NORMA

RAPPORT

ASPECTS JURIDIQUES DE LA MANIPULATION DE L'INFORMATION

JUIN 2025

Clinique Juridique Lawfare Sorbonne

LES JEUNES IHEDN

Avec la collaboration de :

Clinique Juridique Lawfare Sorbonne

LES JEUNES IHEDN

Rapport réalisé et coordonné sous la direction de **NORMA**, représenté par **Alexandre Clabault** et **Baptiste Ferszterowski**, dans le cadre des réflexions initiées par le Campus Cyber, le CNRS, l'état-major des armées et l'INRIA.

Contributeurs :

- **Daniel Mainguy**

  Professeur à l'École de Droit de La Sorbonne – Université Paris I Panthéon-Sorbonne ; agrégé des Facultés de droit (droit privé) ; arbitre.

- **Jean Bruschi**

  Maître de conférences à l'Université Paris VIII – Vincennes Saint-Denis.

- **Alexandre Clabault**

  Of Counsel – Cabinet Bruzzo Dubucq ; président fondateur de Norma.

  Doctorant École de Droit de la Sorbonne : *Méthodologie d'élaboration de décisions opérationnelles tactiques juridique*.

- **Romane Croizet Fontane**

  Doctorante Université Côte d'Azur : *Union européenne et espace extra-atmosphérique Étude de l'action normative de l'Union dans le domaine spatial*.

- **Baptiste Ferszterowski**

  Direction du projet ; cofondateur de Norma.

- **Manon Le Coroller**

  Membre du Comité directeur des Jeunes IHEDN ; responsable de l'*Innovation Lab*.

Institutions ayant collaborées :

- **Les Jeunes IHEDN** – *Innovation Lab et Pôle Publications*
- **Clinique Juridique *Lawfare* de la Sorbonne**

AVERTISSEMENT

Fondée en 2019, NORMA est une association visant à favoriser la circulation des savoirs et contribuer à une meilleure compréhension des usages stratégiques du droit et des enjeux liés à l'intelligence juridique.

En effet, ces dernières années ont vu le développement de nombreux concepts visant à étudier la manière dont le droit peut être instrumentalisé : droit de la guerre atypique, d'opération juridique, *lawfare* etc.

« L'ensemble des techniques et des moyens permettant à un acteur privé ou public – de connaître l'environnement juridique dont il est tributaire, d'en identifier et d'en anticiper les risques et les opportunités potentielles, d'agir sur son évolution et de disposer des informations et des droits nécessaires pour pouvoir mettre en œuvre les instruments juridiques aptes à réaliser ses objectifs stratégiques. »

Dans ce cadre, NORMA est la première association francophone visant à documenter, analyser et partager autour de l'Intelligence juridique de manière transdisciplinaire et communautaire.

Face à la montée en puissance des attaques informationnelles en France, un cycle d'ateliers et de travail sur la Lutte contre la Manipulation de l'information (LMI) a été organisé au Campus Cyber en partenariat avec le CNRS, l'Inria et l'État-major des Armées. Ce cycle a mobilisé 250 participants volontaires issus de la société civile, ainsi que de différentes institutions dans une action d'intelligence collective. Initié en octobre 2024 et jusqu'en juin 2025, ce groupe de travail a posé les fondations d'une réflexion interdisciplinaire sur la LMI en France.

L'objectif est de renforcer les synergies entre la recherche, les décideurs, les industriels, la société civile et les médias, au travers d'ateliers collaboratifs. Dans le prolongement de cette action, une équipe d'universitaires, de professionnels du droit et d'intelligence économique s'est constituée avec la volonté d'apporter des réponses sur le plan juridique en matière de lutte contre la manipulation de l'information.

Les propos exprimés dans cet ouvrage n'engagent que la responsabilité des auteurs.

Comment citer cette publication :

Mainguy D., Bruschi J., Clabault A., Croizet Fontane R., Ferszterowski B. *Aspects juridiques de la manipulation de l'information*. Norma, 2025.

NORMA

contact@norma-project.com

www.norma-project.com

SOMMAIRE

INTRODUCTION ET CONTEXTE

1. Le temps est loin des rapports de force strictement militaires, ou plus exactement, le temps est celui, y compris éventuellement dans des rapports de force militaires, de rapports de force précédés, dépassés, accompagnés, contournés, remplacés, etc., par des rapports de force non militaires et/ou non armés. Ces rapports de force reposent désormais sur des enjeux économiques et culturels devenus majeurs et premiers, sont fondés, entre autres, sur la circulation de l'information dont la possession et le contrôle, notamment à l'heure du numérique, forgent la puissance d'une entité et, lorsque cette entité est un État, la cohésion même de la nation qu'il représente. Dans le domaine public ou privé, le capital immatériel a progressivement pris une place prépondérante non seulement dans les secteurs économiques et culturels, mais aussi stratégiques. L'essor de l'informatique et du cyberespace enfin, sur lesquels évoluent des sociétés privées gigantesques, ont transformé le rapport à l'information à la fois par son mode d'appropriation (données) et son mode de diffusion (plateformes, réseaux sociaux) au point d'en faire un enjeu géopolitique et stratégique majeur. Qui connaît les fondements de la culture de l'adversaire peut chercher à les saper ; qui contrôle l'information peut déstabiliser l'adversaire[1].

2. Ce basculement vers une société de l'information a, assez logiquement, déplacé les théâtres d'opérations vers ces nouvelles sphères où s'échangent des actes franchement hostiles que l'on regroupe, généralement, sous le terme de *guerre informationnelle* dans une *société de la désinformation*, selon l'idée *a priori* farfelue mais efficace selon laquelle la vérité est une *fake news* comme les autres.

Le termes « guerre » ne doit pas induire en erreur : la guerre est ici une image plus qu'une réalité ou plus exactement, une ambiance, une atmosphère, une atmosphère de guerre. C'est précisément ce qui rend délicat le travail de qualification : si nous ne sommes pas en présence d'un acte de guerre à proprement parler, nous ne sommes pas non plus en

[1] D. Colon, *La guerre de l'information*, Texto, Tallandier, 2025 ; C. Marangé et M. Quessard (dir.), *Les guerres de l'information à l'ère numérique*, PUF, 2021.

présence d'un acte d'influence relevant de l'exercice honnête et habile d'un *soft power* légitime. Manifestement, la guerre informationnelle intervient dans une zone grise, dans « cette guerre avant la guerre[2]», qu'évoque le général d'armée Thierry Burkhard, et dont les traits ne peuvent être qu'« atypiques »[3]. La logique du « tout ou rien », c'est-à-dire de la paix ou de la guerre, éventuellement ponctuée par un temps de crise, ou de tension, a fait son temps. Il est primordial de prendre en compte les formes non-armées de conflits dont les contours et les manifestations sont tantôt évidentes, tantôt parfaitement floues, mais toujours dangereuses pour les intérêts fondamentaux de la nation.

L'une des méthodes permettant de percevoir ce changement est de comprendre les différents temps de la conflictualité, ne serait-ce que pour dissocier la phase ultime, celle de l'affrontement armé, de périodes dans lesquelles, même sans de tels affrontements, des agressions dans une atmosphère de guerre pèsent. Ces nouvelles formes d'agressions, la « guerre sans limite » dans la doctrine chinoise[4] ou le « contournement de la lutte armée » dans la conception russe, peuvent en effet être pensées indépendamment des règles et de la doctrine des conflits armés. La formule *« compétition, contestation, affrontement »* également empruntée au général d'armée Burkhard rend parfaitement compte, y compris dans des champs non-armés et non-militaires, de l'échelle de ces tensions[5].

La phase de « *compétition* » correspond aux relations normales entre les États en temps de paix, et en particulier entre les démocraties libérales, qui se font confiance pour respecter l'État de droit et l'ordre international. Pourtant, les comportements agressifs ne sont pas rares, entre États ou à l'égard d'une entité privée, par application par exemple des règles du droit de la concurrence, pénal ou du droit financier à un non-national, dans une logique d'application extraterritoriale qui n'est pas réservée aux seules lois américaines, ou encore des actions d'influence ou de lobbying, voire d'ingérence, souvent perçues comme des *agressions* lorsque les intérêts supérieurs d'un État sont affectés.

[2] T. Burkhard, État-major des armées, communiqué publié le 27 février 2024.
[3] D. Mainguy, *Droit de la « guerre atypique »*, LGDJ, 2023.
[4] Q. Liang, W. Xiangsui, *Unrestricted Warfare*, People's Liberation Army Literature and Arts Publishing House, 1999 (on line).
[5] T. Burkhard, « Vision stratégique du Chef d'État-Major des armées », oct. 2021.

La phase de « contestation » intensifie les tensions avec l'intervention de l'espionnage, des cyberattaques ou des campagnes de désinformation, privées, paramilitaires ou militaires, plus ou moins imputables à un État. À bien des égards, cette phase correspond soit à des exagérations temporaires dans les relations entre démocraties libérales, soit au comportement ordinaire d'un État autoritaire avec ses citoyens ou ses voisins, en particulier les démocraties libérales considérées comme « faibles ». En réponse, ces dernières adoptent, éventuellement, des sanctions économiques, appelant à des contre-sanctions, etc.

Enfin, la phase de « *confrontation* » est celle de la guerre elle-même, à laquelle s'ajoutent à nouveau toutes les règles du droit des conflits armés et des règles internes brutales : confiscation des biens étrangers, arrestations d'étrangers « ennemis », etc. Il existe toutefois une difficulté avec les actions étatiques « en dessous du seuil de la guerre », qui comprennent la cyberguerre, la manipulation massive de l'information, ainsi que le soutien ou le financement d'actions terroristes, voire d'opérations militaires proprement dites. Ces actions sont difficiles à classer, entre la période de « *contestation* » et celle de « *confrontation* ».

3. Dans un contexte de guerre informationnelle, les armes utilisées sont celles qui permettent la *manipulation de l'information* – mot valise derrière lequel sont regroupées toutes les pratiques qui consistent à user malhonnêtement de l'information dans le but de déstabiliser une personne publique ou privée, qu'elle soit morale ou physique. On reconnaîtra derrière cet ensemble de pratiques une évolution du phénomène de propagande, des techniques de désinformation et de la forge du faux – très anciennes au demeurant[6], sans d'ailleurs avoir la manipulation pour unique but[7]– dont l'amplification permise par les nouvelles technologies, le numérique et la mondialisation leur ont conféré une intensité sans précédent. La généralisation des procédés qui dépassent le seul domaine politique, ses modes de diffusion, la diversité de ses provenances et de ses objectifs imposent un danger inédit et permanent à nos

[6] D. Colon, *Propagande – La manipulation de masse dans le monde contemporain*, Champs Flammarion, 2021.
[7] P. Bertrand, *Forger le faux. Les usages de l'écrit au Moyen Age*, Seuil, 2025.

démocraties[8] qui peinent à apporter une réponse dont l'efficacité dépend de la mobilisation de tous les acteurs et secteurs de la société française. Les droits français et européen ont, pour leur part, progressivement mis en place des moyens[9]de lutter contre la manipulation d'information mais n'échappent pas à l'effet brouillard qu'induisent les conflits non-armés.

4. De manière générale en effet, les règles juridiques visant à sanctionner ou encadrer les pratiques hostiles de guerre atypique sont difficiles à identifier. S'il existe, bien évidemment, un droit des conflits armés, il n'existe pas de droit des conflits non-armés – du moins en tant que discipline autonome. Identifier un arsenal juridique dans un contexte de guerre grise suppose ainsi de partir, d'une part, à la recherche de grappes de droit qui appréhendent un phénomène hostile bien précis et se justifient par lui (loi anti-*fakenews*, sanctions économiques, cybercriminalité) ou, d'autre part, de raccorder certaines branches de droit qui pourraient être applicables à un acte hostile sans avoir été pensées pour lutter contre lui (arbitrage, droit international privé, droit des sociétés, droit pénal). Il faut ainsi aller puiser dans différentes sources, ce qui rend difficile, *a priori*, toute tentative de systématisation puisque certains textes relèvent d'un véritable droit de la « guerre atypique[10]» tandis que d'autres sont mobilisés au soutien de celle-ci, quand bien même l'essence du texte n'est pas d'être excipé dans un tel contexte. Il y a donc, comme à l'armée, une armée de métier et une armée conscrite : des textes faits pour lutter, d'autres mobilisés pour lutter dans un contexte donné. Cette vision du droit participe à lui donner les contours d'une véritable arme de guerre[11] que l'on instrumentaliserait et exporterait pour servir des intérêts étatiques ou économiques déterminés. Ce que l'on appelle le *lawfare* (contraction de *law* et de *warfare*) ne doit pas ici induire en erreur : il ne s'agit pas d'instrumentaliser le droit mais simplement de l'appliquer tel qu'il existe – sauf à retenir une acception très large du *lawfare*[12].

[8] D. Chavalarias, *Toxic Data*, Champs, Flammarion, 2025.
[9] J.-B. Jeangène Vilmer, « Panorama des mesures prises contre les manipulations de l'information », in *Les guerres de l'information à l'ère numérique*, PUF, 2021, p.365 et s.
[10] D. Mainguy, *Droit de la « guerre atypique »,* LGDJ, 2023, n°76.
[11] A. Laïdi, *Le droit nouvelle arme de guerre économique*, Actes sud, 2019 ; D. Mainguy, *Droit de la « guerre atypique »,* op. cit., n°6 ; « lawfare et contre-lawfare : la règle de droit comme arme de guerre », *in Mélanges Hervé Le Nabasque*, LGDJ-Lextension, 2025.
[12] D. Mainguy, *Droit de la « guerre atypique »,* op. cit., n°6.

5. La manipulation d'information illustre parfaitement cette zone grise dans laquelle s'échangent des actes manifestement hostiles sans pour autant relever du droit des conflits armés. L'appréhension de la manipulation d'information par le droit est particulièrement délicate en ce qu'elle se trouve aux frontières de la liberté d'expression et que la ligne de démarcation est parfois difficile à tracer. C'est pourquoi les droits des démocraties libérales peinent à mettre en place un système de défense efficace et ne luttent pas à armes égales face à leurs homologues autoritaires[13]. Mais il n'en reste pas moins que les droits français et européen disposent d'un arsenal juridique fourni qui, bien utilisé, permettrait de lutter efficacement contre la manipulation d'information. Dans ce contexte particulier, il y a là aussi, un droit *de* la manipulation d'information et un droit *qui permet* de lutter contre la manipulation d'information ; un droit pensé pour lutter contre la manipulation d'information dans un contexte de guerre atypique et un droit mobilisé pour lutter contre elle. Par exemple, la loi dite anti « fake news » du 22 décembre 2018 a été pensée pour le contexte de la manipulation de l'information *électorale*, tandis que le délit financier de fourniture d'informations fausses ou trompeuses a été pensé sous d'autres cieux mais peut être mobilisé dans un contexte de guerre atypique. Nous constaterons ainsi cette ambivalence, qui permet de solliciter un grand nombre de textes pour lutter contre le phénomène de manipulation de l'information. Un droit spécialisé donc, et un droit mobilisé.

6. Commençons par circonscrire le propos. L'expression « lutte contre la manipulation de l'information » parfois abrégée « LMI » n'est pas une catégorie juridique arrêtée. Certains textes la mentionnent expressément[14] et peuvent donner l'impression que la lutte contre la manipulation de l'information ne concerne que les fausses nouvelles et l'intoxication en période électorale. Or, la lutte contre la manipulation de l'information déborde très largement de ce cadre et il convient d'en adopter la définition la plus large possible pour avoir la plus grande marge d'action.

[13] C. Marangé et M. Quessard, Les guerres de l'information à l'ère numérique, PUF, 2021, pp. 115-227 ; L. Convert, « La fausse information en droit comparé », Jurisclasseur Communications, 2021.
[14] Loi n°2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information en période électorale.

7. Pour appréhender pleinement les dynamiques à l'œuvre dans les manipulations de l'information, il convient d'abord de définir et d'adopter une lecture systémique de l'espace informationnel. À cet égard, une grille d'analyse a été adoptée par l'OTAN et, conséquemment, par la doctrine des opérations informationnelles polonaises. Celle-ci repose sur une décomposition tripartite[15] : physique, virtuelle et cognitive.

8. La première strate de l'espace informationnel renvoie à sa dimension physique, c'est-à-dire à l'ensemble des infrastructures matérielles qui supportent la production, la transmission, le stockage et l'accès aux données. Elle inclut notamment les réseaux câblés (notamment sous-marins), les satellites, les centres de données, les dispositifs terminaux (ordinateurs, smartphones) ainsi que les équipements réseau (routeurs, serveurs, commutateurs, etc.). Cette couche constitue l'ossature technique de l'espace informationnel. Elle en détermine la robustesse, la souveraineté et la vulnérabilité face aux menaces de sabotage, d'espionnage ou de coupure informationnelle. Sa maîtrise conditionne également l'autonomie stratégique des entités publiques et privées dans un environnement géopolitique de plus en plus polarisé.

9. Bien qu'étant le contenant de l'information, cette strate de l'espace informationnel peut faire l'objet d'une manipulation qui aura une influence directe sur son contenu : soit en modifiant son accessibilité, soit en empêchant son accessibilité. Il en est ainsi des risques informationnels pesant par la rupture accidentelles ou provoquées d'infrastructure critique, câble sous-marins notamment, ou par des coupures gouvernementales d'internet.[16]

10. Adossée à l'infrastructure matérielle, la **dimension virtuelle** désigne les espaces numériques où l'information est créée, diffusée, transformée et rendue accessible. Il s'agit des plateformes numériques, des réseaux sociaux, des moteurs de recherche, des forums, des bases de données en ligne ou encore des systèmes de messagerie. Cette strate constitue le théâtre privilégié des campagnes de manipulation. Elle en permet la viralité, l'adaptabilité et la pénétration fine grâce aux algorithmes de recommandation,

[15] Disponible sur : https://www.obranaastrategie.cz/en/archive/volume-2018/1-2018/articles/information-operations-from-the-polish-point-of-view.html.
[16] Voir à ce titre le rapport de l'ONU : https://www.ohchr.org/fr/stories/2022/06/switching-internet-causes-incalculable-damage-un-report.

aux techniques de microciblage et aux logiques de bulle informationnelle. Enfin, la dimension cognitive constitue le cœur névralgique de l'espace informationnel, en tant qu'englobe les processus mentaux, culturels et psychologiques par lesquels les individus perçoivent, interprètent et réagissent à l'information. Elle inclut les croyances, les connaissances, les émotions, les attitudes et les comportements collectifs. L'espace cognitif est par nature complexe, car il est façonné par des flux informationnels externes mais également structuré par des mécanismes internes — notamment les biais cognitifs, les cadres de référence socio-culturels et les routines attentionnelles.

11. C'est, ainsi, dans ce cadre informationnel qu'interviennent les manipulations à proprement parler.

12. La « manipulation » d'abord, ne correspond pas à un concept juridique identifié. Elle désigne le fait « d'orienter la conduite de quelqu'un, d'un groupe dans le sens que l'on désire et sans qu'ils s'en rendent compte » par l'acte de manipuler, c'est-à-dire, étymologiquement, de tenir dans ses mains. On retrouve donc l'idée d'un verbe matriciel qui peut conduire à plusieurs actions : fausser, modifier, révéler, résumer, augmenter, caricaturer, dissimuler, mentir, *etc*. La manipulation doit donc être entendue au sens le plus large possible. C'est d'ailleurs ainsi que l'entendent les branches militaire et stratégique qui n'hésitent pas à considérer, à juste titre, que les moyens de la manipulation informationnelle peuvent résider dans la modification, l'exagération, la falsification mais aussi la divulgation[17] (*leak*) de l'information. Pourront ainsi être convoqués l'ensemble des textes juridiques qui sanctionnent le défaut d'authenticité d'une information mais aussi ceux qui prohibent la divulgation d'une information confidentielle ou dérobée – source tout aussi dangereuse de déstabilisation politique et économique.

13. La notion d'« information » ensuite n'est pas aisée à saisir. Dans le langage courant, l'information désigne n'importe quel renseignement, signe, son, image, fait ou

[17] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les manipulations de l'information : un défi pour nos démocraties*, Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de L'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, 2018, pp. 65-102.

événement porté à la connaissance d'un public plus ou moins large. Sa forme importe peu (image, son, texte) bien que dans le cyberespace, l'information sera considérée analysée comme une donnée numérique permettant ainsi d'attraire des pans du droit numérique.

Juridiquement, une information est à la fois un *lien* et un *bien*, pour reprendre la dichotomie de la Professeure Suzanne Lequette[18]. Elle est un lien puisqu'en tant que fait juridique, l'information est transmise d'une personne à une autre. Toutefois cette transmission ne s'effectue pas nécessairement à l'identique, elle peut être résumée, augmentée, atténuée, etc., sans malveillance ; c'est la malveillance dans la transmission, comme dans la création, d'une information qui crée la manipulation, laquelle peut causer un préjudice. Il s'agit d'un bien ensuite, un bien meuble incorporel, chaque fois du moins qu'à cette information est associée une valeur, de sorte que le « détenteur » de cette information peut se la réserver ou décider des conditions de sa transmission ; à défaut de valeur économique, il s'agit d'une simple chose immatérielle : les informations sont de libre parcours. Exceptionnellement, une information peut être appropriée dans des conditions complexes, chaque fois que la loi valide cette appropriation (droit d'auteur, marque, brevet, logiciel, banque de données, etc.). Par conséquent, l'objet « information » se prête aisément aux concepts de droit privé : contrats, responsabilité, propriété éventuellement, ou de science criminelle, vol, abus de confiance, fausseté de l'information, détournement, etc.

L'information, objet de l'étude, se concentrera principalement sur la manipulation de l'information dans le cyberspace mais n'exclut pas d'autres hypothèses fréquentes comme la diffusion d'information par voie de presse (même si la plupart des organes de presse disposent d'un relai dans le cyberspace) et audiovisuelle (à l'occasion par exemple de la suspension des chaînes russes RT et Spoutnik en mars 2023, ou la chaîne française C8 en 2024).

14. Ainsi donc, la manipulation d'information largement entendue permettra de mobiliser un grand nombre de fondements juridiques destinés à lutter contre elle, c'est-à-dire en

[18] S. Lequette, *Droit du numérique*, LGDJ, 2024, *passim*.

actionnant une sanction juridique visant soit à punir, soit à réparer le dommage, soit à le faire cesser, les unes n'étant pas exclusive des autres. La palette juridique de la lutte contre la manipulation d'information est alors très large et le juriste est moins confronté à un problème de fond que de forme.

15. En effet, le droit d'un État libéral entretient une relation complexe avec les limitations de la liberté d'expression, laquelle est intégralement fondée sur la communication d'information, ce d'autant que lorsqu'il s'agit d'apporter de telles limitations, l'outil principalement utilisé emprunte à la méthode pénale, nécessairement ponctuelle et pondérée dans la mesure où, par hypothèse, une opinion intime ne peut être saisie et encore moins sanctionnée, au moins dans une démocratie libérale, tandis que l'*expression* d'une opinion prohibée peut l'être, avec beaucoup de précaution quant à la saisie de l'objet informationnel de cette interdiction[19].

L'article 27 de la loi de 1881 qui fonde le principe de la liberté d'expression (de la presse) incrimine ainsi « la publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler », mais sans définir la notion de « fausse nouvelle », qui suppose des faits circonstanciés, faux, émis de mauvaise foi et non une simple opinion[20].

16. L'ensemble de cette étude vise à illustrer, dans de nombreuses branches du droit, la manière dont des *types* de manipulation de l'information peuvent être saisis.

Il manque très clairement une réflexion puis une réglementation d'ampleur visant à traiter la question générale, non pas de la désinformation, quels que soient les termes utilisés, ou de manipulation de l'information, mais de la *campagne* de manipulation de l'information. En effet, une campagne malveillante, peut avoir pour objet une information

[19] V. L. Convert, *La fausse information en droit comparé. Les États face au phénomène de désinformation*, J. class. Communication, Fasc. 17, 2021, sp. n° 3. *Adde* : T. Hochmann, *« Lutter contre les fausses informations : le problème préliminaire de la définition »*, RDLF 2018, chron. 16.

[20] Cass. crim., 13 avr. 1999, n° 98-83798, *RSC* 2000, p. 203, obs. Y. Mayaud.

vraie, non déformée, et créer un préjudice, particulier pour telle personne ou entité, ou général, à la nation elle-même, au-delà donc des cas ici visités.

Quelques réglementations[21] proposent des règles qui y ressemblent. La France, depuis 2018, vise à lutter contre les fausses informations en période électorale, ou impose la « *responsabilisation* » des hébergeurs dans la loi du 24 août 2021 sur le respect des principes de la République, dont l'article 42 a modifié la loi du 30 septembre 1986 sur la liberté de communication, en créant un article 62 relatif aux règles applicables aux plateformes en ligne en matière de contenu haineux, par lequel l'Arcom peut formuler des demandes d'information sur des contenus illicites, tels que ceux déterminés par l'article 6 de la loi de 2044 sur la confiance dans l'économie numérique, impliquant alors leur possible responsabilité pénale, outre une amende pouvant être infligée par l'Arcom. De même, la loi *Houlié* du 24 juillet 2024 *visant à prévenir les ingérences étrangères en France* impose un certain nombre de piste, visant notamment à faire obstacle à la rémunération d'agent public par des acteurs étrangers, manque sa cible en n'intégrant pas dans le Code pénal une infraction spécifique.

