interdiction sont généralement le caractère illimité et automatique des dispositifs mis en place par les intermédiaires : dès lors que le filtrage s'exerce de manière systématique sur l'intégralité du contenu dont il a connaissance[121], celui-ci est considéré comme général. L'article 6-I-1 de la LCEN respecte alors cette interdiction en ce que le filtrage n'est pas imposé par l'État, mais proposé facultativement aux utilisateurs ; il s'agit par

[119] Tribunal de Grande Instance de Paris, ord. de réf., 24 janvier 2013.
[120] CJUE, 3e ch., 16 févr. 2012, aff. C-360/10.
[121] CJUE 24 nov. 2011, aff. C-70/10, D. 2011. 2925, obs. Manara.

exemple du fameux « contrôle parental ». Cependant, il existe de nombreux moyens de contourner certaines de ces mesures *via* des outils de connexion anonyme tels que les VPN et les proxys, dont TOR fait partie.

50. Le retrait, blocage et déréférencement. – La troisième obligation incombant à l'intermédiaire responsabilisé relève de la collaboration étroite avec les autorités afin de mettre en œuvre les sanctions qu'elles souhaitent appliquer. Il en existe trois formes : le retrait, le blocage et le déréférencement. Prévu à l'article 6-1 de la loi LCEN, le retrait d'un contenu consiste en la demande faite aux intermédiaires par une autorité administrative, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), afin qu'ils suppriment certains contenus désignés contraires aux articles 421-2-5 et 227-23 du Code pénal. Une telle initiative paraît attentatoire aux droits des utilisateurs car elle revient à une autorité administrative et non judiciaire, laquelle est pourtant gardienne des libertés en vertu de l'article 66 de la Constitution. C'est pourquoi l'OCLCTIC ne peut la formuler qu'à la condition *sine qua none* que soit en cause la diffusion d'images ou de représentation de mineurs prohibées par l'article 227-23 du Code pénal ou la provocation et l'apologie des actes terroristes prohibées par 421-2-5 du Code pénal. Le retrait doit alors suivre un processus précis qui comprend l'affichage d'un message indiquant que le contenu illicite a été supprimé. En second lieu, l'obligation prévue à l'article 6-3 de la loi LCEN consiste en la mise en œuvre d'un blocage par adresse IP : les intermédiaires établissent une « liste noire » d'adresses IP de sites afin que toutes les demandes de connexions vers celle-ci soient bloquées. La demande de blocage provient également de l'OCLCTIC, saisie par « toute personne intéressée » après qu'une « décision judiciaire exécutoire a ordonné toute mesure propre à empêcher l'accès à un service de communication au public en ligne » lorsque le contenu relève des infractions réprimées aux articles précités. L'autorité administrative peut également contraindre les intermédiaires à bloquer des utilisateurs, en l'absence de toute décision judiciaire, à raison des mêmes contenus, en vertu de l'alinéa 2 de l'article 6-3. Enfin, la troisième obligation qui incombe aux intermédiaires responsabilisés est celle du déréférencement, prévue également à l'article 6-3 de la loi LCEN. Également connu sous le nom de « désindexation », le déférencement est le processus par lequel un site Internet est retiré des résultats des moteurs de recherche comme Google ou Yahoo. À nouveau, la demande adressée à l'intermédiaire se fait à l'initiative de l'OCLCTIC, laquelle peut également saisir l'autorité judiciaire à raison de contenus contrevenant aux articles 227-23 et 421-2-5 du Code pénal, en vertu de l'article 62 de la loi LCEN. Les trois obligations convergent donc en ce que l'initiative de leur demande appartient à une autorité administrative. Ainsi que le relève l'auteur Frédérique Chopin, un tel mécanisme porte en son sein l'écueil de ne garantir ni la présomption d'innocence ni

le contradictoire pour l'auteur d'un contenu qui n'a pas nécessairement fait l'objet d'une décision judiciaire établissant son illicéité. Pourtant, le Conseil d'État, dans son examen relatif aux décrets d'applications de la loi[122], affirme que les droits de la défense et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales « ne peuvent être utilement invoqués », tandis que la Conseil Constitutionnel considère, s'agissant du dispositif de blocage, qu'il « assure une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 »[123]. En tout état de cause, ces trois obligations ont une portée relativement médiocre car les utilisateurs possèdent aujourd'hui des moyens très simples pour dupliquer les contenus mis en cause à l'identique et à l'infini. Les contenus qui feront l'objet d'un blocage, d'un retrait ou d'un déréférencement pourront en ce sens être copiés, voire reproduits sur un autre support numérique, et être mis en ligne sur une nouvelle plateforme en bénéficiant d'une nouvelle adresse IP. L'ensemble de ces obligations voient alors leur intérêt être dépassé par les caractéristiques du système d'Internet. En revanche, elles offrent un aperçu très instructif de la cybercriminalité dont elle traite : les rapports annuels d'activité de l'OCLCTIC révèlent en effet qu'environ 90 % du contenu bloqué, retiré ou déréférencé est de la pornographie, et que le contenu à caractère terroriste a connu une baisse prodigieuse à partir de l'année 2018.

51. Obligations particulières. – Aux obligations générales du régime de responsabilisation que l'on vient d'étudier s'ajoutent depuis 2021[124] des obligations prévues à l'article 6-4 de la loi LCEN et dont le champ d'application est restreint aux « opérateurs de plateforme en ligne définis à l'article L.111-7 du code de la consommation qui proposent un service de communication au public en ligne reposant sur le classement, le référencement ou le partage de contenus mis en ligne par des tiers et dont l'activité sur le territoire français dépasse un seuil de nombre de connexions déterminé par décret, qu'ils soient ou non établis sur le territoire français ». Les opérateurs de plateformes en lignes mentionnés par l'article L.111-7 du Code de consommation sont ceux qui ont une activité de « classement » ou de « référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers » ou de « mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ». Sont donc concernés les moteurs de recherches et les sites et plateformes de

[122] Décr.n° 2015-125 du 5 févr. 2015 et Décr. n° 2015-253 du 4 mars 2015 relatif au blocage (1) et relatif au déréférencement (2) des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

[123] Cons. const. 10 mars 2011, n° 2011-625 DC

[124] Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, art. 42.I-2.

commerce électronique dont les places de marchés en ligne, les réseaux sociaux, les plateformes de partage en ligne de contenu de toute nature ainsi que tout service connexe mettant en relation des utilisateurs et des fournisseurs de biens ou de services. Par ailleurs, ils bénéficient pour la plupart du régime de responsabilisation pénale ou de responsabilité pénale atténuée. Le décret d'application[125] prévoit plus précisément que les intermédiaires concernés par les obligations du I de l'article 6-4 de la loi LCEN ont un seuil de visiteurs de dix millions par mois depuis le territoire français tandis que ceux concernés par les obligations prévues par le II du même article ont un seuil de visiteurs de quinze millions par mois depuis le territoire français. Les obligations de l'article 6-4 sont nombreuses ; ainsi, afin de rester concis, nous limiterons leur analyse. L'article 6-4.I 3° prévoit par exemple que les intermédiaires concernés doivent procéder à une mise à disposition au public de certaines informations, telles que les conditions générales d'utilisation, les procédés et moyens de modération du contenu ainsi que les recours internes et judiciaires dont disposent les utilisateurs pour mettre en cause du contenu présentant un caractère illicite et les mesures pouvant être prises à l'encontre de celui-ci. L'article 6-4.II 1° prévoit quant à lui que les intermédiaires concernés doivent procéder à une évaluation des « risques systémiques liés au fonctionnement et à l'utilisation de leurs services en matière de diffusion des contenus mentionnés audit premier alinéa et d'atteinte aux droits fondamentaux, notamment à la liberté d'expression ». Une simple lecture de l'article suffit quoi qu'il en soit pour constater que, malgré la quantité très importante d'obligations mises à charge de ces intermédiaires, aucune d'entre elles n'est réellement contraignante, bien que leur non-respect entraîne des sanctions pénales, notamment des amendes et des peines d'emprisonnement. Une obligation attire toutefois l'attention, l'article 6-4.I 1° c) relatif à la conservation de données de contenu « signalés comme contraires » aux dispositions précitées et aux dispositions relatives à l'injure raciale[126]. La jurisprudence européenne s'était effectivement opposée en premier lieu à ce qu'une obligation de conservation des données généralisée et indifférenciée soit prévue par les législations nationales au motif que la conservation de données constitue une trop grande ingérence dans la vie privée des intéressés[127]. La jurisprudence considère en effet qu'une telle conservation respecte la vie privée des individus si elle est matériellement limitée, tant dans les données, personnes et moyens de communications qu'elle vise, que dans la durée et le lieu de conservation des données (l'Union Européenne). En outre, il est traditionnellement exigé que l'accès des autorités publiques aux

[125] Décret n° 2022-32 du 14 janvier 2022 pris pour l'application de l'article 42 de la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République et relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne concourent à la lutte contre la diffusion publique des contenus illicites.

[126] Loi du 29 juillet 1881 sur la liberté de la presse, art. 33 alinéa 3 et 4.

[127] CJUE 21 déc. 2016, Tele2 Sverige, aff. C-203/15 et C-698/15, V. également F. Chopin, op. cit., p.217.

données soit lui-même conditionné, circonstancié, motivé, et contrôlé par une autorité indépendante. En 2018, la Cour de justice européenne a finalement retenu que « l'accès d'autorités publiques à des données à caractère personnel comporte une ingérence dans les droits fondamentaux, consacrés par la charte des droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave »[128]. L'article 6-4 rentre donc les prévisions européennes relatives à la conservation de données personnelles. Il est par ailleurs le prélude d'un renforcement imminent des obligations à la charge de l'ensemble des intermédiaires d'Internet.

52. Renforcement des obligations. – Récemment, certains instruments européens ont eu vocation à alourdir le régime d'obligations prévus pour les intermédiaires responsabilisés. Le renforcement du régime de responsabilisation tient de la volonté des législations d'être moins indulgent avec l'ensemble des intermédiaires, pénalement irresponsables ou non, en raison de l'amélioration des outils de lutte contre la cybercriminalité et de collaboration avec la justice dont ils disposent désormais. En effet, depuis vingt ans, les progrès techniques des intermédiaires ont été prodigieux : en 1980 le prix du stockage par gigaoctet avoisinait les 440 000 dollars américains alors qu'en 2020 il se situait aux alentours de 0,02 à 0,03 dollar pour les disques durs, et environ 0,15 à 0,25 dollar pour les SSD (Solid State Drives). L'intelligence artificielle permet quant à elle une détection du contenu illicite bien plus précise et est constamment sollicitée à différentes fins par les intermédiaires, qu'ils exercent une surveillance générale proactive de leur contenu ou non. Les législations nationales mettent alors en avant ces avancées pour alourdir la responsabilité des intermédiaires, à l'inclusion des obligations qui leur incombent au titre du régime de responsabilisation pénale. Cependant, si la performance des outils à disposition des intermédiaires a indiscutablement augmenté, le volume de données dont ils traitent a également décollé depuis. En effet, si en 1991 il n'existe qu'un seul site Internet, le site de l'Organisation européenne pour la recherche nucléaire (CERN) créé par Tim Berners-Lee, l'inventeur du World Wide Web (WWW), en 2000 on comptabilise déjà 17 millions de sites Internet tandis qu'en 2020 il en existe entre 1,7 à 1,8 milliard. Les supports numériques sur lesquels peuvent se loger du contenu illicite qui matérialise la commission d'une cyber infraction ont également considérablement augmenté avec l'arrivée de l'Internet 2.0 et résistent aux intelligences artificielles. Par exemple, celles-ci n'ont pas pu détecter la fusillade de Christchurch en Nouvelle Zélande, diffusée en direct sur le service Facebook Live du réseau social en 2019 et reproduite en 1,5 millions d'exemplaires que Facebook a tenté de supprimer. Bref, les outils sont meilleurs mais la tâche est réalistiquement

[128] CJUE 2 oct. 2018, Ministerio Fiscal, aff. C-207/16 , V. également F. Chopin, op. cit., p.218.

loin d'être radicalement plus aisée, contrairement à ce que certains auteurs de doctrine soutiennent ardemment. Le régime a, quoi qu'il en soit, été alourdi, en premier lieu en raison de l'introduction en 2021 de l'article 6-4 de la loi LCEN que l'on connaît, et qui a nettement augmenté le nombre d'obligations à la charge d'intermédiaires dépassant un certain seuil d'utilisateurs. La démarche de l'article 6-4 de la loi LCEN est inspirée d'une méthode de régulation déjà appliquée par le droit européen[129] : faire des intermédiaires concernés des prescripteurs de cybercriminalité, en leur imposant l'élaboration de normes tout en leur « laissant une latitude dans la détermination de leur contenu pour permettre le traitement de situations particulières »[130]. En outre, le règlement relatif à un marché unique des services numériques, le *Digital Service Act* (DSA)[131], dont l'entrée en vigueur est prévue pour 2024, intervient pour alourdir davantage les obligations à la charge des intermédiaires, accompagné du règlement dit *Platform to business* de 2019[132] et du règlement sur les marchés numériques, le *Digital Market Act* (DMA)[133]. Sans faire rupture avec le régime de responsabilisation prévu pour certains intermédiaires, il prévoit une série d'obligations particulièrement nombreuses, finalement de la même trempe que celles de l'article 6-4 de la loi LCEN. Certaines se démarquent toutefois : par exemple, le DSA rend obligatoire la modération après signalement, pour ceux qui ne peuvent l'exercer *a priori*, et laisse une marge de manœuvre pour les intermédiaires dans la mise en place des sanctions à l'issue des résultats de cette modération, afin qu'ils concourent efficacement mais de façon autonome à la lutte contre la cybercriminalité. Le texte impose également la désignation de correspondants, des autorités compétentes spécifiquement désignées, pour veiller à la mise en œuvre des dispositions européennes, autrement dit pour exécuter les sanctions pesant sur les intermédiaires en cas de manquements. En France, il s'agit de l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), née de la fusion entre le Conseil supérieur de l'audiovisuel (CSA) et la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), qui détient à la fois un pouvoir d'injonction et de sanction. Le considérant 5 du DSA souligne la part de responsabilité irréfutable des intermédiaires dans la cybercriminalité d'aujourd'hui « la croissance exponentielle du recours à ces services, principalement à des fins légitimes et socialement bénéfiques de toute nature, a également accru leur

[129] Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.
[130] G. Loiseau, Plateforme en ligne - Dissémination de contenus illicites : la pression monte vis-à-vis des opérateurs numériques, Com. comm. électr. n° 10, Octobre 2021, comm. 72, p.3.
[131] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[132] Règlement (UE) 2019/1150 op. cit.
[133] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828.

rôle dans l'intermédiation et diffusion d'informations, d'activités illégales ou susceptibles de nuire ». Alors, pour reprendre la formule de l'auteur Grégoire Loiseau, c'est non pas dans un esprit de responsabilité alourdie mais de conformité interne, la *compliance*, que le législateur désire voir l'intermédiaire s'exécuter. L'ensemble du texte est en ce sens partagé entre une réglementation au caractère prescriptif et de régulation au caractère incitatif, bien que la réglementation y soit dominante. Si la revalorisation des obligations à la charge des intermédiaires a un intérêt relatif en raison de l'avance prise par la législation française, le texte contient d'autres apports particulièrement pertinents et attendus, telle que l'extension du champ d'application de l'interdiction de surveillance générale proactive et donc du champ d'application du régime exonératoire de responsabilité, ou responsabilisation pénale.

Subsidiairement au régime de responsabilisation, s'applique le régime de responsabilité pénale de droit commun, lorsque l'intermédiaire ne relève pas des catégories d'intermédiaires légalement exonérées de responsabilité ou qu'ils en relèvent mais n'ont pas respecté leurs conditions d'exonération. On le verra, l'application du droit commun de la responsabilité pénale aux intermédiaires d'Internet rencontre quelques difficultés dès lors qu'est en cause la commission d'une cyber infraction par son utilisateur.

***

Section 2. **Régime de responsabilité pénale**

Le régime de responsabilité pénale de l'intermédiaire, lorsqu'il vient à s'appliquer, n'est autre qu'un régime classique de complicité, dont la mise en œuvre n'est pas systématiquement aisée (§1). Pour cette raison, les législations se sont attachées à le développer lorsque la cyber infraction se manifeste tangiblement pour l'intermédiaire, notamment par un contenu intrinsèquement illicite (§2).

§1. **Un régime de complicité des cyber infractions**

53. Complicité des intermédiaires. – La responsabilité des intermédiaires, on le sait, diffère selon le régime dont il relève : soit ils sont pénalement responsables du concours apporté aux cyber infractions commises par leurs utilisateurs, soit ils en sont pénalement irresponsables et sont en contrepartie responsabilisés au titre d'obligations dont le manquement est pénalement sanctionné. On le sait aussi, l'irresponsabilité de l'intermédiaire responsabilisé connaît des limites qui, si elles ne sont pas respectées, engendrent la responsabilité pénale de l'intermédiaire en ce qu'il ne répond plus aux conditions le faisant relever du régime d'exonération de responsabilité pénale, aussi appelé responsabilisation. Le droit commun de la responsabilité pénale s'applique donc à l'ensemble des intermédiaires mais pour différentes raisons, soit parce qu'ils ne relèvent pas du régime de responsabilisation pénale, soit parce qu'ils n'ont pas respecté les conditions d'exonération à celle-ci prévue par le régime de responsabilisation pénale. On constate donc que les deux régimes, en passant par des chemins différents, peuvent *in fine* résulter en de la responsabilité pénale pour les intermédiaires. Nonobstant de conditions d'engagement divergentes d'un régime à l'autre, la responsabilité pénale des intermédiaires s'exerce au titre de la complicité des intermédiaires des cyber infractions commises par les utilisateurs, complicité prévue à l'article 121-7 du droit pénal.

