Les acteurs visés par la législation européenne sur la cybersécurité

Par Michel SÉJEAN
Professeur agrégé de droit privé et sciences criminelles,
Université Sorbonne Paris Nord, IRDA (UR 3970)

Il est impossible de dresser une liste exhaustive, ou même une simple typologie des acteurs visés par les douze textes sur la cybersécurité qui marquent la première moitié de la Décennie numérique. Ces acteurs sont si nombreux, que les architectes de ce monument normatif sont loin d'avoir tout anticipé. Des impensés apparaissent, tant au niveau de la qualification des acteurs concernés que du régime juridique qui correspond.

« Droit et passion du droit sous la Décennie numérique » : si l'on s'autorisait à pasticher le titre du célèbre ouvrage paru il y a trente ans sous la plume du Doyen Carbonnier[1], ce pourrait être l'intitulé d'une monographie à propos de l'emballement législatif qui s'aggrave depuis 2020 en droit de la cybersécurité. Bien malin qui pourrait dresser une liste exhaustive, ou même une simple typologie des acteurs visés par cette ardeur législative : cet exercice relève de la gageure ! Ces acteurs sont si nombreux, que les architectes de ce monument normatif sont loin d'avoir tout anticipé. Des impensés apparaissent, tant au niveau de la qualification des acteurs concernés que du régime juridique qui correspond.

La Décennie numérique est une stratégie de l'Union européenne qui vise à atteindre un objectif numérique en 2030 : « L'Europe veut donner aux entreprises et aux citoyens les moyens d'agir dans un avenir numérique durable, centré sur l'humain et plus prospère », écrit la Commission européenne sur son site internet[2]. En réalité, l'avenir numérique que propose l'Union européenne va de pair avec un risque accru de cyberattaques et d'incidents de sécurité informatique[3]. Une illustration parmi d'autres : lorsque l'Union européenne vise l'adoption de technologies qui transforment l'activité numérique des entreprises, elle fixe comme objectif que « 75 % des entreprises de l'UE utilisent l'informatique en nuage, l'IA ou les mégadonnées »[4]. La surface d'exposition au risque cyber a donc vocation à augmenter de manière continue, et la production de règles préventives et curatives ne

[1] J. Carbonnier, *Droit et passion du droit sous la V^e^ République*, coll. « Forum », Flammarion, 1996, 273 pages.

[2] Site de la Commission européenne, dernière consultation le 10 mai 2025, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

[3] Les cyberattaques sont des menaces volontaires à la cybersécurité, tandis que les incidents de sécurité informatique renvoient plutôt aux événements involontaires qui mettent en danger la cybersécurité (pannes, négligences, avaries, catastrophes naturelles, etc.).

[4] Site de la Commission européenne, préc., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

pouvait que s'emballer. Nous voici donc au mitan de cette Décennie numérique 2020-2030, et trois ans seulement après la déclaration européenne sur les droits et principes numériques du 15 décembre 2022, aux termes de laquelle les États membres s'engagent notamment à « garantir un environnement numérique sûr et sécurisé » (art. 11, a)[5].

Quel est l'état d'esprit des acteurs visés par la législation européenne qui incarne la stratégie de la Décennie numérique ? Reconnaissons-le, ce sont actuellement la lassitude, la surcharge cognitive et la perte de sens qui dominent. Dans les trois dernières années, douze textes aussi fondateurs que la Loi des Douze Tables ont fait leur irruption dans l'organisation interne d'entités[6] déjà mises à l'épreuve par le déploiement du RGPD (2016), de la première directive sur la sécurité des réseaux d'information (dite directive SRI, ou NIS, 2016) et du règlement européen sur la cybersécurité (2019)[7]. Les douze textes entrés en vigueur entre 2022 et 2025 forment ainsi un véritable monceau législatif sans équivalent dans l'histoire récente. Les acteurs concernés ne savent cependant pas toujours qu'ils sont assujettis à certains textes, et l'on peut citer au moins un cas où une règle importante fait la démonstration de ses limites au moment d'être mise en œuvre. C'est dire que des impensés affaiblissent l'opération de qualification juridique et la mise en œuvre du régime juridique applicable aux acteurs concernés.

Un labyrinthe de qualifications juridiques

Qui est concerné ? Les mots se font de plus en plus abstraits pour capturer la variété croissante d'acteurs que vise cet amas de textes, alors que le risque systémique de cyberattaques est, lui, toujours plus concret. Un texte incarne mieux que d'autres la difficulté de l'opération de qualification juridique : le règlement sur la cyberrésilience, qui porte principalement sur la cybersécurité des produits connectés[8]. Non seulement les définitions des acteurs concernés forment un catalogue de qualifications juridiques abstraites juxtaposées les unes à côté des autres, mais ces définitions s'emboîtent, se ramifient, et se renvoient parfois l'une à l'autre, laissant au lecteur la charge de se rendre dans une directive pour trouver le texte de la définition contenue dans un règlement.