La logique de « campagne de manipulation », provenant de l'intérieur ou de l'étranger, est distincte de celle des informations véhiculées et repose sur une finalité et des moyens qui dépassent de très loin les cas ici traités. Il s'agit d'une forme d'intrusion maligne, par des moyens divers mais orchestrés visant à modifier l'état de l'opinion d'un groupe large ou plus spécifique, en vue d'imposer une opinion différente. Peu importe l'« opinion » ou l'« information » en tant que telle donc, dès lors que la campagne, les manœuvres, les techniques pourraient être saisies et juridiquement traitées par des règles civiles, administratives ou pénales, dans le but de faire cesser ces manœuvres, viser des personnes ciblées, en vue d'imposer des sanctions spécifiques, par exemple de gel de fonds, de saisies ou d'interdictions diverses, etc. En matière de lutte antiterroriste, sont définis dans le Code pénal à la fois les actes de terrorisme (C. pén., art. 421-1), le groupement en vue de commettre de tels actes (art. 421-2-1), son financement (art. 421-2-2), etc., peu important la question de la « légitimité » de l'action sous-jacente. Le même type de dispositif pourrait être mis en place pour lutter contre la guerre informationnelle,

[21] *V.* L. Convert, *La fausse information en droit comparé. Les États face au phénomène de désinformation*, *op. cit.*, n° 6-9.

alliant les éléments techniques, cyber, et de campagnes de manipulation, ce dont VIGINUM rend d'ailleurs périodiquement compte, y compris certaines de ces campagnes comme de nature à porter « atteinte aux intérêts fondamentaux de la Nation », ce qui correspond à la formule de l'article 410-1 du Code pénal. L'article 412-1 pourrait servir de modèle à travers la définition de l'attentat : « constitue un attentat le fait de commettre un ou plusieurs actes de violence de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national », ce qui serait un tournant juridique radical.

17. L'idéal serait d'approcher la lutte contre la manipulation d'information en ayant recours à une classification qui, par sa pédagogie et sa clarté, permettrait à n'importe quel acteur de s'y retrouver. L'approche par une classification *étanche* est, toutefois, impossible. Un fait de manipulation d'information peut relever de différentes notions et obéir à plusieurs régimes qui ne sont pas exclusifs l'un de l'autre. Une même pratique peut donc relever d'une multitude de fondements, parce qu'elle apparaît sur plusieurs canaux de diffusion ou porte atteinte à plusieurs intérêts. Toute catégorie est donc, par définition, perméable. Prenons un exemple. Une entreprise russe divulgue un secret d'affaire d'une entreprise française spécialisée dans le nucléaire sur les réseaux sociaux. Cette manipulation d'information peut à la fois relever du droit commercial (violation du secret des affaires[22]), du droit des plateformes (devoir de vigilance de l'hébergeur[23]) et du droit pénal commun (vol[24]) comme spécial (atteinte aux intérêts fondamentaux de la nation[25]).

18. L'exercice est d'autant plus périlleux qu'il n'existe pas, à ce jour, de travaux juridiques ayant eu pour objet de rassembler l'ensemble des fondements permettant de sanctionner la manipulation de l'information. Les instances politiques se sont toutefois saisies de la question[26] et le législateur français comme européen a pris conscience des

[22] *Infra*, n°91 et s.
[23] *Infra,* n°134 et s.
[24] *Infra,* n°108 et s.
[25] *Infra,* n°51 et s., 122 et s.
[26] Sénat, *Rapport fait au nom de la commission d'enquête sur les politiques publiques face aux opérations d'influence étrangères visant notre vie démocratie, notre économie et les intérêts de la France sur le territoire national et à l'étranger afin de doter notre législation et nos pratiques de moyens d'entraves efficients pour contrecarrer les actions hostiles à notre souveraineté*, n°739, 23 juillet 2024 ; Service diplomatique de l'Union européenne (EEAS), *3rd EEAS Report on Foreign Information manipulation ad Interference Threats* (FIMI), Mars 2025.

menaces informationnelles toujours plus nombreuses et sophistiquées qui menacent les intérêts fondamentaux de la nation. Comme nous le verrons, de plus en plus de textes destinés à lutter précisément contre la manipulation d'information ont été consacrés ces dernières années. Nous avons donc fait le choix d'un travail de synthèse et de propositions qui repose sur une classification exhaustive mais poreuse, qui impose au lecteur de garder à l'esprit qu'une manipulation d'information peut relever de plusieurs catégories à la fois et faire ainsi l'objet de sanctions distinctes. Certaines règles se concentrent ainsi sur la *nature* de la manipulation de l'information dans le sens où ce sont ses caractères qui vont être déterminants. Est-elle authentique ? confidentielle ? Ce type de règles vise principalement à sanctionner le responsable direct de la manipulation. D'autres règles se concentrent, en revanche, sur le moyen de produire ou de diffuser ladite information. C'est alors que le droit permet de diriger le tir vers d'autres acteurs : les plateformes, l'hébergeur, le logiciel d'intelligence artificielle ou encore la chaîne de télévision. Il s'agira donc d'étudier la lutte contre la manipulation du point de vue de l'information, puis du point de vue de la diffusion. Il s'agira donc de connaître l'ensemble des fondements juridiques (**I**) qui, parce qu'ils ne sont pas exclusifs les uns des autres, supposeront de faire un choix stratégique (**II**).

L'EXPOSÉ DES FONDEMENTS JURIDIQUES LUTTANT CONTRE LA MANIPULATION DE L'INFORMATION

19. Manipuler l'information peut se faire de bien des manières et les fondements juridiques permettant de sanctionner la falsification, la fabrication, la révélation ou encore l'exagération sont nombreux. D'un autre côté, les canaux de diffusion et les moyens de production d'une information manipulée sont tout aussi divers. C'est la raison pour laquelle, dans un objectif de clarté, les fondements juridiques feront l'objet d'une classification dont les ramifications ne sont pas forcément étanches. Un même fait peut correspondre à plusieurs fondements. Tantôt, le droit part de la nature de la manipulation d'information (**A**), tantôt du canal par lequel la manipulation est produite ou diffusée (**B**).

A. La lutte contre la manipulation de l'information prise du point de vue de l'information

20. Envisagés du point de vue de la *nature* de la manipulation d'information, les fondements juridiques sont nombreux et variés, et permettent de couvrir tout type de manipulation. Le droit sanctionne lorsque l'information revêt un caractère illicite. Tel est le cas lorsqu'une atteinte est portée à l'authenticité de l'information (**1**), à sa confidentialité (**2**), à sa propriété (**3**) ou, plus généralement, à sa fonction (**4**). Là non plus, les catégories ne sont pas nécessairement étanches. Une information confidentielle peut aussi faire l'objet d'un droit de propriété, tandis qu'une fausse information peut également atteinte à la fonction de l'information. Quoi qu'il en soit, il convient d'en dresser l'inventaire.

21. **Attention** (1) - Dans tous les cas, il conviendra de lire les développements qui suivent à la lumière de l'article 8 de la loi n°2024-850 du 25 juillet 2024 *visant à prévenir les ingérences étrangères*. Cette dernière a créé une circonstance aggravante applicable aux

infractions contre les biens ou les personnes dès lors qu'elles sont conduites dans le but de servir les intérêts d'une puissance étrangère ou d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger. Cette nouvelle circonstance aggravante, qui sera d'une aide redoutable pour lutter contre l'ingérence informationnelle, est désormais prévue à l'article 411-12 du Code pénal. La plupart des infractions pénales listées ci-dessous sont, en tant que de raison, concernées par cette circonstance aggravante.

22. **Attention** (2) – Ensuite, il conviendra de lire les développements suivants en gardant à l'esprit que de telles infractions sont, le plus souvent[27], le résultat d'une entente entre plusieurs entités afin de manipuler l'information. Si bien que la circonstance aggravante d'infraction en bande organisée est applicable. L'article 132-71 du Code pénal dispose ainsi que *« constitue une **bande organisée** au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions »*. On ajoutera également que la qualification **d'association de malfaiteurs** pourra être retenue dans un contexte de manipulation de l'information. Cette dernière découle de l'article 450-1 du Code pénal qui dispose que : *« Constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement »* – une telle qualification permet de sanctionner aux mêmes peines, la simple participation à ladite association.

1) Atteintes à la véracité de l'information

23. Seront ici exposés l'intégralité des fondements juridiques, de droit privé ou public, civil ou pénal, qui permettent de sanctionner l'individu qui diffuserait une fausse information. C'est ici l'un des terrains les plus sensibles de la guerre informationnelle puisque les fausses informations sont l'outil privilégié, ces dernières années, des ingérences étrangères et des manœuvres de déstabilisation de la société civile.

[27] J. Saiz in « Cybercriminalité : quels enjeux pour les économies souterraines », rce-revue.com, 28 mars 2014 : 80% des infractions sur internet seraient commises par des groupes.

1. Le droit pénal de la presse : délit de fausse nouvelle et diffamation

24. **Le délit de fausse nouvelle** – L'article 27 de la loi du 29 juillet 1881 sur la liberté de la presse est le texte de droit positif le plus ancien à s'être penché sur la question des « **fausses nouvelles** ». Il montre que, dès le XIX siècle, la question des *fake news* avait été prise en compte par le législateur qui, déjà à cette époque, s'évertuait à protéger la liberté d'expression. Ainsi, il ne suffit pas à la nouvelle d'être fausse pour être sanctionnée. Aussi faut-il qu'elle sa diffusion soit faite de mauvaise foi et trouble ou risque de troubler l'ordre public. L'originalité du mécanisme repose plutôt sur la responsabilité en cascade qu'elle permet car la diffusion par voie de presse suppose qu'un éditeur ait donné son accord de publication, si bien que sa responsabilité pénale sera recherchée en priorité.

25. L'article 27 dispose ainsi que *: « la publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45,000 euros. »* L'alinéa second poursuit *: « Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la nation. »* L'article 27 recouvre ainsi deux délits distincts. Le premier est celui de diffusion de fausses nouvelles de nature à troubler l'ordre public, le second celui de fausses nouvelles de nature à ébranler l'effort de guerre de la nation.

26. Le texte peut être mobilisé pour lutter contre une manipulation d'information grâce à un mécanisme d'action en cascade. En effet, dans le droit de la presse seulement, la responsabilité pénale s'organise selon l'ordre établi par l'article 48 de la loi de 1881. Ainsi, la responsabilité pénale d'une fausse nouvelle doit d'abord être recherchée à l'égard des directeurs de publications ou des éditeurs, à défaut seulement, les auteurs pourront être désignés comme responsables. Si l'auteur n'est pas identifié, ce seront les imprimeurs ou sinon les vendeurs, distributeurs et afficheurs.

27. **Le délit de diffamation** –Par ailleurs, la même loi prévoit en son article 29 le délit de diffamation, qui peut être mobilisé dans un contexte de manipulation de l'information. Ce dernier dispose que *« toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommé, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés. »* L'article 30, quant à lui, dispose que *« la diffamation commise par l'un des moyens énoncés en l'article 23 envers les cours, les tribunaux, les armées de terre, de mer ou de l'air et de l'espace, les corps constitués et les administrations publiques, sera punie d'une amende de 45 000 euros ».*

28. L'action en diffamation est enfermée dans un délai de prescription de 3 mois[28]. Elle obéit, comme le délit d'informations fausses, au système de responsabilité en cascade qui, sur le plan civil, permet l'indemnisation du préjudice subi par la victime.

29. Les ingérences informationnelles peuvent également reposer sur des campagnes massives de diffusion de messages haineux et de contenus illicites qui peuvent faire l'objet d'une sanction sur le fondement du droit pénal de la presse. La manipulation de l'information vise ici à attiser la haine et la tension au sein d'une communauté nationale.

30. **La provocation publique à la discrimination à la haine ou à la violence raciale ou religieuse** est sanctionné par l'article 24 alinéa 7 de la loi de 1881 à cinq ans d'emprisonnement et 45 000 euros d'amende. L'alinéa 8 du même texte sanctionne de la même peine ceux qui auront provoqué à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap ou auront provoqué, à l'égard des mêmes personnes, aux discriminations prévues par les articles 225-2 et 432-7 du Code pénal.

[28] Art. 65, loi du 29 juillet 1881.

31. Enfin, le cinquième alinéa de l'article 24 de la loi de 1881 sanctionne **l'apologie des crimes de guerre**, des crimes contre l'humanité, des crimes ou délits de collaboration avec l'ennemi et des crimes de réduction en esclavage ou d'exploitation d'une personne réduite en esclavage, y compris si ces crimes n'ont pas donné lieu à des condamnation de leurs auteurs.

32. **Extension des délits au secteur audiovisuel et numérique** – Par la suite, les évolutions technologiques permettant de nouveaux canaux de diffusion ont poussé le législateur à adapter la loi. Il a ainsi étendu, par la loi n°82-652 du 29 juillet 1983 – modifiée par la loi n°2004-575 du 21 juin 2004 (LCEN) pour l'étendre au cyberespace – le délit de fausse nouvelles ainsi que tous les autres crimes et délits commis par voie de presse, aux nouvelles technologies audiovisuelles puis numériques. L'article 93-3 dispose ainsi que : *« Au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication ou, dans le cas prévu au deuxième alinéa de l'article 93-2 de la présente loi, le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public. »* On retrouve ici également le mécanisme de responsabilité en cascade permettant d'actionner le directeur de publication, puis l'auteur, puis le producteur. Toutefois, comme nous le verrons[29], la responsabilité des plateformes et des hébergeurs est ici plus difficile à mettre en œuvre et obéit à un régime particulier.

2. Autres infractions pénales sanctionnant la publication d'informations fausses ou haineuses

33. Hors voie de presse, le droit pénal propose de nombreux fondements permettant de lutter contre la manipulation de l'information qui repose sur la diffusion de messages haineux. Là aussi, nous verrons que le législateur cherche à renforcer la sanction et la coopération des plateformes numériques en permettant d'aller chercher la

[29] *Infra*, n°134 et s.

responsabilité de celles-ci en cas de publication de contenu haineux[30]. Sur la sanction de la manipulation à raison de la nature de l'information manipulée, en revanche, c'est le droit pénal qui offre les principaux fondements.

34. **Provocation et apologie des actes terroristes** – L'article 421-2-5 du Code pénal dispose ainsi que *« le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne. Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »*

35. **Harcèlement moral et cyberharcèlement** – Lorsqu'une campagne de manipulation de l'information a pour objet de révéler des informations mensongères sur une personne et que cette dernière fait l'objet d'une campagne de harcèlement, le droit pénal offre plusieurs fondements de nature à sanctionner l'auteur du harcèlement. L'article 222-233-2 du Code pénal dispose ainsi que *« le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou compromettre son avenir professionnel, est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. »* L'infraction est également constituée, nous dit l'article L.222-33-2-2, 4° du Code pénal, lorsque les faits *« ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique. »*

36. **Montage illicite** – L'une des techniques les plus fréquentes de manipulation de l'information consiste à diffuser de fausses images ou vidéos. Le développement des images et vidéos générées par intelligence artificielle (*deepfakes*) offre des possibilités d'une ampleur sans précédent quant à la manipulation de l'information.

[30] *Infra,* n°134 et s.

37. Le délit de montage illicite existe en droit pénal, et est prévu à l'article 226-8 qui réprime le délit de *« publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention. »*

38. Récemment, les progrès de l'intelligence artificielle ont incité le législateur en réagir en adoptant la loi n°2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique. Cette dernière a augmenté l'article 226-8 du Code pénal en insérant le texte suivant : *« est assimilé à l'infraction mentionnée au présent alinéa et puni des mêmes peines le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore généré par un traitement algorithmique et représentant l'image ou les paroles d'une personne, sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un contenu généré algorithmiquement ou s'il n'en est pas expressément fait la mention. »* Le cas suivant en donne un témoignage alarmant : La société d'ingénierie britannique Arup a été victime d'une grave fraude au début de 2024, qui a entraîné une perte totale de plus de 25 millions de dollars. Au cours d'une vidéoconférence, en présence de *deepfakes*, usurpant le directeur financier de l'entreprise et d'autres employés, un membre du personnel a été dupé en effectuant 15 transactions d'un montant total de 200 millions de dollars de Hong Kong (près de 26 millions de dollars) de la société.[31]

39. Dans les deux cas, les peines sont portées à deux ans d'emprisonnement et à 45 000 euros d'amende lorsque les délits prévus au présent article ont été réalisés en utilisant un service de communication en ligne. Lorsqu'ils sont commis par voie de presse, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

40. Ensuite, la même loi a créé une nouvelle infraction pour réprimer les montages à caractère sexuel[32] à l'article 226-8-1 du Code pénal qui punit de deux ans

[31] https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video.
[32] A noter que ce type de comportement a été identifié comme menace émergente dans une perspective d'utilisation militaire. Cf : www.defnat.com/e-RDN/vue-tribune.php?ctribune%3D1205&sa=D&source=docs&ust=1748244163064826&usg=AOvVaw09kfSN5BElDUAKh3_8zGs4

d'emprisonnement et de 60 000 euros d'amende le fait de porter à la connaissance du public ou d'un tiers un montage à caractère sexuel réalisé avec les paroles ou l'image d'une personne, sans son consentement. Il en va de même lorsque l'information est réalisée par un traitement algorithmique.

41. **Usurpation d'identité numérique** - Enfin, une infraction à relier aux droit des cyberattaques[33] (car l'on s'empare souvent d'un mot de passe, d'un nom de compte) consiste à usurper l'identité d'autrui à des fins de manipulation de l'information. Ainsi, l'article 226-4-1 du Code pénal dispose que *« le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »* Le fait de pirater le compte de quelqu'un et de se faire passer pour lui est, en effet, un redoutable outil de manipulation de l'information. Imagine-t-on les effets désastreux du piratage du compte X du P-DG d'une société du CAC 40 prendre la parole pour annoncer que sa société est en état de cessation des paiements ou qu'un plan de licenciement a été adopté.

42. Dans tous les cas, l'article 8 de la loi n°2024-850 du 25 juillet 2024 visant à prévenir les ingérence étrangères a mis en place une circonstance aggravante applicable aux infractions contre les biens ou les personnes dès lors qu'elles sont conduites dans le but de servir les intérêts d'une puissance étrangère ou d'une entreprise ou d'une organisation étrangère ou sous contrôle étranger que l'on retrouve l'article 411-12 du Code pénal.

3. La lutte contre la manipulation de l'information en période électorale

43. L'unique loi dans laquelle est précisément mentionné l'occurrence « manipulation de l'information » est de facture récente, et concerne moins la presse que le droit électoral

[33] *Infra*, n°105 et s.

et les plateformes numériques. Emmanuel Macron, ayant lui-même fait l'objet d'une campagne de désinformation lors de sa première campagne présidentielle, avait souhaité l'instauration d'un cadre légal visant spécifiquement à lutter contre la manipulation de l'information et plus particulièrement contre ce que l'on appelle les *fake news* mais dans un contexte électoral uniquement.

44. La loi n°2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information* a mis en place un régime juridique d'exception qui se déclenche pendant les trois mois précédant le premier jour du mois d'élections générales et qui se termine à la date du tour de scrutin où celles-ci sont acquise (C. électoral, art. L.163-1). Elle se rajoute à l'article L.97 du code électoral qui permettait déjà de sanctionner des individus qui surprennent ou détournent des suffrages à l'aide de « fausses nouvelles ». Des obligations nouvelles sont imposées aux plateformes, tandis que les parties prenantes disposent d'une action spéciale destinée à faire cesser rapidement l'illicite.

45. **Du côté des plateformes** – Des obligations de transparence sont imposées aux opérateurs de plateformes en ligne telles que définies par l'article 33[34] du règlement (UE) 2002/2065 (*Digital Services Act* – DSA). Elles ont ainsi l'obligation, au sein d'un registre spécial, de mettre à la disposition de l'utilisateur les informations suivantes[35].

46. Tout d'abord, une information loyale, claire et transparente sur l'identité de la personne physique ou sur la raison sociale, le siège social et l'objet social de la personne morale et de celle pour le compte de laquelle, le cas échéant, elle a déclaré agir, qui verse à la plateforme des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général. Ensuite, une information loyale, claire et transparente sur l'utilisation de ses données personnelles dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général. Enfin, le montant des rémunérations reçues en contrepartie de la promotion de tels contenus d'information lorsque leur montant est supérieur à un seuil déterminé.

[34] Correspond au nombre mensuel moyen de destinataires actifs est égal ou supérieur à 45 millions et qui sont désigné comme de très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne en vertu du paragraphe 4.
[35] V° également, *infra* n°146 et s.

47. **Du côté des parties prenantes** – L'article L.163-2 introduit une action spéciale devant le juge des référés du tribunal judiciaire de Paris qui reçoit compétence exclusive. Cette action naît dès lors que des *« allégations trompeuses ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne »***.**

48. À ce moment-là, le ministère public, un candidat, un parti ou groupement politique ou toute personne ayant un intérêt à agir peut saisir le juge des référés, qui doit statuer dans un délai de quarante-huit-heures à compter de la saisine, pour que ce dernier prescrive aux plateformes des mesures proportionnées et nécessaire ne nature à faire cesser la diffusion. Une telle action en cessation de l'illicite ne préjudicie pas d'une éventuelle action en réparation du dommage.

49. Toutefois, le Conseil constitutionnel a émis une réserve d'interprétation, sur le fondement de la liberté d'expression, quant à l'appréciation des allégations trompeuses ou inexactes. En effet, il considère que ces dernières, pour tomber sous le coup de la loi, doivent revêtir un caractère inexact ou trompeur « manifeste[36]». La loi s'en est trouvée considérablement affaiblie[37] dans la mesure où seules les informations les plus grossièrement fausses entrent dans son champ d'application. Or, la manipulation d'information est souvent pernicieuse et discrète. Le texte ne permet donc pas de lutter efficacement contre la manipulation d'information : dès lors qu'il existe un doute, la procédure d'urgence sera rejetée. En témoigne un arrêt du tribunal judiciaire de Paris du 17 mai 2009[38] qui a adopté une approche très restrictive de la notion de fausse nouvelle.

50. Ainsi, le droit électoral, même augmenté d'un texte spécial destiné à lutter précisément contre la manipulation de l'information, rencontre des difficultés d'application au regard de la proportionnalité de l'atteinte à la liberté d'expression qu'il permet. Son objet et sa raison d'être, sanctionner la fausse information de manière *réactive*, échouent devant les

[36] Cons. const., 20 décembre 2018, n°2018-773 DC.
[37] G. Thierry, F. Saint-Bonnet, B. Warusfel, « Fake news et manipulations de l'information, la difficile réponse juridique », D. act., juillet 202G. Haas, A. Dubarry, « Lutter contre les fake news, un défi juridique et démocratique », Dalloz IP/IT, 2020, p.240.
[38] TGI Paris, 17 mai 2019, n°19/53935.

réserves du Conseil constitutionnel et l'interprétation des juges des référés. L'entrée en vigueur des règlements européens destinés à accroître la responsabilité des plateformes lui offrira, peut-être, une seconde vie[39].

4. Le délit de fourniture d'une fausse information aux autorités civiles ou militaire

51. Les deux textes précédemment mentionnés sont très largement indifférents au fait de savoir si la manipulation de l'information intervient pour le compte ou non d'une entité étrangère. Ils englobent la manipulation d'information au sens large du terme, que la malveillance soit purement personnelle ou bien instrumentalisée pour servir les intérêts d'autrui. Le fait de ne pas mentionner l'intelligence avec une puissance étrangère dans les lois électorales de 2018 a de quoi surprendre tant on sait que la manipulation d'information, dans ce contexte, trouve ses origines et ses instigateurs à l'étranger. Aucune circonstance aggravante ne semble, cependant, en tenir compte. Mais cela ne signifie pas que le droit français ne s'intéresse pas à la manipulation d'information dans un contexte géopolitique plus marqué.

52. En effet, le droit pénal renferme un livre IV intitulé « des crimes et délits contre la nation, l'État et la paix publique » dont le premier titre concerne « les atteintes aux intérêts fondamentaux de la nation ». Ces derniers dressent une liste particulièrement dense de délits qui concernent de près ou de loin la manipulation de l'information et dont les sanctions sont bien plus importantes et dissuasives. Comme nous le verrons, ces textes sont restés en marge de la pratique judiciaire. Pourtant, ils offrent un potentiel inexploité pour appréhender les nouvelles formes de manipulation informationnelle[40].

53. Les intérêts fondamentaux de la nation sont définis à l'article 410-1 du code pénal. Ils s'entendent comme *« son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et*

[39] *Infra*, n°134 et s.
[40] V° not. le sabotage : *Infra*, n°122 et s.

de son environnement et des éléments essentiels de son potentiel scientifique et économique, notamment agricole, et de son patrimoine culturel ».

54. On le voit, les atteintes aux intérêts fondamentaux de la nation sont entendues de façon suffisamment large pour pouvoir agréger les cas de manipulation d'information. Plus précisément, la fausse information est prévue par l'article 411-10 du Code pénal. Ce dernier dispose que *« le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la nation est puni de sept ans d'emprisonnement et de 100 000 euros d'amende »*.

55. Un tel article pourrait être très utile lorsque la fausse intervention est délivrée à une cible publique déterminée (banque centrale, hôpitaux) mais trouve ses limites lorsque la fausse information est publiée sur les plateformes. En effet, le destinataire de l'information doit impérativement être une autorité civile ou militaire de la France ce qui exclut, en principe, les cas les plus fréquents de manipulation d'information qui visent la population prise en son sens général.

5. Le délit de transmission d'informations fausses ou trompeuses en droit financier

56. La lutte contre la manipulation d'information en matière financière vise à préserver le bon fonctionnement des marchés financiers et à préserver la confiance des investisseurs. C'est la raison pour laquelle le code monétaire et financier, ainsi que le droit européen, ont érigé un certain nombre de textes permettant de sanctionner lourdement quiconque tenterait de manipuler l'information sur les marchés par une atteinte à sa transparence. Qui plus est, la manipulation de l'information en matière financière ne s'arrête pas qu'aux seuls cas de spéculations illicites mais, dans un contexte de guerre hybride, est une arme redoutable pour quiconque souhaiterait déstabiliser l'économie d'un pays ou les activités d'une entreprise. L'étude de cas suivante en donne un témoignage alarmant.