54. Conditions de complicité. – Par conséquent, toutes les règles relatives à la complicité s'appliquent à l'intermédiaire pénalement responsable au titre du régime du droit commun. À cet égard, le régime de complicité paraît tant inadapté que difficile à mettre en œuvre. Ainsi que le rappelle l'auteur Jacques-Henri Robert, la complicité est « un mode d'imputation appliqué à une personne qui a participé à la réalisation d'une situation infractionnelle sans pour autant accomplir matériellement aucun des actes décrits par le texte d'incrimination »[134]. La complicité requiert naturellement un élément matériel, l'aide ou l'assistance, qu'elle soit matérielle ou intellectuelle, mais aussi la provocation et un élément moral. Si l'élément matériel ne pose que peu de difficulté en ce que la nature même des cyber infractions implique que leur mode de commission et/ou leurs éléments constitutifs implique l'utilisation de services d'intermédiaires d'Internet, lesquels concourent donc *de facto* à la commission de la cyber infraction (V. 25), l'élément moral de la complicité des ces derniers semble plus difficile à établir. Dans un premier temps, l'élément moral du complice est autonome et se distingue de l'élément moral de l'auteur principal puisque « l'intention du complice ne se rapporte pas au résultat de l'infraction

[134] J.-H. Robert, Complicité, JurisClasseur Droit pénal, Fasc. 20, 30 septembre 2022.

principale mais seulement au comportement de son auteur »[135], raison pour laquelle une complicité peut être intentionnelle alors que l'acte principal ne l'était pas. Ainsi, lorsque la responsabilité pénale de l'intermédiaire est engagée, il doit être établi que celui-ci a eu la conscience et la volonté du concours qu'il apporte à l'auteur. Le complice doit logiquement avoir eu une telle intention *a priori* ou simultanément à son concours. Pourtant, sans révéler encore l'entièreté des tenants et aboutissants des conditions d'engagement de la responsabilité pénale des intermédiaires responsabilisés, on constate qu'une telle exigence n'est pas nécessairement respectée par la mise en œuvre de leur complicité. En effet, lorsque la responsabilité pénale de l'intermédiaire responsabilisé est retenue au titre de sa complicité en raison de son inertie face au contenu illicite de l'utilisateur (V. 53), on s'interroge légitimement : l'inertie de l'intermédiaire n'intervient qu'*a posteriori* de la mise en ligne du contenu illicite, or l'élément moral accompagnant son concours doit en théorie y être postérieur ou concomitant. Le défaut d'élément intentionnel est d'autant plus palpable que la jurisprudence qualifie certains délits de presse, dont les intermédiaires sont également responsables (V. 57), tels que la diffamation, l'injure, le négationnisme et certaines formes d'apologie de délits instantannés et non d'infractions continues « qui auraient supposé la réitération constante de la volonté coupable de l'auteur après l'acte initial »[136]. Comment l'élément moral de la complicité de l'intermédiaire pourrait-elle en ce sens intervenir postérieurement à de telles diffusions sans enfreindre les principes mêmes de la complicité ? Dans cette logique la loi LCEN avait proposé un report du *dies a quo* de la prescription des infractions de presse, prévu à l'article 65 de la loi du 29 juillet 1881, mais la disposition fût censurée par le Conseil constitutionnel[137]. Lorsque l'intermédiaire est soumis au régime de droit commun de responsabilité pénale et non de responsabilisation, l'existence de son intention au concours de la cyber infraction commise par l'utilisateur semble quant à elle difficile à établir pour les cyber infractions qui ne supposent pas de diffusion de contenus illicites. Une innovation et un changement de paradigme pour le titre de culpabilité de l'intermédiaire pénalement responsable des cyber infractions commises par ses utilisateurs ne seraient-ils pas en ce sens souhaitables ? Car, s'il est matériellement parlant un complice, l'est-t-il véritablement moralement parlant ? On pourrait tenter de sortir des mécanismes du droit commun en matière de titre de culpabilité pour en imaginer un plus adapté aux particularités de l'Internet et de ses intermédiaires : un titre de culpabilité moins exigeant en élément intentionnel que le régime de complicité et à cet égard moins sévère s'agissant de la peine. Son application serait peut-être plus systématique et effective en contrepartie.

[135] F. Rousseau, Complice ou auteur indirect d'une infraction non intentionnelle, Dr. pén. 2007, étude 11. – I. Moine-Dupuis, Complicité et contribution à une infraction nonintentionnelle, RPDP 2005.
[136] J. Bossan, op. cit. p. 213.
[137] Cons. constit., Loi pour la confiance dans l'économie numérique, décision n° 2004-496 DC du 10 juin 2004.

55. Approche des cyber infractions. – Pour pallier à un tel écueil, le législateur aurait pu construire différemment le régime de culpabilité et délaisser l'approche horizontale, ou transversale, consacrée par le législateur. Cette approche consiste à « envisager le sujet globalement, dans son ensemble, pour tous les contenus illicites »[138], autrement dit à appréhender la responsabilité des intermédiaires d'Internet de façon identique, quelque soit la cyber infraction en cause. Une autre approche, sectorielle et verticale aurait permis, selon l'auteur Laure Marino de « régler chaque question de façon spécifique, afin de tenir compte des particularités de chaque domaine concerné »[139]. Elle aurait permis de faire différer le régime, et notamment ses conditions d'engagement, selon la matérialité et la spécificités des infractions en cause car : « Quoi qu'on dise, ce n'est pas la même chose de pourchasser les pédophiles, racistes ou négationnistes et de faire respecter la propriété intellectuelle en général et le droit d'auteur en particulier... »[140]. Sans avoir totalement mis en place une approche sectorielle des cyber infractions qui aurait fait divergé les conditions d'engagement de la responsabilité de l'intermédiaire d'une infraction à l'autre, le législateur a compris que certaines d'entre elles devaient bénéficier d'une plus grande attention dans la loi, car elles se manifestent mieux pour l'intermédiaire : il s'agit des cyber infractions qui se manifestent par un contenu intrinsèquement illicite.

§2. **Un régime centré autour de la diffusion de contenus illicites**

56. Conséquence du défaut d'intention. – Il est entendu que les intermédiaires d'Internet ne peuvent répondre par leur complicité de l'entièreté des infractions commises par l'utilisation d'un réseau Internet, pour la raison que l'on vient d'exposer qui tient du défaut d'élément intentionnel de l'intermédiaire. Un tel défaut est en effet ostensible lorsque la cyber infraction en cause ne s'est pas tangiblement manifestée pour l'intermédiaire. Ainsi, seul un champ restreint de cyber infraction peut logiquement engager la responsabilité pénale de l'intermédiaire au titre d'une complicité. Par exemple, l'abus de confiance qui consiste au détournement à des fins personnelles, telles que la consultation de sites pornographiques, d'une connexion Internet remise à titre professionnel, ne se manifeste pas tangiblement pour l'intermédiaire puisque ce dernier ne peut avoir connaissance de l'existence du détournement de la connexion et *a fortiori* du caractère illicite et préjudiciable du détournement. Il serait alors impensable de faire de la plateforme de contenus pornographiques un complice de

[138] L. Marino, op. cit., p.3.
[139] Ibid.
[140] A. Lucas, H.-J. Lucas et A. Lucas-Scholetter, Traité de la propriété littéraire et artistique : LexisNexis, 4e éd. 2012, n° 1109, p. 904.

ce détournement. L'existence de la cyber infraction doit alors nécessairement se manifester pour l'intermédiaire, sans quoi son élément intentionnel ne peut logiquement être établi. Les cyber infractions deviennent visibles pour les intermédiaires notamment lorsqu'elles répriment une diffusion (par exemple d'images pédopornographiques), une mise en ligne, une publication, ou simplement le fait de rendre disponible l'objet délictuel (par exemple le débit d'une œuvre contrefaite), de toute nature (échange de messages, audio, vidéo, transfert d'informations ou de biens, transaction de toute nature, émission de signaux ou signes). Au fond, elles se manifestent tangiblement pour l'intermédiaire lorsque le réseau et système d'Internet en constitue le support, pour reprendre la tripartie des cyber infractions de l'auteur Frédérique Chopin. Dès lors que la cyber infraction est en ce sens ostensible pour l'intermédiaire, l'examen de son élément intentionnel au titre de sa complicité fait sens. Ainsi, toutes les cyber infractions qui répriment la diffusion d'un contenu déterminé vont faire l'objet d'une attention particulière et de dispositions spéciales s'agissant de la responsabilité des intermédiaires dont les services concourent à leur commission. Particulièrement, les cyber infractions dite « de presse » et les cyber infractions protégeant le droit d'auteur sont au cœur du régime de responsabilité pénale de l'intermédiaire.

57. Cyber infractions de presse. - Avant même l'arrivée de la loi LCEN, la Cour de cassation avait eu la présence d'esprit d'appliquer le régime d'infractions dite de presse, provenant de la loi de 1881 sur la liberté de la presse et 1892 sur la communication audiovisuelle aux services de communication au public en ligne[141]. Comme on le sait, la loi reprend certaines des infractions de presse comme fondement des obligations des intermédiaires exonérés de responsabilité pénale. La loi LCEN en étend également le champ d'application puisque son article 6.V prévoit que « les dispositions des chapitres IV et V de la loi du 29 juillet 1881 précitée sont applicables aux services de communication au public en ligne et la prescription acquise dans les conditions prévues par l'article 65 de ladite loi », les chapitres mentionnés étant ceux des infractions commises par voie de presse ou par tout autre moyen de publication et leur mécanisme de répression. Ainsi, les trois mois de prescription et la responsabilité en cascade des auteurs viennent à s'appliquer aux intermédiaires complices. En raison de ce mécanisme en cascade, la responsabilité de l'intermédiaire gérant le service de communication au public peut être retenu de différentes façons car, s'il qualifie au titre de complice de l'auteur de l'infraction de presse, il peut également prétendre au titre de producteur, dont la responsabilité s'applique à défaut de celle de l'auteur. En effet, si la notion de producteur de communication au public en ligne n'a pas été explicitement définie par la loi, la doctrine rapproche à juste titre cette notion du producteur d'œuvre audiovisuelle définie par le Code de

[141] Crim. 6 mai 2003, no 02-81.587 , D. 2003. 2192, note Dreyer.

propriété intellectuelle (« la personne physique ou morale qui prend l'initiative et la responsabilité de la réalisation de l'œuvre »)[142], bien qu'elle ne soit pas toujours adaptée au contenu litigieux. En sus, la jurisprudence avait, dès 1998 pour le minitel, considéré que le producteur de service de communication au public consistait en la personne qui prend l'initiative de créer un service de communication au public par voie électronique, notamment « en vue d'échanger des opinions sur des thèmes définis à l'avance »[143]. La même définition est reprise pour l'intermédiaire producteur du service de communication en ligne et l'application de la responsabilité en cascade de celui-ci s'est ensuite constamment confirmée en jurisprudence[144]. Ainsi, de l'identification de l'auteur de la cyber infraction dépend le régime applicable de l'intermédiaire : lorsqu'elle est établie, l'intermédiaire est responsable en tant que complice de la commission d'une cyber infraction de presse mais, lorsqu'elle ne l'est pas, il est pénalement responsable, à titre personnel, de sa commission d'une cyber infraction de presse. Les deux hypothèses, subsidiaires et différentes en tout point, s'appliquent pourtant à une même situation.

58. Terrorisme et pédopornographie. – Les contenus à caractère terroriste et pédopornographique font en droit interne l'objet d'incriminations au titre des infractions commises par voie de presse ou par tout autre moyen de publication, dont on a pris connaissance, mais sont également au centre d'instruments européens qui les protègent spécialement et incitent les États à prévoir la responsabilité pénale des intermédiaires à raison de tels contenus. Il s'agit par exemple du règlement du 29 avril 2021 relatif à la lutte contre la diffusion de contenus à caractère terroriste[145] et, plus récemment, de la proposition de règlement du 11 mai 2022 en vue de prévenir et de combattre les abus sexuels sur enfants[146]. Cette dernière prévoit en effet dans son chapitre IV l'établissement d'un Centre de l'Union Européenne en soutien à la lutte contre les contenus pédopornographiques en ligne ainsi qu'un renforcement d'obligations pour les intermédiaires responsabilisés dans son chapitre II et III, par exemple par la mise en place d'un dispositif d'évaluation des risques liés à « l'utilisation à mauvais escient de leurs services aux fins de la diffusion de matériel connu ou nouveau relatif à

[142] CPI, art. 132-23.

[143]Cass. crim., 8 déc. 1998, n° 97-83.709 : JurisData n° 1998-005123 ; Bull. crim. n° 335 ; Rev. sc. crim. 1999, p. 607, obs. J. Francillon ; JCP G 1999, II, 10135, note J.-Y. Lassalle.

[144] Cass. crim., 15 sept. 2020, n° 19-82.124 et 19-82.125, QPC : JurisData n° 2020-014488 et 2020-017847 ; Dr. pén. 2020, comm. 207, obs. Ph. Conte ; D. 2021, p. 201-202, n° 11, obs. E. Dreyer ; Légipresse 2020, p. 536. – Cass. crim., 6 mai 2003, n° 02-81.587 : D. 2003, p. 2192, note E. Dreyer ; Comm. com. électr. 2003, comm. 89, obs. A. Lepage.

[145] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

[146] Proposition de Règlement (UE) 2022/0155 du Parlement européen et du Conseil du 11 mai 2022 établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, COM/2022/209 final.

des abus sexuels sur enfants ou de la sollicitation d'enfants », par la mise en œuvre de « mesures adaptées et proportionnées afin d'atténuer les risques recensés, ou par du filtrage proactif en principe spécifique et des mesures de retrait ou rendant l'accès au contenu impossible, le tout déclenché par injonction ».

59. Contrefaçon. – Également, la diffusion de contenus illicites mettant en cause le droit d'auteur fait l'objet de dispositions spéciales. En ce sens, la directive relative au droit d'auteur et les droits voisins dans le marché unique numérique[147], transposée en France par l'ordonnance du 12 mai 2021[148], écarte expressément du régime d'exonération de responsabilité, ou responsabilisation pénale, les « services de communication au public en ligne dont l'objectif principal ou l'un des objectifs principaux est de stocker et de donner au public accès à une quantité importante d'œuvres ou d'autres objets protégés téléversés par ses utilisateurs ». Il s'agit ici de leur responsabilité pénale au titre de la mise en ligne de contenus par des utilisateurs qui ne sont pas autorisés à les mettre à disposition du public en raison du droit d'auteur[149]. Ainsi, les plateformes multimédia telles que les plateformes de partage de vidéos, comme YouTube ou Dailymotion, sont concernées et ne peuvent par conséquent bénéficier du régime de responsabilisation lorsqu'est en cause du contenu protégé par le droit d'auteur qui engage leur responsabilité pénale ; la jurisprudence européenne l'a ainsi reconnu[150].

La présentation globale des régimes applicables à l'intermédiaire, bien que nécessaire, ne permet pas de cerner la réalité complexe de sa responsabilité pénale. Comment les régimes s'articulent-ils ? Quels intermédiaires y sont soumis ? Étudions dans un second temps de notre étude l'épineuse mise en œuvre des régimes de responsabilité pénale, atténués ou de droit commun, afin de saisir tout l'enjeu qu'elle représente pour les intermédiaires.

[147] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE

[148] Ordonnance n° 2021-580 du 12 mai 2021 portant transposition du 6 de l'article 2 et des articles 17 à 23 de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE

[149] G. Loiseau, Hébergeur - La responsabilité des plateformes de partage de vidéos, Com. comm. électr. n° 9, Septembre 2021, comm. 62

[150] CJUE, gde ch., 22 juin 2021, aff. C-682/18, M. X c/ Google et YouTube, et aff. C-683/18, Elsevier Inc. c/ Cyando AG, V. également CJUE, gde ch., 26 avr. 2022, aff. C-401/19, Pologne c/ Parlement et Conseil

PARTIE SECONDE

LA MISE EN OEUVRE DE LA RESPONSABILITÉ PÉNALE DES INTERMÉDIAIRES D'INTERNET

La mise en œuvre de la responsabilité pénale de l'intermédiaire repose essentiellement sur la détermination du régime applicable, entre responsabilisation pénale et responsabilité pénale de droit commun. Naturellement, l'applicabilité du régime vient se coller au degré d'implication de l'intermédiaire dans la cybercriminalité de l'utilisateur, autrement dit le concours par commission ou omission qu'il apporte à l'utilisateur qui commet la cyber infraction. Un tel concours est déterminé par la neutralité de l'intermédiaire dans la conduite de son activité (Chapitre 1). La neutralité de l'intermédiaire n'est néanmoins pas librement établie ; elle est au contraire légalement définie et encadrée puisque certaines activités d'intermédiaires relèvent expressément de l'un ou de l'autre régime à raison de celle-ci. L'identification de l'activité de l'intermédiaire devient alors un fort enjeu de contentieux (Chapitre 2).

Chapitre 1

LA NEUTRALITÉ DE L'INTERMÉDIAIRE, PIERRE ANGULAIRE DE SA RESPONSABILITÉ PÉNALE

De la même manière que la responsabilisation pénale de l'intermédiaire d'Internet est justifiée par la neutralité qu'il possède lorsqu'il conduit son activité, sa responsabilité pénale de droit commun est justifiée par la limite ou l'absence de cette neutralité. Celle-ci constitue en ce sens l'*alpha* et l'*omega* de la responsabilité de l'intermédiaire.

Ainsi, lorsque l'intermédiaire est neutre, il est exonéré de responsabilité pénale (Section 1). En revanche, lorsqu'il a l'obligation de sortir de sa neutralité, celle-ci possédant des limites, et que l'intermédiaire ne s'y plie pas, ce dernier voit sa responsabilité pénale de droit commun se substituer à son régime d'exonération (Section 2). En outre, l'intermédiaire sera pénalement responsable si *ab initio* il ne présentait pas de neutralité dans la conduite de son activité (Section 3).

Section 1. **Neutralité et irresponsabilité pénale**

La neutralité de l'intermédiaire d'Internet s'entend non pas comme une neutralité dans la commission de la cyber infraction mais comme une neutralité dans la conduite de son activité (§1). Lorsqu'est examinée la responsabilité de l'intermédiaire en cas de commission d'une cyber infraction par un utilisateur, sa neutralité agit alors comme une cause d'irresponsabilité pénale qui justifie l'appartenance de l'intermédiaire neutre au régime exonératoire de responsabilité (§2).

§1. **La neutralité de l'intermédiaire dans la conduite de son activité**

60. La neutralité dans la conduite de l'activité. – La neutralité des intermédiaires a été affirmée tant en droit européen qu'en droit français en tant que source de leur irresponsabilité pénale. *A fortiori,* la notion même d'intermédiaire d'Internet a été construite originellement autour de sa neutralité dans la conduite de son activité puisque le droit européen en avait fait une composante de sa définition. En quoi consiste-t-elle ? Dans la proposition de loi relative à la neutralité de l'Internet[151] de 2010, le législateur français avait prévu de définir la neutralité des intermédiaires comme étant « l'interdiction de discriminations liées aux contenus, aux émetteurs ou aux destinataires des échanges numériques de données ». Le même raisonnement se retrouve dans les règlements européens[152] et dans la loi du 7 octobre 2016 pour une République numérique qui définissent ainsi le principe de neutralité et l'imposent à certains intermédiaires tels que le FAI. La directive commerce

[151] J.-M. Ayrault et a., Proposition de loi relative à la neutralité de l'Internet : AN, prop. de loi n° 3061, 20 déc. 2010.

[152] Règlement (UE) n°2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un Internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

électronique prévoit, quant à elle, en mentionnant les intermédiaires neutres, que leur activité « revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées » dans son considérant 42, formule reprise par la jurisprudence[153]. La neutralité de l'intermédiaire suppose donc que l'intermédiaire participe à la mise à disposition de contenu Internet sans exercer de contrôle *a priori* de cette mise à disposition, autrement dit sans filtrer, sans faire transiter certains flux plus rapidement ou sans bloquer arbitrairement l'accès au contenu pour des utilisateurs[154].

61. Principe de neutralité. – La neutralité de l'intermédiaire est constitutive d'un principe lorsqu'elle est imposée par la loi pour une catégorie définie d'intermédiaire au titre d'une interdiction de surveiller proactivement et de manière générale les données (V. 45). Pour ceux-là, c'est parce que le législateur leur interdit une telle surveillance et un tel contrôle qu'ils sont logiquement définis comme neutres et bénéficient d'un régime de responsabilité conforme à cette neutralité imposée. Toutefois, la neutralité peut également être librement exercée par les intermédiaires qui ne seraient pas expressément concernés par la loi. Lorsque c'est le cas, la neutralité de l'intermédiaire devient un enjeu déterminant de son régime applicable et de leur responsabilité, puisqu'en démontrant une telle neutralité il peut bénéficier du même régime allégé de responsabilité que les intermédiaires neutres expressément visés par la loi (V. 73). En tout état de cause, qu'elle soit librement pratiquée ou imposée légalement aux intermédiaires, leur neutralité ne signifie pas qu'ils n'ont pas la capacité de pouvoir prendre connaissance des données dont ils traitent et de conduire leur activité de façon discriminatoire – car ils la possèdent toujours pleinement – seulement, elle leur impose de renoncer à en user. En conséquence, s'agissant de la responsabilité des intermédiaires, la neutralité signifie l'absence de connaissance de l'infraction auquel ils apportent un concours malgré eux et donc l'absence d'élément moral, ce pourquoi on les en exonère. Autrement dit, c'est parce que l'intermédiaire exerce son activité avec neutralité qu'il n'est pas censé prendre connaissance du fait qu'une cyber infraction est commise à travers son service et donc qu'il ne présente pas d'élément moral, quand bien même il participe de fait à la commission de ladite infraction. À cet égard, certains auteurs, tels qu'Emmanuel Dérieux, ont souligné le caractère partisan de la neutralité de l'intermédiaire dans la mesure où, si elle est une source admise d'irresponsabilité pénale, ceux qui souhaitent exempter les intermédiaires de

[153] CJUE, Cour, 15 sept. 2016, C-484/14. Lire en ligne : https://www.doctrine.fr/d/CJUE/2016/CJUE62014CJ0484.
[154] D. Legall, La responsabilité pénale des acteurs de l'Internet, Fiches pratiques LexisNexis N° 4496, p.5.

responsabilité pénale pour laisser Internet être librement régulé par les lois du marché la brandissent comme argument et souhaitent l'étendre à toutes les catégories d'intermédiaires.

§2. **Une neutralité cause d'irresponsabilité pénale**

62. Irresponsabilité pénale des intermédiaires. – La neutralité des intermédiaires dans la commission de la cyber infraction est l'élément qui le fait échapper au régime de responsabilité pénale de droit commun, et donc au titre de complice d'une cyber infraction, pour le faire relever du régime de responsabilisation. Elle est « l'*alpha* et l'*oméga* de la question, à la fois fondement de l'irresponsabilité pénale des différents acteurs, mais aussi la limite de celle-ci » l'affirme l'auteur Jérôme Bossan[155]. Si elle n'a jamais été expressément qualifiée de telle, la neutralité des intermédiaires s'apparente en tout point à une cause d'irresponsabilité pénale. Les causes d'irresponsabilité pénale, qui existent traditionnellement aux articles 122-1 à 122-3 du Code pénal, agissent en neutralisant l'existence de l'élément moral d'une infraction, et se distinguent ainsi des faits justificatifs qui viennent, sans en nier l'existence, justifier l'élément moral – *ratione personae* – ou légal – *ratione materiae* – d'une infraction en leur enlevant tout caractère illicite[156]. Ici, si la neutralité implique l'ignorance de la commission de la cyber infraction, c'est donc qu'elle neutralise bien l'élément moral du concours apporté par l'intermédiaire aux cyber infractions, non pas dans son caractère illicite mais dans son existence même. En conséquence du défaut d'élément moral de l'intermédiaire, la neutralité dans la conduite de son activité l'exonère de toute responsabilité pénale, c'est ce qu'à prévu l'article 6.I-2 et 6.I-3. L'article 6.I-7 de la loi LCEN, dispose en outre que ces intermédiaires ne peuvent être considérés comme des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, et donc ne peuvent être considérés pour le mécanisme en cascade de responsabilité pénale au titre du régime spécial des infractions commises au moyen d'un service de communication au public par voie électronique.

63. Rupture avec les solutions antérieures. – La neutralité de l'intermédiaire est une innovation des années 2000, apportée expressément par la directive commerce électronique en Europe et la loi LCEN en

[155] J. Bossan, op. cit., p. 299.

[156] V. C. pén., art. 122-4 à 122-9, V. également CEDH, 14 mars 2013, Eon c. France Requête n° 26118/10, CEDH, 13 octobre 2022, Bouton c. France Requête n° 22636/19, Cass. crim., 13 déc. 2022, n° 22-82.189, JurisData n° 2022-021519, Cass. crim., 26 oct. 2016, n° 15-83.774 : JurisData n° 2016-022303 ; Bull. crim. n° 278, Cass. crim., 11 mai 2004, n° 03-85.521 : JurisData n° 2004-023992 ; Bull. crim., n° 117.

France. En effet, avant une célèbre affaire de paparazzade datant de 1999, aucune responsabilité pénale n'était admise par les juges pour les intermédiaires qui faisaient souvent l'objet de contentieux relatifs au contenu hébergé[157]. Par un revirement du 10 février 1999[158], à l'occasion d'un litige opposant Valentin L à la mannequin Estelle H, dont il est l'hébergeur de photos de nu, les juges français ont pu admettre que la seule capacité des intermédiaires à contrôler les données afin d'en faire différer le traitement suffisait à engager leur responsabilité, bien qu'il était établi dans les faits qu'une telle capacité n'était pas effectivement exercée par les intermédiaires. Autrement dit, les juges français considéraient à l'époque que, dès lors qu'un contrôle effectif des données traitées et du contenu pouvait être exercé par les intermédiaires, ils étaient soumis à un devoir de vigilance et une obligation de prudence de vérification des contenus qui pouvait engager leur responsabilité, et ce malgré leur neutralité apparente en l'espèce[159]. La loi LCEN, à l'instar de la directive commerce électronique qu'elle transpose, est venue mettre un terme à cette jurisprudence en affirmant l'irresponsabilité pénale des intermédiaires neutres et en les nommant. L'obligation de prudence et de vigilance des contenus se retrouve toutefois dans les limites de la responsabilisation pénale (V. 64) et dans le mécanisme subsidiaire de responsabilité pénale. La neutralité de l'intermédiaire d'Internet est donc, à ce jour, le point pivot de son régime applicable et de sa responsabilité pénale.

La neutralité de l'intermédiaire d'Internet n'a pas vocation à être absolue, elle est au contraire limitée. En ce sens, le législateur exige parfois de l'intermédiaire qu'il sorte de sa neutralité pour faire obstacle à la commission d'une cyber infraction : c'est la condition à son exonération de responsabilité qui, en cas de non-respect, engage la responsabilité pénale de l'intermédiaire.

[157] Cass., Crim 17 nov 1992.
[158] Paris, 10 février 1997.
[159] V. Ch. Féral-Schuhl, *Cyberdroit : le droit à l'épreuve de l'Internet*, Paris, Dalloz, 2010, n° 114.24.

⁂

Section 2. **Neutralité limitée et responsabilité pénale**

La neutralité des intermédiaires est limitée pour une certaine catégorie d'intermédiaires en ce qu'ils doivent lutter activement contre la cybercriminalité, notamment en étant réactif au contenu intrinsèquement illicite qui se manifeste sur leurs services et par le biais de leurs infrastructures, sous peine d'engager leur responsabilité pénale (§1). Une telle exigence respecte-t-elle alors véritablement la conduite neutre qu'ils sont supposés, parfois obligés d'avoir dans la conduite de leur activité et qui fonde leur régime exonératoire de responsabilité, la responsabilisation pénale ? (§2).

§1. **La répression de l'inertie face au contenu illicite**

64. Limite à la responsabilisation pénale. – La neutralité de l'intermédiaire, qu'elle soit imposée par la loi à des activités d'intermédiaires nommées (V. 73), ou découverte par les juges pour d'autres intermédiaires, connaît ses limites. Les dépasser signifie pour l'intermédiaire l'exclusion du régime de responsabilisation pénale et l'applicabilité du régime de responsabilité pénale de droit commun : le régime de responsabilisation pénale est en cela un véritable régime exonératoire, dont le bénéfice suppose le respect des conditions d'exonération pour les intermédiaires concernés. L'intermédiaire responsabilisé qui ne respecte pas une telle limite constitutive d'une condition d'exonération voit la responsabilité pénale de droit commun s'appliquer exclusivement dans le cadre de ce non-respect, pour son concours apporté à la cyber infraction commise par l'utilisateur. S'agissant alors du fournisseur d'accès à Internet, l'un des deux intermédiaires bénéficiant du régime de responsabilisation, les limites de son irresponsabilité pénale ne posent aucune difficulté : prévues à l'article 12 de la directive commerce électronique, elles concernent les cas d'une extrême rareté dans lesquels le fournisseur est à l'origine de la demande de transmission litigieuse, a sélectionné le destinataire de la transmission ou a modifié les contenus faisant l'objet de la transmission. La limite de l'irresponsabilité pénale du fournisseur d'hébergement, en revanche, est particulièrement intéressante et mérite d'être plus amplement analysée. L'article 14 de la directive et 6-I.2 et 6.I-3 de la loi LCEN prévoit en effet que l'irresponsabilité pénale de celui-ci ne joue pas s'il n'avait pas effectivement connaissance de l'activité ou de l'information illicite ou si, dès le moment où il en a eu

connaissance, il n'a pas agi promptement pour retirer ces informations ou en rendre l'accès impossible. Il s'agit là de punir, par l'engagement de sa responsabilité pénale, l'inertie de l'intermédiaire face au contenu illicite qu'il stocke. Autrement dit, la loi le contraint expressément à quitter sa neutralité dans la conduite de son activité pour faire cesser le contenu illicite, dès lors qu'il en prend connaissance, sous peine de responsabilité pénale. L'initiative date d'avant la LCEN puisque l'ensemble des intermédiaires d'Internet étaient jadis tenus responsables lorsqu'ils n'accomplissaient pas les « diligences normales » pour faire cesser un contenu illicite[160]. Le même raisonnement se retrouve ici dans la limite de la neutralité des intermédiaires responsabilisés prévue pour l'activité d'hébergeur : c'est l'abstention fautive de l'intermédiaire, résultant de la violation de règles spéciales en la matière qui est ici sanctionnée. À défaut de pouvoir établir la complicité de l'intermédiaire concerné, on pourrait alors imaginer envisager l'application de l'article 121-3 du Code pénal, lequel sanctionne la violation de façon manifestement délibérée d'une obligation particulière de prudence ou de sécurité ainsi que la faute caractérisée qui expose autrui à un risque grave. On pourrait la considérer soit en rapprochant l'article 6-I.3 de la loi lCEN d'une obligation particulière de prudence qui assigne non seulement le résultat mais également les moyens pour atteindre celui-ci, soit en rapprochant l'inertie de l'intermédiaire ainsi sanctionnée à une faute caractérisée qui viole un standard de diligence, à condition que la teneur du contenu expose la victime à un danger, plus difficile à établir. L'hébergeur en serait un imprudent conscient selon Merle ou un imprudent téméraire selon Pradel, et sa responsabilité pénale au titre d'une imprudence ferait de lui non pas un complice mais un auteur principal. Ainsi, intéressons-nous à la mise en œuvre d'une telle limite à l'exonération de responsabilité de l'hébergeur, avant de s'interroger légitimement sur la cohérence de celle-ci avec la neutralité supposée de l'intermédiaire. L'action pour retirer du contenu ou en rendre l'accès impossible n'est pas explicitée au surplus mais elle ne nous est pas étrangère puisqu'il s'agit en réalité de l'emploi des mêmes outils constitutifs d'obligations du régime de responsabilisation (retrait, blocage, déréférencement) dont relève l'intermédiaire dont il est ici question. Le caractère prompt d'une telle action est quant à lui soumis à des interprétations *in concreto* variables mais renvoie généralement à une réaction immédiate qui ne nécessite pas de décision de justice[161] et dont l'appréciation pose rarement des difficultés. L'inertie de l'intermédiaire responsabilisé sanctionnée par sa responsabilité pénale consiste en l'absence d'action prompte de sa part dès lors qu'il prend connaissance du contenu. Arrêtons-nous alors sur cette connaissance du contenu illicite, préalable de l'engagement de la responsabilité pénale de tout intermédiaire qui répond de la qualification d'hébergeur (V. 84).

[160] V., en ce sens, Rapport du Conseil d'État, Internet et les réseaux numériques, 1998, La Documentation française, p. 185.
[161] Tribunal de grande instance de Toulouse, Ord. de réf., 13 mars 2008, M. K. / Pierre G., Amen.

65. Connaissance du contenu illicite. – La connaissance du contenu illicite par l'intermédiaire n'est pas un élément laissé à l'appréciation souveraine du juge. L'article 6.I.5 de la loi LCEN prévoit en effet que « La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants : - la date de la notification ; - si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; - si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ; - les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ; - la description des faits litigieux et leur localisation précise ; - les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ; - la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté. » Au cœur de la connaissance de l'intermédiaire se trouve alors une procédure de signalement par un tiers qualifiée également de « *notice and take down* ». C'est là le résultat de l'obligation de l'article 6.I-7 de la loi LCEN, consistant en la mise en place d'un dispositif de signalement. L'obligation est donc suivie d'effectivité car, à l'issue de celle-ci, et à condition que la notification réponde aux conditions de l'article 6.I.5 de la loi LCEN, l'intermédiaire responsabilisé est présumé connaître le contenu illicite, or cette connaissance est le préalable de sa responsabilité pénale puisqu'elle fait sortir l'intermédiaire de son régime exonératoire de responsabilité lorsqu'elle est suivie d'une inertie de sa part. Il y a alors un avant et un après signalement[162]. La notification doit dès lors nécessairement contenir les éléments énumérés par la loi, à défaut de quoi la présomption ne peut pas jouer. Par exemple les juges avaient considéré que Wikimédia Foundation était irresponsable en raison d'une notification incomplète de contenu illicite, celle-ci ne faisant « nulle mention des dispositions légales essentielles pour la vérification par le destinataire du caractère manifestement illicite que doit revêtir le contenu en question »[163] . De la même manière, bien que Dailymotion ait été condamné, les juges avaient retenus « qu'il ne suffit pas prétendre subir une contrefaçon d'œuvres dont on prétend détenir les droits, encore faut-il préciser, en les nommant, les dénombrant et les identifiant, les œuvres dont on revendique la paternité pour justifier de sa qualité à agir et de son intérêt à agir »[164]. Pour rappel, le fait, pour toute personne, de signaler un contenu ou une activité comme étant illicite

[162] J. Bossan, op. cit., p. 302.
[163] Tribunal de grande instance de Paris, Ord. de réf., 29 octobre 2007, Marianne B. et autres / Wikimedia Foundation.
[164] Tribunal de grande instance de Paris, 18 décembre 2007, Jean Yves Lafesse / Dailymotion.

dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 Euros d'amende[165].