57. En 2016, la société Vinci a été victime d'une manipulation boursière particulièrement désastreuse. Le 22 novembre 2016 à 16h, des individus ont envoyé à plusieurs médias un communiqué frauduleux dont les formes usurpaient celles de Vinci. Le communiqué annonçait la découverte d'irrégularités comptables de 3,5 milliards d'euros et le licenciement du directeur financier. Certaines agences de presse diffusent la fausse information ce qui cause une chute de 19% de l'action Vinci (6 milliards d'euros de capitalisation boursière). Malgré un démenti presque instantané, les conséquences boursières ne peuvent être résorbées. Les auteurs n'ayant pas été identifiés, c'est vers les intermédiaires que les autorités se sont tournées. L'AMF a ouvert une enquête pour diffusion d'informations fausses ou trompeuses de nature à agir sur les cours qui a débouché sur une condamnation de l'agence Bloomberg pour avoir diffusé le communiqué sans vérification suffisante[41].

58. La manipulation d'information est ainsi très fréquente dans le monde financier, et sont légalement regroupés dans le code monétaire et financier qui distingue plusieurs délits de manipulation de marché. En ce qui nous concerne, le délit de fausse information intègre pleinement la lutte contre les manipulations de l'information. Il faut encore souligner qu'une telle pratique peut constituer simultanément une pratique commerciale trompeuse, une escroquerie ou une infraction de présentation ou de publication de comptes inexacts mais que le délit de fausse information sera retenu de préférence.

59. Le délit de fausse information repose sur un triptyque de textes qui se divise entre un texte général centré sur les ordres et comportements (CMF, art. L.465-3-1), un texte sanctionnant la diffusion d'informations fausses ou trompeuses (art. L.465-3-2) et un autre sanctionnant le même comportement à propos des indices de référence (art. L.465-3-3). Ils sont ainsi rédigés :

[41] L'amende a été contestée devant la Cour de cassation, sans succès - : Com., 14 février 2024, n°22-10.472 ; v° également : E. Rogey, « Les « fake news » à l'ère de MAR : l'AMF sanctionne une agence de presse pour diffusion de fausses informations », Revue de droit bancaire et financier, n°3, mai-juin 2020, ét. 9.

60. **Comportement et ordres trompeurs - L. 465-3-1, CMF** : *« Est puni des peines prévues au A du I de l'article L. 465-1 le fait, par toute personne, de réaliser une opération, de* ***passer un ordre*** *ou* ***d'adopter un comportement*** *qui donne ou est susceptible de donner des* ***indications trompeuses*** *sur l'offre, la demande ou le cours d'un instrument financier ou l'offre, la demande ou le prix d'un crypto-actif ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier ou le prix d'un crypto-actif. (…).* ***II****. – Est également puni des peines prévues au A du I de l'article L. 465-1 le fait, par toute personne, de réaliser une opération, de passer un ordre ou d'adopter un comportement qui affecte le cours d'un instrument financier ou qui influence ou est susceptible d'influencer le prix d'un ou plusieurs crypto-actifs, en ayant recours à des procédés fictifs ou à toute autre forme de tromperie ou d'artifice.* ***III****. – La tentative des infractions prévues aux I et II du présent article est punie des mêmes peines ».*

61. **Diffusion d'informations fausses ou trompeuses - L. 465-3-2, CMF** : *« I. – Est puni des peines prévues au A du I de l'article L. 465-1 le fait, par toute personne, de* ***diffuser****, par tout moyen, des informations qui donnent des* ***indications fausses ou trompeuses*** *sur la situation ou les perspectives d'un émetteur ou sur l'offre, la demande ou le cours d'un instrument financier ou sur l'offre, la demande ou le prix d'un crypto-actif ou qui fixent ou sont susceptibles de fixer le cours d'un instrument financier ou le prix d'un crypto-actif à un niveau anormal ou artificiel. II. – La tentative de l'infraction prévue au I du présent article est punie des mêmes peines ».*

62. **Informations fausses ou trompeuses pour le calcul d'un indice - L. 465-3-3, CMF** : *« I. – Est puni des peines prévues au A du I de l'article L. 465-1 le fait, par toute personne : 1° De fournir ou de transmettre des données ou des informations fausses ou trompeuses utilisées pour calculer un indice de référence ou des informations de nature à fausser le cours d'un instrument financier ou d'un actif auquel est lié un tel indice ou de nature à fausser le prix d'un cryptoactif ; 2° D'adopter tout autre comportement aboutissant à la manipulation du calcul d'un tel indice. (…) I. – La tentative de l'infraction prévue au I du présent article est punie des mêmes peines. »*

63. Les trois articles font ainsi référence à l'article L. 465-1, I, A qui prévoit, pour le délit de fausses informations, la sanction suivante : cinq ans d'emprisonnement et 100 millions d'euros d'amende, ce montant pouvant être porté jusqu'au décuple du montant de l'avantage retiré du délit, sans que l'amende puisse être inférieure à cet avantage.

64. Dans tous les cas, le CMF ne distingue pas qui peut ou ne peut pas être auteur de l'infraction. Si bien qu'une personne physique ou morale, connue ou anonyme, professionnelle ou non, peut faire l'objet d'une sanction. Le mode de diffusion de l'information importe également peu.

65. **La prohibition des manipulations de marché** - Au niveau européen, on citera enfin l'article 12, 1, c, du règlement (UE) n°596/2014 du 16 avril 2014 sur les abus de marché (règlement MAR) qui considère comme une manipulation de marché le fait de « ***diffuser*** *des informations, que ce soit par l'intermédiaire des médias, dont l'internet, ou par tout autre moyen, qui donnent ou sont susceptibles de donner des indications fausses ou trompeuses en ce qui concerne l'offre, la demande ou le cours d'un instrument financier, d'un contrat au comptant sur matières premières qui lui est lié ou d'un produit mis aux enchères sur la base des quotas d'émission, ou fixent ou sont susceptibles de fixer à un niveau anormal ou artificiel le cours d'un ou de plusieurs instruments financiers, d'un contrat au comptant sur matières premières qui leur est lié ou d'un produit mis aux enchères sur la base des quotas d'émission, y compris le fait de répandre des rumeurs, alors que la personne ayant procédé à une telle diffusion savait ou aurait dû savoir que ces informations étaient fausses ou trompeuses.* »

66. Enfin, la Cour de cassation a récemment admis que la commission des sanctions de l'AMF pouvait prononcer une sanction à l'encontre de toute personne qui, sur le territoire français ou à l'étranger, s'est livrée à une manipulation de cours dès lors que les actes de manipulation concernent un instrument financier lié à un instrument financier admis aux négociations sur un marché réglementé français ou sur un système multilatéral de négociation français[42]. Ainsi, le fait que l'auteur de l'infraction soit à l'étranger n'a aucune incidence sur la compétence de l'AMF pour sanctionner la pratique.

[42] Com., 12 mars 2025, n°23-20.432.

67. **La sanction du diffuseur de la fausse information** - Le droit européen, permet, ensuite, de sanctionner un organe médiatique pour avoir diffusé une fausse information à l'article 12. L'article 21 du même règlement dispose cependant que *« lorsque des informations sont divulguées ou diffusées et lorsque des recommandations sont produites ou diffusées à des fins journalistiques ou aux fins d'autres formes d'expression dans les médias, cette divulgation ou cette diffusion d'information est appréciée en tenant compte des règles régissant la liberté de la presse et la liberté d'expression dans les autres médias et des règles ou codes régissant la profession journalistiques (…). »* C'est d'ailleurs sur les fondements des articles 12 et 21 que l'AMF a sanctionné l'agence Bloomberg pour avoir diffusé de fausses informations sur Vinci.[43] Il s'agit de la première décision de sanction rendue par l'AMF à l'égard d'un professionnel de presse. Comme nous le verrons, prise depuis les canaux de diffusion, la lutte contre la manipulation de l'information peut parfois trouver dans les diffuseurs institutionnels ou les plateformes des coupables commodes lorsque le véritable auteur n'est pas identifiable.

6. La prohibition des informations mensongères ou calomnieuses en droit commercial

68. Le monde des affaires n'échappe pas aux manipulations de l'information qui constituent des pratiques commerciales déloyales susceptibles de restreindre la libre concurrence sur un marché.

69. Ainsi, l'article L.442-9 puni de de deux ans d'emprisonnement et de 30 000 euros d'amende le fait d'opérer la hausse ou la baisse artificielle soit du prix de biens ou de services, soit d'effets publics ou privés, en *« diffusant, par quelque moyen que ce soit, des informations mensongères ou calomnieuses. »* Le II., du même article, dispose que lorsque la hausse ou la baisse artificielle des prix concerne des produits alimentaires, la peine est portée à trois ans d'emprisonnement et 45 000 euros d'amende.

[43] https://www.amf-france.org/fr/sanctions-transactions/communiques-de-la-commission-des-sanctions/la-commission-des-sanctions-de-lamf-sanctionne-la-societe-bloomberg-lp-pour-diffusion-de-fausses

7. Les pratiques commerciales trompeuses en droit de la consommation

70. Initialement cantonnées aux publicités, les pratiques commerciales trompeuses ont vu leur champ d'application considérablement élargi à la suite de l'adoption de la loi n°2008-3 du 3 janvier 2008 *pour le développement de la concurrence au service des consommateurs*.

71. L'article L.121-2 du code de la consommation dispose ainsi qu'une pratique commerciale est trompeuse dès lors qu'elle repose sur des **allégations, indications ou présentations fausses ou de nature à induire en erreur** et portant sur l'un ou plusieurs des éléments listés par l'article : l'on retrouve ainsi les informations qui concerne l'existence du produit (a), ses caractéristiques essentielles (b), son prix (c), son service après-vente (d), la portée des engagements, notamment environnementaux, de l'annonceur (e), l'identité, les qualités et aptitudes du professionnel (f) et le traitement des réclamations (g). L'article L.121-4 du même code dresse une liste de pratiques réputées trompeuses. Les pratiques commerciales trompeuses sont sanctionnées pénalement par un emprisonnement de deux ans et d'une amende de 300 000 euros. Les actions civiles qu'elles induisent peuvent être mises en œuvre par les consommateurs, non-professionnels et les professionnels (C. cons., art. L.121-5). Si c'est un concurrent professionnel en revanche, ce dernier devra se placer sur le terrain de la concurrence déloyale pour obtenir réparation du préjudice qu'elle permet[44].

72. Concernant l'auteur de la pratique déloyale, celui-ci ne peut être qu'un professionnel[45]. L'assertion a son importance, en matière de lutte contre la manipulation d'information, car elle empêche que l'incrimination soit portée à l'égard d'une personne physique ou d'une personne morale non-professionnelle (une association, par exemple). Enfin, l'article L.132-1 du code de la consommation dispose que le délit est constitué dès lors que la pratique est mise en œuvre ou qu'elle produit ses effets en France. La manipulation de l'information peut donc provenir de l'étranger et être sanctionnée par les tribunaux français. En toute hypothèse, le droit des pratiques commerciales

[44] *Infra*, n°127 et s.
[45] Crim., 19 mars 2019, n°17-83.543.

trompeuses ne sera utile qu'en face d'une entreprise qui diffuse des fausses informations.

73. Par exemple, une entreprise agroalimentaire installée en France, détenue par un fonds souverain étranger, décide de lancer une campagne de publicité déclarant que les produits de ses concurrents sont fabriqués avec des ingrédients toxiques. Cela a pour effet de déstabiliser la confiance des consommateurs dans les marques nationales et les répercussions économiques se font sentir. Une plainte pourra être déposée pour pratique commerciale trompeuse. Les consommateurs se verront indemnisés sur fondement-ci, tandis que les concurrents pourront agir sur le fondement de la concurrence déloyale[46].

8. La prohibition de tromper le consentement du contractant par des manœuvres ou réticences dolosives

74. Les vices du consentement permettent d'annuler un contrat dont le consentement a été surpris par l'erreur, la violence ou le dol. Le droit de la manipulation de l'information ne peut faire l'économie de l'annulation du contrat pour dol en ce qu'il permettra la réparation des conséquences civiles d'une manipulation d'information qui aurait eu pour conséquence la conclusion d'un contrat. Le dol est prévu aux articles 1137 à 1139 du Code civil. Il consiste à obtenir le consentement de l'autre partie par des manœuvres, des mensonges ou par la dissimulation intentionnelle d'une information. Dans un contexte de guerre économique, le fondement du dol peut être utile pour réparer les conséquences redoutables d'une manipulation d'information à des fins d'ingérence étrangère.

75. Par exemple, une société française innovante dans un domaine stratégique est approchée par une société d'investissement qui se présente comme un fonds privé et neutre souhaitant prendre une participation capitalistique. En réalité, ce fonds est une structure écran contrôlée indirectement par un état étranger hostile à des fins

[46] *Infra*, n°127 et s.

d'espionnage industriel et de transfert de technologie. En se fondant sur le dol, la société française pourra ainsi annuler la prise de participation du fonds en raison de la manœuvre dolosive qu'il a effectuée.

2) Atteintes à la confidentialité de l'information

76. La manipulation d'information ne consiste n'est pas qu'une affaire de mensonges et de falsification. En effet, la manipulation est suffisamment large pour inclure dans ses manifestations toutes les hypothèses dans lesquelles une information a été diffusée alors qu'elle ne devait pas l'être. Ainsi, la manipulation d'information peut aussi consister en une divulgation d'information (*leak*)[47]. Juridiquement, pour pouvoir sanctionner cette pratique, il faut que l'information soit marquée du sceau de la confidentialité.

1. Délit de livraison d'informations à une puissance étrangère

77. Les infractions pénales destinées à protéger les intérêts fondamentaux de la nation permettent non seulement de sanctionner le diffuseur d'une information mensongère mais également celui qui transmettrait une information protégée. Ainsi, l'article 411-6 du Code pénal dispose que : *« le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont* ***l'exploitation, la divulgation ou la réunion*** *est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225 000 euros d'amende »*. L'article 411-7 sanctionne, quant à lui, le fait de recueillir ou de rassembler des renseignements en vue de les livrer, tandis que l'article 411-8 sanctionne le fait d'exercer une activité ayant pour but l'obtention et la livraison de tels renseignements.

[47] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les manipulations de l'information : un défi pour nos démocraties*, Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de L'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, 2018, pp. 65-102.

78. L'article 411-6 s'intéresse surtout aux effets de la livraison d'une information sensible. Pour être sanctionné la personne doit non seulement avoir transmis ou rendu accessible des informations, mais aussi que l'entité étrangère **l'ait exploité** de telle sorte à porter atteinte aux intérêts fondamentaux de la nation. L'article permettrait de sanctionner l'auteur de la transmission, si cette transmission a eu pour conséquence une manipulation de l'information par **divulgation** ou **exploitation** (la diffusion au public de l'information sensible, par exemple). Le champ d'application de l'article 411-6 permet de sanctionner la personne qui a livré l'information à l'entité étrangère, et non la personne qui l'a exploité. Il s'agit d'un outil efficace en ce sens qu'il permet de sanctionner lourdement la personne identifiée comme étant à l'origine de la transmission de l'information alors que l'entité étrangère demeurerait difficile à atteindre.

79. Dans **l'affaire Michelin** par exemple, dans lequel un salarié avait tenté de vendre des informations sensibles à un concurrent, ce fondement n'avait pas pu être soulevé faute pour le concurrent d'avoir exploiter les informations. En revanche, il est tout à fait possible d'imaginer l'exemple d'un salarié d'une entreprise de gestion des eaux potables qui transmettrait les failles de cybersécurité à une société russe. Quelques semaines plus tard, plusieurs médias russes publient des articles sensationnalistes affirmant que la France est, preuve à l'appui, dans l'incapacité de garantir l'intégrité de ses infrastructures d'eau. Il sera donc possible de sanctionner le salarié à l'origine de la transmission sur le fondement de l'article 411-6, en plus du droit du travail applicable.

2. Atteinte au secret de la défense nationale

80. L'article 413-9 du code pénal définit le secret de la défense nationale : *« présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatiques ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès. »* Dans des conditions assez similaires au paragraphe précédent, le Code pénal sanctionne de sept ans d'emprisonnement et de 100 000 euros d'amende le fait ou la tentative pour toute personne dépositaire, de

subtiliser une information ayant un caractère de secret de la défense nationale pour, en ce qui nous intéresse, le porter à la connaissance du public (413-10, Code pénal). Pour les personnes non-dépositaires, les mêmes actions sont sanctionnées par cinq ans d'emprisonnement et 75 000 euros d'amende (413-11, Code pénal).

3. Atteinte à certains services ou unités spéciales par divulgation d'une information qui pourrait conduire à l'identité d'un individu concerné

81. Enfin, toujours dans la partie du Code pénal relative à la protection des **intérêts fondamentaux de la nation**, un autre texte permet de sanctionner la révélation d'une information confidentielle dès lors qu'elle concerne l'identité d'une personne visée par le texte. L'article 413-13 du Code pénal dispose ainsi que la révélation de toute information qui pourrait conduire, directement ou indirectement, à la découverte de l'usage d'une identité d'emprunt ou d'une fausse qualité, de l'identité réelle d'un agent d'un service visé par le texte est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. Les peines sont aggravées lorsque la révélation a causé une atteinte à l'intégrité physique ou à la mort de ladite personne, ou encore que cette révélation ait été commise par imprudence ou négligence par une personne dépositaire. L'article 413-4 propose une sanction de même nature dès lors qu'une information relative à l'identité d'une personne membre de certaines unités des forces spéciales est révélée.

82. Ainsi, l'acte de manipulation de l'information qui consisterait à révéler l'identité réelle de certaines personnes peut donner lieu à des sanctions importantes, a fortiori lorsque la révélation de ces informations a conduit à des actes portant atteinte à leur intégrité physique.

4. Atteinte au secret des correspondances

83. Hors du cadre de la protection des intérêts fondamentaux de la nation, le Code pénal permet de sanctionner la révélation d'un certain nombre de secret (secret professionnel, secret des sources journalistes ou encore secret de la vie privée). Parmi eux, l'infraction de violation du secret des correspondances est particulièrement intéressante pour lutter

contre la manipulation de l'information tant l'on sait que les ingérences étrangères peuvent prendre la forme d'une révélation d'un contenu de boîte mail (voir l'affaire des courriels d'Hillary Clinton, par exemple). Le texte pourrait venir au soutien des articles du Code pénal relatif à la protection des intérêts fondamentaux de la nation. L'article 226-15 du Code pénal dispose ainsi que : *« le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende »*. L'alinéa second dispose que *« est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de* ***divulguer*** *des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions. »*

5. Délit d'atteinte au secret de fabrication par un directeur ou un salarié

84. Les collaborateurs internes à l'entreprise peuvent également être à l'origine du vol de données. Ils peuvent, très souvent, viser certaines informations à des fins de captation ou d'espionnage industriel. Les acteurs malveillants vont notamment cibler des données relatives à la stratégie commerciale des entreprises, à leur savoir-faire et leurs développements technologiques, à leur organisation et fonctionnement interne, ou encore à la sécurité de leurs systèmes d'information. Ils peuvent également chercher à supprimer des données, à les modifier ou à en empêcher l'accès. Les personnels les plus à risque sont : les **salariés en fin de contrat**, les stagiaires et les prestataires de service externe (par exemple les contrats de recherche et d'invention passé avec un prestataire en droit des brevets) et les salariés de nationalité étrangère. Les vols peuvent survenir dans les locaux de l'entreprise, ils peuvent parfois être commis depuis l'extérieur, notamment dans le cadre du télétravail grâce aux accès à distance. Ces vols interviennent pour plusieurs raisons : revente, réutilisation pour le compte du nouvel employeur, création d'une entreprise concurrente, vengeance ou transmission pour le compte d'un concurrent ou d'un agent étranger[48]. C'est la raison pour laquelle aux côtés du délit de

[48] Flash DGSI, n°106, 2024.

livraison d'informations à une entité étrangère[49] qui suppose une intention de s'entendre avec cette dernière, le code du travail prévoit un délit pénal qui permet de sanctionner un salarié qui déroberait une information sans intention de trahir les intérêts de la nation.

85. L'article L.1227-1 du code du travail dispose ainsi que *: « le fait pour un directeur ou un salarié de révéler ou de tenter de révéler un secret de fabrication est puni d'un emprisonnement de deux ans et d'une amende de 30 000 euros. La juridiction peut également prononcer, à titre de peine complémentaire, pour une durée de cinq ans au plus, l'interdiction des droits civiques, civils et de famille prévue par l'article 131-26 du code pénal. »*

6. Le délit d'initié

86. Rejoignant les développements relatifs à la manipulation de l'information sur les marchés financiers par la transmission d'une information fausse ou trompeuse, le droit positif français permet la sanction de certaines personnes qui utiliseraient une **information dite *« privilégiée »*** et donc, très souvent, confidentielles, pour mener pour elle-même ou autrui des opérations boursières.

87. L'article L.465-1 du code monétaire et financier dispose ainsi que : *« Est puni de cinq ans d'emprisonnement et de 100 millions d'euros d'amende, ce montant pouvant être porté jusqu'au décuple du montant de l'avantage retiré du délit, sans que l'amende puisse être inférieure à cet avantage, le fait, par le directeur général, le président, un membre du directoire, le gérant, un membre du conseil d'administration ou un membre du conseil de surveillance d'un émetteur concerné par une information privilégiée ou par une personne qui exerce une fonction équivalente, par une personne disposant d'une information privilégiée concernant un émetteur au sein duquel elle détient une participation, par une personne disposant d'une information privilégiée à l'occasion de sa participation à la commission d'un crime ou d'un délit, ou par toute autre personne disposant d'une information privilégiée en connaissance de cause, de faire usage de cette information privilégiée en réalisant, pour elle-*

[49] *Supra*, n°77.

même ou pour autrui soit directement, soit indirectement, une ou plusieurs opérations ou en annulant ou en modifiant un ou plusieurs ordres passés par cette même personne avant qu'elle ne détienne l'information privilégiée, sur les instruments financiers ou sur les crypto-actifs émis par cet émetteur ou sur les instruments financiers ou sur les crypto-actifs concernés par ces informations privilégiés ».

88. Le texte peut avoir une importance fondamentale dans la mesure où le délit d'initié, souvent perçu comme un outil classique de régulation boursière, peut devenir une arme indirecte dans une stratégie d'ingérence étrangère via la manipulation de l'information sensible à des fins de **déstabilisation financière**. Prenons un exemple. Un analyste travaillant au sein du ministère de l'Économie est informé d'une décision imminente de la nationalisation partielle d'un groupe stratégique du CAC 40. Cette information est strictement confidentielle. L'analyste transmet volontairement l'information à une ONG ayant partie liée avec une puissance étrangère. Quelques heures avant l'annonce officielle, des fonds souverains achètent massivement des actions et une rumeur est orchestrée sur les réseaux sociaux. Dans cet exemple, le salarié commettrait ainsi un délit d'initié dont les acteurs étrangers seraient complices.

7. Atteinte à la vie privée

89. La vie privée est protégée civilement et pénalement. Le célèbre article 9 du Code civil, qui consacre un droit à la vie privée, permet également d'obtenir des dommages-intérêts pour réparer le préjudice qui en découle. Il dispose ainsi que *« chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »* Le droit pénal, de son côté, sanctionne également toute violation de la vie privée. Les articles 226-1 à 226-7 du code pénal dressent ainsi de nombreuses hypothèses et sanctions permettant de manipuler une information certes authentique, mais délibérément manipulée. Ainsi, l'article 226-1 dispose que *« est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque,*

volontairement de porter atteinte à l'intimité de la vie privée d'autrui » que ce soit en captant ses paroles, son image ou sa localisation. On soulignera que l'alinéa 5 du même article aggrave la sanction dès lors que les faits *« sont commis au préjudice d'une personne dépositaire de l'autorité publique, chargée d'une mission de service public, titulaire d'un mandat électif public ou candidate à un tel mandat ou d'un membre de sa famille »*. Les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende.

8. La protection du secret des affaires

90. Les fondements précédents relevaient principalement du droit pénal et de leur action civile consécutive. Or, la diffusion d'une information confidentielle aux fins de manipulation d'information peut également faire l'objet d'une **action civile visant à réparer le dommage subi** par la personne morale ou physique victime de ladite manipulation. La diffusion d'une information confidentielle peut être le résultat d'un vol de données, mais peut également résulter d'une subtilisation reposant sur la tromperie. Or, dans un contexte de guerre hybride, les entreprises doivent pouvoir protéger leurs secrets de manière efficace et attendre une réponse judiciaire forte.

91. L'entreprise peut, en principe, protéger sa recherche et ses innovations en recourant à propriété intellectuelle. Par exemple, une invention brevetée est protégée au titre de la propriété industrielle par une action en contrefaçon mais les données du brevet sont publiées, si bien qu'il n'est plus secret. Dès lors, si l'entreprise désire garder une information secrète, n'a d'autres choix que de protéger ses informations sensibles sur le mode du secret qui, pendant longtemps, n'était pas une catégorie juridique pleine et entière. La seule pratique des clauses de confidentialité et le droit commun de la responsabilité civile protégeaient bien lâchement le savoir d'une entreprise. Face à la multiplication des affaires d'espionnage industriel et à la maigre réponse judiciaire (on sait, par exemple, que les entreprises préfèrent taire les affaires d'espionnage pour ne pas porter atteinte à leur réputation) le législateur européen s'est emparé de la question grâce à la directive 2016/943 du 8 juin 2016, transposée par la loi n°2018-670 du 30 juillet 2018 aux articles L.151-1 et suivants du code de commerce. Désormais, **la violation du**

secret des affaires obéit à un régime propre et aménage, de plein droit, les conséquences civiles de l'obtention et divulgation illicites d'une information secrète. Le texte sera utile pour réparer les conséquences civiles d'une manipulation d'information, cette fois-ci dans des conditions particulièrement dissuasives pour l'auteur de la faute.