66. Le standard du manifestement illicite. – La connaissance du contenu illicite pour l'engagement du régime de responsabilisation a été précisé par le standard du manifestement illicite. En effet, afin d'éviter tout risque d'erreur et d'arbitraire de la part des intermédiaires dans la conduite de leur action prompte face à un contenu illicite, le Conseil constitutionnel a exigé à l'occasion de sa réserve d'interprétation de la loi LCEN[166] que ledit contenu ou sa notification démontre l'illicéité avec un certain degré : « ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge »[167]. L'exigence a donc été introduite dans l'article 6.I-2 et 6.I-3 de la loi LCEN dès 2004. En quoi consiste-t-elle ? Un arrêt récent du 23 novembre 2022 de la Cour de cassation l'illustre parfaitement puisque le contenu en question était proposé par un site espagnol qui offrait un recours à la gestation pour autrui (GPA)[168]. La Cour a retenu que le caractère manifestement illicite du contenu en question relevait de l'illicéité incontestable de la pratique de la GPA en France. Autrement dit, l'illicéité qui présente un caractère manifeste est une illicéité sur laquelle il n'y a pas lieu de s'interroger au regard d'une législation qui ne laisse pas place à interprétation, peu importe l'existence d'un éventuel débat sur la question[169]. Un tel standard permet certes d'amoindrir le risque d'erreur mais n'ôte pas le principal écueil du mécanisme : les intermédiaires, généralement des entreprises privées, par leur appréciation autonome de l'illicéité d'un contenu, se substituent *de facto* à l'autorité judiciaire en bafouant la présomption d'innocence des auteurs du contenu. Le standard d'un contenu relevé comme étant manifestement illicite, consacré par la loi LCEN était censé réduire en ce sens la difficulté d'appréciation des intermédiaires. Ceux-ci en rencontrent toutefois encore, se prévalant régulièrement d'absence de décision de justice pour les aiguiller ou du fait qu'il ne leur appartient pas de se substituer à l'autorité judiciaire pour qualifier un contenu comme étant illicite[170]. L'arrêt de 2022 répond alors à ces motifs en affirmant que l'illicéité du contenu était sans équivoque au regard des règles d'ordre public ou de protection des

[165] Loi n° 2004-575, op. cit., art. 6.I-4.
[166] Cons. const., 10 juin 2004, n° 2004-496 DC, § 9.
[167] Cons. const., 10 juin 2004, n° 2004-496 DC, § 9.
[168] Cass. 1re civ., 23 nov. 2022, n° 21-10.220 – Sté OVH c/ assoc. Juristes pour l'enfance, JurisData n° 2022-019611.
[169] G. Loiseau., Le standard du « manifestement illicite » dans la responsabilité des hébergeurs, Com. et comm. électr. N°11, janvier 2023, comm. 2. p.2.
[170] TGI Versailles, 26 févr. 2019, n° 16/ 07633, Assoc. des Juristes pour l'Enfance c/ OVH et Subrogalia SL : JurisData n° 2019-004243 ; Comm. com. électr. 2019, comm. 31, note G. Loiseau.

droits des tiers au regard des lois françaises[171]. Autrement dit, de la même manière qu'une plateforme ne peut faire commerce de cannabis à destination du public français à raison d'un débat sur sa légalisation, un site espagnol ne peut mettre en lien mères porteuses et clients. Cette exigence est néanmoins propre au droit interne, les deux instruments principaux de droit européen en charge de la question de la responsabilité de l'intermédiaire, la directive 2000/31/CE sur le commerce électronique [172] et le règlement des services numériques dont l'entrée en vigueur est prévu pour 2024, le Digital Service Act (DSA)[173], n'en faisant pas mention express. Le DSA, bientôt en vigueur, prévoit toutefois en son article 16 que le contenu illicite sera considéré comme tel dès lors que sa notification à l'intermédiaire permet « d'identifier l'illégalité de l'activité ou de l'information concernée sans examen juridique détaillé »[174] et codifie ainsi d'une jurisprudence européenne *praeter legem* déjà bien établie[175]. Le standard du « manifestement illicite » se place donc pour le droit européen sur la notification qui en sera faite à l'intermédiaire et non sur le contenu en lui-même : ce sont les éléments présentés dans la notification du contenu illicite qui doivent suffire à établir de façon manifeste le caractère illicite du contenu, sans qu'un examen de celui-ci par l'intermédiaire soit nécessaire. Les raisonnements français et européens sont alors inversés dans la mesure l'article de la 6.I.5 de la loi de 2004 prévoit que si la notification fait présumer à l'intermédiaire le caractère manifestement illicite c'est à celui-ci de l'apprécier de façon autonome tandis que le droit européen prévoit que la notification doit faire apparaître le caractère illicite de façon manifeste de telle sorte que l'intermédiaire n'a pas à procéder à une appréciation autonome. Le standard européen du « manifestement illicite » semble à ce titre plus protecteur de la liberté des utilisateurs et de la présomption d'innocence puisque l'illicéité ne nécessitant pas d'examen de l'intermédiaire apparaît logiquement de manière plus frappante encore que celle qui le nécessite ; le risque d'erreur en est davantage amoindri. En tout état de cause, l'application du standard du « manifestement illicite » demeure attentatoire : l'appréciation de l'illicéité du contenu, qu'elle soit établie manifestement par sa substance même ou sa notification, ne revient pas à l'autorité judiciaire mais à un intermédiaire et aux tiers qui le notifient. L'écueil est organique, ce qu'aucun standard ne pourra neutraliser. De surcroît, la Cour de cassation, voulant éviter un contentieux prophylactique

[171] G. Loiseau, Com. et comm. électr. N°11, op. cit., p.2.
[172] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).
[173] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).
[174] G. Loiseau, Com. et comm. électr. N°11, op. cit. p. 1.
[175] CJUE, 22 juin 2021 Google Youtube, affaire C-683/18, Elsevier Inc. c/Cyando AG : Comm. com. électr. 2021, comm. 61, note P. Kamina,et comm. 62, note G. Loiseau.

sur le droit au refus de suppression du contenu, refuse la saisine préventive visant à établir l'existence du contenu manifestement illicite qui aurait pu alléger les atteintes aux libertés des utilisateurs. Certes, l'activité prohibée par des règles d'ordre public, telle que celle des mères porteuses dont l'arrêt de 2022 traite, ne pose généralement aucune difficulté, malgré la persistance inévitable du contentieux. Mais, ainsi que le relève l'auteur Grégoire Loiseau, *quid* du contenu qui nécessite une analyse plus subjective, comme les contenus haineux ? Ostensible ou non, le caractère manifestement illicite des contenus sera soumis à l'examen de l'intermédiaire qui devra se plonger dans des contingences de faits et d'intérêts privés pour en livrer une analyse quoi qu'on en dise juridique. La solution est donc irrémédiablement attentatoire à la liberté des utilisateurs.

67. Étendue du contenu manifestement illicite. – L'autre difficulté majeure rencontrée par l'appréhension d'un tel contenu relève du caractère illimité, fuyant d'Internet. Le contenu mis en cause peut en effet être reproduit à l'infini sous presque toutes les formes possibles et à presque tous les endroits d'Internet. Ainsi, s'il existe un contenu pédopornographique sur un site A, celui-ci peut être dupliqué à l'identique sur un site B. Cela va sans dire, la rapidité d'une telle manœuvre bat la « célérité » de la justice. À ce titre, la jurisprudence assimile strictement tout contenu identique ou équivalent au contenu reconnu comme illicite[176]. Auparavant, la position de la Cour de cassation et des juges du fond était divergente : ceux-ci avaient déjà considéré que les diffusions successives de l'œuvre ne constituaient pas un nouveau contenu illicite nécessitant une nouvelle notification, et qu'il appartenait donc à l'hébergeur de prendre les mesures nécessaires pour y contrevenir, tandis que la Cour avait retenu que le retrait du contenu illicite dupliqué relève d'une surveillance générale proactive, proscrite pourtant au titre de la directive commerce et de la loi LCEN[177]. Ainsi, depuis 2019, l'injonction de suppression d'un contenu illicite émanant de la justice n'oblige pas l'intermédiaire à procéder à une recherche autonome de tout contenu identique ou équivalent à un contenu précédemment déclaré illicite et étant passé force jugée (ce qui serait constitutif d'une violation de l'interdiction de surveillance générale des données) mais l'oblige toutefois à étendre l'objet de la suppression enjointe à tout contenu identique ou équivalent, présent sur son infrastructure numérique ou par le biais de son service. Si l'interprétation du contenu identique au contenu illicite ne pose aucune difficulté, il fallut toutefois que la doctrine précise celle qui pouvait en être faite s'agissant d'un contenu dit équivalent. Selon l'auteur Grégoire Loiseau, il s'agit du contenu

[176] CJUE, 3e ch., 3 oct. 2019, aff. C-18/18, Eva Glawischnig-Piesczek c/ Facebook Ireland Limited.

[177] Cass. 1re civ., 12 juill. 2012, n° 11-13.666 : JurisData n° 2012-015877 ; Bull. civ. I, n° 166 ; Comm. com. électr. 2012, comm. 91 , C. Caron ; RIDA 2012, n° 234, p. 413 , obs. P. Sirinelli ; Propr. intell. 2012, p. 416 , obs. A. Lucas ; Légipresse 2012, n° 298, p. 566 , note Ph. Colombet.

qui, « tout en véhiculant en substance le même message, est formulé de manière légèrement différente, en raison des mots employés ou de leur combinaison, par rapport à l'information dont le contenu a été déclaré illicite »[178]. La contenance, l'enveloppe dudit contenu est indifférente pour sa qualification d'identique ou d'équivalent à un contenu reconnu comme illicite : c'est l'exemple d'une apologie de génocide que l'on aurait transposée d'un post déclaré illicite vers un commentaire. La solution contraire rendrait une telle injonction facilement contournable et dépourvue d'effectivité. Le contenu déclaré illicite est alors étendu à tout contenu équivalent ou identique et les règles de responsabilité de l'intermédiaire qui en découle et dont on prendra connaissance s'y alignent dès lors en conséquence.

§2. **Compatibilité avec la neutralité de l'intermédiaire**

68. Compatibilité avec le principe de neutralité. – L'irresponsabilité pénale au titre d'une neutralité de l'intermédiaire ne l'exempte pas pour autant de toute responsabilité juridique dès lors que ceux-ci ne respectent pas les conditions à leur exonération, comme on vient de le voir. La répression d'une inertie face aux contenus illicites respecte-t-elle alors bien la neutralité supposée des intermédiaires qu'elle vient sanctionner ? La question a fait grand débat en doctrine, les auteurs relevant une incohérence fondamentale entre l'attitude neutre de l'intermédiaire, légalement imposée au titre du régime de responsabilisation pénale, et l'obligation parallèle d'agir contre le contenu manifestement illicite. Elle se pose en effet dès lors qu'il est contraint de filtrer, bloquer ou supprimer du contenu illicite à la demande des autorités européennes et nationales, le tout sous peine d'engager sa responsabilité pénale. La neutralité ne supposerait-elle pourtant pas la non-intervention de l'intermédiaire dans le contrôle des données afin de le discriminer ? L'auteur Emmanuel Derieux l'affirme : « Qu'elle soit perçue comme positive, par les uns, ou négative, par d'autres, une telle attitude n'est évidemment pas neutre »[179]. L'interdiction d'avoir une conduite « non-neutre » sauf accord d'une autorité administrative, sous couvert de neutralité, fait questionner la cohérence entre le contenu du projet de loi et son nom. Quelques années auparavant, c'était la directive commerce électronique qui l'autorisait pour les États membres en son article 45 : l'autorisation ou l'obligation de faire intervenir l'intermédiaire et donc de rompre avec sa neutralité peuvent « revêtir la forme de décisions de tribunaux », mais aussi « d'autorités administratives exigeant qu'il soit

[178] G. Loiseau, Responsabilité de l'hébergeur - La suppression de contenus identiques ou équivalents au contenu déclaré illicite, Communication Commerce électronique n° 11, Novembre 2019, comm. 67, p. 1.
[179] E. Derieux, op. cit., p.627.

mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible »[180]. Ainsi que le laisse penser l'auteur Emmanuel Derieux, la liberté sur Internet ne peut être que conditionnelle et ne peut aller sans responsabilité relative aux contenus mis en ligne, *a minima* pour participer à la répression des auteurs des cyber infractions, leurs utilisateurs[181]. En réalité, la responsabilisation de l'intermédiaire n'est pas entièrement incompatible avec sa neutralité car celle-ci n'agit qu'*a priori* d'un signalement de contenu illicite, ce pourquoi c'est la surveillance générale *proactive* des données qui est prohibée. Une fois le signalement déclenché, la neutralité s'efface et laisse place à la responsabilité de l'intermédiaire. La neutralité de l'intermédiaire dans la conduite de son activité n'a en effet jamais eu vocation à être absolue, l'inverse nous ferait retomber dans une conception d'Internet comme étant une zone de non droit. Autrement dit, la neutralité de l'intermédiaire est un simple constat sur la manière que celui-ci a de conduire son activité, constat qui vient moduler son régime de responsabilité, mais elle n'est pas l'inertie absolue de l'intermédiaire en cas de signalements ou de demandes provenant de la justice. Ainsi, si la responsabilité pénale paraît, elle, être incompatible avec la neutralité de l'intermédiaire qui elle neutralise l'élément moral de l'infraction, la responsabilisation de l'intermédiaire par une série d'obligations et la cessation de son exonération de responsabilité dès sa connaissance d'un contenu illicite semble relativement cohérente avec une neutralité qui possède d'évidentes limites.

Naturellement, l'absence de neutralité de l'intermédiaire dans la conduite de son activité suppose l'exclusion du régime exonératoire de responsabilité de droit commun, la responsabilisation pénale. La jurisprudence s'est donc attachée à identifier cette absence en creux de la neutralité de l'intermédiaire, afin de déterminer les cas dans lesquels l'intermédiaire pouvait être tenu pénalement responsable des cyber infractions commises par leurs utilisateurs.

[180] Directive européenne, op. cit., cons. 45.
[181] E. Derieux, op. cit., p. 622.

⁂

Section 3. **Absence de neutralité et responsabilité pénale**

L'absence de neutralité de l'intermédiaire dans la conduite de son activité, facteur clé du régime applicable, doit ainsi être définie, au même titre que sa neutralité. C'est la jurisprudence qui s'en est chargée, en considérant que l'absence de neutralité de l'intermédiaire était établie dès lors qu'il avait joué un rôle actif dans la conduite de son activité (§1). Les juges ont à ce titre développé des critères d'appréciation *in concreto* du rôle actif de l'intermédiaire, tel que le contrôle intellectuel exercé sur les données (§2).

§1. **L'absence de neutralité de l'intermédiaire**

69. Absence de neutralité. – L'auteur Jérôme Bossan souligne toute la difficulté et l'intérêt fondamental qu'il y a à déterminer l'absence de neutralité de l'intermédiaire dans la participation à la commission de l'infraction : « c'est, en effet, parce que le juge a estimé que la neutralité alléguée par l'intermédiaire n'était pas avérée qu'il considère tel ou tel acteur comme l'éditeur d'un service en ligne. L'enjeu est, du point de vue de la responsabilité, très important : faut-il que l'intermédiaire soit informé de l'existence d'un contenu illicite sur le site concerné pour que sa responsabilité pénale soit engagée ? »[182]. Si la neutralité de l'intermédiaire implique qu'il ne prenne pas connaissance et qu'il ne contrôle pas *a priori* le contenu qu'il fait transiter, met à disposition ou dont il assure le stockage, l'absence de neutralité revient alors à considérer que l'intermédiaire en prend bien connaissance et le contrôle activement. Autrement dit, là où la neutralité suppose que l'intermédiaire a la capacité de connaître et de contrôler les données mais n'en use pas, l'absence de neutralité suppose qu'il en use à l'occasion de la conduite de son activité. En ce sens, selon le considérant 42 de la directive commerce électronique et l'article L. 32-3-3 du Code des postes et communications électroniques, le fournisseur d'accès à Internet voit sa responsabilité pénale engagée s'il est à l'origine de la demande de transmission litigieuse, s'il sélectionne le destinataire de la transmission ou qu'il sélectionne ou modifie les contenus faisant l'objet de la transmission. L'irresponsabilité pénale du FAI répond à une logique nettement différente de celle de l'hébergeur que l'on a présenté (V. 67) : il ne s'agit pas ici de réprimer la neutralité de l'intermédiaire face à la présence de contenu illicite dont il prend connaissance, mais de réprimer l'absence de sa neutralité par l'inapplication du

[182] J. Bossan, op. cit. p.314

régime exonératoire de responsabilité. Autrement dit, là où l'article 6-I.3 de la loi LCEN prévoit pour l'hébergeur une limite à sa neutralité et à son irresponsabilité pénale, l'article L. 32-3-3 du CPCE constate pour le fournisseur l'inexistence *ab initio* de sa neutralité. Néanmoins, les hébergeurs ne sont bien entendu pas en reste et peuvent également démontrer d'une absence de neutralité *ab initio* qui les fera relever du régime de responsabilité pénale de droit commun. Pour l'hébergeur, la consécration a été construite prétoriennement : étant confrontés à l'apparition de nouveaux acteurs et de nouvelles affaires, les juges se sont attachés à rechercher l'absence de neutralité de l'intermédiaire en examinant son rôle dans la conduite de son activité.

70. Rôle actif. – En effet, la jurisprudence a très vite retenu la responsabilité pénale de l'intermédiaire ayant joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées[183], par opposition au rôle passif et de nature opposée. Celui qui joue un tel rôle ne peut alors pas être caractérisé d'intermédiaire neutre, c'est l'enseignement de l'arrêt précité mettant en cause Google dans plusieurs affaires pour avoir renvoyé les utilisateurs vers des liens de sites proposant de la contrefaçon par leur programme de publicité Google Ads, anciennement Google Adwords. La jurisprudence Google Adwords est devenue constante, régulièrement confirmée par exemple dans l'arrêt L'Oréal e.a. c/ eBay international[184], la Cour traitant en l'espèce d'un exploitant qui prêtait une assistance consistant à promouvoir et optimiser la présentation des offres à la vente[185]. La même exigence est alors reprise en jurisprudence interne, régulièrement rappelée, celle du « rôle actif de nature à [lui] conférer la connaissance ou le contrôle des données » qu'il stocke est de nature à le « priver du régime exonératoire de responsabilité prévu par l'article 6.1.2 de la loi du 21 juin 2004 et l'article 14 § 1 de la directive 2000/31 »[186]. En vertu de l'existence d'un rôle actif dans la conduite de l'activité de ces intermédiaires, ceux-ci sont donc exclus du régime exonératoire de responsabilité pénale, la responsabilisation pénale : c'est le contrôle exercé *a priori* sur les données qui font d'eux des outils vecteurs de commission de l'infraction et donc des responsables pénal[187]. La responsabilité pénale de ces intermédiaires n'est alors que la

[183] CJUE, 23 mars 2010, Google France SARL et Google Inc. contre Louis Vuitton Malletier SA (C-236/08), § 120, Google France SARL contre Viaticum SA et Luteciel SARL (C-237/08) et Google France SARL contre Centre national de recherche en relations humaines (CNRRH) SARL et autres (C-238/08) .

[184] CJUE, 12 juill. 2011, aff. C-324/09, L'Oréal e.a. c/ eBay international e.a. : JurisData n° 2011-021879 ; Comm. com. électr. 2011, comm. 99, note C. Caron

[185] G. Loiseau, Le rôle actif de l'exploitant d'un site de mise en relation de revendeurs et d'acheteurs de billets donnant accès à des événements sportifs, Comm. com. électr. n°9, septembre 2022, comm. n°58.

[186] Cass. com., 3 mai 2012, n° 11-10.508 , publié : JurisData n° 2012-009435 ; Bull. civ. V, n° 89 ; JCP G 2012, 789, note A. Debet ; D. 2012, p. 1684, note L. Mauger-Vielpeau. – Cass. com., 3 mai 2012, n° 11-10.505, non publié : JurisData n° 2012-009758. – Et Cass. com., 3 mai 2012, n° 11-10.507, non publié : JurisData n° 2012-009759

[187] J. Bossan, op. cit., p. 310

contrepartie de la surveillance générale *proactive* de leurs données qu'ils exercent et que d'autres, les irresponsables, ne peuvent pas exercer.

§2. **Critères du rôle actif de l'intermédiaire**

71. Le contrôle intellectuel. – La jurisprudence européenne, reprise en interne, s'est attachée à préciser les critères qui démontrent que l'intermédiaire n'est en aucun cas neutre dans la conduite de son activité et qu'il exerce, *a contrario,* un contrôle bien actif sur ses données dont il fait usage à certaines fins. Notamment, l'argument porté à l'encontre de la neutralité de l'intermédiaire devant les juridictions pour caractériser le manque de neutralité de l'intermédiaire était de façon récurrente le bénéfice, le profit tiré des contenus par leur exploitation commerciale : avait été ainsi avancé et admis le critère pécuniaire dans un arrêt controversé de la Cour de cassation mettant en cause l'hébergeur Tiscali[188]. Un an plus tard, l'arrêt précité Google Adwords de la Cour de Justice Européenne réfute une telle analyse et affirme l'indifférence de l'exploitation commerciale du service et du profit touché par l'intermédiaire pour établir l'existence d'un rôle actif joué par l'intermédiaire : « la seule circonstance que le service de référencement soit payant, que Google fixe les modalités de rémunération, ou encore qu'elle donne des renseignements d'ordre général à ses clients, ne saurait avoir pour effet de priver Google des dérogations en matière de responsabilité prévues par la Directive 2000/31 »[189]. L'arrêt rejette donc également le critère des « renseignements d'ordre général » donnés par l'intermédiaire à ses clients (dans le cadre du moteur de recherche qui commercialise son référencement il peut s'agir de directives quant à la forme que doit prendre le message commercial qui accompagne le lien dirigeant vers le site client du moteur de recherche) et se montre ici plus exigeant en acceptant la qualification de rôle actif si le moteur de recherche présente lui-même le contenu litigieux à ses utilisateurs, par exemple en rédigeant le message commercial qui accompagne le lien qu'il a référencé contre rémunération. C'est donc le critère de l'absence de contrôle intellectuel – autrement dit, pour le moteur de recherche dont il était question, l'absence de sélection et de choix de contenu – qui caractérise au sens de la Cour de Justice européenne sa neutralité ; et par conséquent son contrôle intellectuel, sa « capacité d'action sur les contenus mis en ligne » qui caractérise le rôle actif joué par celui-ci. La même grille de lecture est adoptée

[188] Cass. 1re civ. 14 janv. 2010, n° 06-18.855 : JurisData n° 2010-051043 ; Comm. com. électr. 2010, comm. 25, note Ph. Stoffel-Munck ; RTD com. 2010, p. 307, obs. F. Pollaud-Dulian ; Propr. intell. 2010, n° 35, p. 725, note J.-M. Bruguière ; RIDA 2010, n° 223, p. 417, note P. Sirinelli ; D. 2010, p. 837, obs. L. Thoumyre.
[189] C-236/08, op. cit., §116.

par l'arrêt Dailymotion de la Cour de cassation qui, en se conformant à la jurisprudence européenne, revire la solution Tiscali s'agissant du critère pécuniaire et s'attache à analyser si l'intermédiaire en l'espèce, la plateforme de vidéos Dailymotion, procédait à un « choix » quant au contenu posté. L'arrêt constate alors que, malgré la « mise en place de cadres de présentation et la mise à disposition d'outils de classification permettant de rationaliser l'organisation », aucun choix quant au contenu posté sur la plateforme n'est opéré par Dailymotion, c'est bien une appréciation *in concreto* de l'existence de la réalité du rôle actif qui est exercée par le juge.

72. Critiques. – L'interprétation du rôle actif de l'intermédiaire dans la conduite de son activité, réaffirmée à l'occasion de l'arrêt précité opposant L'Oréal et eBay et devenue constante depuis, peut néanmoins être discutée à certains égards. En premier lieu, si le contrôle intellectuel exercé sur les données a été désigné comme critère de prédilection pour analyser le rôle actif de l'intermédiaire, pour quelles raisons le critère pécuniaire devrait-il y être pour autant indifférent ? Dans les faits, il est entendu que les moteurs de recherche tels que Google ou les plateformes de vidéos telles que Dailymotion commercialisent leurs services, notamment en mettant en avant du contenu, sans pour autant systématiquement vérifier quelle en est la substance : chacun peut par exemple créer un site et rémunérer Google *via* le programme Ads, anciennement Adwords, afin que son site soit référencé avantageusement et bénéficier en ce sens de publicité. Si les algorithmes empêchent une bonne partie du contenu notamment discriminatoire et haineux, certains sites passent naturellement à travers les mailles du filet. La connaissance de ces sites par Google n'est donc pas nécessairement établie à cet égard. En revanche, elle peut l'être avec moins de difficulté lorsque les annonceurs qui rémunèrent Google sont des clients tels que la maison Chanel. Ainsi, si le profit tiré n'avait pas nécessairement vocation à devenir critère – la sélection et le choix du contenu étant des critères pertinents caractérisant réalistiquement l'existence d'un rôle actif – rien ne l'empêchait de demeurer un indice de la connaissance et du contrôle intellectuel exercé par ceux-ci, dès lors que l'on sait que certains profits incitent fortement les intermédiaires à jeter un œil plus attentif sur le contenu qu'ils mettent à disposition d'une façon ou d'une autre. Le critère pécuniaire du profit tiré de l'activité illicite de l'utilisateur aurait par ailleurs été une source potentiellement double de responsabilité pénale : d'une part il aurait pu être un indice du rôle actif de l'intermédiaire, de son appartenance conséquente au régime de responsabilité pénale de droit commun et donc de sa complicité, mais il aurait pu d'autre part donner éventuellement lieu à l'application de l'article 321-1 du Code pénal car, dès lors que l'intermédiaire bénéfice à son compte d'une infraction en connaissance de cause, ne commet-il pas un recel ?

On l'a donc compris, la neutralité de l'intermédiaire justifie tant l'exclusion que l'engagement de la responsabilité pénale des intermédiaires d'Internet. Bien que les juges aient nourri et développé les théories de neutralité et de rôle actif de l'intermédiaire, la question n'a pas été complètement déléguée aux prétoires : en outre d'affirmer que les intermédiaires irresponsables étaient neutres, le législateur s'est attaché à nommer expressément certains intermédiaires qui relèveraient de l'un ou de l'autre régime en raison de cette neutralité. La neutralité des intermédiaires ne doit donc pas être comprise *per se* mais bien à travers le prisme de l'activité matérielle d'intermédiaire.

***

Chapitre 2

L'ACTIVITÉ DE L'INTERMÉDIAIRE, ÉLÉMENT DÉTERMINANT DU RÉGIME APPLICABLE

L'activité matérielle de l'intermédiaire régit ainsi la neutralité qu'il peut avoir dans la conduite de son activité. Les activités d'intermédiaires et leurs conséquences sur la responsabilité de ces derniers ont été légalement déterminées (Section 1), pourtant, elles continuent de constituer une source intarissable de contentieux, faisant basculer le régime applicable à l'intermédiaire d'une solution à l'autre (Section 2).

Section 1. **L'activité de l'intermédiaire au cœur de la loi**

Le législateur n'a pas laissé les choses aux hasard en nommant légalement les activités qui devaient être soumises à l'un et l'autre régime de responsabilité pénale, la responsabilisation et le droit commun (§1). Néanmoins, vingt

ans après, certaines carences de la loi quant à des statuts d'intermédiaires manquants n'ont pas encore été corrigées, ceux-ci demeurant dans le flou juridique et à la merci de la jurisprudence (§2).

§1. **Responsables légalement déterminés**

73. Activités neutres nommées. – En 2000, trois activités d'intermédiaires sont déterminées et décrites comme étant purement techniques, automatiques, passives et donc « neutres » au sens du considérant 42 de la directive commerce électronique. L'article 12 de la directive fait part du transport d'information sur un réseau, le « mere conduit », l'article 13 d'une forme de stockage automatique et temporaire visant à réduire les temps de latence et à améliorer la performance du système qui l'utilise, la mise en cache ou *caching*, tandis que l'article 14 vise l'hébergement de données. Pour la loi LCEN, ce sont deux types d'intermédiaires qui bénéficient du privilège d'avoir leur responsabilité expressément régie : le fournisseur d'accès à Internet, par renvoi à l'article 12 de la directive, et le fournisseur d'hébergement, par renvoi à l'article 14 de la directive. Bien que la loi LCEN ne l'ai pas expressément inclus dans ses dispositions, l'opérateur de communication électronique, dont la mission est définie par l'article L.32 15° du Code des postes et communications électronique (assurer la transmission des contenus et effectuer une sauvegarde automatique des données en vue de fluidifier la circulation de celle-ci), pourra être rattaché à l'un ou l'autre, dans la mesure où il est également, de façon quasi systématique, fournisseur d'accès à Internet ou d'hébergement. En outre, l'irresponsabilité de ces intermédiaires est réaffirmée dans la loi LCEN puisque l'article 6.I-6 exclut les activités d'intermédiaires mentionnées aux articles 6.I-1 et 6.I-2 de la qualification de producteur de service de communication au public, lequel est pénalement responsable de son service.

74. Statut légal du FAI. – L'article 6.I-1 de la loi LCEN définit l'activité de FAI comme étant l'offre d'un accès à des services de communication au public en ligne, tandis que l'article 32-3-3 du Code des postes et communications électroniques pose comme principe son irresponsabilité civile et pénale, ainsi que ses limites (V. 64), laquelle s'applique également à l'OCE. Le statut et la responsabilité du fournisseur d'accès à Internet est réaliste et conforme à la conduite de son activité, à l'occasion de laquelle, bien qu'il ait la capacité de contrôler les données qu'il fait transiter, le FAI n'en use pas et réalise son activité de transmission sans discrimination du contenu et des demandes.

75. Statut légal de l'hébergeur. – L'article 6.I-2 de la loi LCEN définit l'hébergeur comme étant la personne physique ou morale qui assure, même à titre gratuit, « pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ». Son irresponsabilité, découlant également de sa neutralité dans la conduite de son activité, et ses limites, est prévue à l'article 6.I-3 de la loi LCEN. Elle paraît parfaitement appropriée et cohérente avec la réalité de l'activité de l'hébergeur, lequel se borne à fixer les modalités de son service de stockage des données, à en informer ses clients, à exercer ledit stockage ainsi qu'à se faire rémunérer : il ne procède à aucun traitement de données puisqu'en faisant du stockage il fait tourner les programmes et algorithmes de ses clients qui s'en chargent eux-mêmes. L'activité d'hébergement peut être exercée par d'autres intermédiaires qui stockent du contenu et ne procèdent pas non plus à un traitement des données. Ce constat est bien ancré en jurisprudence puisque les juges considèrent systématiquement que l'intermédiaire exerçant une activité d'hébergement « n'est pas responsable du traitement des données à caractère personnel »[190].

76. Interprétation stricte. – La directive commerce électronique énonce alors clairement en son considérant 42 que seules les activités qu'elles mentionnent, et qui sont définies dans ses articles 12 à 14, peuvent bénéficier du régime exonératoire de responsabilité pénale : « Les dérogations en matière de responsabilité prévues par la présente directive ne couvrent que les cas où l'activité du prestataire de services dans le cadre de la société de l'information est limitée au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission ». De la lettre de la directive ressort, en apparence du moins, une volonté d'interpréter strictement les activités d'intermédiaire qui bénéficient d'une irresponsabilité pénale. Par conséquent, seul ceux nommés par la directive et dont l'activité « revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées », selon le même considérant, pourront jouir d'une irresponsabilité pénale.

77. Responsables nommés. – Certains intermédiaires, peu nombreux, sont en revanche expressément soumis au régime de responsabilité pénale de droit commun. En premier lieu, les activités d'intermédiaires ne

[190] Paris, 1er mars 2019, M.X c/ Oxeva.

bénéficiant pas d'une irresponsabilité au titre de leur neutralité au sens de la directive sont tous les prestataires de « la société de l'information »[191] qui ne répondent pas aux exigences du considérant 42 de la directive commerce électronique, et donc ne possèdent pas de caractère automatique, passif et purement technique. La directive se garde toutefois de nommer expressément les intermédiaires qui seront exclus du régime exonératoire de responsabilité pénale. Quant à elle, la loi LCEN mentionne la responsabilité pénale des éditeurs de services de communication de public en ligne, car ceux-ci sont naturellement responsables des contenus mis en ligne sur leur plateforme – raison pour laquelle ils ont obligation de mettre à disposition quelques informations telles que le contact de leur hébergeur[192] – et peuvent à ce titre revêtir le titre de complice ou de producteur (V. 57). « L'éditeur de services de communication en ligne » n'est toutefois pas explicitement défini et peut par conséquent renvoyer à de très nombreuses hypothèses, au gré de l'interprétation que l'on lui en donne[193]. Pire, la loi LCEN induit en erreur en évoquant le service de communication au public en ligne dans le chapitre des prestataires techniques, alors que qu'ils se définissent par opposition[194]. C'est pourquoi certaines activités d'intermédiaires, bien qu'elles peuvent en relever, sont considérées comme absentes des prévisions de la loi LCEN (V. 79), dans la mesure où il est techniquement très difficile d'appréhender une telle qualification, sans définition au surplus, dans la réalité des intermédiaires d'aujourd'hui. On comprend en tout état de cause que l'éditeur sera celui qui contrôle la diffusion du contenu, raison pour laquelle il en est responsable. Enfin, en vertu de la récente directive du 17 avril 2019 sur le droit d'auteur, transposée en 2021 en France, les plateformes numériques, notamment multimédia, sont expressément tenues responsables des contenus contrevenant au droit d'auteur (V. 59).

§2. **Carences de la loi**

78. Transposition partiellement satisfaisante. – En premier lieu, si la loi LCEN transpose bien le régime d'irresponsabilité prévu pour les activités exercées par le fournisseur d'accès à Internet et l'hébergeur,

[191] Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information(21) et dans la directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel (22).
[192] Loi 2004-575 op. cit., art. 6.III.
[193] T. Azzi, op. cit., p.72.
[194] E. Dreyer, *Droit de la communication*, LexisNexis, 2021.

celle-ci se garde de prévoir l'irresponsabilité des intermédiaires au titre de l'exercice d'une activité de mise en cache, le stockage automatique et temporaire permettant d'améliorer et d'accélérer le fonctionnement du système qui la sollicite. Et pour cause, le *caching* n'est originellement pas une activité d'intermédiaire *per se*, puisqu'elle est l'accessoire d'autres activités d'intermédiaires. L'article 12.2 de la directive commerce électronique, définissant le fournisseur d'accès à Internet, prévoit en ce sens que la mise en cache définie à l'article 13 est englobée par l'activité de transmission d'information sur un réseau, autrement dit par l'activité de fourniture d'accès à Internet : « Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire de la transmission ». Cependant, depuis les années 2000, de nombreux autres intermédiaires font de la mise en cache, notamment les bases de données et les moteurs de recherches, qui l'utilisent pour stocker des ressources telles que des images, des fichiers CSS et JavaScript afin de réduire le temps de chargement des résultats des recherches. En outre, certains intermédiaires ont fait de la mise en cache une prestation de service proposée à tout type d'intermédiaires, de la plateforme multimédia au service de messagerie : ce sont les réseaux de distribution de contenu, Content Delivery/Distribution Network (CDN) (V. 14). Autrement dit, la fourniture d'accès à Internet ne peut plus réalistiquement englober la mise en cache, qui est devenue l'accessoire de d'autres activités d'intermédiaires d'une part et une activité *per se* pour les CDN d'autre part. Ainsi, la situation juridique des intermédiaires autres que le FAI ayant accessoirement recours à la mise en cache, ou faisant une prestation de service de mise en cache à titre principal, reste en théorie floue : si la directive prévoit que cette activité revête un caractère neutre, elle ne la conçoit en son article 12 et 13 que dans le cadre du fournisseur d'accès à Internet, tandis que la loi LCEN reste silencieuse. En pratique, la mise en cache, lorsqu'elle est mise en cause, octroie l'irresponsabilité pénale de l'intermédiaire qui l'emploie en vertu de l'article 13 et du considérant 42 de la directive, c'est entendu.