92. Désormais, le droit commercial, à l'article L.151-1 du code de commerce, définit ce qu'est une information secrète protégée : il s'agit d'une information qui n'est pas connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité (1°) ; qui revêt une valeur commerciale, effective ou potentielle (2°) ou qui fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables (3°). Ainsi, le droit de la manipulation d'information est pleinement visé par ce texte. Toute information visée par le texte et rendue illicitement publique pourra déclencher le régime de protection du secret des affaires.

93. Le droit commercial sanctionne, en effet, l'obtention d'un secret, c'est-à-dire réalisé sans le consentement de son détenteur (L.151-4, C. com.). Elle peut procéder d'un vol pur et simple (1°) comme d'un comportement déloyal (2°) pour englober aussi les hypothèses de documents échangés dans le cadre d'une négociation. Il sanctionne aussi, et surtout, l'utilisation et la divulgation du secret (L.151-1, C. com.) qui sont entendues très largement comme toute forme d'exploitation ou de transmission de l'information.

94. Le plus intéressant, pour lutter contre la manipulation de l'information, réside dans les sanctions offertes par le droit commercial. Il va de soi que le contrevenant engage sa responsabilité civile (C. com., art. L.152-1). Mais l'article L.152-3 offre à la victime une palette de mesures judiciaire destinées à atténuer ou prévenir les conséquences de la violation du secret : mesures de cessation de l'illicite, destruction, rappel de produits, mesures provisoires et conservatoires en référé (C. com., art. L.152-4). Plus performante encore sont les mesures de réparation qu'offre le code de commerce : en plus de **la perte financière classique** (C. com., art. L.152-6, 1° : ici les conséquences économiques, la perte financière et le manque à gagner) du **préjudice moral** (C. com., art. L.152-6, 2°), comme l'atteinte à la réputation par exemple) le texte permet d'octroyer ce qui se rapproche de que l'on appelle des **dommages-intérêts restitutoires** (ou confiscatoire,

en ce sens où ils vont confisquer le profit réalisé par l'auteur de la faute) qui vont permettre de sanctionner la faute lucrative de l'auteur de la faute.

95. On notera que c'est précisément dans un contexte d'espionnage que les dommages-intérêts restitutoires ont été inventés par la Chambre des Lords en Angleterre. George Blake, ancien agent du MI6, devenu agent double au profit de l'URSS, a été condamné à 42 ans de prison, s'est évadé et a rejoint Moscou. En 1989, il publie ses mémoires relatant ses activités d'espionnage et révèle de nombreux secrets qu'il s'était engagé à ne pas révéler en raison de l'existence d'une clause de confidentialité signée lors de son engagement au MI6. Le gouvernement britannique intente une action en justice pour empêcher Blake de percevoir les profits générés par la vente de son livre. Pour la première fois, dans l'arrêt *Attorney General v. Blake* (27 juillet 2000), la Chambre des lords a ordonné au défendeur de restituer les profits tirés de sa violation contractuelle et donc du bénéfice réalisé, quand bien même l'État n'avait pas subi de préjudice financier direct. Il s'agissait de sanctionner la faute lucrative de l'espion, en l'empêchant de tirer profit de sa propre faute.

96. L'article L.152-6 du code de commerce s'inscrit donc dans ce mouvement de réparation à la fois plus complet et plus punitif. En effet, le juge doit prendre en compte « ***les bénéfices réalisés par l'auteur de l'atteinte au secret des affaires, y compris les économies d'investissements intellectuels, matériels et promotionnels que celui-ci a retirées de l'atteinte*** ». La faute lucrative est ainsi prévenue et sanctionnée. Ces dernières permettent à l'auteur de commettre volontairement une faute qui lui rapportera davantage que ce qu'il paiera de dommages-intérêts (le paparazzi qui viole le droit à l'image d'une célébrité, celui qui vole une information dans une entreprise pour la revendre, etc.). Or, au nom du principe de réparation intégrale du dommage, le droit de la responsabilité civile français n'indemnise pas la faute lucrative, sauf exception (et clause contraire en matière contractuelle). C'est donc un corps de règles remarquable en ce sens qu'il prend en compte dans le calcul du préjudice l'ensemble des bénéfices réalisés par l'auteur de la faute et le dissuade de commettre une faute lucrative.

97. Prenons un exemple, appliqué à la manipulation de l'information. Une société française est spécialisée dans l'intelligence économique et élabore un rapport confidentiel destiné à un ministère sur la vulnérabilité informationnelle des médias français face à l'ingérence étrangère. Le rapport contient une cartographie des risques, des recommandations et des données sensibles collectées par voie contractuelle et confidentielle. Un ancien salarié de ladite société transmet sous pseudonyme à un média sous contrôle étranger autorisé à émettre en France. Ce média publie une version du document, en insistant sur une prétendue volonté du gouvernement français de censurer les médias visés. Grâce à cette fuite, le média sous contrôle étranger voit sa fréquentation augmenter, et engrange de nombreux revenus publicitaires. Notre société française pourra saisir le juge pour ordonner la restitution des bénéfices tirés de l'atteinte, quand bien même elle n'aurait pas subi de préjudice financier direct. Ceci, en plus des mesures de cessation de l'illicite et de la réparation d'autres chefs de préjudice.

98. Les dommages-intérêts compensatoires sont, par conséquent, un outil redoutable de lutte contre la manipulation de l'information dès lors que celle-ci repose sur la révélation d'une information confidentielle. Elle incitera, sans aucun doute, les victimes à agir en réparation puisque la compensation financière est bien plus intéressante qu'auparavant, et que l'effet dissuasif de la sanction est considérablement plus efficace. Dans l'affaire Michelin, par exemple, si le concurrent étranger avait décidé d'exploiter le vol d'information, la seconde serait obligée à l'égard de la seconde sur les bénéfices réalisés grâce à ce vol.

9. Le droit des obligations

99. Les développements précédents peuvent laisser penser que les informations confidentielles qui ne sont pas soumises, pour une raison ou pour une autre, au droit des secrets d'affaires, ne pourraient pas recevoir une protection aussi efficace. La réponse doit être nuancée.

100. En droit commun des contrats, la réforme du 10 février 2016 a consacré une obligation de confidentialité de plein droit applicable aux informations obtenues pendant les

négociations. Ainsi, l'article 1112-2 du Code civil dispose que *« celui qui utilise ou divulgue sans autorisation une information confidentielle obtenue à l'occasion des négociations engage sa responsabilité dans les conditions du droit commun. »* La protection n'est manifestement pas aussi optimale qu'en droit commercial mais permet à quiconque est victime d'une manipulation de l'information par révélation d'agir en justice, quand bien même aucune clause n'aurait été prévue au contrat.

101. En effet, en pratique, et bien avant la consécration d'un régime de protection du secret en droit commun ou en droit commercial, les parties avaient l'habitude de stipuler des clauses de confidentialité par lesquelles elles s'obligeaient à ne pas révéler ni utiliser les informations obtenues à l'occasion de la conclusion d'un contrat. La technique contractuelle peut venir parer et augmenter la protection superficielle qu'offre le droit commun. En effet, les parties peuvent imaginer des clauses pénales ou des clauses aménageant les dommages-intérêts dus en cas de violation de la clause. Dans les deux cas, l'idée est de prévoir un montant de dommages-intérêts en cas de violation de la clause nettement supérieur à ce que l'auteur de la faute aurait dû en l'absence de clause.

102. Ensuite, comme nous le verrons[50], la manipulation de l'information par révélation peut aussi être un cas de concurrence déloyale qui désorganise une entreprise et qui, dans une certaine mesure, la réparation de la faute lucrative. Enfin, le projet de réforme de la responsabilité civile souhaite reconnaître le principe de la faute lucrative et la sanctionner par une amende civile. Toutefois, la réforme est au point mort et ne semble pas devoir être adoptée dans l'immédiat.

---

103. Pour conclure, la manipulation de l'information par révélation d'une information confidentielle peut faire l'objet d'une large palette de sanctions visant tantôt celui qui a subtilisé l'information, tantôt celui qui la manipule et en tire des fruits. Une réponse pénale adaptée devra être mise en œuvre selon que la soustraction de la donnée est simplement crapuleuse, à destination d'un concurrent ou, pire, d'une entité ou d'un

[50] Sur la concurrence déloyale : v° *infra* n°127 et s.

concurrent étrangers. La gradation de la réponse pénale (de la violation du secret au délit d'initié, en passant par le droit pénal du travail) sera équivalente à la menace pour les intérêts de la personne physique visée ou de l'entreprise qui se recouperont parfois à ceux de la nation. La réponse civile, elle aussi, s'adapte de mieux en mieux à ce type de délit. L'émergence d'un droit des secrets d'affaires permet de voiler les informations sensibles d'une protection de plein droit dont les sanctions renforcent leur protection et minent la pratique des fautes lucratives plus efficacement que ce que ne le faisait déjà le droit commun. Reste que l'un des éléments déterminant sera parfois d'identifier l'auteur car de son identification dépend l'indemnisation et la sanction. D'où la nécessité de coupler la connaissance du droit avec une approche solide des moyens matériels de sécurité et de défense dans l'entreprise.

3) Atteintes à la propriété de l'information

104. La manipulation de l'information, comme nous l'avons vu, résulte souvent d'une subtilisation d'informations qui n'ont pas vocation à être rendues publiques, soit parce qu'elles sont confidentielles[51], soit parce qu'elles appartiennent à une personne physique ou morale, soit les deux en même temps. Les développements qui vont suivre sont intimement liés à la confidentialité de l'information puisque le vol de données peut porter sur des informations confidentielles. Ils concernent, cependant, les hypothèses dans lesquelles l'information appartient à son détenteur mais ne fait pas forcément l'objet d'une mesure de confidentialité. Dans tous les cas, elle ne peut pas être diffusée ou utilisée sans autorisation de son titulaire. C'est ici le vol d'information, cyber ou non, qui sera à l'origine de la manipulation de l'information. L'auteur du dommage et celui qui en tire bénéfice seront visés par des sanctions.

1. Cyberattaques et vol de données

105. La guerre informationnelle a pour principal champ de bataille le cyberespace et ses manifestations principales résident dans les cyberattaques. Cette guerre

[51] V° *Supra,* n°76 et s.

informationnelle peut prendre de nombreuses formes : intrusions, saturation du système (*Distributed denial of service* - DDoS), vol de données ou encore sabotage. Du point de vue de la seule lutte contre la manipulation de l'information, les cyberattaques sont particulièrement redoutables puisqu'elles vont très souvent être à l'origine de ladite manipulation. Par exemple, une diffusion de données privées qui auraient d'abord été piratées, ou encore une intrusion dans un système de données pour diffuser une fausse information. Ainsi du compte d'un réseau social d'un membre du gouvernement dont le pirate usurperait l'identité pour diffuser des fausses informations.

106. La cybersécurité passe ainsi par un droit permettant de lutter contre les cyberattaques. En droit français, c'est principalement la loi LCEN du 21 juin 2004 qui a posé les bases d'un arsenal juridique destiné à lutter contre les cyberattaques aux articles 323-1 à 323-8 du Code pénal que l'on retrouve au sein du livre consacré aux crimes et délits contre les biens. Listons les textes qui intéressent la manipulation de l'information.

107. Tout d'abord, l'article 323-1 pose une interdiction de principe de toute action frauduleuse dans un système de traitement automatisé de données (STAD) : *« Le fait **d'accéder** ou de se **maintenir**, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la **suppression** ou la **modification** de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende. »* L'article 323-2, quant à lui, sanctionne le fait d'entraver ou de fausser le fonctionnement d'un système automatisé de données. Ainsi, l'article 323-1 intéresse la manipulation de l'information en ce sens qu'il sanctionne la pratique qui consiste à s'introduire frauduleusement dans un STAD pour supprimer ou modifier une information – ce qui, sans aucun doute, constitue une manipulation de l'information.

108. Plus encore, l'article 323-3 du Code pénal dispose que *« le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende. Lorsque cette infraction a été commise par à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende. »* C'est sur ce fondement qu'un vol de données pourra être sanctionné lorsqu'il s'accompagne d'une manipulation de l'information. On s'est, en effet, longtemps demandé si une chose immatérielle, telle qu'une information, pouvait faire l'objet d'un vol. L'article 311-1 du Code pénal dispose que *« le vol est la soustraction frauduleuse de la chose d'autrui. »* Le vol semblait nécessiter la soustraction d'une chose matérielle. Très tôt cependant, la Cour de cassation l'a parfaitement admis et la loi susmentionnée a formellement consacré le vol de données.

109. Concernant l'intrusion, il faut distinguer plusieurs situations. Tout d'abord, la loi n'exige pas, a priori, que le STAD soit protégé pour que l'infraction soit caractérisée. Toutefois, le fait pour le maître du système de présenter son système comme « protégé » va avoir une incidence sur l'appréciation judiciaire du caractère intentionnel et frauduleux de l'infraction. En effet, ce n'est que lorsqu'un système est manifestement protégé que l'on peut reprocher à l'intrus de s'être introduit. Lorsque le système n'a aucune mesure de protection, il n'est pas possible de reprocher à un individu de s'être introduit. Ainsi, fort logiquement, le fait de protéger techniquement le système facilite la démonstration du caractère frauduleux et/ ou intentionnel de l'acte. Cependant, la question se complique lorsque des failles de sécurité sont constatées, car les juges vont pouvoir opposer au maître du système sa négligence et sanctionner indirectement les personnes dont le STAD ne présente pas un système suffisamment protégé. On a ainsi vu un individu s'introduire dans un système sécurisé présentant une défaillance technique être exonéré de sa responsabilité pénale du fait de s'être introduit – mais non de s'être maintien[52].

[52] Crim., 20 mai 2015, n°14-81336.

110. D'autres décisions sont encore plus surprenantes. En témoigne un jugement du tribunal judiciaire de Paris rendu le 1er décembre 2023[53], qui a, pour des raisons identiques, refusé de condamner un prévenu qui avait su exploiter une faille dans un code. L'affaire oppose la plateforme *Platypus* à un individu passionné d'informatique accusé d'avoir siphonné les fonds de la plateforme au point de lui causer un préjudice s'élevant à 9,5 millions de dollars. *Platypus* est une plateforme de finance décentralisée (*DeFi*) qui ne s'adosse, comme son nom l'indique, à aucune banque centrale. L'avantage, ou l'inconvénient, c'est que toutes les transactions réalisées par son biais ne passent par aucun intermédiaire et s'adossent à la technologie des *smartcontracts (blockchain)*. Hormis la technique sur laquelle elle repose, la finance décentralisée propose peu ou prou les mêmes services que la finance classique : obtention de prêts, transferts d'argent, placements, *etc*. La plateforme *Platypus* générait ainsi divers *smartcontracts* dans lesquels le prévenu avait repéré une faille. Ce dernier va alors lui-même programmer divers *smartcontracts* dans le but de mettre la main sur des fonds appartenant à la plateforme. Pour y parvenir, il va souscrire deux emprunts successifs. Le premier va servir à garantir le second, ce dernier consistant à emprunter un cryptoactif émis par la plateforme. Puis, il va mettre immédiatement en œuvre la possibilité, offerte par le même *smartcontract*, de retrait d'urgence et va rembourser le premier prêt. Les liquidités du second prêt, qui aurait dû être bloquées faute de garantie, sont toujours disponibles. Telle était la faille. Il échangera ensuite les liquidités contre d'autres cryptoactifs sur la plateforme. Le prévenu est alors poursuivi pour escroquerie, vol, abus de confiance, blanchiment et accès et maintien dans un système de traitement automatisé des données. Mais le tribunal balaiera une par une toutes ces qualifications. Selon le tribunal, l'escroquerie ne pouvait être qualifiée, car la faille exploitée par le prévenu avait pour origine une négligence de la plateforme. Un tel raisonnement peut surprendre. Ce n'est pas parce qu'il existe une faille que la fraude est impossible. En matière civile et commerciale, la fraude se définit comme *« un acte réalisé en utilisant des moyens déloyaux destinés à surprendre un consentement, à obtenir un avantage matériel ou moral indu, ou réalisé avec l'intention d'échapper à l'application d'une loi impérative ou prohibitive »*[54]. Sa conception pénale ne

[53] Tribunal judiciaire de Paris, 13e chambre criminelle, 1er décembre 2023 ; confirmé par Cour d'appel de Paris, 21 novembre 2024 – un pourvoi a été formé.
[54] Com., 13 décembre 2017, n°16-21.498.

diffère guère. Un système mal codé n'est pas si différent d'une automobile mal fermée, ou d'un distributeur automatique dysfonctionnel. En la matière, la fraude ne devrait pas dépendre de la possibilité de frauder. Les explications sont probablement à chercher ailleurs : peut-être les juges cherchent-ils à inciter les acteurs à se doter de services plus sécurisés, comme la loi du 17 août 2015, transposant la directive n°2013/40 relative aux attaques contre les systèmes d'informations, leur impose sous peine de sanctions pénales. Bien que de telles décisions n'aient pas été rendues dans un contexte de manipulation de l'information, il est nécessaire que la Cour de cassation abandonne cette approche naïve[55] de la cyberdéfense pour ne pas, un jour, permettre à un acteur hostile de l'ingérence informationnelle de s'en tirer à bon compte.

111. On ajoutera, enfin, que les deux circonstances aggravantes sont applicables aux infractions ci-dessus qui intéressent directement la lutte contre la manipulation de l'information : l'association de malfaiteurs (450-1) et l'ingérence étrangère (411-12).

2. La contrefaçon

112. La contrefaçon est traditionnellement mobilisée dans le champ de la propriété intellectuelle pour protéger les œuvres de l'esprit, les brevets, les dessins et modèles, les marques ou encore le savoir-faire. Bien connu du secteur culturel, économique et industriel, la contrefaçon peut également devenir un fondement juridique original mais redoutablement efficace pour lutter contre la manipulation de l'information. En effet, certaines opérations de désinformation ou d'influence ne se contentent pas de diffuser des contenus mensongers – elles peuvent s'attacher à imiter, détourner, usurper, donner *l'impression de*, mentir pour atteindre leurs objectifs. La propriété intellectuelle peut être manipulée pour plusieurs raisons. La première consiste à imiter les signes d'identification d'une source légitime pour renforcer l'effet de persuasion (faux sites de presse, faux communiqués, fausses informations concernant telle ou telle marque). La seconde consiste à imiter les produits protégés par un droit de propriété intellectuelle à des fins de déstabilisation économique.

[55] D. Mainguy, D*roit de la guerre "atypique"*, *op. cit*.,, n°162, p.274.

113. La contrefaçon est constituée par toute atteinte portée aux droits du propriétaire du droit de propriété intellectuelle. Elle est sanctionnée par une action spécifique. Les moyens de lutte contre la contrefaçon sont multiples. La victime peut agir en contrefaçon devant le juge civil ou devant le juge pénal. Il lui est, la plupart du temps, conseillé d'agir au civil car les dommages-intérêts obtenus sont généralement plus élevés. Elle a intérêt, au préalable, à se ménager la preuve de la contrefaçon en recourant à une saisie-contrefaçon. Dans la plupart des cas, la victime de la contrefaçon dispose d'une action civile et d'une action pénale dont les sources et sanctions sont à rechercher dans le code de la propriété intellectuelle (CPI). Elles peuvent, dans la plupart des cas, se coupler à une action en concurrence déloyale[56]. La circonstance aggravante d'ingérence étrangère n'est pas, *a priori*, applicable dans ce type de contentieux.

114. En matière littéraire et artistique, c'est l'article L.335-2 du code de la propriété intellectuelle qui fonde l'action pénale en contrefaçon. Celui-ci dispose que *« toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit. La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende. Seront punis des mêmes peines le débit, l'exportation, l'importation, le transbordement ou la détention aux fins précitées des ouvrages contrefaisants. Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende »*. L'article L.335-2-1 du code de la propriété intellectuelle offre également une protection spécifique pour le logiciel : *« Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait : 1° d'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés »*. L'action civile, quant à elle, est prévue aux articles L.331-1 et suivants du même code.

[56] *Infra*, n°127 et s.

115. En matière de propriété industrielle**,** la sanction civile et pénale de la contrefaçon est répartie sur plusieurs textes en fonction de l'objet du droit de propriété. Nous ne citerons que ceux qui intéressent les dessins et modèles, les brevets et les marques.

116. **Les dessins et modèles** - L'article L.521-1 du code de la propriété intellectuelle dispose que *« toute atteinte portée aux droits du propriétaire d'un dessin ou modèle, tels qu'ils sont définis aux articles L.513-4 à L.513-8, constitue une contrefaçon engageant la responsabilité civile de son auteur ».*

117. **Le brevet d'invention** - La violation d'un brevet est prévue à l'article L.615-1 du CPI : *« toute atteinte aux droits du propriétaire du brevet, tels qu'ils sont définis aux articles L.613-3 à L.613-6 constitue une contrefaçon. La contrefaçon engage la responsabilité civile de son auteur. »* L'action pénale est, de son côté, prévue aux articles L.615-12 et suivants du CPI. Là-aussi, trois ans d'emprisonnement et 300 000 euros d'amende viennent sanctionner le contrefacteur.

118. **Les marques et autres signes distinctifs** – La contrefaçon de marque, enfin, est prévue à l'article L.716-4 et suivants du CPI. Ce dernier dispose que : *« l'atteinte portée au droit du titulaire de la marque constitue une contrefaçon engageant la responsabilité civile de son auteur. Constitue une atteinte aux droits attachés à la marque la violation des interdictions prévues aux articles L.713-2 à L.713-3-3 et au deuxième alinéa de l'article L.713-4 »*. Une action pénale est également prévue aux articles L.716-8-9 et suivants du CPI qui prévoient une peine de quatre ans d'emprisonnement et de 400 000 euros d'amende pour le contrefacteur.

119. Selon les cas, des sanctions originales peuvent être prononcées : la confiscation de l'objet contrefaisant, la fermeture de l'établissement, le retrait du marché ou encore l'affichage du jugement. Encore, et surtout, l'action en réparation du dommage causé par la contrefaçon peut profiter à la victime en ce sens que le juge doit impérativement tenir compte des gains réalisés par le contrefacteur. Si bien que la victime peut espérer davantage que la seule réparation de son préjudice et confisquer les bénéfices réalisés par le contrefacteur l'empêchant, ainsi, de commettre une faute lucrative. Par exemple,

en droit des marques, l'article L.716-4-10 du CPI explique ainsi que le juge doit tenir compte *« des conséquences économiques négatives de la contrefaçon »*, du *« préjudice moral »* et des *« bénéfices réalisés par le contrefacteur, y compris les économies d'investissements intellectuels, matériels et promotionnels que celui-ci a retirées de la contrefaçon »* (un article similaire est prévu pour les brevets (L.615-7) et les œuvres de l'esprit (L.331-1-3)).

120. Sur le plan civil, l'action en contrefaçon pourra donc se révéler d'une redoutable efficacité lorsque le manipulateur s'appuiera sur des détournements de propriété intellectuelle pour manipuler l'information. Récemment, une tendance virale sur la plateforme TikTok en a donné un exemple parlant. Dans un contexte de guerre commerciale entre la Chine et les Etats-Unis, et faisant directement suite aux annonces du président Trump visant à rehausser les droits de douane à l'égard de la Chine, TikTok a été le théâtre d'un phénomène de manipulation de l'information de nature à porter préjudice aux intérêts économiques des grandes sociétés occidentales spécialisées dans le luxe et la mode. Une trend TikTok est une tendance virale, c'est-à-dire une série de vidéos qui fait l'objet d'une poussée dans les algorithmes et qui va toucher de nombreux utilisateurs, invités eux-mêmes à reproduire ou diffuser la trend. Sur l'application, une vidéo faisant l'objet d'une trend virale a infiniment plus de chance d'apparaître dans le fil de l'utilisateur. S'il se montre réceptif, son fil est alors inondé de vidéos similaires qu'une trend est un phénomène suffisamment visible et viral que la plateforme ne peut ignorer. Cette trend, intitulée par les utilisateurs et les manipulateurs « *Trade War TikTok* » a mis en scène un certain nombre de personnes se présentant comme les producteurs et fabricants directs des grandes marques de luxe occidentales, autorisés par le gouvernement à rompre leurs clauses de confidentialité dans le contexte de la guerre commerciale. Du point de vue de la manipulation de l'information, la campagne a lieu à un moment propice de tension commerciale et permet aux entreprises chinoises de porter atteinte à la réputation et de déstabiliser les grandes entreprises occidentales. Le message est double : il permet de capter des parts de marché, mais aussi d'exposer un narratif trompeur selon lequel les grandes marques occidentales bernent leurs clients en leur vendant à prix d'or des objets fabriqués en Chine. L'intégralité des influenceurs se sont révélés être des contrefacteurs. Pour les victimes, deux pistes contentieuses : La première est de

tenter une action pénale contre les auteurs directs de l'infraction. Le fondement pénal de la contrefaçon et de la pratique commerciale trompeuse peut être mobilisé. Au civil, un tel fondement permet d'être indemnisé selon un préjudice qui tient compte des bénéfices réalisés par le contrefacteur et sanctionne ce que l'on appelle la faute lucrative. Une autre piste est de tenter une action directe contre la plateforme TikTok. Sur le fondement du DSA, mais aussi, plus simplement, de la loi LCEN, les plateformes ont un devoir de vigilance qui n'est pas forcément très contraignant, mais qui leur impose un devoir de réaction dès lors qu'ils sont face à un contenu manifestement illicite (première hypothèse) ou un contenu signalé comme tel[57] (seconde hypothèse). Parallèlement, l'ARCOM peut être saisie pour constater la violation d'une obligation légale de la part de la plateforme, enjoindre la plateforme de supprimer le contenu, ce qui facilitera les actions civiles. Les entreprises françaises victimes de cette campagne de désinformation peuvent s'unir et agir contre TikTok pour tenter d'obtenir une indemnisation. Celle-ci n'a pas réagi, et ne réagit toujours pas, face à un contenu que l'on doit logiquement considérer comme manifestement illicite tant il est grossier, et qu'ayant fait l'objet d'une trend, la plateforme ne pouvait ignorer.