79. Statuts absents de la loi. – Néanmoins, si l'on devait faire un quota des intermédiaires qui voient leur statut et leur responsabilité être régulés par la loi par rapport à la multitude d'intermédiaires existants, le résultat serait bas. Est-il alors décevant ou reflète-il simplement la volonté du législateur européen et français de ne cantonner le régime d'irresponsabilité pénale qu'à quelques activités d'intermédiaires, nommées, qui présentent un caractère passif et neutre, ce dont ne démontrent pas les autres ? On pourrait le croire, seulement la jurisprudence européenne et interne – s'étant largement appuyé depuis 2010 sur le caractère neutre de

l'activité examinée en l'espèce pour reconnaître l'irresponsabilité pénale d'intermédiaires dont les activités étaient matériellement distinctes en tout point de celles nommés légalement au titre du régime exonératoire – laisse penser que ces autres intermédiaires mériteraient également de voir leur statut défini légalement et leur responsabilité, ou irresponsabilité, prévue expressément. En effet, outre les quelques responsables nommés pour des cyber infractions particulières (V. 79), certains intermédiaires sont oubliés par le droit européen et la loi des régimes de responsabilisation ou responsabilité pénale. Pourtant, ils relèvent bien nécessairement de l'un ou l'autre. Ces intermédiaires absents sont parfois qualifiés « d'éditeurs de services »[195] par la doctrine ou de « fournisseurs de services de médias »[196] par certains instruments européens, en opposition aux prestataires techniques tels que les FAI et les hébergeurs. Les éditeurs de services se découpent classiquement en une catégorie d'intermédiaires qualifiés « d'éditeur de contenu » d'une part et en une catégorie appelée « éditeurs d'outils de recherche et d'échanges »[197] ou « fournisseurs de moyen »[198] d'autre part. La première catégorie, les « éditeurs de contenu », voient leur activité mentionnée, sans être définie, à l'occasion d'un énoncé d'obligations à l'article 6.III-1 de la loi LCEN (« les personnes dont l'activité est d'éditer un service de communication au public en ligne ») et peut renvoyer aux sites et applications non participatifs proposant du contenu de toute nature à leurs utilisateurs (V. 11). La seconde renvoie quant à elle aux intermédiaires qui permettent à leurs utilisateurs de rechercher et d'accéder à du contenu ou bien d'échanger, tels que les moteurs de recherche et les sites et applications participatifs (V. 12). On avait d'ores et déjà souligné la confusion que pouvaient apporter ces qualifications doctrinales et le rapprochement de prestataires *in fine* tous techniques et bien distincts sous de tels termes parapluie (V. 10). Le risque de confusion est d'autant plus important que, si l'éditeur de service est une notion en principe construite par opposition et en creux du prestataire technique, certains éditeurs bénéficient bien du régime de responsabilisation pénale de l'hébergeur, nous le verrons. À ce sujet, l'auteur Céline Castets-Renard avait par ailleurs souligné que « la place des éditeurs de services de communication au public en ligne est particulièrement délicate à définir, entre prestations techniques et éditions de contenus » [199]. Plus simplement, tout intermédiaire qui n'exerce pas d'activité de fourniture d'accès à Internet ou d'hébergement a donc volontairement été exclu du régime de responsabilisation pénale prévu légalement pour les intermédiaires d'Internet. On le sait cependant, certains ont pu être assimilés aux intermédiaires irresponsables par le biais

[195] S. Albrieux, La complicité du fournisseur de moyens de communication électronique, Légipresse 2005, n° 220, II.
[196] Directive 2007/65/CE du 11 déc. 2007, Art. 1 2°, d.
[197] J. Bossan, op. cit., p. 314.
[198] S. Albrieux, op. cit., p. 40.
[199] C. Castets-Renard, Droit de l'Internet, Montchrestien-Lextenso, 2009, n° 809.

d'une conduite neutre de leur activité, ce pourquoi celle-ci, clef de leur irresponsabilité, devient un enjeu phare du contentieux (V. 81).

80. Difficultés inhérentes à la polymorphie des intermédiaires. – À la source des carences de la loi se trouvent entre autres quelques difficultés quant à l'identification des intermédiaires et de leurs activités. L'une d'entre elles tient notamment de la convergence, de la concentration de plusieurs activités d'intermédiaires en une seule activité. En effet, de nombreux sites et applications possèdent un caractère simultanément participatif et non-participatif : tout en proposant du contenu selon une ligne éditoriale bien définie, ils permettent en parallèle aux utilisateurs d'échanger en proposant eux-mêmes du contenu. Amazon ou les marchés en ligne de particuliers, les *marketplace*, présents sur les plateformes classiques de commerce en ligne, en sont les meilleures illustrations puisqu'ils alimentent leur plateforme en contenu mais autorisent également que des utilisateurs mettent à disposition leur contenu sur celle-ci. Pareillement, les journaux en ligne offrent la possibilité aux utilisateurs de commenter les articles, et donc de créer eux-mêmes du contenu sous forme de commentaire. Ces sites et applications seront généralement considérés comme étant participatifs si la majorité du contenu existant sur leur plateforme est celui des utilisateurs ou non-participatifs si la majorité du contenu existant sur leur plateforme est le leur, mais leur ambivalence complexifie l'appréhension juridique de leur responsabilité. La difficulté majeure tient toutefois de la volonté pour les intermédiaires de diversifier leur offre et donc de cumuler des services particulièrement différents les uns des autres, ce qu'a reconnu très tôt la jurisprudence. La pratique est courante et les sociétés possèdent en conséquence plusieurs casquettes qu'ils portent alternativement, selon l'activité exercée relativement au litige. Par exemple, Google est à la fois un moteur de recherche, à la fois une plateforme d'échange (Gmail, Google Drive, Google Meet) et à la fois un hébergeur (Google Cloud) ; Free est un fournisseur d'accès à Internet mais aussi un hébergeur de particuliers (Pages Perso Free) ; Amazon cumule, entre autres, des activités de plateforme de commerce en ligne et d'hébergement (Amazon Web Services, AWS). La même difficultée est rencontrée pour les plateformes de vidéos[200], telles que YouTube et Dailymotion, qui hébergent les vidéos postées par les utilisateurs chez leur société mère mais qui détiennent en parallèle des licences d'exploitation sur certains contenus qu'elles contrôlent en conséquence, ainsi que pour les géants des réseaux sociaux[201], comme Facebook qui héberge en interne le contenu posté par ses utilisateurs mais qui propose également des activités marchandes du type F-commerce, telles que la création d'une page d'entreprise

[200] L. Marino, op. cit., p. 8.
[201] Ibid. p. 9.

Facebook ou l'ouverture d'une boutique Facebook, ainsi que des activités commerciales assimilables à de la publicité... Bref, il existe autant de formules que d'intermédiaires. Par surcroît, la Cour admet non seulement le cumule d'activités d'intermédiaires mais également le cumul de l'activité d'intermédiaire avec d'autres activités qui y sont parfaitement étrangères[202] (en l'espèce, la Cour d'appel de Paris reconnaît que le prestataire exerçant une activité technique de stockage est un hébergeur, nonobstant de son activité principale, la banque). Cette polymorphie sans fin pose naturellement la question de savoir si la responsabilité pénale de l'intermédiaire doit être analysée à travers son statut ou ses activités, et donc de savoir si la loi et le juge doivent identifier l'intermédiaire ou l'activité d'intermédiaire dans le cadre de la détermination de celle-ci.

En raison de ces carences et de la polymorphie des intermédiaires - mais également surtout parce que la loi a justifié l'irresponsabilité de certaines activités intermédiaires par leur neutralité - un contentieux non négligeable s'est formé pour déterminer le régime applicable à l'intermédiaire. Les intermédiaires s'arrachent en effet le titre d'intermédiaire neutre pour jouir du régime de responsabilisation pénale, en démontrant que leur activité est matériellement assimilable aux activités bénéficiant du régime exonératoire de responsabilité et/ou qu'elle est conduite avec neutralité.

***

Section 2. **L'activité de l'intermédiaire au cœur du contentieux**

Démontrons en quoi l'activité de l'intermédiaire est déterminante de l'enjeu phare du contentieux, le régime applicable (§1) avant d'étudier les nombreuses solutions en la matière (§2) et de critiquer le mécanisme global d'identification du régime applicable (§3).

[202] Paris, 14e ch., 4 févr. 2005, n° 04/20259, BNP Paribas.

§1. **Une activité déterminante du régime applicable**

81. Enjeu de contentieux. – Les avancées techniques d'Internet et l'apparition de nouveaux acteurs et de nouvelles cybercriminalités apportant avec eux de nouveaux contentieux ont fait sortir l'appréhension de la responsabilité des intermédiaires du mince sentier battu tracé par la loi. Ainsi, les intermédiaires dont la neutralité n'était pas légalement établie, parce qu'ils n'étaient pas expressément nommés par la loi ou la directive, ont vu leur responsabilité pénale être déterminée par la jurisprudence. Étant l'élément déterminant du régime applicable, et la clef de l'irresponsabilité pénale des intermédiaires, leur neutralité est devenu à ce titre l'enjeu majeur du contentieux car les nouveaux intermédiaires, étrangers à la loi, s'efforcent d'exposer leur rattachement aux catégories d'intermédiaires bénéficiant d'une exonération de responsabilité au titre de leur neutralité. Comment procéder ?

82. L'activité d'intermédiaire. – La première difficulté rencontrée tient à l'évolution des intermédiaires d'Internet qui cumulent les activités d'intermédiaires. Ils peuvent exercer certaines d'entre elles avec neutralité et d'autres sans. Plusieurs façons d'établir la neutralité de l'intermédiaire sont alors possibles lorsque ce dernier cumule les activités d'intermédiaires (V. 80). D'une part, il est possible de considérer *in globo* la neutralité de l'intermédiaire, en examinant la conduite de l'ensemble de ses activités. D'autre part il est possible d'identifier, de différencier les activités d'intermédiaire exercées et puis de distinguer l'existence ou l'absence de neutralité de l'intermédiaire pour chacune d'entre elles[203]. La première approche tendrait alors à examiner la neutralité de l'activité générale de l'intermédiaire, tandis que la seconde tendrait à identifier l'activité d'intermédiaire mis en cause *ratione materiae* dans le litige et d'en examiner la neutralité : un intermédiaire qui cumule les activités serait alors retenu pénalement responsable à la seule condition que celle qui est mise en cause ne soit pas exercée avec neutralité. La première peut donc être qualifiée de globale, la seconde de distributive. Ainsi que le souligne l'auteur Laure Marino, il est souhaitable de « ventiler les régimes de responsabilité »[204] et de retenir la qualification distributive car celle-ci permet de respecter la réalité des intermédiaires d'aujourd'hui qui, depuis l'avènement d'Internet 2.0, multiplient prestations et activités d'intermédiaires, comme on a pu le voir. Il serait en effet très insatisfaisant d'examiner la neutralité globale d'un intermédiaire aux casquettes multiples, alors même que l'ensemble de ses activités sont fondamentalement disparates et ne présentent aucunement le même degré de neutralité par rapport au contrôle exercé sur les données et contenus en cause. Si l'approche distributive

[203] L. Marino, Google au pays des publicités : du droit des marques au droit de la responsabilité : JCP G 2010, p. 642.
[204] L. Marino, Fasc. 670, op. cit., p.7.

semble avoir être consacrée pour la jurisprudence européenne[205], les solutions des juridictions du fond n'ont toutefois pas encore trouvé l'uniformité souhaitée. Ainsi, pour un même intermédiaire, eBay – une plateforme de commerce en ligne permettant aux particuliers et aux professionnels d'acheter et de vendre des biens et services via des enchères ou à prix fixe – les arrêts persistent à diverger : certaines juridictions le qualifie *in globo* d'hébergeur[206], d'autres réfutent cette qualification[207] tandis que d'autres font appel à la méthode distributive pour distinguer ses activités et examiner sa responsabilité[208]. La méthode distributive a également été employée s'agissant de plateformes de multimédia[209], telle que Dailymotion qui, s'il a pu être reconnu comme un hébergeur de contenu de ses utilisateurs, a été qualifié d'éditeur de contenu responsable s'agissant du contenu sur lequel il détenait une licence d'exploitation[210]. Pour eBay, la question était de savoir comment le qualifier sachant qu'il héberge un contenu d'annonces commerciales posté par les utilisateurs sur sa plateforme en même temps qu'il propose la création de liens pour promouvoir les ventes et met donc, parfois, en relation le vendeur et l'acheteur comme le ferait un courtier. Comment départager alors entre les activités cumulées des intermédiaires, au titre de cette approche distributive ? La question peut paraître simple lorsque les activités cumulées des intermédiaires sont particulièrement distinctes, mais, en raison de la polymorphie sans fin des activités d'intermédiaires d'Internet, elle n'est pas toujours évidente. On peut tenter d'y apporter un début de réponse : la participation à la commission d'une cyber infraction par l'utilisateur étant au fond de la responsabilité pénale de l'intermédiaire, c'est l'activité qui a « le plus concouru » à la commission cyber infraction qui est logiquement mise en cause. Ainsi, si plusieurs activités d'intermédiaires exercées par le même intermédiaire concourent à différentes échelles à la commission de la cyber infraction par son utilisateur, il est pertinent que l'activité ayant le plus importé dans le concours apporté à cette commission soit celle qui doit voir sa neutralité être examinée. Il faudrait presque se replonger dans la théorie de la causalité adéquate du droit civil, qui veut que la cause la plus efficiente, déterminante, adéquate doive être considérée pour l'examen du lien de causalité... En outre, la directive commerce électronique et la loi LCEN raisonnent bien en termes non pas d'intermédiaire mais bien

[205] CJUE, 12 juill. 2011, aff. C-324/09, L'Oréal et a. c/ eBay International.
[206] TGI Paris, 3e ch., 1re sect., 13 mars 2012, n° 10/11914.
[207] CA Paris, pôle 5, ch. 12, 23 janv. 2012, n° 11/746., eBay ;TGI Paris, 3e ch., 1re sect., 13 mars 2012, eBay, n° 10/11914. ; CA Paris, pôle 5, 1re ch., 4 avr. 2012, n° 10/00878, Groupement des brocanteurs de Saleya : JurisData n° 2012-010537.
[208] CA Reims, ch. civ., 1re sect., 20 juill. 2010, n° 08/01519, eBay France et International c/ Hermès International et a. : JurisData n° 2010-030753. ; CA Paris, pôle 5, ch. 2, 3 sept. 2010, n° 08/12821, eBay Inc, eBay International c/ Christian Dior Couture : JurisData n° 2010-015040.
[209] L. Marino, op. cit., p. 8.
[210] TGI Paris, 4e sect., 13 sept. 2012, n° 09/19255, TF1 et a. c/ Dailymotion : Comm. com. électr. 2012, comm. 122, note A. Debet ; RLDI 2012/88, n° 2948, note B. Vandevelde.

d'activités d'intermédiaires, nommées aux articles 12, 13 et 14 de la directive et aux articles 6.I-1 et 6.I-2 de la loi LCEN. Conformément à ces textes, il serait alors pertinent que l'approche distributive soit uniformément appliquée par les juridictions dans leur examen de la responsabilité de l'intermédiaire car, dès lors lorsque l'on mentionne de façon générique l'hébergeur, c'est bien entendu à son activité d'hébergement que l'on fait référence. En tout état de cause, une fois l'activité d'intermédiaire identifiée et mise en cause, il faut s'attacher à en examiner la neutralité, l'élément déterminant pour le régime applicable, telle qu'elle est définie par le considérant 42 de la directive électronique pour l'hébergeur, le fournisseur d'accès à Internet et l'opérateur de communication électronique.

83. Neutralité de l'activité. – En raison de l'interprétation stricte des catégories des intermédiaires neutres bénéficiant d'une irresponsabilité pénale en raison de leur neutralité, exigée *a priori* par ledit considérant de la directive commerce électronique (V. 76), les intermédiaires doivent démontrer que leur activité est bien assimilable à celles expressément mentionnées pour identifier les irresponsables. À ce sujet, l'arrêt de la Cour de Justice Européenne Google Adwords a eu une portée considérable puisqu'à la question de savoir si l'intermédiaire mis en cause était un hébergeur, la Cour a répondu sur le terrain du rôle actif, en définissant l'hébergeur avant tout comme un intermédiaire neutre au sens de la directive et en exigeant des juridictions nationales qu'elles devaient en priorité vérifier si les intermédiaires ne jouent pas de rôle actif avant de déterminer leur responsabilité. Autrement dit, en s'appuyant sur le considérant 42 de la directive, la Cour est sortie de l'examen purement matériel de l'activité de l'hébergeur pour l'analyser en premier lieu sous le prisme de sa neutralité. L'arrêt porte à cet égard, sans aucun doute, une part de *praeter legem* en son sein. En effet, si la directive restreint bien le régime exonératoire de responsabilité à certaines activités en son considérant 42, en raison de leur caractère technique, automatique et passif, elle s'attache également à les nommer expressément dans ses articles 12 à 14 de la directive (V. 73). Les activités d'intermédiaires qui bénéficient d'un régime d'irresponsabilité ne se définissent donc pas exclusivement à travers leur caractère neutre mais également à travers leur matérialité : d'autres activités, si elles sont conduites avec neutralité, peuvent matériellement différer de celles définies à ces articles. Cependant, en conséquence de la jurisprudence Adwords, l'assimilation d'un intermédiaire à celui bénéficiant d'une irresponsabilité passe désormais essentiellement par l'examen de sa neutralité et non de la matérialité de son activité. Bien souvent, c'est en réalité l'activité de l'intermédiaire qui, parce qu'elle est matériellement identique ou assimilable à celles définies par la loi comme étant neutres, va pouvoir démontrer l'absence de rôle actif joué par l'intermédiaire, et donc sa neutralité et son irresponsabilité. Ainsi, depuis l'arrêt

Adwords, on peut être tenté de considérer que l'unique prisme d'analyse du régime applicable est la neutralité de l'intermédiaire, mais au fond c'est l'activité de celui-ci qui établit tangiblement cette neutralité et fait basculer le régime applicable, soit parce que ses caractéristiques établissent effectivement cette neutralité, soit parce qu'elle est matériellement rattachable aux activités exonérées de responsabilité pénale nommées par la directive et la loi. Bref, l'examen de l'irresponsabilité de l'intermédiaire, applicable en raison de sa neutralité, se concentre bien sur l'activité qu'il mène mais surtout, depuis 2010, sur la façon dont il la conduit.

§2. **Une activité source de contentieux**

84. Assimilation des intermédiaires à l'hébergeur. – Sans aucun doute, l'activité à la source du plus large contentieux est celle d'hébergeur. Pourtant, la définition même de l'activité d'hébergement ne porte pas plus à confusion que celle de la fourniture d'accès à Internet : *stricto sensu*, il s'agit simplement d'un stockage de données (qui n'est pas temporaire sinon il s'agit de mise en cache). En vingt ans, l'hébergement est l'une des activités d'intermédiaires dont le processus et les méthodes n'ont que très peu changé, s'adaptant simplement aux nouveaux programmes et avancées technologiques permettant d'améliorer leurs performances. Ainsi, lorsqu'il est dit que l'arrivée d'un Internet 2.0 a grandement compliqué la détermination du statut d'hébergeur, on peut s'interroger : si depuis le Web 2.0 il est vrai que l'hébergeur accueille désormais du contenu alimenté par des utilisateurs finals, en quoi sa définition, la matérialité de son activité et de ses méthodes ont-elles pour autant été bouleversées par le Web 2.0 ? Ce sont plutôt les autres intermédiaires, les « éditeurs de services », qui ont vu leur activité être transformée par cette nouvelle version d'Internet. En effet, depuis, l'utilisateur prend une toute nouvelle place dans leurs services qui ont été grandement modulés, contrairement à l'hébergement qui renvoie toujours, comme avant, à l'activité de stockage de données, peu importe d'où elles proviennent. En réalité, la confusion vient donc de ces intermédiaires-là, dans la mesure où il arrive qu'à l'occasion de leurs activités eux aussi se mettent à faire de l'hébergement ou à exercer des activités qui peuvent être assimilées à de l'hébergement.