4) Atteintes à la fonction de l'information

121. Les infractions informationnelles mentionnées ci-dessus portent, bien évidemment, toutes atteinte à la fonction de l'information qui repose, en principe, sur la transmission d'un renseignement authentique, licite et loyal. Toutefois, la plupart insiste sur la nature (fausse, confidentielle, appropriée) de l'information et chaque texte est, finalement, assez étanche avec les autres. Une information ne peut pas être fausse et confidentielle, par exemple. Il existe cependant des régimes juridiques à portée générale qui peuvent être mobilisés pour saisir et sanctionner la manipulation d'information sous toutes ses formes, qu'elle repose sur du faux ou du vraie. Il ne s'agit plus ici de se demander si l'information est vraie ou fausse, mais simplement de savoir si elle est manipulée. L'on se rapproche ainsi d'un régime idéal, celui qui serait basé sur l'intention de manipuler.

[57] *Infra*, n°134 et s.

1. Le sabotage

122. Juridiquement, le sabotage est une notion assez confuse dans la mesure où il recouvre et entrecroise incriminations de droit commun (ce peut être un abus de confiance, ou encore une destruction de bien) et de droit spécial (crimes et délits contre la nation) qui le vident de sa substance et renvoient très souvent le criminel et sa victime dans les filets d'un régime juridique moins sévère. Son large champ d'application est à la fois sa force et sa faiblesse. Sa force, car le texte a un potentiel efficace contre la manipulation de l'information. Sa faiblesse, car son utilisation semble si dangereuse que rares sont les juges à s'en saisir.

123. Le sabotage intègre le livre du code pénal consacré aux crimes et délits contre la nation. Il est prévu à l'article 411-9 du code pénal qui dispose que : *« le fait de détruire, détériorer ou* ***détourner*** *tout document, matériel, construction, équipement, installation, appareil,* ***dispositif technique ou système de traitement automatisé d'informations*** *ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter atteinte* ***aux intérêts fondamentaux de la nation****, est puni de quinze ans de rétention criminelle et de 225 000 euros d'amende. »* L'alinéa second dispose que *« lorsqu'il est commis dans le but de servir les intérêts d'une* ***puissance étrangère, d'une entreprise ou une organisation étrangère ou sous contrôle étranger,*** *le même fait est puni de vingt ans de détention criminelle et de 300 000 euros d'amende. »*

124. Pris à la lettre, le sabotage est salvateur. Il pourrait s'appliquer à n'importe quel cas de manipulation de l'information dès lors qu'elle intervient sur un STAD et qu'elle porte atteinte, comme c'est souvent le cas, aux intérêts fondamentaux de la nation. Toutes les hypothèses visées dans la présente étude semblent pouvoir entrer dans son champ d'application : une fausse nouvelle russe publiée sur les réseaux sociaux qui polluerait une intelligence artificielle, la révélation d'une information confidentielle sur les réseaux sociaux ou encore une campagne de contrefaçon. Le texte est donc particulièrement intéressant du point de vue de la lutte contre la manipulation de l'information. L'on sait que, du point de vue militaire et stratégique, la manipulation de l'information peut être

identifiée comme une technique de sabotage[58] Il faudrait, dès lors, coupler la notion de sabotage au sens stratégique du terme, avec son sens juridique. Or, de ce point de vue-là, rien ne semble empêcher de s'appuyer sur le délit de sabotage pour porter la lutte contre la manipulation de l'information. Ainsi, le fait, pour un groupement, d'orchestrer une manipulation de grande ampleur sur un réseau social doit être qualifié comme le détournement d'un traitement automatisé d'informations dans un but antinational. Les avantages sont nombreux puisque les sanctions sont particulièrement importantes et dissuasives ; tandis que l'effet, en termes de communication stratégique, est bien plus conforme à la dangerosité de la pratique.

125. Toutefois, c'est un euphémisme, l'article 411-9 du code pénal est très rarement appliqué. La rareté de son application s'explique à la fois en raison d'un problème d'opportunité, et un problème de champ d'application. D'une part, l'incrimination semble pouvoir s'appliquer à n'importe quel bien dès lors qu'un intérêt pour la nation entre en jeu (au sens de l'article 410-1 du code pénal) et peut revêtir un caractère manifestement excessif. Ainsi, celui qui pollue un champ, détruit une usine ou macule une toile de maître peut virtuellement être coupable de sabotage. On le voit, le délit de sabotage doit être manié avec parcimonie et les juges sont frileux à l'idée de manier un texte si dangereux. D'autre part, la « destruction de bien » est déjà sanctionnée par l'article 322-3 du même code qui prévoit, en ses 5° et 6°, des circonstances aggravantes de destruction de biens ordinaires. Faut-il, dès lors, considérer qu'il s'agit d'un doublon ou limiter l'article 411-9 du code pénal aux seuls biens reliés à la défense nationale ? Il y a donc un conflit de qualification non résolu que la doctrine pénale a du mal à démêler. Certains considèrent que l'article ne s'applique qu'aux biens appartenant à la défense nationale, d'autres que le sabotage intervient quand l'intention de nuire aux intérêts de la nation est caractérisée. Le délit de sabotage est donc confronté à un problème **d'opportunité** (aucune action sur ce fondement n'a été envisagée), de **potentialité** (le champ d'application est très large et les juges peuvent se méfier de la potentialité d'un tel texte) et **d'interprétation** (des textes plus spéciaux croisent son champ d'application et incitent les juges à s'appuyer sur eux). Il n'en reste pas moins que de tels arguments relèvent de la doctrine et que **rien ne**

[58] J. Rovner, "Théorie du Sabotage", Études françaises de renseignement et de cyber, PUF, n°1/2023, p. VII et s.

fait obstacle, juridiquement, à l'application du délit de sabotage à la manipulation de l'information. Nous soutenons donc que le texte pourrait sans aucun doute s'appliquer et qu'il souffre principalement d'un défaut d'opportunité.

126. Les avantages seraient nombreux. Du point de vue de la **communication stratégique**, d'abord. Le terme de sabotage reflète de manière percutante, pour l'opinion publique, une forme d'ingérence étrangère grave et malveillante dont le but est principalement de saper la confiance de la société civile dans les pouvoirs publics ou les entreprises françaises. Du point de vue de la **dissuasion**, ensuite. Les sanctions sont extrêmement importantes et de nature à dissuader les manipulateurs. De plus, le fait qu'il s'agisse d'un crime permet d'enjoindre aux plateformes numériques d'agir rapidement pour supprimer tel ou tel contenu. Du **point de vue de l'action**, enfin, se fonder sur le sabotage permettrait de ne plus s'intéresser à la nature de l'information (vraie, fausse, illicite – ce qui peut causer des débats sans fin) ni à son canal de diffusion (le sabotage supposer le détournement d'un STAD, donc n'importe quelle plateforme ou IA) mais seulement à l'intentionnalité de la manipulation de l'information. S'il est prouvé que le manipulateur a eu l'intention de saboter, la nature de l'information et son canal de diffusion importent peu. L'action en sera, *in fine*, facilitée.

2. La concurrence déloyale

127. Du point de vue de la lutte contre la manipulation de l'information, la concurrence déloyale est l'équivalent de l'infraction de sabotage dans le monde des affaires. En effet, il permet de sanctionner n'importe quel type de manipulation de l'information dès lors que celle-ci est fautive. Comme pour le sabotage, l'analyse se détache de la nature de l'information et de son canal de diffusion pour se concentrer uniquement sur le comportement du manipulateur. Par ailleurs, l'action en concurrence déloyale se distingue de l'action en contrefaçon (qui peuvent d'ailleurs se coupler) qui vise à protéger un droit privatif. L'action en concurrence déloyale se veut plus large : le titulaire d'une licence de brevet ou de marque, qui n'a pas de droit privatif, peut ainsi agir au titre de la concurrence déloyale pour protéger ses activités économiques. La flexibilité de son champ d'application et ses méthodes d'indemnisation en font un instrument majeur de

lutte contre la manipulation de l'information, dès lors que celle-ci évolue dans un contexte économique.

128. La concurrence déloyale est sanctionnée sur le fondement du droit commun de la responsabilité civile qui trouve son siège à l'article 1240 du Code civil. Elle permet à un commerçant de sanctionner son concurrent pour divers comportements jugés déloyaux et incompatibles avec la morale des affaires. Dans la mesure où elle est fondée sur la responsabilité pour faute, elle est subordonnée à la démonstration d'une faute, d'un préjudice et d'un lien de causalité entre les deux. Par ailleurs, il n'est pas nécessaire que les entreprises soient en concurrence pour bénéficier de l'action : seuls des faits fautifs générateurs d'un préjudice sont à démontrer[59].

129. Commençons par la faute. Il est possible d'en dresser une typologie. Nous verrons que certaines catégories intéressent directement la manipulation de l'information : il y a la **désorganisation**, le **dénigrement**, la **confusion** et le **parasitisme.**

130. **La désorganisation –** La désorganisation d'une entreprise consiste à déstabiliser intentionnellement un concurrent par des manœuvres déloyales qui vont porter directement atteinte à un élément essentiel de l'entreprise : son salariat, son savoir-faire, sa clientèle, *etc*. Très souvent, la désorganisation de l'entreprise prend la forme d'une captation de sa clientèle par des manœuvres déloyales, ou bien de la violation délibérée de la loi. Lorsque les contrefacteurs, sur TikTok, se présentent comme les producteurs directs des grandes marques de luxe, ils captent la clientèle par des procédés déloyaux dont la manipulation de l'information est un exemple évident.

131. Le dénigrement est au cœur de la lutte contre la manipulation de l'information et constitue la forme de concurrence déloyale la plus redoutable pour le manipulateur. Il consiste à discréditer publiquement une entreprise, ses produits ou services. Ici, c'est surtout l'hypothèse des commentaires sur les moteurs de recherche et les réseaux sociaux. L'on imagine sans peine une campagne de manipulation de l'information qui aurait pour objet d'abaisser les notes et avis de certaines entreprises dans un but

[59] Com., 12 février 2008, n°06-17.501.

d'ingérence et de déstabilisation. Là non plus, l'auteur de la faute n'a pas à être en concurrence avec la victime[60]. Toutefois, pour qualifier le dénigrement, il est nécessaire que l'information soit injustifiée et ne participe à aucun sujet d'intérêt général[61]. Il se distingue de la diffamation, qui doit nécessairement porter sur une personne et qui s'interprète restrictivement. Le Professeur Dimitri Houtcieff note, à ce sujet, que *« peu importe en effet que le dénigrement repose sur un fond de vérité, dès lors qu'il porte atteinte à l'image du produit ou du service considéré, au point que la publicité donnée à des poursuites judiciaire a parfois été considérée comme un acte de dénigrement. (…) La Cour de cassation a en effet clairement affirmé que la divulgation d'une information de nature à jeter le discrédit sur un concurrent constitue un dénigrement, peu important qu'elle soit exacte »*[62]. Ainsi, le manipulateur qui se saisirait d'une information, même vraie, pour monter en épingle la mauvaise réputation d'un concurrent dans le but de lui nuire, pourrait être sanctionné. Le fondement est redoutable en matière de manipulation de l'information puisque seul compte l'intention du manipulateur.

132. **La confusion et le parasitisme** – Ces deux dernières formes de concurrence déloyale intéressent de manière moins évidente la manipulation de l'information mais pourraient trouver une utilité si d'aventure le manipulateur fondait sa stratégie sur celles-ci. La confusion résulte de l'utilisation, par le concurrent, d'un signe proche de celui d'un tiers et d'en tirer profit. La confusion réside donc dans l'ambiguïté, tandis que le parasitisme cherche l'identification totale. Dans cette dernière hypothèse, une entreprise tire profit du comportement d'une entreprise sans faire aucun effort. Il s'agit de sanctionner l'entreprise qui s'est placée dans le sillage d'une autre[63].

133. La réparation des préjudices induits par la concurrence déloyale est particulièrement intéressante en matière de lutte contre la manipulation de l'information. En effet, en plus de réparer le préjudice financier (baisse du chiffre d'affaires et perte de chance) et le

[60] Com., 9 janvier 2019, n°17-18.350.
[61] D. Houtcieff, *Droit commercial*, 5e éd., Sirey, 2022, n°1284.
[62] *Ibid.*, : Com., 23 mars 1999, n°96-22.334 : "Ayant relevé que les sociétés Fabre "n'ont pas agi, comme le journaliste et l'hebdomadaire L'express, dans le but d'une information objective des consommateurs ou des éventuels usagers des produits Korff, mais bien dans l'intention de nuire à leur concurrent, leur méthode ayant pour cible les pharmaciens distributeurs essentiels pour la société CPF, l'objectif était bien de dénigrer le produit concurrent pour s'emparer de la part de marché. »
[63] D. Houtcieff, Droit commercial, 5e éd., Sirey, 2022 n°1289 et n°1293.

préjudice moral, la Cour de cassation admet la sanction de la faute lucrative et impose aux juges du fond de tenir compte des économies réalisées par le concurrent déloyal. Ainsi, depuis un arrêt très remarqué du 12 février 2020[64] la Cour de cassation a jugé : « *Sur la réparation d'un préjudice résultant d'une pratique commerciale trompeuse pour le consommateur, conférant à son auteur un avantage concurrentiel indu par rapport à ses concurrents, la cour d'appel a pu, pour évaluer l'indemnité devant être alloué à la société X,* ***tenir compte de l'économie injustement réalisée*** *par la société Cristal* ». Ainsi, sur le modèle de ce que l'on connaît en matière de contrefaçon et de violation du secret d'affaire, la manipulation de l'information qui consisterait en un acte de concurrence déloyale permet à la victime de voir son préjudice réparé par la rétribution des bénéfices et économies réalisées par le concurrent déloyal. La sanction permet de couper court aux incitations économiques de la manipulation de l'information et doit être mobilisée toutes les fois qu'une entreprise subira une campagne de manipulation de l'information.

B. La lutte contre la manipulation de l'information prise du point de vue du producteur ou diffuseur de l'information

1) Le devoir de vigilance des fournisseurs d'hébergement en droit interne

134. À l'origine, le régime de responsabilité des hébergeurs était essentiellement jurisprudentiel. Avant l'adoption d'un régime légal spécial, les juges avaient bâti un régime de compromis dont on retrouve l'esprit dans les lois les plus récentes. Sans admettre une irresponsabilité aveugle des hébergeurs, ni tomber dans le piège d'une responsabilité automatique qui eut nuit à la liberté d'expression, les juges ont très vite considéré que le fournisseur d'un service d'hébergement ne pouvait être tenu responsable des contenus publiés sur les pages hébergées mais qu'il était tout de même tenu à un devoir de prudence et de diligence lui imposant d'adopter des mesures de

[64] Com., 12 février 2020, n°17-31.614.

vigilance raisonnables et de réagir rapidement lorsque le contenu d'un site est manifestement illicite ou qu'il fait l'objet d'un signalement.

135. C'est, en substance, ce qu'a consacré le législateur dans la loi n°2004-575, loi pour la confiance dans l'économie numérique (LCEN) adoptée le 21 juin 2004 et retouchée par de nombreuses lois successives dont la dernière date du 21 mai 2024, a profondément modifié le contenu pour tenir compte de l'adoption du règlement européen DSA.

136. Néanmoins, le contenu de l'ancienne loi peut encore servir aux contentieux en cours ou aux faits générateurs antérieurs à la loi du 21 mai 2024.

137. L'article 6, I, 2 de la loi du 21 juin 2004 disposait ainsi que : *« Les personnes physiques ou morales qui assurent, 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 ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou, si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. »*

138. Autrement dit, la responsabilité civile d'un hébergeur ne peut en principe pas être engagée sauf deux exceptions : lorsque le contenu est manifestement illicite, ou bien lorsque l'hébergeur n'a pas réagi à la suite d'un signalement. Depuis lors, de nombreux hébergeurs ont été sanctionnés pour ne pas avoir réagi rapidement. Par exemple, il a été reproché à un hébergeur de ne pas avoir retiré un contenu illicite le jour même de la réception de la notification[65].

139. Par ailleurs, le législateur a étendu le régime de responsabilité des fournisseurs d'hébergement aux contenus contrefaisant partagés par leurs utilisateurs. L'ordonnance n°2021-580 du 12 mai 2021, en transposant la directive 2019/790 (UE) du 17 avril 2019, a

[65] TGI Toulouse, 13 mars 2008, M.K. c/ Pierre G., Amen, RLDI 2008/38, n°01177, obs. J.-B. Auroux.

ajouté dans le code de la propriété intellectuelle l'article L.137-2 qui instaure une présomption de responsabilité à l'égard de l'hébergeur qui donne accès à une œuvre protégée par le droit d'auteur. Pour échapper à sa responsabilité au titre de la contrefaçon, l'hébergeur doit démontrer qu'il a fourni les meilleurs efforts pour obtenir l'autorisation du titulaire des droits et garantir l'indisponibilité de certaines œuvres, mais surtout qu'il a *« en tout état de cause, agi promptement, dès réception d'une notification suffisamment motivée de la part des titulaires de droits, pour bloquer l'accès aux œuvres faisant l'objet de la notification ou pour les retirer de son service ».*

140. La loi du 21 juin 2004 a été refondue par la loi du 21 mai 2024, pour adapter le droit interne aux dispositions du règlement (UE) 2022/2065 (DSA).

141. Par conséquent, de nombreuses dispositions de la loi LCEN ont été modifiées ou abrogées pour éviter les doublons et ne conserver que les dispositions particulières au droit français. Le règlement DSA étant d'application directe, c'est désormais sur lui qu'il faut se fonder pour sanctionner l'absence de réaction de la plateforme dans des conditions similaires à ce que proposait le droit antérieur.

142. Désormais, les articles 6 (6-1 à 6-2-2) et suivants de la loi LCEN ne concernent que les contenus pédopornographiques, pornographiques et terroristes. Les éditeurs sont pleinement responsables, tandis que les fournisseurs d'hébergement doivent réagir promptement pour retirer tout contenu conformément signalé par les autorités administratives compétentes. 250 000 euros d'amende et un an d'emprisonnement menacent l'hébergeur qui n'aurait pas réagi.

143. Par ailleurs, les hébergeurs doivent concourir à la lutte contre la diffusion de contenu constituant des infractions pénales listées à l'article 6, IV, A de la loi LCEN[66] dont plusieurs intéressent directement la manipulation de l'information, notamment l'article 24 de la loi du 29 juillet 1881. Elles ont l'obligation d'informer promptement les autorités

[66] Articles 211-2 ; 222-33 ; 222-33-1-1 ; 222-33-2 à 222-33-2-3 ; 222-39 ; 223-13 ; 225-4-13 ; 225-5 ; 225-6 ; 227-18 à 227-21 ; 227-22 à 227-24 ; 412-8 ; 413-13 ; 413-14 ; 421-2-5 ; 431-6 ; 433-3 ; 433-3-1 ; 521-1-2 et 521-1-3 et au deuxième alinéa de l'article 222-33-3 du code pénal ainsi qu'aux cinquième, septième et huitième alinéas de l'article 24 et à l'article 24 bis de la loi du 29 juillet 1881 sur la liberté de la presse.

compétentes de toutes les activités illicites mentionnées dans la liste précitée sous peine d'un an d'emprisonnement et de 250 000 euros d'amende.

144. Toutefois, la modification de la loi LCEN ne signifie pas que le devoir de vigilance des fournisseurs d'hébergement a été supprimé ou qu'il obéit à des conditions plus drastiques. Ce dernier a été consacré par le DSA, et c'est désormais en se fondant sur l'article 6 de ce dernier qu'il convient d'engager la responsabilité des hébergeurs. Ce dernier dispose que *« en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le fournisseur de services n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que le fournisseur : a) n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite et, en ce qui concerne une demande de dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent ou b) dès le moment où il en prend connaissance ou conscience, agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible ».*

145. Par exemple, lorsque la plateforme TikTok fait l'objet d'une tendance virale dans laquelle des contrefacteurs proposent des produits illicites, l'article 6 du DSA permettrait d'engager la responsabilité de la plateforme pour ne pas avoir retiré les contenus manifestement illicite, ou de ne pas avoir réagi suffisamment vite pour les retirer face à leur signalement. Cette action en responsabilité ne préjudicie pas des autres actions administratives ou civiles que le DSA permet lorsque ladite plateforme n'a pas été suffisamment diligente dans l'évaluation et la prévention des risques, dont les modalités sont étudiées dans le paragraphe suivant

2) Les règlements européens au service de la lutte contre la manipulation de l'information

146. La manipulation de l'information – qu'elle prenne la forme de désinformation, de propagande algorithmique, ou de perturbation des processus démocratiques – ne fait pas encore l'objet d'un régime juridique autonome en droit européen. Pourtant,

plusieurs instruments récents peuvent être mobilisés à cette fin, notamment le *Digital Services Act* (DSA), le *Digital Markets Act* (DMA), et *l'Artificial Intelligence Act* (IA Act). Ces textes, bien que conçus pour encadrer des pratiques numériques plus larges, introduisent des obligations et mécanismes qui constituent des leviers utiles dans la lutte contre la manipulation de l'information. Tous trois partagent une approche extraterritoriale : ils s'appliquent aux acteurs qui ciblent ou affectent le marché européen, indépendamment de leur lieu d'établissement. Cette portée étendue est cruciale pour ne pas laisser les acteurs globaux échapper aux régulations européennes.

147. Ainsi d'autres règles se concentrent, en revanche, sur le moyen de produire ou de diffuser ladite information. C'est alors que le droit permet de diriger le tir vers d'autres acteurs : les plateformes, l'hébergeur, le logiciel d'intelligence artificielle ou encore la chaîne de télévision.

148. Dans une logique de *droit mobilisé*, les textes du DSA, IA Act et DMA ou encore les principes de neutralité du net, ou entourant les satellites et opérateurs, s'inscrivent moins dans un encadrement direct du contenu manipulé, que dans une régulation des *vecteurs* de production, de diffusion ou de monétisation de l'information. Ces textes participent d'un basculement : plutôt que de viser directement les contenus problématiques, ils encadrent les vecteurs de production, de diffusion ou de recommandation de ces contenus. C'est alors que le droit permet de diriger le tir vers d'autres acteurs : les plateformes, l'hébergeur, le logiciel d'intelligence artificielle, ou encore la chaîne de télévision. Ces acteurs, sans être nécessairement les auteurs des contenus, deviennent les points d'entrée régulés de leur circulation. Ils permettent de cibler les infrastructures et les interfaces techniques qui rendent possible ou amplifient la manipulation de l'information, en mobilisant des régimes non conçus spécifiquement pour lutter contre la désinformation, mais juridiquement activables à cette fin.

1. Le DSA : prévention des risques systémiques

149. Le *Digital Services Act* (DSA)[67], entré en vigueur le 17 février 2024, constitue aujourd'hui le cadre juridique le plus avancé de l'Union européenne pour encadrer les contenus numériques, et notamment lutter contre la désinformation, les messages trompeurs et les ingérences informationnelles[68]. En affirmant que ce qui est illégal hors ligne l'est également en ligne, le DSA consacre une logique de responsabilisation accrue des plateformes, leur imposant désormais de mettre en œuvre des mécanismes de signalement accessibles, réagir rapidement à la diffusion de contenus illicites (discours haineux, contrefaçons, désinformation) et coopérer avec les autorités publiques ainsi qu'avec des acteurs certifiés comme les *trusted flaggers*[69]. Ces obligations *de diligence raisonnable (Due diligence obligations)* recoupent les obligations générales pour tous les services intermédiaires et les obligations spécifiques pour les services d'hébergement, plateformes en ligne, très grandes plateformes et moteurs de recherche[70] - afin d'atténuer les risques liés à ces acteurs[71]. Le DSA met en place une obligation pour les fournisseurs de services d'hébergement de mettre en place un mécanisme accessible pour notifier des contenus illégaux, avec des notifications suffisamment claires, précises et motivées. Cette action doit être réalisée de manière diligente et non arbitraire, en tenant compte de la gravité et de l'urgence du contenu notifié – et en informant les

[67] « Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance) », 277 OJ L § (2022), http://data.europa.eu/eli/reg/2022/2065/oj/eng.
[68] « REPORT - ÉTATS GÉNÉRAUX DE L'INFORMATION A NINE-MONTH STUDY BY A FRENCH INDEPENDANT ORGANIZATION ON THE RIGHT TO INFORMATION », consulté le 14 avril 2025, https://etats-generaux-information.fr/la-restitution.
[69] Article 22, considérants 61-62 : « Les signalements des trusted flaggers doivent être traités en priorité et sans délai indu, le statut est accordé par le Digital Services Coordinator du pays d'établissement, aux entités ayant une expertise avérée et indépendantes ». Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[70] Articles 11 à 15, considérants 40-42, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[71] Transparence algorithmique et atténuation des risques — Article 35 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

destinataires[72]. Le DSA prohibe ainsi explicitement des pratiques qui altèrent de manière significative la capacité des utilisateurs à faire des choix autonomes et éclairés[73].

150. Il met également sous la coupe de ces obligations les fournisseurs de services intermédiaires, considérant que « *la croissance exponentielle du recours à ces services, principalement à des fins légitimes et socialement bénéfiques de toute nature, a également accru leur rôle dans l'intermédiation et la diffusion d'informations et d'activités illégales ou susceptibles de nuire* »[74]. A cette large application, l'Union rajoute un élément d'extraterritorialité puisque le DSA a vocation à s'appliquer « *aux fournisseurs de services intermédiaires, quel que soit leur lieu d'établissement ou leur situation géographique, dans la mesure où ils proposent des services dans l'Union* », et ce à la condition « *qu'un lien étroit avec l'Union soit avéré* »[75].