85. Assimilation matérielle. – Dans un premier temps, celles-ci peuvent être matériellement assimilées à l'activité d'hébergement. Il s'agit d'intermédiaires qui exercent une activité qui, en outre d'être conduite avec neutralité, est tangiblement identique, assimilable, ou englobée par l'activité d'hébergement décrite par la directive et la loi. La jurisprudence a par exemple reconnu que les activités de réencodage (le processus de

conversion d'un type de données ou de code en un autre) et de formatage (le processus de préparation et d'organisation de données, de fichiers ou de supports de stockage) sont « des opérations techniques qui participent de l'essence du prestataire d'hébergement »[211], sous entendu que l'hébergement en lui-même suppose l'exercice de ces activités, qui « n'induisent en rien une sélection (...) des contenus mis en ligne ». Le formatage et le réencodage sont effectivement exercés par des hébergeurs mais aussi par des plateformes multimédia et des réseaux de diffusion de contenu, les CDN, qui proposent la mise en cache comme prestation de services à d'autres intermédiaires. Également, ont été assimilés à une activité d'hébergeur les services proposés par la plupart des sites participatifs, lesquels consistent à présenter, organiser et classifier de façon automatisée les contenus alimentés par les internautes, ce qui est « encore en cohérence avec la fonction de prestataire technique » et ne laisse à l'intermédiaire aucun « choix quant au contenu » nous enseigne la jurisprudence Dailymotion précitée. À quoi renvoie cette notion de « prestataire technique », utilisée en jurisprudence mais qui n'existe nulle part ailleurs ? Certains intermédiaires proposent une prestation de services qui consiste à vendre des services purement techniques, parfois à des intermédiaires, tandis que d'autres mettent à disposition un service qui n'est pas technique mais qui est nécessairement réalisé au moyen de ces techniques. Par cette notion de « prestataire technique », la Cour tente de rapprocher Dailymotion et les autres de cette première catégorie d'intermédiaires, à laquelle appartiennent également hébergeurs et FAI, et dont la neutralité par rapport au contenu litigieux apparaît de façon plus tangible. Plus précisément, si la société se contente de « structurer et classifier les informations mises à la disposition du public pour faciliter l'usage de son service mais que cette société n'était pas l'auteur des titres et des liens hypertextes, ne déterminait ni ne vérifiait les contenus du site », alors les juridictions du fond ont « exactement déduit que relevait du seul régime applicable aux hébergeurs, la responsabilité de ce prestataire, fût-il créateur de son site, qui ne jouait pas un rôle actif de connaissance ou de contrôle des données stockées »[212]. Si la neutralité des intermédiaires en cause dans ces affaires ne soulevait que peu de doutes, on regrette toutefois la complexité de ces motifs puisque Dailymotion propose, outre la présentation et l'organisation de son infrastructure, une réelle activité de stockage des vidéos, en tout point identique à l'activité d'hébergement. Celle-ci était alors suffisante pour établir son irresponsabilité. La même logique a été retenu pour les autres sites participatifs, tels que les réseaux sociaux Facebook et Twitter[213], qui se contentent d'organiser leur infrastructure et de stocker le contenu posté par leurs utilisateurs,

[211] Cass. 1re civ., 17 févr. 2011, n° 09-67.896, Sté Nord-Ouest, Sté UGC Images et a. c/ Sté Dailymotion : JurisData n° 2011-001684 :
[212] Cass. 1re civ., 17 février 2011 n° 09-13.202, 09-67.896 et 09-15.857
[213] TGI Paris, Ord. réf.,13 avr. 2010, Hervé G. c/ Facebook France ; TGI Paris, 24 janv. 2013, n° 13/50262

soit par des serveurs internes, soit en ayant recours à de la sous-traitance d'hébergement, parfois les deux, mais sans jamais contrôler ou prendre connaissance du contenu litigieux. *In fine,* toutes ces activités sont matériellement identiques ou matériellement assimilables à de l'hébergement *strico sensu,* en ce qu'elles consistent bien en du stockage de données. C'est pourquoi, par le biais d'un rattachement matériel tangible avec l'hébergement, leur caractère passif et automatique permettant d'établir la neutralité de l'intermédiaire qui les exerce ne pose que peu de difficultés.

86. Assimilation formelle. – En parallèle, une partie du contentieux se loge également dans une assimilation que l'on peut qualifier de formelle à l'activité d'hébergeur : des activités qui diffèrent matériellement de celle d'un hébergeur *stricto sensu* sont assimilées à celui-ci et bénéficient du régime exonératoire de responsabilité au motif que l'intermédiaire les exerce avec une neutralité formellement identique à celle d'un hébergeur. Les solutions en ce sens remontent dès 2005 et se sont justifiées en référence à la définition communautaire du prestataire d'hébergement qui « ne limite pas l'activité d'hébergement à la prestation purement technique, mais identifie plus précisément l'ensemble des fonctions d'intermédiation qui ne relèvent pas du simple transfert d'information »[214]. Rien dans la directive ne semblait pourtant appuyer cette interprétation. Notamment, c'est le cas du moteur de recherche, qui, s'il référence et indexe du contenu *via* des programmes, ne le stocke pas et ne peut donc pas matériellement s'apparenter à un hébergeur. En effet, bien que les moteurs de recherche aient une activité drastiquement différente de celle d'un hébergeur, la jurisprudence postérieure à la directive et à la loi LCEN s'est constamment appuyée sur le caractère automatique et passif de leur activité, faisant du moteur de recherche un intermédiaire neutre assimilé à l'hébergeur pour établir sa responsabilité pénale au titre de son régime[215] : dans un arrêt relatif à Google image, la Cour a par exemple considéré que « le lien n'est dès lors qu'un outil permettant à l'utilisateur d'accéder facilement à une image qui est à la disposition des internautes du fait du propriétaire du site cible » ; dès lors, « en fournissant ce moyen de consultation, le prestataire de service est neutre ; [...] il n'excède donc pas dans son service de référencement les limites d'un prestataire intermédiaire, ne mettant pas en œuvre une fonction active au sens de la LCEN »[216]. Plus généralement, les juges retiennent régulièrement qu'en raison d'un référencement purement « robotique »

[214] Tribunal de grande instance de Lyon, 21 juillet 2005, n° 9999

[215] V. en ce sens : Cass. 1re civ., 12 juill. 2012, n° 11-15.165 et n° 11-15.188, Aufeminin.com et Google c/ X. et a. : JurisData n° 2012-015812 ; Comm. com. électr. 2012, comm. 91, note Caron ; Gaz. Pal. 18 oct. 2012, n° 292, p. 19, note L. Marino ; D. 2012, p. 2075, note C. Castets-Renard ; D. 2012 p. 2071, concl. C. Petit ; Légipresse 2012, n° 298, p. 566, note Ph. Allaeys ; Propr. intell. 2012, n° 45, p. 416, note A. Lucas ; RTD com. 2012, p. 771, note F. Pollaud-Dulian ; JCP E 2012, 1627, note J.-M. Bruguière

[216] CA Paris, pôle 5, 1re ch., 26 janv. 2011, n° 08/13423, Société des auteurs des arts visuels et de l'image fixe [SAIF] c/ Google

et de la position de tiers des moteurs de recherche par rapport au contenu référencé, ceux-ci n'exercent *a priori* aucun contrôle sur les données et peuvent par conséquent bénéficier du régime de responsabilisation pénale prévu légalement. Bien que formellement l'activité d'intermédiaire de référencement de contenu soit conduite avec une neutralité sensiblement similaire à celle d'un hébergeur, les moteurs de recherche réalisent une prestation de service matérielle distincte en tout point d'un hébergement de données. Il serait donc souhaitable que l'activité exercée par les moteurs de recherche, le référencement de liens dits naturels (car indexés par des programmes mathématiques), voit son statut expressément défini et déterminé comme source d'irresponsabilité du moteur de recherche. En effet, si l'exonération de celui-ci fait sens, il reste peu rigoureux de l'assimiler à un hébergeur en raison de sa seule neutralité. La jurisprudence qui approuve cette assimilation ouvre *de facto* la porte à l'exonération d'intermédiaires sensiblement distincts de ceux légalement nommés comme étant neutres et irresponsables. Ainsi, le moteur de recherche dont l'activité mise en cause n'est pas le référencement de liens « naturels », mais de liens « commerciaux », bénéficie lui aussi du régime de responsabilisation de l'hébergeur, ce qui est plus discutable. Une telle activité s'apparente à de la publicité en ce que les moteurs de recherche font rémunérer un service de référencement avantageux pour leur client ; c'est celle qui était mise en cause dans la jurisprudence Google Adwords de 2010. Le contentieux s'était notamment développé, on l'a vu, suite à des référencements commerciaux de liens de contrefaçons de marque. Si l'avocat général Poiares Maduro avait suggéré que l'activité du moteur de recherche consistant à référencer des liens commerciaux pouvait relever d'une mise en cache et bénéficier d'une irresponsabilité en vertu de l'article 13 de la directive commerce électronique[217], la Cour avait bien décidé de le faire relever du régime de l'hébergeur de l'article 14 de la directive. L'assimilation au régime de l'hébergeur est ici pourtant nettement moins tangible que pour l'activité de référencement de liens naturels : matériellement, l'activité de référencement de liens commerciaux est étrangère à l'hébergement et, formellement, sa neutralité a été reconnue au prix d'une interprétation très stricte du rôle actif, excluant tout indice quant au critère pécuniaire (V. 71). Ainsi que le relève l'auteur Laure Marino, quelques résistances des juges du fond se sont faites sentir à cet égard, le rôle actif étant à leur sens établi dès lors que l'intermédiaire « ne s'est pas bornée à stocker des informations de nature publicitaire, mais qu'elle a inséré, de façon délibérée, dans sa page d'accueil, le mot clef SNCF, lequel dirigeait l'internaute vers des liens concurrents, et retient qu'elle avait l'accès et la maîtrise des mots-clés dans la mesure où elle a pu supprimer cette

[217] L. Marino, op. cit. p. 13.

mention en exécution de la décision de première instance », tentatives systématiquement sanctionnées par la Cour de cassation[218].

87. Refus d'assimilation. – Néanmoins, toutes les activités d'intermédiaires n'ont pas eu la chance de se faire qualifier d'activité technique neutre et de bénéficier d'un régime de responsabilité amoindri. Rappelons-nous, la question s'était posée pour eBay de savoir s'il pouvait être exonéré de responsabilité, alors même qu'il exerçait simultanément une activité de « réception » et d'organisation de contenu d'annonces commerciales ainsi qu'une activité lucrative qui pouvait s'apparenter à du courtage. La Cour de justice européenne, en usant de l'approche distributive qu'elle consacra, reconnut de cette façon que l'activité de mise en relation de vendeurs et d'acheteurs était celle qui avait concouru à la commission de la cyber infraction par l'utilisateur et refusa en ce sens d'assimiler eBay à un hébergeur, c'était en 2011[219]. De la même façon, plus récemment, Airbnb s'est vu être privé d'un tel régime en jurisprudence européenne puis française[220]. De la même façon qu'eBay réceptionne et organise des contenus d'annonces commerciales, Airbnb réceptionne du contenu relatif à des biens de location saisonnière. Toutefois, les deux plateformes participatives divergent matériellement sur quelques points : Airbnb, contrairement à eBay, est issue de l'économie collaborative et possède quelques caractéristiques particulières. Notamment, elle suppose plusieurs relations contractuelles, dont une qui s'applique entre Airbnb et les utilisateurs et une autre qui s'applique entre les utilisateurs eux-mêmes. Airbnb donne donc non seulement des directives à l'ensemble de ses utilisateurs, mais possède également un droit de regard sur les annonces ainsi qu'un droit de sanction, matérialisé, par exemple, en un retrait de contenu, lorsque les utilisateurs ne respectent pas les obligations contractuelles qui leur incombent. En raison de ces caractéristiques particulières, la Cour de justice européenne et la Cour de cassation retiennent en 2019 et 2020 qu'Airbnb est un « éditeur de la société de l'information » selon la formule européenne et se voit être exclu du régime de l'hébergeur.

88. Bilan. – On l'aura donc compris, des intermédiaires appartenant à une même catégorie, les sites participatifs, dont la particularité est d'être massivement alimentés par les internautes, ne répondent pas aux mêmes régimes de responsabilité : certains, comme les réseaux sociaux, relèvent du régime de l'hébergeur, tandis

[218] Cass. com., 20 janv. 2015, n° 11-28.567, Tuto4pc.com c/ SNCF : JurisData n° 2015-000636 ; Comm. com. électr. 2015, comm. 21, note G. Loiseau ; D. 2015, p. 1079, note S. Chatry.
[219] CJUE, 12 juill. 2011, aff. C-324/09, L'Oréal et a. c/ eBay International.
[220] TI Paris, 5 juin 2020, n° 11-19-005405, K. c/ G. et sté Airbnb Ireland, V. également (CJUE, 19 déc. 2019, aff. C-390/18, YA et Airbnb Ireland UC c/ Hôtellerie Turenne SAS et Assoc. AHTOP et Valhotel : JurisData n° 2019-023777 ; Comm. com. électr. 2020, comm. 12, note G. Loiseau.

que d'autres, comme Airbnb, relèvent du régime opposé de « l'éditeur de la société de l'information » et que d'autres encore, comme eBay ou Dailymotion, relèvent alternativement des deux régimes selon que la cyber infraction en cause ait été commise *via* leur activité de réception de contenu, auquel cas ils seront hébergeurs, ou d'exploitation ou de courtage, auquel cas ils seront éditeurs. Comment l'expliquer ? La *ratio decidendi* tourne bien entendu autour de l'appréciation du rôle actif de l'intermédiaire : lorsque celui-ci a un pouvoir de modération qu'il exerce *a priori*, consistant à contrôler et gérer le contenu proactivement, on considère que l'intermédiaire exerce la conduite de son activité sans neutralité tandis que lorsqu'il fait de la modération *a posteriori*, il relève de la qualification de l'hébergeur en raison de sa neutralité dans la conduite de son activité. Une intervention de la loi pour actualiser ces dispositions et notamment pour nommer certaines activités qui, certes, réalisent de la modération *a posteriori* et sont conduites avec neutralité, mais ne correspondent pas matériellement aux activités listées aux articles 12 et 14 de la directives électroniques et 6.I-1 et 6.I-2 de la loi LCEN, serait en ce sens souhaitable. On ne peut dès lors que louer l'arrivée du règlement DSA qui, enfin, étend expressément le régime d'irresponsabilité pénale et de responsabilisation conséquente aux services de référencement, autrement dit les moteurs de recherche, et aux plateformes de partage de vidéos[221]. S'il ne constitue pas encore du droit positif, on se réjouit tout de même de pouvoir bientôt, en 2024, enlever ces intermédiaires de la catégorie d'intermédiaires qui souffrent des carences de la loi.

§3. **Réflexion sur la cohérence des solutions**

89. Changement de *ratio decidendi*. – Dans un premier temps, on constate à la lecture de la jurisprudence que le paradigme établi par la loi a changé et que l'intérêt des catégories nommées d'activités d'intermédiaires est en déclin : si l'on pensait raisonner depuis le début à travers le prisme de l'hébergeur, lequel est légalement défini et tenu pour irresponsable, c'est en réalité à travers celui de l'éditeur que la jurisprudence raisonne désormais. En effet, depuis que des activités d'intermédiaires relativement éloignées de l'activité telles que l'hébergement ont été assimilées à celle-ci en vertu du critère de la neutralité, la réflexion s'est bel et bien inversée : il ne s'agit plus d'exclure du régime de responsabilisation toute activité qui ne relèverait pas de celles légalement exonérées mais d'exclure du régime de responsabilité pénale de l'éditeur tout intermédiaire qui n'en serait pas un, peu importe la pertinence de son assimilation avec les catégories d'intermédiaires exonérés.

[221] Règlement (UE) 2022/2065 op. cit.