151. Les très grandes plateformes en ligne (VLOPs) et très grands moteurs de recherche (VLOSEs), en raison de leur impact systémique[76], sont soumises à des obligations spécifiques, et doivent conduire une évaluation annuelle des risques, incluant la manipulation électorale, les campagnes de désinformation et les atteintes aux droits fondamentaux. Elles sont tenues d'adapter leurs systèmes algorithmiques, notamment leurs systèmes de recommandation, en garantissant la transparence et la possibilité

[72] Mécanisme de notification et d'action (Notice and action mechanism) — Article 16, considérants 50-54, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[73] DSA, considérant 67 et article 25, sur les darks patterns, compris comme « *practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions* ». Voir https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf

[74] « *Cons 5) Le présent règlement devrait s'appliquer aux fournisseurs de certains services de la société de l'information tels qu'ils sont définis dans la directive (UE) 2015/1535 du Parlement européen et du Conseil (5), c'est-à-dire tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire. Plus particulièrement, le présent règlement devrait s'appliquer aux fournisseurs de services intermédiaires, et notamment de services intermédiaires consistant en des services dits de «simple transport», de «mise en cache» et d'«hébergement», dès lors que la croissance exponentielle du recours à ces services, principalement à des fins légitimes et socialement bénéfiques de toute nature, a également accru leur rôle dans l'intermédiation et la diffusion d'informations et d'activités illégales ou susceptibles de nuire* »Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[75] Article 2 "*Le présent règlement s'applique aux services intermédiaires proposés aux destinataires du service dont le lieu d'établissement est situé dans l'Union ou qui sont situés dans l'Union, quel que soit le lieu d'établissement des fournisseurs de ces services intermédiaires*. » et Considérant 7, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[76] Article 33, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

pour les utilisateurs d'opter pour des versions non personnalisées, tout en documentant les ajustements apportés[77]. En effet, le législateur européen a identifié quatre grandes catégories de risques : la diffusion de contenus illicites, tels que la pédopornographie, les discours de haine ou les produits contrefaits, souvent amplifiés par des comptes à large audience ou des mécanismes automatisés de recommandation, les atteintes aux droits fondamentaux, notamment à la liberté d'expression, à la vie privée ou à la non-discrimination, pouvant résulter de conceptions algorithmiques biaisées ou d'utilisations abusives des interfaces, les atteintes aux processus démocratiques, incluant les risques pour l'intégrité électorale, la sécurité publique et la qualité du débat civique, et les atteintes à la santé publique et au bien-être des utilisateurs, comme la désinformation sanitaire, l'exposition des mineurs à des contenus nuisibles ou les mécanismes addictifs favorisant la violence sexiste[78]. Dans ce cadre, les évaluations doivent être menées selon une méthodologie rigoureuse, avec une attention particulière portée aux systèmes algorithmiques impliqués (recommandation de contenus, publicité ciblée, collecte de données personnelles), avec la recommandation de prendre en compte des contenus licites mais trompeurs, comme la désinformation, en analysant leur diffusion potentiellement manipulée via des bots, faux comptes ou comportements automatisés. L'évaluation doit en outre être contextualisée, en tenant compte des différences linguistiques et culturelles entre les États membres de l'Union[79].

152. Le DSA ne crée pas une responsabilité automatique des fournisseurs d'intermédiation, mais leur impose une série d'obligations de diligence (analyse, transparence, modération, coopération). En effet, le DSA définit uniquement les cas où un fournisseur de services intermédiaires ne peut pas être tenu responsable du contenu illicite publié par les utilisateurs, les conditions dans lesquelles sa responsabilité peut être engagée

[77] Article 34 « *Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne recensent, analysent et évaluent de manière diligente tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services* » Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[78] Considérants 80 à 83, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[79] Considérant 84, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

restent du ressort du droit national ou de l'Union[80]. Les exemptions de responsabilité s'appliquent à tout type de contenu illicite, quelle qu'en soit la nature, en revanche, ces exemptions ne s'appliquent pas si le fournisseur joue un rôle actif dans la diffusion du contenu (ex. : connaissance ou contrôle éditorial), ou s'il fournit lui-même les informations. Aussi, les fournisseurs peuvent bénéficier des exemptions de responsabilité pour les services de simple transport ou de mise en cache, à condition de ne pas modifier l'information transmise ou accessible[81]. Les manipulations techniques neutres (ex. : compression, routage) sont autorisées si elles ne modifient pas l'intégrité du contenu, mais l'exemption ne s'applique pas si l'utilisateur agit sous l'autorité ou le contrôle du fournisseur[82]. Dans le même temps, les fournisseurs peuvent agir volontairement pour détecter et supprimer des contenus illicites sans perdre le bénéfice des exemptions de responsabilité, à condition d'agir de bonne foi ; avec diligence, de manière objective, proportionnée et non discriminatoire ; et en garantissant la protection des contenus licites (éviter les suppressions abusives)[83]. Dans le même temps, le DSA n'impose pas aux fournisseurs d'assumer seuls la lutte contre les contenus illicites et les utilisateurs sont responsables des contenus qu'ils publient, conformément au droit applicable. Les fournisseurs de services intermédiaires ne peuvent pas être tenus à une surveillance générale, ni à rechercher activement les contenus illicites – sans exclusion des injonctions ciblées émises par des autorités compétentes dans des cas spécifiques, sous conditions strictes[84]. Des injonctions judiciaires ou administratives peuvent imposer de retirer un contenu illicite ou de fournir des informations précises, à ce titre, le DSA fixe uniquement des conditions minimales de validité (ex. : clarté, proportionnalité,

[80] Considérants 17 et 18, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[81] Pour les services d'hébergement, l'exemption s'applique seulement si le fournisseur agit rapidement après avoir eu connaissance effective d'un contenu illicite (via signalements ou vérifications internes). La réaction doit respecter les droits fondamentaux, comme la liberté d'expression. Une connaissance générale que le service peut contenir du contenu illicite ne suffit pas pour engager la responsabilité. (≠ connaissance spécifique).
[82] Considérants 21 à 23, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[83] L'usage d'outils automatisés est autorisé s'ils sont fiables et permettent de minimiser les erreurs. Les mesures prises pour se conformer au droit de l'UE (ex. : mise en œuvre des CGU) n'empêchent pas de bénéficier de l'exemption de responsabilité. Toutefois, ces activités ne garantissent pas automatiquement l'exemption : elles ne doivent pas servir à contourner les obligations du DSA. Considérant 26, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[84] Article 8 : Absence d'obligation générale de surveillance ou de recherche active des faits « *Les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales.* ».

notification de l'exécution), et ne crée pas de base juridique pour émettre ces injonctions, ni n'harmonise leur portée territoriale ou leur exécution transfrontalière. Le droit national ou de l'Union applicable reste la base pour leur mise en œuvre, sous réserve de compatibilité avec le droit de l'UE (Charte, TUE, TFUE). En cas de nécessité d'action, les injonctions doivent viser le fournisseur techniquement capable d'agir, pour éviter les atteintes injustifiées aux contenus légaux.

153. Les fournisseurs de services intermédiaires sont tenus d'agir sans délai dès réception d'une injonction judiciaire ou administrative visant un contenu illicite spécifique, en informant l'autorité émettrice de la suite donnée (date et action prise), ainsi que l'utilisateur concerné, en précisant les motifs de l'injonction, les voies de recours disponibles et son champ d'application territorial. Pour être valable, l'injonction doit inclure une base juridique claire (UE ou droit national conforme), des motifs précis justifiant le caractère illicite du contenu, l'identification de l'autorité émettrice, une description détaillée du contenu ciblé (URL, etc.)[85]. Les informations sur les recours ouverts aux parties, la désignation de l'autorité destinataire des réponses, un champ d'application limité au strict nécessaire, et être rédigée dans la langue déclarée par le fournisseur ou accompagnée d'une traduction[86].

154. En cas de manquement, la Commission européenne peut imposer des amendes allant jusqu'à 6 % du chiffre d'affaires mondial[87], ou des astreintes journalières[88]. En période électorale, les plateformes doivent anticiper les pics de désinformation et renforcer leur

[85] Art. 9 §1 & §5
[86] Art. 9 §2
[87] La Commission peut infliger des amendes pouvant aller jusqu'à 6 % du chiffre d'affaires mondial annuel de l'exercice précédent aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche qui, de manière délibérée ou par négligence, enfreignent les dispositions du règlement, ne respectent pas une décision ordonnant des mesures provisoires (article 70) ou ne se conforment pas à un engagement contraignant (article 71). La Commission peut également infliger des amendes allant jusqu'à 1 % du chiffre d'affaires mondial annuel aux fournisseurs, ou à d'autres personnes visées, lorsqu'ils fournissent des informations inexactes, incomplètes ou trompeuses, omettent de répondre ou de rectifier ces informations dans les délais, refusent de se soumettre à une inspection (article 69), ou ne respectent pas les mesures adoptées (article 72) ou les conditions d'accès au dossier (article 79, paragraphe 4) - de manière délibérée ou par négligence
[88] La Commission peut imposer des astreintes quotidiennes allant jusqu'à 5 % des revenus ou du chiffre d'affaires mondial journaliers moyens de l'exercice précédent, à partir d'une date fixée dans sa décision, visant à contraindre le fournisseur à fournir des informations exactes et complètes en réponse à une demande (article 67), à se soumettre à une inspection ordonnée (article 69), à respecter une décision de mesures provisoires (article 70), à honorer des engagements juridiquement contraignants (article 71) ou à se conformer à une décision prise en application de l'article 73, y compris les exigences relatives au plan d'action de l'article 75.

vigilance, en lien avec les obligations émergentes du futur IA Act. Si le DSA exclut toute obligation générale de surveillance, il permet cependant une action ciblée via des injonctions encadrées, en assurant la traçabilité et le respect des droits fondamentaux. À court terme, ce règlement offre ainsi un socle concret pour agir contre les manipulations informationnelles, en mobilisant un droit général mais structuré, capable de diriger la régulation non pas vers le contenu, mais vers ses vecteurs[89].

155. En matière de *soft law* et dans le cadre du DSA, la Commission européenne a publié des lignes directrices à destination des très grandes plateformes afin de prévenir les risques électoraux, notamment avant les élections européennes de 2024[90]. Ces recommandations visent à adapter les algorithmes, encadrer l'IA générative, renforcer la transparence de la publicité politique, promouvoir des contenus fiables et coopérer avec les autorités. Les plateformes doivent soit appliquer ces mesures, soit prouver l'efficacité équivalente de leurs alternatives, sous peine de procédures formelles. Dans ce texte on retrouve d'ailleurs la mention d'un encouragement à respecter les bonnes pratiques proposées pour réduire la propagation de la désinformation[91]. Ces lignes directrices anticipaient l'entrée en vigueur du règlement (UE) 2024/900 sur la transparence et le ciblage de la publicité politique[92] et du règlement sur l'intelligence artificielle (ci-après IA Act). Elles intègrent également les engagements volontaires pris dans le cadre du Pacte sur l'IA[93], par lesquels certains fournisseurs de très grandes plateformes en ligne (VLOPs) et de très grands moteurs de recherche (VLOSEs) s'engagent à respecter dès lors les

[89] A ce jour, des sanctions en la matière ne sont pas encore tombées mais la Commission européenne a saisi la Cour de justice de l'Union européenne contre la Tchéquie, l'Espagne, Chypre, la Pologne et le Portugal pour non-respect de leurs obligations en vertu du DSA. Voir https://ec.europa.eu/commission/presscorner/detail/fr/ip_25_1081

[90] « Communication from the Commission – Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065 » (2024), http://data.europa.eu/eli/C/2024/3014/oj/eng.

[91] « *Dans la mesure où cela est pertinent pour la conformité des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne avec le règlement (UE) 2022/2065, les lignes directrices tiennent également compte de plusieurs engagements et mesures visant à réduire la propagation de la désinformation en ligne qui figurent dans le code de bonnes pratiques contre la désinformation (9), le premier cadre mondial établi à l'initiative des entreprises du secteur du numérique, qui constitue une source de bonnes pratiques pour lutter contre la désinformation. Les lignes directrices tiennent également compte des travaux réalisés par les institutions de l'UE et les États membres en ce qui concerne les manipulations de l'information et ingérences étrangères, et notamment du cadre global fourni par la boîte à outils de l'UE relative aux manipulations de l'information et ingérences étrangères, ainsi que du récent rapport du Service européen pour l'action extérieure (SEAE) consacré aux menaces en la matière (10) et axé sur la réaction à ces opérations dans le contexte des élections* ».

[92] Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique (Texte présentant de l'intérêt pour l'EEE).

[93] Disponible sur : https://digital-strategy.ec.europa.eu/fr/policies/ai-pact.

obligations à venir, avant la fin de la période de transition - bien qu'il soit lui aussi non contraignant.

2. L'IA Act : prévenir les dérives des systèmes génératifs et prédictifs

156. Le règlement européen sur l'intelligence artificielle (IA Act)[94], adopté en 2024, constitue le premier cadre juridique mondial classant les systèmes d'IA selon un niveau de risque (inacceptable, élevé, limité, minimal), et impose des obligations spécifiques aux fournisseurs de modèles génératifs. Pensé à l'origine pour encadrer les usages à fort impact (santé, justice, sécurité), l'IA Act s'avère aussi être un outil juridique mobilisable contre les dérives informationnelles, en particulier face à la prolifération de contenus synthétiques (*deepfakes*, textes générés, faux comptes automatisés). L'article 50 impose aux fournisseurs de signaler et marquer clairement tout contenu généré par IA, notamment en cas de risque de tromperie du public, renforçant ainsi la traçabilité et la transparence[95]. Cette obligation de divulgation porte notamment sur les *deepfakes* et contenus synthétiques puisque toute image, audio ou vidéo manipulée qui pourrait induire en erreur le public doit être clairement signalée[96] - permettant de combattre l'amplification involontaire de contenus biaisés ou issus de sources manipulatoires. Les

[94] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*) (Text with EEA Relevance) » (2024). Disponible sur : http://data.europa.eu/eli/reg/2024/1689/oj/eng.

[95] Article 50 « *2. Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. Cette obligation ne s'applique pas dans la mesure où les systèmes d'IA remplissent une fonction d'assistance pour la mise en forme standard ou ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière.* » Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

[96] Article 50, 4. : « *Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage indiquent que les contenus ont été générés ou manipulés par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre* ».

exigences de transparence des modèles d'IA peuvent être mobilisés pour limiter la diffusion de désinformation et garantir la traçabilité des contenus manipulés.

157. Innovation issue de l'IA Act, les systèmes d'IA sont classifiés, et encadrés, selon le niveau de risque qu'ils comportent. Les systèmes d'intelligence artificielle sont considérés comme « à haut risque » lorsqu'ils sont intégrés à des produits soumis à une évaluation de conformité obligatoire (comme ceux relevant des réglementations européennes listées à l'annexe I) ou lorsqu'ils remplissent certaines fonctions critiques mentionnées à l'annexe III du règlement[97]. Cette qualification implique qu'ils peuvent avoir un impact significatif sur la santé, la sécurité ou les droits fondamentaux des personnes. Toutefois, un système de l'annexe III peut être exclu de cette classification s'il ne présente pas de risques importants, par exemple s'il assiste simplement une tâche humaine ou prépare une évaluation sans influence directe sur la décision finale[98]. En revanche, tout système d'IA qui réalise un profilage de personnes reste systématiquement classé à haut risque. Les systèmes utilisés pour influencer les comportements électoraux sont classés comme IA à haut risque, conformément au considérant 62, ce qui entraîne des obligations renforcées : audits, supervision humaine, documentation des risques, résilience aux pannes et aux attaques adversariales. L'IA Act met également l'accent sur la lutte contre les biais algorithmiques et la dégradation auto-alimentée des modèles, qui, nourris par des données manipulées ou de faible qualité, pourraient amplifier involontairement des narratifs de désinformation.

158. Dans son article 5, le règlement interdit la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA reposant sur des techniques subliminales ou manipulatrices altérant la capacité de décision des individus, notamment par l'exploitation de vulnérabilités liées à l'âge, au handicap ou à la situation sociale[99]. Il proscrit également les systèmes d'évaluation sociale, le profilage criminel fondé uniquement sur des caractéristiques personnelles, la création de bases de données de reconnaissance faciale

[97] Article 6, 1. a), b), 2).
[98] Article 6, 3).
[99] Cette interdiction pourrait recouvrir l'usage de techniques subliminales ou délibérément manipulatrices, ce qui recoupe avec certaines formes de *dark patterns* dans les systèmes d'IA.

par moissonnage d'images en ligne, l'inférence émotionnelle sur le lieu de travail ou à l'école (hors finalité médicale ou sécuritaire), et la catégorisation biométrique basée sur des données sensibles (ex. orientation sexuelle, opinions politiques). S'agissant des systèmes d'identification biométrique à distance en temps réel dans l'espace public à des fins répressives, leur usage est strictement encadré, limité à des cas précis (lutte contre le terrorisme, recherche de personnes disparues, enquêtes pénales graves) et soumis à autorisation judiciaire préalable, à des garanties de proportionnalité, et à un suivi strict par les autorités nationales et européennes.

159. L'IA Act peut également être mobilisé pour lutter contre les biais et opacité des modèles puisque le règlement reconnaît le risque lié aux jeux de données biaisés et au manque de transparence des modèles d'IA, qui peuvent alimenter des narratifs de désinformation. Il encourage ainsi des pratiques de labellisation et d'audit des modèles pour garantir une information fiable. De même pour la prévention des risques liés à l'auto-dégradation des modèles – bien que le cadre européen favorise des approches d'évaluation continue pour limiter cette dégradation et éviter une amplification involontaire de la désinformation. De fait, l'article 15 du règlement impose que les systèmes d'IA à haut risque soient conçus de manière à garantir un niveau adéquat d'exactitude, de robustesse et de cybersécurité tout au long de leur cycle de vie. Cela inclut la capacité à résister aux erreurs internes, aux défaillances, aux interactions humaines imprévues, ainsi qu'aux tentatives d'attaques malveillantes. Ces systèmes doivent être accompagnés de mesures techniques telles que des sauvegardes ou des plans de sécurité après défaillance, et éviter les effets de boucles de rétroaction biaisées dans le cas d'un apprentissage continu. Des mesures spécifiques doivent aussi être mises en place pour contrer les menaces liées à la cybersécurité, notamment les manipulations de données d'entraînement, les attaques par inférence, ou les tentatives de compromission des performances du modèle. Les niveaux d'exactitude et les indicateurs associés doivent être précisés dans la documentation technique du système.

160. Le régime de sanctions prévu par l'IA Act repose sur des amendes administratives qui doivent être effectives, proportionnées et dissuasives. Le non-respect des pratiques

interdites (article 5) peut entraîner une amende allant jusqu'à 35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial de l'entreprise, le montant le plus élevé étant retenu. Pour d'autres manquements aux obligations du règlement (transparence, obligations des fournisseurs, déployeurs, etc.), les amendes peuvent atteindre 15 millions d'euros ou 3 % du chiffre d'affaires. En cas de fourniture d'informations inexactes ou incomplètes, une amende de 7,5 millions d'euros ou 1 % du chiffre d'affaires peut être appliquée. Les PME bénéficient de plafonds allégés. Les institutions de l'UE peuvent également être sanctionnées jusqu'à 1,5 million d'euros. Par ailleurs, les fournisseurs de modèles d'IA à usage général risquent jusqu'à 3 % de leur chiffre d'affaires mondial ou 15 millions d'euros s'ils enfreignent leurs obligations spécifiques.

161. Du point de vue de la *soft law*, l'on peut noter le *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*[100]*, qui* repose sur des engagements volontaires entre entreprises pour lutter contre les usages trompeurs de l'IA durant les élections, mais il reste non contraignant car dépourvu de mécanisme de sanction[101]. Il marque néanmoins une avancée en faveur d'une réponse coordonnée au risque informationnel, en misant sur la coopération, la détection technologique et la sensibilisation du public.

3. Le DMA : contre la concentration des moyens de diffusion

162. Le *Digital Markets Act* (DMA)[102], bien qu'il ne vise pas spécifiquement la lutte contre la désinformation, constitue un levier juridique mobilisable pour en limiter les vecteurs structurels. En s'attaquant aux pratiques anticoncurrentielles des grandes plateformes numériques, le DMA impose une régulation ex ante qui limite leur pouvoir de modeler l'accès à l'information. L'interdiction de l'auto-préférence et l'obligation d'interopérabilité ou de libre promotion réduisent la capacité des géants du Net à favoriser leurs propres services ou contenus, y compris ceux susceptibles d'orienter indûment l'opinion

[100] Munich Security Conference, « Tech Accord to Combat Deceptive Use of AI in 2024 Elections » (2025), https://securityconference.org/en/aielectionsaccord/.
[101] Munich Security Conference, « Tech Accord to Combat Deceptive Use of AI in 2024 Elections » (2025), https://securityconference.org/en/aielectionsaccord/.
[102] « Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance) » (2022), http://data.europa.eu/eli/reg/2022/1925/2022-10-12/eng.

publique[103]. De même, les obligations de transparence concernant les données publicitaires, les algorithmes de recommandation[104] ou les fusions-acquisitions[105] participent à lever l'opacité qui entoure les mécanismes d'amplification algorithmique. Le DMA intègre également une clause anti-contournement qui permet de cibler les pratiques abusives des grandes plateformes, notamment celles qui visent à orienter le comportement des utilisateurs via des interfaces trompeuses[106] - qui pourrait être mobilisée dans la lutte contre les *dark patterns* dans une certaine mesure.

163. Malgré les difficultés que posent la mise en œuvre du DMA, des mécanismes de sanction peuvent être mobilisés. Lorsqu'un *gatekeeper* ne respecte pas ses obligations (articles 5, 6, 7, ou des mesures spécifiques décidées par la Commission), celle-ci peut adopter une décision de non-conformité, enjoignant l'entreprise de remédier à ses manquements dans un délai donné[107]. Cette décision peut s'accompagner d'amendes pouvant atteindre 10 % du chiffre d'affaires mondial, voire 20 % en cas de récidive dans les huit années précédentes. D'autres violations, comme la fourniture d'informations inexactes ou le refus de coopération, peuvent entraîner des sanctions allant jusqu'à 1 % du chiffre d'affaires mondial[108]. En complément, des astreintes journalières pouvant aller jusqu'à 5 % du chiffre d'affaires quotidien mondial peuvent être imposées pour contraindre les *gatekeepers* à exécuter les décisions de la Commission. Ces mesures, bien que complexes à mettre en œuvre, témoignent d'une volonté claire d'assurer le respect strict du DMA, en dissuadant les comportements anticoncurrentiels des grandes plateformes[109].

164. En encadrant les conditions d'accès au marché numérique et en empêchant les abus de position dominante, le DMA agit ainsi indirectement sur les dynamiques de diffusion de contenus, et contribue à rééquilibrer le paysage informationnel – en complémentarité avec le DSA, plus directement centré sur les risques systémiques liés aux manipulations de l'information. Il faut toutefois prendre en compte que le DMA ne s'applique pas aux

[103] Article 5 et 7 (interopérabilité).
[104] Article 5.
[105] Article 14.
[106] Article 13.
[107] Article 29.
[108] Article 30.
[109] Article 31.

marchés liés aux réseaux de communications électroniques tels que définis au point 1 de l'article 1 de la directive (UE) 2018/1972 du 11 décembre 2018 établissant le Code européen des communications électroniques[110].

4. Réseaux, neutralité et rôle des opérateurs dans la circulation de l'information

165. Les opérateurs de communication électronique, qu'il s'agisse de fournisseurs d'accès à Internet ou d'acteurs satellitaires, occupent une position clé dans l'architecture informationnelle contemporaine. Leur rôle, en tant qu'infrastructures essentielles au transport de données, est encadré par des régimes juridiques européens visant à préserver un équilibre entre liberté d'accès et capacité de contrôle. Le règlement (UE) 2015/2120 consacre notamment le principe de neutralité du net : les fournisseurs doivent acheminer le trafic Internet sans discrimination ni blocage arbitraire, indépendamment du contenu, de l'émetteur ou de l'usage[111]. Ils ne peuvent intervenir que dans des cas limités, tels qu'une injonction légale, une menace pour la sécurité du réseau ou une congestion exceptionnelle[112]. En parallèle, ils doivent informer les utilisateurs des éventuels impacts sur la qualité de service et garantir des voies de recours en cas de non-conformité. Cette neutralité garantit une circulation libre de l'information, condition essentielle au pluralisme, mais limite aussi la capacité d'action proactive des opérateurs contre la désinformation.

166. Le *Digital Services Act* (DSA) complète cette logique en qualifiant les opérateurs de « services intermédiaires », au sens des articles 4 à 8 du règlement. À ce titre, ils bénéficient d'exemptions de responsabilité pour les contenus qu'ils transmettent, dès lors qu'ils n'interviennent pas activement dans leur sélection ou leur diffusion. Toutefois, cette neutralité n'est pas absolue : les opérateurs peuvent être contraints, par voie judiciaire ou administrative (article 9 DSA), à bloquer certains contenus ou à coopérer

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

[111] « Règlement (UE) 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) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (Texte présentant de l'intérêt pour l'EEE) », 310 OJ L § (2015), http://data.europa.eu/eli/reg/2015/2120/oj/fra.

[112] Article 3.

avec les autorités compétentes. Ces mécanismes préservent la liberté d'accès tout en permettant, dans des conditions encadrées, une réponse ciblée aux dérives informationnelles.

167. Ce cadre juridique s'étend également aux opérateurs satellitaires, qui assurent une part croissante du transport des contenus audiovisuels et Internet, souvent à l'échelle transnationale. Grâce au mécanisme de « l'effet satellite », prévu à l'article 2 (§4 à §6) de la directive SMA (2010/13/UE)[113], un État membre peut être considéré comme compétent pour réguler un signal émis via un satellite relevant de sa juridiction, même si l'émetteur est établi en dehors de l'UE[114]. Cette extension de compétence permet à l'Union européenne d'appliquer ses règles aux services audiovisuels accessibles sur son territoire, qu'ils soient émis depuis un *uplink* situé dans l'UE ou via une capacité satellitaire européenne. Cette extraterritorialité constitue un levier intéressant pour réguler des flux potentiellement manipulateurs diffusés depuis l'étranger, notamment en période électorale ou en situation de crise.

168. En somme, même si les opérateurs ne sont pas éditeurs de contenus, leur rôle structurel dans la circulation de l'information fait d'eux des points d'appui possibles pour les politiques de lutte contre les manipulations. Ce rôle dans la circulation de l'information est lié notamment aux câbles sous-marins, aux satellites ou encore aux centres de données. Ces infrastructures physiques, souvent transfrontalières, soulèvent également des enjeux d'extraterritorialité : la localisation des serveurs, des points d'interconnexion

[113] « Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive Services de médias audiovisuels) (Version codifiée) (Texte présentant de l'intérêt pour l'EEE) », 095 OJ L § (2010), http://data.europa.eu/eli/dir/2010/13/oj/fra.

[114] Le mécanisme dit « effet satellite » permet à l'UE de revendiquer compétence sur des services de diffusion qui, même émis depuis l'extérieur de l'UE, utilisent un satellite relevant d'un État membre, ou un faisceau dirigé vers l'UE. « *4. Les fournisseurs de services de médias auxquels ne s'applique pas le paragraphe 3 sont réputés relever de la compétence d'un État membre dans les cas suivants : a) s'ils utilisent une liaison montante vers un satellite située dans cet État membre ; b) si, bien que n'utilisant pas une liaison montante vers un satellite située dans cet État membre, ils utilisent une capacité satellitaire relevant de cet État membre. » ("Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels ; 5. Si l'État membre compétent ne peut être déterminé conformément aux paragraphes 3 et 4, l'État membre compétent est celui dans lequel le fournisseur de services de médias est établi au sens des articles 49 à 55 du traité sur le fonctionne ment de l'Union européenne. 6. La présente directive ne s'applique pas aux services de médias audiovisuels exclusivement destinés à être captés dans des pays tiers et qui ne sont pas reçus directement ou indirectement au moyen d'équipements standard par le public d'un ou de plusieurs États membres.* ». *in :* Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive Services de médias audiovisuels) (Version codifiée) (Texte présentant de l'intérêt pour l'EEE).

ou des liaisons montantes satellitaires peut justifier la compétence d'un État membre ou de l'Union pour encadrer des flux informationnels étrangers, notamment ceux véhiculant des contenus manipulés. Ainsi, la régulation européenne veille à ne pas transformer ces acteurs en censeurs, mais elle prévoit des marges d'action ciblées, fondées sur l'injonction, la coopération et la transparence. Dans un contexte de désinformation croissante et de conflits hybrides, ces dispositifs permettent de concilier l'exigence d'un Internet ouvert avec la nécessité d'interventions ciblées, dans le respect de la liberté d'expression – et l'inclusion des opérateurs de réseau, notamment satellitaire, permet à l'Union de revendiquer une compétence extraterritoriale sur les flux informationnels, notamment pour encadrer la diffusion de chaînes étrangères ou de contenus manipulés transmis par satellite. Toutefois, cette même neutralité du net peut constituer un outil à double tranchant, limitant la possibilité de contrôler les contenus puisqu'elle interdit intervention arbitraire sur les flux d'information, mais limite aussi les moyens techniques de bloquer certains contenus, sauf injonctions ciblées ou cas exceptionnels.

5. Le RGPD : protection des données personnelles et lutte contre la désinformation.

169. Bien que le Règlement général sur la protection des données (RGPD)[115] n'ait pas été conçu spécifiquement pour répondre aux défis posés par la manipulation de l'information, plusieurs de ses dispositions peuvent être activées à cette fin, dans une logique de mobilisation du droit existant. Le RGPD impose tout d'abord que tout traitement de données personnelles, notamment dans le cadre de campagnes de désinformation ciblée ou de microciblage politique, repose sur une base juridique valable, le plus souvent un consentement explicite[116], libre et éclairé, dont le retrait doit être possible à tout moment. Ce principe est renforcé par l'interdiction stricte du traitement de données sensibles, telles que les opinions politiques ou les croyances religieuses, sauf consentement explicite ou motif d'intérêt public[117]. Le règlement protège également les

[115] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (s. d.).
[116] RGPD, articles 6 et 7, considérant 32.
[117] RGPD, article 9.

individus contre les risques liés au profilage et à la prise de décision automatisée[118], en imposant une intervention humaine et des garanties renforcées lorsque ces traitements ont un impact significatif sur les personnes, ce qui peut couvrir des pratiques algorithmiques visant à influencer l'opinion ou les comportements électoraux. Les responsables du traitement doivent également démontrer leur conformité, intégrer la protection des données dès la conception et par défaut, et encadrer précisément les responsabilités en cas de traitement conjoint[119] — ce qui est particulièrement pertinent pour les services d'IA ou les plateformes diffusant du contenu. Cette logique est pleinement cohérente avec l'IA Act, qui affirme que le droit à la vie privée et à la protection des données doit être garanti tout au long du cycle de vie des systèmes d'IA[120]. Dans la même logique, le RGPD interdit en principe les décisions fondées uniquement sur un traitement automatisé, y compris le profilage, ayant des effets juridiques ou significatifs pour la personne concernée[121].

170. En outre, le RGPD prévoit une application extraterritoriale[122], permettant à l'UE de soumettre des acteurs non européens à ses règles dès lors qu'ils ciblent des personnes situées dans l'Union, ce qui peut constituer un levier pour contrer des opérations informationnelles conduites depuis l'étranger. Les obligations de transparence, d'information[123] et de limitation du traitement[124] permettent aussi d'exiger des plateformes et intermédiaires qu'ils informent les utilisateurs de la manière dont leurs données sont utilisées, en particulier à des fins de profilage politique ou de diffusion de contenus manipulés. Enfin, un utilisateur dispose d'un droit d'opposition à tout moment,

[118] RGPD, article 22, et considérants 71 à 73.
[119] RGPD, articles 24 à 26.
[120] Voir notamment le considérant 69 de l'IA Act.
[121] RGPD, article 22, considérants 71 à 73 qui précisent que ces règles visent directement les risques liés à l'usage d'algorithmes dans les pratiques de désinformation ou de microciblage politique, en imposant une intervention humaine, une explication claire et un droit de contestation.
[122] RGPD, Article 3, Champ d'application territorial : « *1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. 4.5.2016 L 119/32 Journal officiel de l'Union européenne ; 2.Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées: a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. 3.Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.* »
[123] RGPD, articles 12 à 14.
[124] RGPD, article 5.

notamment au traitement à des fins de prospection (par exemple, le ciblage politique sur les réseaux sociaux)[125]. Dans les contextes sensibles (élections, sécurité publique, conflits hybrides), les États membres peuvent restreindre certains de ces droits pour prévenir des atteintes graves à la démocratie[126], ce qui pourrait être mobilisé pour lutter contre les manipulations de l'information dans ces contextes. Enfin, en cas de violation de ces règles, le RGPD prévoit des sanctions dissuasives allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial (article 83), renforçant ainsi son efficacité comme outil indirect mais puissant dans la lutte contre les dérives informationnelles.

171. Il convient toutefois de relever les inquiétudes quant à l'articulation de l'article 25 du DSA avec les autres instruments juridiques européens. Bien que cet article interdise l'usage de *dark patterns* par les plateformes en ligne, il exclut de son champ les pratiques déjà encadrées par la directive sur les pratiques commerciales déloyales (UCPD[127]) et le Règlement général sur la protection des données (RGPD). Le RGPD ne traite pas explicitement des *dark patterns*, mais certaines techniques utilisées pour obtenir le consentement des utilisateurs pourraient être qualifiées comme telles, laissant place à des interprétations divergentes qui risquent de limiter la portée réelle du DSA. Ainsi, lorsqu'un *dark pattern* enfreint le RGPD, c'est ce dernier qui s'applique, et non le DSA, une superposition dans les outils du droit de l'Union qui engendre une certaine incertitude juridique.

[125] RGPD, article 21.
[126] RGPD, article 23.
[127] *V.* la DIRECTIVE (UE) 2019/2161 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs.

LES OPÉRATIONS JURIDIQUES DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION

A. Introduction

1) A propos de cette partie

171. Cette partie traite des motivations, de la philosophie, de l'utilisation et des intentions du modèle NORMA appliqué de lutte contre la désinformation. Il fait partie du rapport traitant de la manière dont les principes et les pratiques de juridique peuvent être utilisés pour améliorer notre compréhension de la sécurité cognitive et améliorer les réponses aux opérations d'information, et plus particulièrement aux campagnes et incidents de désinformation.

2) Structure de la présente section

172. La présente section s'articule autour de sections sur la conception et l'utilisation d'e NORMA LMI blue, et peut être résumé comme suit :

- Cette section d'introduction : histoire de la création de NORMA LMI blue ;
- Conception et philosophie de NORMA LMI blue : pourquoi et comment nous avons construit les cadres, et les choix de conception que nous avons faits ;
- Conceptions des composants de NORMA LMI blue ;
- Utilisation de NORMA LMI Blue : outils, technique et utilisations suggérées ;
- Travaux futurs : notes et idées pour améliorer ce travail.

Ce document accompagne la description des instruments juridiques dans la lutte contre les manipulations de l'information et la copie principale des modèles NORMA LMI Blue, contenus dans le dépôt github : https://github.com/NormaProject/LMI-Framework/.

Ce rapport est un document évolutif. Il s'agit de la version **1.0**.

3) Lutte contre les manipulations de l'information

173. Les acteurs étatiques, et les opérateurs d'influence privés exploitent l'ouverture et la portée de l'internet pour manipuler les populations à distance. Il s'agit d'une extension de la lutte pour les « cœurs et les esprits » menée depuis des décennies par le biais de la propagande, des opérations d'influence et de la guerre de l'information. Ces manipulations de l'information, qu'elles soient d'origine étrangère ou non, constituent aujourd'hui une menace hybride majeure pour les démocraties modernes. Face à la sophistication croissante de ces opérations, il est devenu nécessaire de développer des outils d'analyse et de réponse adaptés.

174. La structure et les modes de propagation des attaques de désinformation présentent de nombreuses similitudes avec celles observées dans le domaine de la sécurité de l'information et du piratage informatique.

175. Ces similitudes sont documentées dans le *framework* DISARM (*Disinformation Analysis and Risk Management*) offrant un panorama détaillé des comportements rencontrés. Conçu pour cartographier et contrer les campagnes de désinformation, il constitue un modèle d'analyse interdisciplinaire inspiré des pratiques en cybersécurité.

176. Le cadre DISARM s'inspire directement du *framework* MITRE ATT&CK®, reconnu pour sa classification structurée des tactiques, techniques et procédures (TTP) des cyber-adversaires. Transposé au domaine informationnel, DISARM repose sur une approche systémique des *Foreign Information Manipulation and Interference* (FIMI), intégrant les dimensions comportementales et opérationnelles des acteurs malveillants.

177. Le *DISARM Red Framework* cartographie ainsi les comportements offensifs selon une grille comportementale et tactique issue des travaux de la communauté professionnelle de la lutte contre la désinformation. Il mobilise les concepts de *kill chain*, de *TTP* et d'empreinte comportementale dans un effort de normalisation de la menace. Un exemple d'application concrète de ce modèle est fourni dans l'étude *Cyber Influence Defense: Applying the DISARM Framework to a Cognitive Hacking Case from the Romanian Digital Space*, qui illustre la pertinence de ce cadre pour modéliser des cas réels de désinformation.

178. Le cadre DISARM se distingue également par son ambition de normalisation internationale. Une traduction française est disponible en open source sur GitHub, réalisée par VIGINUM, le service opérationnel de l'État français chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Créé le 13 juillet 2021, VIGINUM promeut une lecture systémique et interopérable des menaces informationnelles, essentielle au développement de réponses coordonnées.

179. Si DISARM Red se concentre sur l'analyse offensive, le DISARM Blue Framework structure la réponse défensive. Il propose une taxonomie des tactiques et techniques utilisables par les « *blue teams* » – les équipes de défense contre la désinformation – tout au long du cycle de réponse à une campagne FIMI.

180. Dans une démarche équivalente et sur le même socle théorique, le *framework* NORMA blue, développé par l'association éponyme et les travaux académiques d'Alexandre Clabault, vise à cartographier les comportements d'instrumentalisation du droit.

181. Ces types de guerres atypiques[128] ont amené de nombreuses armées et gouvernements a développé une réflexion autour des usages stratégiques du droit. Le bureau juridique du SHAPE a ainsi développé une cartographie des opérations juridiques menées par des

[128] Daniel Mainguy, *Droit de la guerre atypique: réflexions sur les conflits non armés et non militaires (lawfare, guerre économique et informationnelle)* (Paris-La-Défense: LGDJ, 2023), https://univ-droit.fr/recherche/actualites-de-la-recherche/parutions/50943-droit-de-la-guerre-atypique.

acteurs identifiés pour permettre l'identification de menace et l'organisation de riposte : politique, médiatique et/ou juridique[129].

182. En analysant et en exploitant les similitudes avec les cadres de sécurité de l'information, les défenseurs disposent de meilleurs moyens pour décrire, identifier et contrer les attaques basées sur les manipulations de l'information (LMI).

183. Parmi les contres mesures identifiées par le Framework DISARM, quelques-unes traitaient de moyens juridiques. Nous avons choisi d'étendre les réflexions sur ce sujet en développant NORMA LMI Blue.

184. Ces cadres sont au cœur de notre réflexion sur l'intégration de réponses juridiques opérationnelles face aux manipulations de l'information. L'approche défensive des DISARM Blue et NORMA Blue permet d'articuler les capacités juridiques avec les tactiques de réponse technique et stratégique, dans une logique analogue à celle de la cybersécurité.

4) NORMA et NORMA LMI Blue

185. NORMA est un ensemble de normes de données et une base de connaissances à source ouverte recensant les tactiques, techniques et procédures composant les opérations juridiques de l'équipe rouge et de l'équipe bleue. Il s'adresse aux professionnels du droit.

186. Son objectif est de leur donner la capacité de répondre tactiquement au *lawfare*, de planifier des défenses et des contre-mesures, et de transférer les principes de sécurité de l'information aux opérations juridiques.

187. Il fournit une taxonomie commune pour les opérations juridiques, un cadre pour partager rapidement les renseignements sur les menaces et un outil conceptuel pour

[129] Perrin, « La conduite des opérations juridiques au sein de l'Otan ».

renforcer les défenses par le biais d'une équipe rouge, d'une analyse des risques, de rediffusions et de simulations.

188. NORMA se compose de modèles d'équipe bleue (défense) et d'équipe rouge (attaque), ainsi que d'un référentiel de descriptions, d'atténuations et d'exemples. NORMA LMI Blue détaille les opérations juridiques envisageables dans le cadre de la lutte contre les manipulation de l'information.

189. Pour créer NORMA LMI Blue, nous avons placé les composants des opérations juridiques de lutte contre les manipulations de l'information dans un cadre basé sur les *frameworks* de référence (notamment DISARM, ATT&CK et STIX - *Structured Threat Information Expression*) couramment utilisées pour décrire les incidents liés à la sécurité de l'information.

190. Le *framework* NORMA LMI blue est conçu pour s'adapter aux mêmes ensembles d'outils et aux mêmes cas d'utilisation que DISARM et ATT&CK.

B. Conception et philosophie de l'ensemble d'outils NORMA

191. L'ensemble d'outils NORMA est né de la nécessité de disposer d'un langage commun pour les opérations juridiques.

192. Au moment de sa création, notre communauté comprenait des universitaires, des professionnels de droit et de l'intelligence économique, des designers, des représentants d'associations professionnelles et des personnes d'autres disciplines qui avaient tous des mots différents pour désigner les concepts et les objets des opérations juridiques.

193. Les outils NORMA devraient idéalement permettre à des personnes issues de différents domaines de parler d'opérations juridiques sans confusion.

194. Cette section explique pourquoi et comment nous avons construit le Framework NORMA LMI Blue, comment ses modèles sont reliés les uns aux autres et les choix de conception que nous avons faits lors de leur création.

1) Les manipulations de l'information en tant qu'écosystème

195. Dans un monde interconnecté où l'information circule en temps réel, la manipulation de celle-ci ne saurait être perçue comme une simple série d'actes isolés, mais doit être comprise dans une logique systémique. Elle s'inscrit dans un écosystème structuré, animé par des acteurs variés, des objectifs hétérogènes, et des technologies évolutives. Ce paradigme invite à dépasser une approche binaire ou moraliste de la désinformation pour appréhender la complexité des dynamiques sous-jacentes.

196. Un écosystème informationnel se compose d'un ensemble d'acteurs (étatiques, privés, hybrides), de vecteurs (médias traditionnels, plateformes numériques, réseaux sociaux, bots, etc.), de contenus (rumeurs, *fake news*, narratifs biaisés, *deepfakes*), et de publics cibles. Ces composantes interagissent au sein d'un environnement technique, juridique, économique et culturel donné. Le terme d'« écosystème » souligne la dimension organique, interdépendante et adaptative de ce phénomène, où chaque élément peut influencer la stabilité ou l'expansion des opérations manipulatoires.

197. Ainsi, le succès d'une manipulation dépend de sa capacité à mobiliser les ressorts cognitifs du public (biais de confirmation, effet de halo, heuristiques émotionnelles), mais aussi à exploiter les structures de diffusion des plateformes numériques. Les algorithmes de recommandation, les mécanismes de viralité et les logiques d'amplification favorisent des boucles de rétroaction positive qui renforcent la visibilité des contenus polarisants. Ce faisant, l'écosystème renforce des récits dominants ou contestataires sans que leur véracité ne soit interrogée.

2) Mettre en relation les acteurs de la défense

198. Lorsque nous avons commencé, nous savions que notre meilleure chance de créer de bonnes défenses contre la désinformation impliquait de mettre en relation des personnes issues de mondes très différents :

- Les spécialistes des opérations d'information, expert en intelligence économique ou en opérations psychologiques, analysant les rapports de force et l'instrumentalisation des flux informationnels ;
- Les scientifiques des données, qui analysaient des ensembles d'objets et des flux d'informations sur internet en utilisant des techniques telles que l'apprentissage automatique et l'analyse des réseaux sociaux pour démêler les modèles de comptes, de textes, de hashtags, d'urls, de groupes, et les relations entre eux tous ;
- Les spécialistes des sciences sociales et les psychologues qui ont étudié les vulnérabilités cognitives humaines, la dynamique de groupe, ainsi que le flux et l'effet des récits sur les croyances et les émotions ;
- Les experts en sécurité de l'information (infosec), qui avaient déjà construit des outils, des techniques et des processus pour protéger les informations détenues dans des topologies très similaires, qui au lieu d'être des communautés de personnes étaient des réseaux de machines ;
- Les professionnels du droit qui, de par leur pratiques du droit des affaires, du contentieux ou/des arcanes de la procédure, disposent d'une connaissance fine des instruments mobilisables un fois le fait juridique qualifié.

3) Modèles de manipulation de l'information basés sur les composants

199. Il est utile de considérer une opération juridique ou une manipulation de l'information comme un ensemble d'objets et de relations entre eux.

200. De nombreux chercheurs en désinformation organisent déjà leurs informations de cette manière (tout comme les recherches inspirées de l'OSINT, du renseignement et du journalisme sur lesquelles repose une grande partie de ce travail), certains de nos premiers collaborateurs allant même jusqu'à construire des « murs du meurtre » pour suivre les groupes et les incidents.

201. Ces modèles sont formalisés en tant que modèles de systèmes sociotechniques, c'est-à-dire des modèles de réseaux complexes de communautés, de comptes et de technologies en interaction qui constituent une opération juridique, un incident ou une campagne de manipulation de l'information.

202. Les communautés de l'infosec et de lutte contre les manipulation disposent déjà d'une norme de données à cet effet, STIX : https://oasis-open.github.io/cti-documentation/, qui s'accompagne également d'une norme, TAXII, sur la manière de partager les données STIX entre les systèmes.

203. Le projet NORMA développe une version de STIX pour les opérations juridiques, en adaptant ses types d'objets existants à la manipulation de l'information.

204. Il existe d'autres modèles de désinformation basés sur les composants, notamment le modèle ABC « *Actor, Behaviour, Content* » (Acteur, Comportement, Contenu) de Camille François et son extension, ABCDE (« Acteur, Comportement, Contenu, Degré, Effet »), qui ajoute des composants d'évaluation des risques à l'évaluation d'un incident[130].

[130] Disponible sur : https://carnegieendowment.org/research/2020/09/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework?lang=en.

Phase	Définition
Acteur	Quels sont les types d'acteurs impliqués ? Cette question peut aider à déterminer, par exemple, si l'affaire implique un acteur étatique étranger
Comportement	Quelles sont les activités manifestées ? Cette question peut aider à établir, par exemple, des preuves de coordination et d'inauthenticité
Contenu	Quels types de contenu sont créés et distribués ? Cette ligne de questions peut aider à établir, par exemple, si les informations déployées sont trompeuses.
Degré	Quel est l'impact global de l'affaire et qui cela affecte-t-il ? Cette question peut aider à établir les préjudices réels et la gravité de l'affaire.
Effet	Quel est l'impact global de l'affaire et qui cela affecte-t-il ? Cette question peut aider à déterminer les préjudices réels et la gravité de l'affaire.

205. L'élaboration d'un modèle de lutte juridique contre les manipulation de l'information basé sur STIX permet aux analystes de partager et de comparer les informations sur les acteurs de la menace, les récits, les TTP, les artefacts et autres objets dans chaque incident et campagne, en utilisant les outils déjà construits pour STIX.

206. Il permet également aux données relatives à la manipulation de l'information de transiter par les mêmes systèmes que les données relatives à la sécurité de l'information, ce qui facilite la description et la lutte contre les méthodes hybrides (combinaisons de désinformation et d'autres méthodes de sécurité de l'information).

4) Modèles de manipulation de l'information fondés sur le comportement

207. La communauté de l'infosécurité dispose de plusieurs modèles qui décrivent les comportements des créateurs d'incidents et des personnes chargées d'y répondre. Plusieurs de ces modèles, dont le cadre ATT&CK de MITRE, se concentrent sur les techniques, tactiques et procédures (TTP) utilisées par les créateurs d'incidents et les intervenants.

Capture d'écran de la matrice Mitre & Attack[131]

208. Cette approche a été adapté au contexte spécifique des manipulations de l'information par le projet AMITT devenu Disarm, servant de socle à *OpenCTI* adopté par VIGINUM solution développée initialement par l'ANSSI, le CERT-EU et l'association *Luatix,*

[131] Disponible sur le site https://attack.mitre.org/

permettant de décrire, de capitaliser et d'échanger sur la menace, notamment cyber et informationnelle.

209. En tant qu'entité à la fois technique et opérationnelle, VIGINUM s'investit depuis plusieurs années dans la promotion et la mise en œuvre de standards communs visant à renforcer la réponse aux manipulations de l'information. En 2024, l'agence a notamment publié une version française de la matrice DISARM, outil structurant pour la caractérisation des campagnes de désinformation. Parallèlement, elle participe activement aux travaux du *Defending Against Deception Common Data Model* (DAD-CDM) dont l'objectif est d'adapter le langage STIX aux besoins spécifiques de la lutte contre les opérations d'influence informationnelle.

210. La plupart des efforts de NORMA ont porté sur la manière d'adapter ces modèles, et les outils qui les utilisent, aux opérations juridiques et dans le cas présent à leur application dans la lutte contre les manipulations de l'information.

C. Présentation générale des frameworks DISARM & NORMA

211. Le *framework* développé propose en sa version 1, disponible librement sur GitHub[132], une méthodologie structurée pour traiter les cas de désinformation et de manipulation d'information à travers un cadre juridique et procédural clair. Il s'articule autour de quatre phases permettant d'identifier, préparer, exécuter et évaluer des actions juridiques adaptées face à différents types de manipulation de l'information.

212. Ce modèle est basé sur le *framework* DISARM Blue reconnu pour sa classification structurée des tactiques, techniques et procédures (TTP) répondant aux menaces informationnelles.

[132] La première version ainsi qu'une base de données de cas d'usage est disponible au lien suivant : https://github.com/NormaProject/LMI-Framework

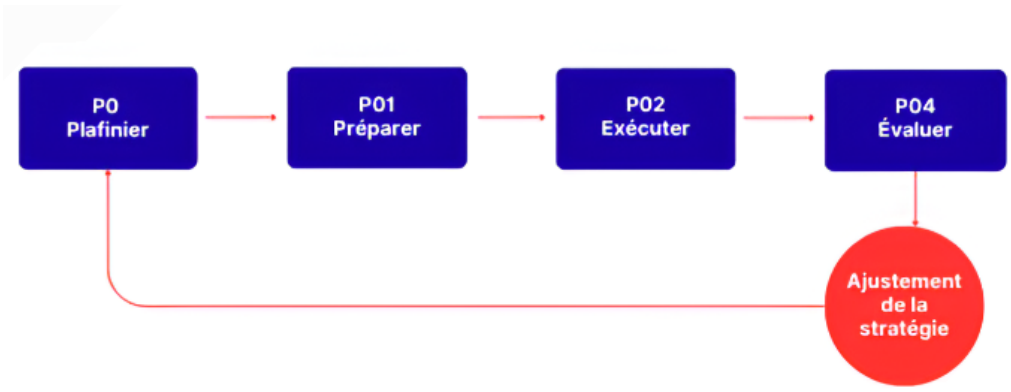
213. Les modèles évoqués contiennent de nombreux types d'objets, notamment des **tactiques** (effets recherchés d'une opération) et des **techniques** (activités possibles permettant d'accomplir une tactique).