90. Superficialité des critères d'identification. – Ensuite, on constate une articulation relativement superficielle entre les critères d'identification de l'activité d'intermédiaire, le rôle actif et la neutralité de l'intermédiaire dans la conduite de celle-ci, et la substance de régimes de responsabilisation pénale et de responsabilité pénale. En effet, en relevant du régime des activités nommées auxdits articles, les intermédiaires ne bénéficient pas uniquement d'une irresponsabilité pénale ; ils deviennent également soumis à l'interdiction de surveillance générale proactive des données de l'article 15 de la directive commerce électronique et 6.I-7 de la loi LCEN. L'examen de la jurisprudence semble à cet égard insatisfaisant car, afin d'identifier les intermédiaires responsabilisés soumis à cette interdiction, les juges s'attachent à découvrir s'ils exercent un rôle actif dans la conduite de leur activité, auquel cas ils seront pénalement responsables. Or, le rôle actif de ces derniers n'est autre que le résultat de la surveillance proactive prohibée – en particulier lorsqu'il est compris comme étant un contrôle intellectuel exercé sur les données (V. 71), et par opposition à une neutralité qui implique l'absence de contrôle de données *a priori* d'un signalement. En effet, la sémantique censée différenciée la « surveillance » du « contrôle » exercé par l'intermédiaire ne trompe pas : la surveillance générale proactive est interdite notamment en raison de l'éventuel contrôle attentatoire aux libertés que l'intermédiaire irait exercer sur les données à l'issue de cette surveillance (c'est pourquoi la recherche active de faits illicites est également prohibée au titre de cette même interdiction). Surveiller proactivement toutes les données et rechercher activement des faits illicites n'est que le préalable d'un contrôle intellectuel exercé sur les données tandis que le rôle actif n'est que la matérialisation de ce contrôle intellectuel. Alors, la surveillance proactive des données est-elle une interdiction appliquée à certains intermédiaires nommés, en raison de leur neutralité et en contrepartie de leur irresponsabilité, ou bien est-elle le préalable du critère d'identification du rôle actif de l'intermédiaire, le rendant pénalement responsable et exclu du régime de ces intermédiaires nommés ? Les deux à la fois. Une telle solution vide l'interdiction de son intérêt et de sa portée dans la mesure où, lorsqu'elle est respectée par un intermédiaire, ce dernier sera identifié comme un intermédiaire neutre et y sera soumis tandis que, lorsqu'elle n'est pas respectée par un intermédiaire qui surveille et, le cas échéant, contrôle les données, elle peut devenir un élément qui le fera relever du régime de responsabilité pénale. *Quid* alors de l'intermédiaire absent des mentions expresses de la directive et de la loi qui exerce un rôle actif, mais dont l'activité est matériellement assimilable à l'une des catégories d'intermédiaires soumises à l'interdiction de surveillance générale ? À la lecture de la jurisprudence, la solution qui s'appliquerait ne s'impose pas avec clarté : on pourrait relever la violation de l'interdiction précitée comme on pourrait considérer qu'en dépit des caractéristiques de son activité, le rôle actif joué par

l'intermédiaire dans la conduite de celle-ci l'exclut d'un tel régime. Le même niveau de rigueur était de mise lorsqu'à l'inverse il fallait assimiler un moteur de recherche à un hébergeur pour l'en faire relever, or même que les activités exercées étaient en tout point distinctes. Ainsi, l'incohérence que nous tentons de pointer du doigt n'est pas l'existence du critère de rôle actif ou celle de l'interdiction de surveillance générale proactive d'Internet mais bien leur existence simultanée. Si certains intermédiaires légalement nommés sont soumis à une telle interdiction et bénéficient d'un régime exonératoire, il était incohérent de s'attacher à les identifier à travers leur neutralité et par opposition aux intermédiaires responsables qui auraient eu un rôle actif dans la conduite de leur activité, puisque celui-ci est rien d'autre que le résultat de l'interdiction auxquels les irresponsables sont soumis. Le critère d'identification et l'interdiction sont en fait circulaires : seule l'assimilation matérielle aux activités neutres aurait dû être admise par la jurisprudence. Quant à la loi, il aurait été plus rigoureux de prévoir les écarts de la jurisprudence en s'en tenant à la définition matérielle des intermédiaires irresponsables, dans la mesure où la neutralité n'est pas un critère d'identification mais la simple conséquence du respect de leur interdiction et qu'elle ne peut constituer les deux sous peine de vider l'interdiction de toute portée. La jurisprudence n'aurait plus eu plus qu'à se demander si l'activité relevait matériellement d'une transmission ou d'un stockage de données pour déterminer le régime applicable. Quel intérêt y-a-t-il en réalité à dire qu'une activité de stockage ou de transmission de données possède un caractère technique et passif qui rend l'intermédiaire neutre si ce n'est pour prévoir et amortir les interprétations prétoriennes englobantes et extensives, presque dynamiques, des définitions légales ? L'activité de stockage *strico sensu* et de transmission *stricto sensu* d'une connexion Internet ne peuvent jamais donner lieu à autre chose que de la neutralité dès lors qu'ils respectent l'interdiction de surveillance générale *proactive* des données. La neutralité ne devait donc pas être un ticket d'entrée vers le régime de responsabilisation pénale pour des intermédiaires comme le moteur de recherche mais bien la conséquence exclusive du respect de l'interdiction des données. À charge pour le législateur d'étoffer la liste des activités d'intermédiaires. Quel sens y-avait-t-il enfin à distinguer ceux qui seront soumis à une interdiction de ceux qui ne le seront pas par un critère d'identification qui n'était autre que le résultat du respect ou de la violation de ladite interdiction ? L'arrivée du *Digital Service Act*, vingt ans après la directive commerce électronique, allongeant la liste des intermédiaires qui voient leur situation légalement régie, pallie à cette instabilité pour certains intermédiaires. On ne peut alors qu'espérer attendre moins de vingt ans pour le prochain instrument en la matière.

CONCLUSION

In fine, la responsabilité pénale des intermédiaires en cas de commission de cyber infractions par leurs utilisateurs est un sujet qui ne souffre pas d'une trop grande simplicité. Au contraire, il est en proie à une complexité inhérente à la définition même de l'intermédiaire et de son activité, voire de ses activités, ainsi qu'aux caractéristiques particulières d'Internet, lesquelles ne sont pas toujours appréhendées avec justesse par le droit (ou qui parfois le sont mais quelques années après). Le rôle central des intermédiaires dans le fonctionnement d'Internet les expose à une multitude de comportements délictueux et impose alors naturellement la question de leur responsabilité pénale à raison de ces cyber infractions, commises par leurs utilisateurs. Celle-ci se trouve à un carrefour d'enjeux et d'impératifs : d'une part la nature dualiste des intermédiaires, à la fois vecteurs potentiels de cybercriminalité et acteurs essentiels dans la lutte contre celle-ci, offre un terrain complexe pour la régulation, d'autre part l'équilibre entre les libertés fondamentales - vie privée, liberté d'expression et économique - et la nécessité de protéger la société contre la criminalité en ligne est constamment menacé par le degré de responsabilité des intermédiaires. On retrouve inlassablement, une énième fois, le dilemme classique du droit pénal qui oppose sécurité et liberté, ici appliqué à l'espace cyber et aux acteurs de cet espace. La complexité technique de la matière est en cela doublée d'une importante complexité juridique.

Dans ce contexte, le législateur a fait preuve d'un réalisme et d'un pragmatisme louable dès les années 2000, et ses mécanismes ont su perdurer malgré les évolutions incontrôlables d'Internet et de ses intermédiaires. Pourtant avide d'extension et d'expansion de textes incriminants, de sanctions pénales et de responsabilité pénale à l'ère contemporaine, le législateur a su composer avec prudence pour soumettre les intermédiaires à un mécanisme de responsabilité qui colle avec la réalité d'Internet : certains intermédiaires ne peuvent connaître des cyber infractions commises par leurs utilisateurs, notamment parce qu'ils ont l'interdiction de surveiller leurs données lorsqu'ils exercent un certain type d'activité, et donc ne peuvent être tenus pénalement responsables à raison de celles-ci, tandis que d'autres le peuvent et peuvent en ce sens être considérés comme de potentiels responsables. Jamais le législateur n'est tombé dans l'écueil grave d'une véritable responsabilité pénale du fait d'autrui.

Alors, les quelques critiques se concentrent naturellement sur les mises à jour trop espacées des dispositions en la matière, peu surprenantes, sur les interprétations parfois bancales de la jurisprudence, elles non plus peu surprenantes, ou sur les mécanismes de droit commun un peu décalés avec la réalité des intermédiaires, comme

l'application parfois marginale du régime de la complicité. Bref, le bilan semble globalement satisfaisant à l'égard de la complexité particulière de la matière, car disons-le, il pourrait être pire.

La question de la responsabilité pénale des intermédiaires d'Internet nécessite néanmoins une attention constante et renouvelée de la part des législateurs et des juristes, car Internet avance vite, très vite. Si vite, que, quand viendra le temps d'Internet 3.0, où la gestion d'internet sera entre les mains des intelligences artificielles et son stockage entre celles des utilisateurs par un réseau de noeuds mondialement distribués, le droit sera confronté à une nouvelle question : comment retenir la responsabilité pénale de robots ? On reviendra alors, peut-être, à la solution originelle selon laquelle seuls les utilisateurs sont pénalement responsables de leurs méfaits en regrettant le temps où l'on pouvait retenir la responsabilité des intermédiaires et les faire participer à la lutte contre la cybercriminalité.

BIBLIOGRAPHIE

I.- Traités et manuels

- T. Azzi, La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ?, in Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le WEB 2.0 : LexisNexis, coll. IRPI, 2009.
- C. Castets-Renard, Droit de l'Internet, Montchrestien-Lextenso, 2009, n° 809.
- F. Chabas, H. & L. Mazeaud, A. Tunc, Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, 6e éd., t. 1, Montchrestien, 1965.
- G. Cornu, Vocabulaire juridique, 12ème édition, Association Henri Capitant, Presses Universitaires de France - P.U.F.
- M. Delmas-Marty, Le relatif et l'universel. Les forces imaginantes du droit, T. 1, Seuil, coll. La couleur des idées, 2004.
- E. Dreyer, in Traité de droit de la presse et des médias, dir. B. Beigner, B. de Lamy et E. Dreyer, LexisNexis, coll. Traités, 2009.
- E. Dreyer, Droit de la communication, LexisNexis, 2021.
- Ch. Féral-Schuhl, Cyberdroit : le droit à l'épreuve de l'Internet, Paris, Dalloz, 2010, n° 114.24.
- F.-H. Knight, D.-E. Jones, Risk, Uncertainty and Profit, Cornell University Library's print collections, 1921.
- A. Lucas, H.-J. Lucas et A. Lucas-Scholetter, Traité de la propriété littéraire et artistique : LexisNexis, 4e éd. 2012, n° 1109.
- E. Plenel, Le droit de savoir, Don Quichotte éd., coll. « Points 3207 », 2013
- P. Riché, Internet a rendu concrète la liberté d'expression, gare au retour en arrière !, in Justice et liberté d'expression, PULIM, coll. « D'Aguesseau », 2014.
- N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, The MIT Press, 1948.
- N. Wiener, The human use of human beings, 1950, Eyre & Spottiswoode.

II.- Ouvrages.

- R. Bismuth, Pour une appréhension nuancée de l'extraterritorialité du droit américain – Quelques réflexions autour des procédures et sanctions visant Alstom et BNP Paribas, Annuaire français de droit international, 2015.
- F. Chopin, Cybercriminalité, Répertoire de droit pénal et de procédure pénale, 2021
- R. Gassin, Le droit pénal de l'informatique, D. 1986. Chron. 35.
- D. Legall, La responsabilité pénale des acteurs de l'Internet, Fiches pratiques LexisNexis N° 4496.
- L. Marino, Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement, JurisClasseur Communication, Fasc. 670, 30 août 2015.
- J.-H. Robert, Principe de responsabilité personnelle, JurisClasseur Droit pénal, Fasc. 20, 24 août 2020
- J.-H. Robert, Complicité, JurisClasseur Droit pénal, Fasc. 20, 30 septembre 2022.

III. Articles

- S. Albrieux, La complicité du fournisseur de moyens de communication électronique, Légipresse 2005, n° 220, II.
- J. Bossan, Le droit pénal confronté à la diversité des intermédiaires d'internet, Revue de droit pénal et sciences criminelles n° 2, 2013.
- C. Caron, Fin de siècle, Com. comm., électr n° 12, décembre 2021.
- V.-G. Cerf, R.-E. Kahn, A Protocol for Packet Network Intercommunication, IEEE Transactions on Communications, 1974.
- A. De La Grange, Comment la Chine contrôle Internet, Figaro international, Paris : 22 janvier 2010.
- M. Quéméner et J. Ferry, Cybercriminalité : défi mondial et réponses, Economica, 2007.
- S.-M. Cabon, L'influence du cyberespace sur la criminalité économique et financière, Dr. pénal 2018, no 3, Étude 5.
- L. De Brabandere, Aux origines du mot « cyber », La tribune, Paris : 13 février 2017.
- X. De La Porte, Internet n'est pas neutre, c'est un pharmakon, Ce qui nous arrive sur la toile, Matins Matins de France Culture, Radio France, 14 janvier 2014.

- E. Derieux, Neutralité et responsabilité des intermédiaires de l'Internet. Mythe ou réalité ? La semaine de la doctrine, La semaine juridique - édition générale, n°13, 26 mars 2012.
- J. Derrida, La pharmacie de Platon, in La dissémination, Paris : Seuil, 1972. ; R. Brague, En marge de « La pharmacie de Platon » de J. Derrida, Revue Philosophique de Louvain.
- M. Harzoune, 1980-2022 : lois sur l'immigration, le mille-feuilles législatif, Musée de l'histoire de l'immigration, Paris : janvier 2023.
- A. Lepage, Libertés et droits fondamentaux à l'épreuve de l'Internet, Litec, 2003, p. 86 et M. Vivant, « Cybermonde : Droit et droits des réseaux », JCP G. 1996, I, 3969, n° 23.
- G. Loiseau, Plateforme en ligne - Dissémination de contenus illicites : la pression monte vis-à-vis des opérateurs numériques, Com. comm. électr. n° 10, Octobre 2021, comm. 72.
- G. Loiseau, Hébergeur - La responsabilité des plateformes de partage de vidéos, Com. comm. électr. n° 9, Septembre 2021
- G. Loiseau., Le standard du « manifestement illicite » dans la responsabilité des hébergeurs, Com. et comm. électr. N°11, janvier 2023, comm. 2.
- G. Loiseau, Responsabilité de l'hébergeur - La suppression de contenus identiques ou équivalents au contenu déclaré illicite, Communication Commerce électronique n° 11, Novembre 2019, comm. 67.
- G. Loiseau, Le rôle actif de l'exploitant d'un site de mise en relation de revendeurs et d'acheteurs de billets donnant accès à des événements sportifs, Comm. com. électr. n°9, septembre 2022, comm. n°58.
- L. Marino, Google au pays des publicités : du droit des marques au droit de la responsabilité : JCP G 2010.
- V. Malingre et A. Leparmentier, TikTok, menacé d'interdiction aux États-Unis, veut jouer l'opinion contre les gouvernements occidentaux, Le Monde, Paris : 23 mars 2023., V. également : P. Escande, TikTok : Les États-Unis entendent faire tomber le rideau sur les appétits des marchands chinois, Le Monde, Paris : 16 mars 2023.
- Y. Padova, Un aperçu de la lutte contre la cybercriminalité en France, RSC 2002.
- F. Rousseau, Complice ou auteur indirect d'une infraction non intentionnelle, Dr. pén. 2007, étude 11. – I. Moine-Dupuis, Complicité et contribution à une infraction non intentionnelle, RPDP 2005.

TABLE DES MATIÈRES

INTRODUCTION

PARTIE PREMIÈRE : LE RÉGIME DE RESPONSABILITÉ PÉNALE DES INTERMÉDIAIRES D'INTERNET

24. La cyber infraction et Internet
25. La cyber infraction et l'intermédiaire d'Internet

II. L'intermédiaire-remède : un allié cardinal dans la lutte contre la cybercriminalité

26. Pouvoirs de l'intermédiaire

III. L'intermédiaire-bouc émissaire : un responsable expiatoire de cybercriminalité

27. Responsables idéaux
28. Identification de l'intermédiaire
29. Solvabilité de l'intermédiaire
30. Théorie du risque

Section 2. **Limites du fondement**

I. Libéralisme économique et liberté d'expression

31. Libéralisme économique
32. Liberté d'expression
33. Limite à la limite

II. Incidences sur la construction du régime de l'intermédiaire

34. Respect des libertés
35. Respect du principe de responsabilité personnelle

Chapitre 2. **Scission de la responsabilité pénale des intermédiaires d'Internet**

Section préliminaire. **Le droit applicable**

I. Le droit substantiellement applicable

36. Spécialité du droit pénal

II. Le droit territorialement applicable

37. Applicabilité territoriale du droit pénal aux intermédiaires
38. Applicabilité de la loi pénale dans l'espace
39. Applicabilité de la loi pénale dans l'espace cyber
40. Conséquences d'une compétence territoriale souple
41. Nécessité d'uniformiser les législations nationales
42. Uniformisation des législations relatives à la cybercriminalité
43. Uniformisation des législations relatives aux Intermédiaires d'Internet

Section 1. **Régime de responsabilisation pénale**

I. Un régime exonératoire de responsabilité pénale

44. Introduction d'un régime par contraste
45. Interdiction de la surveillance générale proactive d'Internet
46. Libéralité du régime de responsabilisation

II. Un régime d'obligations incombant à l'intermédiaire

47. Obligations à charge des intermédiaires irresponsables
48. Le dispositif de signalement
49. Le dispositif de filtrage
50. Le retrait, blocage et déréférencement
51. Obligations particulières
52. Renforcement des obligations

Section 2. **Régime de responsabilité pénale**

I. Un régime de complicité des cyber infractions

53. Complicité des intermédiaires
54. Conditions de la complicité
55. Approche des cyber infractions

II. Un régime centré autour de la diffusion de contenus illicites

56. Conséquence du défaut d'intention
57. Cyber infractions de presse
58. Terrorisme et pédopornographie
59. Contrefaçon

PARTIE PREMIÈRE : LA MISE EN OEUVRE DE LA RESPONSABILITÉ PÉNALE DES INTERMÉDIAIRES D'INTERNET

Chapitre 1. **La neutralité de l'intermédiaire, pierre angulaire de sa responsabilité pénale**

Section 1. **Neutralité et irresponsabilité pénale**

I. La neutralité de l'intermédiaire dans la conduite de son activité

60. La neutralité dans la conduite de l'activité
61. Principe de neutralité

II. Une neutralité cause d'irresponsabilité pénale

62. Irresponsabilité pénale des intermédiaires
63. Rupture avec les solutions antérieures

Section 2. **Neutralité limitée et responsabilité pénale**

I. Répression de l'inertie face au contenu illicite

64. Limite à la responsabilisation pénale
65. Connaissance du contenu illicite
66. Le standard du manifestement illicite
67. Étendue du contenu manifestement illicite

II. Compatibilité avec la neutralité de l'intermédiaire

68. Compatibilité avec le principe de neutralité

Section 3. **Absence de neutralité et responsabilité pénale**

I. Absence de neutralité de l'intermédiaire

69. Absence de neutralité
70. Rôle actif

II. Critères du rôle actif de l'intermédiaire

71. Contrôle intellectuel
72. Critiques

Chapitré 2. **L'activité de l'intermédiaire, élément déterminant du régime applicable**

Section 1. **L'activité de l'intermédiaire au coeur de la loi**

I. Responsables légalement déterminés

73. Activités neutres nommées
74. Statut légal du FAI
75. Statut légal de l'hébergeur
76. Interprétation stricte
77. Responsables nommés

II. Carences de la loi

78. Transposition partiellement satisfaisante
79. Statuts absents de la loi
80. Difficultés inhérentes à la polymorphie des intermédiaires d'internet

Section 2. **L'activité de l'intermédiaire au coeur du contentieux**

I. Une activité déterminante du régime applicable

81. Enjeu de contentieux
82. L'activité d'intermédiaire
83. Neutralité de l'activité

II. Une activité source de contentieux