1) Phase

214. Ces objets se regroupent autour de phase, le plus haut niveau de regroupement des tactiques et des techniques associées, correspondant à une étape logique dans l'exécution d'une opération d'intelligence juridique. Ces phases sont les suivantes :

- Planifier : Déterminer son environnement afin de permettre de s'y préparer au mieux. Envisager le résultat souhaité. Présenter des moyens efficaces pour y parvenir. Communiquer la vision, l'intention et les décisions, en se concentrant sur les résultats attendus ;
- Préparer : Activités menées avant l'exécution pour améliorer la capacité à mener l'action (ex. : développement de l'écosystème nécessaire pour soutenir l'action : personnes, réseau, canaux, contenu, etc.) ;
- Exécuter: Exécuter l'action, de l'exposition initiale à la conclusion et/ou au maintien de la présence, etc. ;
- Évaluer : Évaluation de l'efficacité de l'action, en vue d'une utilisation dans les plans futurs.

Ainsi schématiquement, le *framework* repose sur un cycle en quatre phases principales :



215. A chacune de ces phases est associées un ensemble d'étapes logiques dont la nécessité d'accomplissement est liée à la nature de la réponse envisagée et au théâtre. Ainsi à titre d'exemple, une opération envisageant une réponse judiciaire (nature) devant le tribunal de commerce de Paris (théâtre) devra suivre les étapes spécifiques et le cadre imposées par ce mode opératoire.

En résumé : une opération se découpe en quatre temps, les phases, subdivisées en étape logique liées à la nature et au théâtre de l'opération.

2) Étape

216. A chacune de ces phases est associées un ensemble d'étapes logiques dont la nécessité d'accomplissement est liée à la nature de la réponse envisagée et au théâtre. Ainsi, à titre d'exemple, une opération envisageant une réponse judiciaire (nature) devant le tribunal de commerce de Paris (théâtre) devra suivre les étapes spécifiques et le cadre imposées par ce mode opératoire.

En résumé : une opération se découpe en quatre temps, les phases, subdivisées en étapes logiques liées à la nature et au théâtre de l'opération.

3) Tactique

217. Une tactique est une manière ou un moyen d'atteindre les objectifs (finalités), qui ne prescrit pas les techniques ou procédures spécifiques utilisées pour y parvenir. Au sein des phases et des étapes sont regroupées les tactiques. Ces dernières sont entendues comme une manière ou un moyen d'atteindre les objectifs de l'opération lesquels sont déterminés et précisés lors de la phase de planification. La phase de planification ne prescrit pas les techniques ou procédures spécifiques utilisées pour y parvenir.

218. Les tactiques sont rédigées sous la forme d'un verbe d'action qualifié afin d'incarner l'effet recherché qu'elles poursuivent. Elles peuvent être résumées comme le

« *pourquoi* » d'une opération. Exemple : **[Ralentir un processus]** est une tactique visant à retarder délibérément son déroulement ou la progression normale d'une situation. Cela peut être réalisé en introduisant des obstacles, des retards intentionnels, ou en limitant les ressources disponibles.

4) Technique

219. Les techniques sont le *"comment"* d'une tactique particulière. Les techniques sont associées à une ou plusieurs tactiques, car une technique particulière peut être utilisée pour atteindre différents objectifs.

> Exemple : Afin de **[Ralentir un processus]**, il est possible suivant le domaine applicable, de procéder à un **[Obstruction parlementaire]** ou par exemple une grève **[Grève de zèle]**.

Les techniques sont associées à une ou plusieurs tactiques, une technique particulière pouvant être utilisée pour atteindre différents objectifs.

> Exemple : la **[Conformité malveillante]** peut servir à **[Ralentir un processus]** mais également dans certains cas à Communiquer de l'information

220. Grâce à un cadre fondé sur le comportement, nous pouvons commencer à enregistrer et à rappeler les contre-mesures antérieures aux techniques utilisées, et trouver et exploiter les faiblesses et les lacunes dans les opérations de l'adversaire, de la même manière que nous exploitons les faiblesses de l'adversaire dans les lacunes dans d'autres tableaux de situation, y compris ceux de la cybersécurité. Cette méthode autorise également une approche probabiliste, et l'identification de *patterns*.

D. Présentation détaillée du *framework* NORMA Blue

Les étapes suivantes ont été identifiées en matière de lutte juridique contre les manipulations de l'information.

P01.1 - Planifier la stratégie

221. *Résumé* : La planification de la stratégie consiste à définir **l'effet final recherché**, c'est-à-dire l'ensemble des conditions requises permettant d'atteindre les objectifs stratégiques. Communiquer la vision, l'intention et les décisions, en se concentrant sur les résultats attendus.

Étapes de la phase P01.1 :

P01.1E01 - Déterminer les finalités

222. *Résumé* : Fixer les finalités des opérations

- Recueillir les attentes exprimées par la personne, l'organisation ou l'entité concernée par le litige ou la situation sensible ;
- Clarifier la finalité de la démarche engagée : réparation, cessation, sanction, dissuasion, communication, ou sécurisation préventive ;
- Identifier les enjeux stratégiques, réputationnels, financiers ou politiques sous-jacents à la situation ;
- Hiérarchiser les finalités selon leur urgence, leur faisabilité et leur impact ;
- Vérifier la cohérence des finalités poursuivies avec le cadre juridique applicable et les risques contentieux encourus.

P01.1E02 - Recherche démographique / analyse de l'audience

223. *Résumé* : Déterminer son environnement afin de permettre de s'y préparer au mieux. Théâtre, actants, tendance.

P01.1E03 - Conception des opérations

224. *Résumé* : concevoir la ou les opérations nécessaires pour atteindre les finalités recherchées.

P01.1E04 - OPSEC pour P01.1

225. *Résumé* : La sécurité des opérations (OPSEC) est un processus qui permet d'identifier les informations critiques afin de déterminer si les actions amies peuvent être observées par les services de renseignement ennemis, déterminer si les informations obtenues par les adversaires pourraient être interprétées de manière à leur être utiles, puis exécuter des mesures sélectionnées qui éliminent ou réduisent l'exploitation par les adversaires des informations critiques amies.

P01.2 - Planifier les objectifs

226. *Résumé* : Définir des objectifs intermédiaires permettant d'atteindre l'état final recherché.

Étapes de la phase P01.2 :

P01.2E01 - Déterminer les objectifs

227. *Résumé* : Fixer des objectifs clairement définis, mesurables et réalisables. Dans certains cas, la réalisation des objectifs est liée à l'exécution de tâches tactiques pour atteindre l'état final stratégique souhaité. Dans d'autres cas, lorsqu'il n'existe pas d'état final stratégique clairement défini, l'objectif tactique peut se suffire à lui-même. L'énoncé de l'objectif ne doit pas préciser la manière et les moyens d'y parvenir, mais plutôt le but que l'acteur de la menace souhaite atteindre. Dans le cadre des travaux menés au sein de cette cellule, une les objectifs principaux suivants ont été isolés :

Code	Objectif	Description
OB01	Suspendre la diffusion d'un contenu	Limitation du taux de désinformation pour en réduire les effets
OB02	Ralentir la production de contenu	Circonscrire la circulation d'un contenu malveillant ou trompeur
OB03	Acquérir de l'information	Comprendre qui produit la désinformation, comment et pourquoi
OB04	Confisquer le profit réalisé	Récupérer la somme gagnée par l'usage du comportement incriminé
OB05	Réparation du préjudice	Compenser les victimes d'une manipulation de l'information
OB06	Rétablir les faits	Action corrective pour faire émerger la vérité
OB07	Sanctionner le comportement	Appliquer des mesures répressives contre les auteurs
OB08	Légitimer une action	Rendre légitime juridiquement un comportement

Objectif de la mobilisation juridique dans la LMI

P01.2E02 - Définir le niveau de visibilité souhaité des opérations

228. *Résumé* : Définir le niveau de visibilité souhaité des opérations et des opérateurs (discrétion, médiatisation, signal fort ou action de principe).

P01.2E03 - Détermination des solutions techniques déployés

229. *Résumé* : Évaluation et détermination des meilleures opportunités techniques permettant la réalisation des objectifs fixés.

P01.2E04 - OPSEC pour P02

230. *Résumé* : La sécurité des opérations (OPSEC) est un processus qui permet d'identifier les informations critiques afin de déterminer si les actions amies peuvent être observées par les services de renseignement ennemis, déterminer si les informations obtenues par les adversaires pourraient être interprétées de manière à leur être utiles, puis exécuter des mesures sélectionnées qui éliminent ou réduisent l'exploitation par les adversaires des informations critiques amies.

P02 – Préparer

231. *Résumé* : Activités menées avant l'exécution pour améliorer la capacité à mener l'action. Exemples : développement de l'écosystème nécessaire pour soutenir l'action : personnes, réseau, canaux, contenu, etc.

Éléments de la phase P02 :

P02E01 - Identifier la nature de l'information

232. Étapes d'identification :

- Qualifier cette information : fait, opinion, donnée personnelle, contenu journalistique, document administratif ou confidentiel ;
- Vérifier si l'information porte atteinte à des droits protégés (droit à la vie privée, à l'image, secret des affaires, présomption d'innocence, etc.) ;
- Identifier le support d'origine et le format de l'information (texte, image, vidéo, montage, *deepfake*, etc.) ;

- Documenter les sources de l'information pour retracer sa trajectoire de diffusion et de modification ;
- Identifier les éléments susceptibles de créer une confusion dans l'esprit du public ou de porter atteinte à une réputation, une autorité ou une décision.

233. Types d'informations identifiés :

- Informations classifiées
- Secret des correspondances
- Secret de fabrication
- Secret des affaires
- Données personnelles
- Acte authentique

P02E02 - Identifier la nature de la manipulation

234. Détecter les procédés mis en œuvre pour altérer, orienter ou dissimuler l'information initiale *(cf. matrice disarm red.)*.

235. Types de manipulations identifiés :

- Atteinte à la véracité de l'information
- Atteinte à la confidentialité
- Atteinte à la propriété
- Atteinte à la fonction de l'information

P02E03 - Identifier la nature de l'intérêt violé

236. *Étapes d'identification :*

- Qualifier juridiquement l'intérêt en cause : personnel, patrimonial, moral, collectif ou institutionnel ;
- Vérifier si l'intérêt invoqué est protégé par une norme juridique (texte législatif, réglementaire, convention internationale, jurisprudence) ;

- Distinguer les intérêts strictement individuels de ceux présentant une dimension sociale ou collective ;
- Apprécier le caractère direct, actuel et légitime de l'intérêt, notamment pour établir l'intérêt à agir ;
- Évaluer si l'atteinte concerne un droit subjectif ou un intérêt juridiquement protégé.
- Considérer les spécificités du contexte pour ajuster la qualification de l'intérêt en jeu ;
- Recenser les décisions de jurisprudence analogues permettant de conforter l'identification retenue ;
- Confronter l'analyse à la typologie des préjudices réparables pour préparer la phase de chiffrage ;
- Adapter la stratégie contentieuse en fonction de la nature et de la portée de l'intérêt violé.

237. Types d'intérêts identifiés :

- Intérêt fondamental de l'État
- Intérêt industriel ou économique
- Intérêt privé

P02E04 - Identifier le lieu de la diffusion de l'information

238. *Étapes d'identification :*

- Recenser les canaux par lesquels l'information litigieuse a été rendue accessible au public ;
- Déterminer la localisation des serveurs ou des infrastructures techniques lorsque la diffusion est numérique ;
- Identifier la localisation géographique du public destinataire ou effectivement touché par l'information ;
- Analyser le périmètre de diffusion en fonction du support utilisé ;
- Vérifier la présence de relais secondaires ou de rediffusions ayant prolongé ou étendu la diffusion initiale ;

- Consulter les éléments matériels de preuve ;
- Établir un lien entre le lieu de diffusion et la compétence juridictionnelle potentielle ;
- Croiser les éléments de localisation avec les règles de compétence territoriale et matérielle applicables ;
- Prendre en compte les particularités liées à la diffusion transfrontalière ou en ligne.

239. Types de canaux identifiés :

- Médias traditionnels ;
- Canaux numériques & plateformes ;
- Canaux interpersonnels ;
- Canaux institutionnels et officiels ;
- Supports physiques & analogiques.

P02E05 - Identifier la possibilité d'une pluralité de responsable

240. *Étapes d'identification :*

- Examiner les faits générateurs du dommage afin d'identifier l'intervention de plusieurs acteurs ;
- Reconstituer la chaîne des causalités possibles entre les différents intervenants.
- Analyser les rôles respectifs ;
- Vérifier l'existence de liens contractuels, organisationnels ou fonctionnels entre les parties impliquées ;
- Identifier les régimes spécifiques de responsabilité solidaire ou *in solidum* prévus par la loi ou la jurisprudence ;
- Rechercher les clauses contractuelles susceptibles d'élargir ou de limiter la responsabilité d'un intervenant ;
- Évaluer les incidences procédurales d'une pluralité de responsables ;
- Anticiper les stratégies de défense croisées ou divergentes susceptibles d'émerger.

241. Types de responsables identifiés :

- Auteur ;
- Hébergeur ;
- Éditeur du site ;
- Fournisseur d'accès à internet ;
- Commanditaire ;
- Directeur de la publication ;
- Imprimeur ;
- Distributeur ;
- Concepteur.

P02E06 - Identifier l'organisme public ou judiciaire vers lequel se tourner

242. *Étapes d'identification :*

- Identifier les autorités compétentes selon la nature de la violation ;
- Vérifier la compétence territoriale et matérielle des juridictions ou organismes visés ;
- Analyser les voies de recours, dispositifs de signalement ou mécanismes spécifiques existants ;
- Apprécier le niveau de réactivité, de légitimité et d'impact attendu de l'organisme envisagé selon les objectifs poursuivis ;
- Évaluer les conditions d'accès à la saisine ;
- Recenser les précédents ou décisions rendues dans des affaires similaires par l'organisme envisagé ;
- Prendre en compte les contraintes politiques, diplomatiques ou médiatiques pesant sur certains recours institutionnels ;
- Croiser les possibilités de saisine pour envisager une action parallèle ou complémentaire ;
- Choisir l'organe le plus pertinent au regard de la stratégie globale.

243. Types de compétences identifiées :

- Compétence territoriale
- Compétence d'attribution

P02E07 - Identifier le fondement juridique idoine

244. *Étapes d'identification :*

- Analyser les faits matériels du litige à la lumière des qualifications juridiques possibles ;
- Qualifier juridiquement les comportements, manquements ou atteintes reprochés à la partie adverse ;
- Déterminer la nature du régime de responsabilité applicable ;
- Rechercher les textes de loi pertinents en fonction de la matière concernée ;
- Explorer la jurisprudence constante ou récente susceptible d'éclairer l'interprétation des règles applicables ;
- Intégrer, le cas échéant, les normes européennes ou internationales pertinentes.
- Identifier les règles de procédure qui encadrent les prétentions ;
- Vérifier les conditions d'application des textes invoqués ;
- Hiérarchiser les fondements pour construire une argumentation claire, solide et stratégique ;
- Adapter les fondements aux évolutions possibles du litige.

P02E08 - Chiffrer le préjudice

245. *Étapes :*

- Évaluer l'étendue des dommages subis par la partie demanderesse ;
- Identifier chaque chef de préjudice, qu'il soit matériel, moral, corporel ou financier ;
- Distinguer les préjudices patrimoniaux des préjudices extra-patrimoniaux ;
- Collecter l'ensemble des justificatifs probants ;
- Valoriser chaque élément de préjudice à l'aide d'outils jurisprudentiels.

246. Types de préjudices identifiés :

- **Préjudices patrimoniaux :**
  - Perte subie
  - Gain manqué
- **Préjudices extra-patrimoniaux :** préjudice moral (dont atteinte à la vie privée ou à l'image)

P03 – Exécuter

247. *Résumé* : Cette phase concerne la mise en œuvre concrète des actions planifiées et préparées dans les phases précédentes. C'est le moment où l'on applique la stratégie établie pour atteindre les objectifs fixés.

P03E01 - Engager la procédure appropriée

248. *Étapes :*

- Rédiger et déposer la demande/plainte/requête auprès de l'autorité compétente identifiée ;
- Respecter les formalités procédurales (délais, forme, pièces justificatives) ;
- Verser les frais de procédure éventuels ;
- Notifier la partie adverse dans les formes requises.

P03E02 - Mettre en œuvre les mesures conservatoires

249. *Étapes :*

- Solliciter des mesures provisoires ou de sauvegarde (référé, sursis à exécution) ;
- Demander le retrait temporaire du contenu litigieux ;
- Requérir la préservation des preuves ;
- Obtenir le gel des avoirs ou profits illicites le cas échéant.

P03E03 - Assurer le suivi procédural

250. *Étapes :*

- Participer aux audiences et comparutions ;
- Répondre aux demandes d'informations complémentaires ;
- Respecter le calendrier de procédure ;
- Adapter la stratégie aux événements procéduraux.

P03E04 - Communiquer sur l'action en cours

251. *Étapes :*

- Informer les parties prenantes de l'évolution de la procédure ;
- Gérer les relations avec les médias si nécessaire ;
- Diffuser des communications publiques en cohérence avec la stratégie globale ;
- Anticiper et contrer les récits adverses ;

252. Actions spécifiques aux objectifs déterminés :

Pour l'objectif OB01 - Suspendre la diffusion d'un contenu

- Procédure de référé ;
- Notification formelle aux plateformes concernées ;
- Demande de retrait auprès des hébergeurs selon procédure LCEN.

Pour l'objectif OB02 - Ralentir la production de contenu

- Multiplication des procédures judiciaires stratégiques ;
- Envoi de mises en demeure formelles ;
- Demandes de contradictoire systématiques.

Pour l'objectif OB03 - Acquérir de l'information

- Procédures de *discovery* ou de communication forcée de pièces ;
- Réquisitions judiciaires ;
- Demandes d'accès aux données personnelles (RGPD).

Pour l'objectif OB04 - Confisquer le profit réalisé

- Demande de saisie conservatoire ;
- Procédure de recouvrement des bénéfices illicites.

Pour l'objectif OB05 - Réparation du préjudice

- Action en responsabilité civile ;
- Demande d'indemnisation chiffrée et justifiée ;
- Mise en place d'accords transactionnels si approprié.

Pour l'objectif OB06 - Rétablir les faits

- Demande de publication d'un droit de réponse ;
- Action en rectification d'information ;
- Diffusion de communications correctives.

Pour l'objectif OB07 - Sanctionner le comportement

- Dépôt de plainte pénale ;
- Constitution de partie civile ;
- Signalement aux autorités de régulation compétentes.

P04 – Évaluer

253. *Résumé* : Cette phase consiste à mesurer et analyser les résultats obtenus à la suite de l'exécution des actions, afin d'ajuster la stratégie si nécessaire et de tirer des enseignements pour les situations futures.

Étapes de la phase P04 :

P04E01 - Mesurer l'efficacité des actions entreprises

254. *Étapes :*

- Évaluer l'atteinte des objectifs initialement fixés ;
- Mesurer les effets directs et indirects des actions menées ;

- Comparer les résultats obtenus aux résultats escomptés ;
- Identifier les écarts et leurs causes.

P04E02 - Analyser les coûts et bénéfices

255. *Étapes :*

- Calculer le rapport entre les ressources engagées et les résultats obtenus ;
- Évaluer les coûts financiers, temporels et réputationnels ;
- Mesurer la valeur des bénéfices tangibles et intangibles ;
- Déterminer le retour sur investissement global.

P04E03 - Capitaliser sur l'expérience

256. *Étapes :*

- Documenter les bonnes pratiques et les enseignements tirés ;
- Identifier les points d'amélioration pour les actions futures ;
- Mettre à jour les procédures internes en conséquence ;
- Partager les connaissances avec les parties prenantes concernées.

P04E04 - Assurer le suivi post-procédural

257. *Étapes :*

- Veiller à l'application effective des décisions obtenues ;
- Surveiller les évolutions ultérieures de la situation ;
- Maintenir une veille sur les acteurs impliqués ;
- Anticiper les récidives potentielles.

RECOMMANDATIONS

Les présentes recommandations sont le fruit du travail collectif d'un groupe de bénévoles, réunissant des expertises pluridisciplinaires en droit, intelligence économique et sciences sociales. Elles ont été élaborées à titre exploratoire, dans un souci de contribution au débat public et institutionnel sur les réponses juridiques à apporter aux manipulations de l'information.

En l'absence de moyens institutionnels ou budgétaires dédiés, ces propositions n'ont pu faire l'objet ni d'un approfondissement systématique, ni d'un processus complet de consultation intersectorielle. Elles constituent dès lors une base préliminaire de réflexion, appelant à être discutée, affinée et complétée dans le cadre d'un travail de recherche structuré, doté de ressources adéquates et d'un temps d'analyse proportionné à la complexité des enjeux.

1. **Élargir l'appréhension juridique de la manipulation de l'information** en la considérant comme un **phénomène global**, qui excède le seul champ politique. Le secteur économique, notamment, en est une cible fréquente. En ce sens, la manipulation ne saurait être juridiquement réduite à la diffusion de fausses informations : elle implique des dynamiques d'intentionnalité, d'influence et de déstabilisation qui méritent une approche normative plus large.

2. **Multiplier les opportunités judiciaires** de sanctionner la manipulation d'information sur des fondements originaux recherchant *l'intention* de manipuler, plutôt que la *nature illicite* de l'information ou son *canal de diffusion*.

   À cet égard, le droit pénal offre le fondement du *sabotage* qui, pour le moment peu utilisé, peut être mobilisé pour sanctionner pénalement la manipulation d'information. Sur le **plan civil et commercial**, la responsabilité civile pour concurrence déloyale

offre une arme redoutable aux entreprises victime de manipulation de l'information. Dans les deux cas, l'intention de manipuler légitimerait le fondement.

3. **Promouvoir l'adoption d'un corps de règles propre à la manipulation de l'information** sur le modèle de ce que l'on connaît en matière de lutte anti-terroriste. L'adoption d'un texte spécial permettrait de saisir les enjeux de manière plus précise et d'accroître les moyens judiciaire et policier de lutte contre la manipulation de l'information. Ce cadre devrait être accompagné de la **création d'une autorité ou d'une juridiction spécialisée**, dotée de compétences techniques et juridiques pour instruire les cas de manipulation de l'information.

4. **Renforcer la coordination public-privé par des mécanismes structurels.** Il convient d'instituer des actions thématiques et régulières réunissant VIGINUM, l'ARCOM, des acteurs du fact-checking, des collectifs OSINT et des juristes spécialisés. Ces plateformes de coordination permettraient l'analyse conjointe des narratifs hostiles, la formulation de recommandations partagées, le partage de référentiels communs, la définition d'actions judiciaires, y compris issues de la société civile (et notamment par le biais de contentieux de masse).

5. **Créer une réserve civile d'expertise juridique.** Le renforcement du dispositif étatique passe par la création d'une réserve civile d'analystes juridiques mobilisables en temps de crise. Elle s'appuierait sur les collectifs existants et serait intégrée à une section pluridisciplinaire de réservistes, incluant des compétences en droit, en cybersécurité, en renseignement et en communication stratégique.

6. **Développer une méthode automatisée d'aide à la qualification juridique.** Un prototype de classification automatique, conçu par la cellule, permet déjà de confronter des situations de manipulation à l'ensemble des fondements juridiques disponibles. Il est recommandé de :

    - Doter ce projet d'un budget dédié pour assurer son passage à l'échelle ;
    - Intégrer le module à des solutions d'analyse existantes (DISARM, STIX - OpenCTI) ;

- Le rendre accessible aux personnes physiques et morales afin de leur permettre d'identifier les voies de droit les plus adaptées à leur situation.

7. **Adopter une stratégie contentieuse offensive.** Il est nécessaire de passer d'une posture essentiellement préventive et défensive à une stratégie contentieuse offensive. Cela implique :
    - La multiplication des procédures civiles et pénales à l'encontre des grands opérateurs numériques, dans une logique de responsabilisation structurelle ;
    - La mise en place d'un réseau de juristes et de cabinets d'avocats spécialisés en droit informationnel ;
    - Le développement d'un contentieux de masse, visant tant les auteurs de manipulation que les plateformes qui les hébergent ou facilitent leur diffusion sans vigilance suffisante.

8. **Institutionnaliser la recherche et le développement du *lawfare* à la française**, ce que l'on pourrait désigner comme le *« droit de la guerre atypique »* ou le *lawfare*, en créant une branche doctrinale dédiée permettant de clarifier les concepts, les responsabilités et les mécanismes d'activation du droit.

    En parallèle, il est essentiel de renforcer l'enseignement universitaire de ces enjeux par l'introduction de modules spécialisés dans les facultés de droit, de sciences politiques et de relations internationales.

9. **Adopter une communication stratégique différente** consistant à présenter la manipulation de l'information comme un *sabotage informationnel*. Il faut donc abandonner la première notion au profit de la seconde. La notion de sabotage insiste sur le caractère étranger et dangereux de l'ingérence tandis qu'il accentue son caractère pernicieux et indécelable. Le terme de *manipulation* ou *encore de fake news*, pour la plupart des citoyens, n'est pas à la mesure de la dangerosité. Ces derniers ne pensent pas, à tort, être suffisamment vulnérables pour être atteint.

NORMA

contact@norma-project.com

www.norma-project.com