Voyez l'article 3 du règlement sur la cyberrésilience : il comporte cinquante et une définitions. Au paragraphe 12 de cet article 3, l'« opérateur économique » est défini comme étant « le fabricant, le mandataire, l'importateur, le distributeur ou une autre personne physique ou morale soumise à des obligations liées à la fabrication de produits comportant des éléments numériques ou à la mise à disposition sur le marché de produits comportant des éléments numériques conformément au présent règlement ».

---

[5] Déclaration européenne des droits et principes numériques pour la Décennie numérique, 2023/C 23/01, 15 décembre 2022, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32023C0123(01)

[6] « Entité » : voir spéc. Directive (UE) n°2022/2555 du Parlement européen et du Conseil, 14 décembre 2022, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), dont l'article 6 point 38 définit une « entité » comme étant « une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations ». Cela renvoie concrètement aux entreprises, aux associations, aux administrations, aux hôpitaux, ou encore aux collectivités locales.

[7] Pour une présentation des quinze textes de législation européenne entre 2016 et 2025, voir le tableau, réalisé par l'auteur de ces lignes.

[8] Règlement du Parlement européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

Mais qu'est-ce qu'un fabricant, un mandataire, un importateur, ou encore un distributeur ? Les paragraphes 13 et suivants de l'article 3 ramifient la définition de l'opérateur économique. Par exemple, un fabricant est « une personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux, monétisé ou gratuit » (art. 3§13). Sur le même mode, les définitions du mandataire, d'importateur et de distributeur sont données aux paragraphes 15, 16 et 17. Après ce fastidieux inventaire, l'on aurait tort de se croire au bout de sa peine : il faut encore digérer la définition d'un « intendant de logiciels ouverts » (art. 3§14) ou encore d'un « organisme d'évaluation de la conformité » (art. 3§28), d'un « organisme notifié » (art. 3§29) ou encore d'un « CSIRT désigné comme coordinateur » (art. 3§51). Les lectrices et les lecteurs des *Annales des Mines* seront certainement plus à l'aise avec les CSIRT que ne le sont les juristes en charge du déploiement des mesures prévues par ce règlement[9]. Si ces mêmes juristes voulaient trouver un éclairage dans la définition du « CSIRT désigné comme coordinateur », avertissons-les sans tarder : ils seront déçus ! En effet, la définition qu'en donne l'article 3§51 semble tout droit sortie des Douze Travaux d'Astérix, où l'irréductible Gaulois se trouve piégé dans un labyrinthe administratif qui le renvoie de bureau en bureau : c'est ainsi qu'un « CSIRT désigné comme coordinateur » est défini comme « un CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555 » (art. 3§51). Autrement dit : débrouillez-vous !

À côté des cas où il est ardu de rattacher la situation d'une entité à une ou plusieurs qualifications juridiques, un problème d'une autre nature se dessine à l'horizon. Une catégorie d'entreprises n'est pas toujours au courant qu'elle est assujettie à certains textes : il s'agit des entreprises qui contribuent à la « chaîne d'approvisionnement » des entités essentielles (EE) importantes (EI) d'après la directive SRI 2[10], ou qui sont des « prestataires tiers de services numériques » au sens du règlement DORA sur la cybersécurité des services financiers.

L'article 21 de la directive SRI 2 énonce, en effet, que les entités essentielles et importantes doivent prendre des mesures de gestion des risques en matière de cybersécurité concernant « la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs » (art. 21§2, d). Si la réglementation du risque cyber dans les chaînes d'approvisionnement est une des questions les plus sensibles de la Décennie numérique[11], c'est sans aucun doute parce que les entreprises de la chaîne d'approvisionnement sont difficiles à identifier : jusqu'à quel rang une entreprise sous-traitante ou prestataire tierce à l'entité assujettie doit-elle être aspirée dans le champ d'application de la directive SRI 2 ? Le rang 1 ? Sans aucun doute ! Mais ensuite ? Jusqu'au rang 10 ? 100 ? Il faudra sans doute que des lignes directrices précisent qui fait partie des acteurs concernés par la directive SRI 2, à moins que ce ne soit le contentieux qui s'en occupe.

---

[9] Voir spéc. pour plus d'informations sur les CSIRT, M. Séjean, « Tiers de confiance numérique et centres de réponse aux incidents de sécurité informatique (CSIRT) », Dalloz IP/IT, décembre 2024, p. 641 s, https://shs.hal.science/halshs-04836188v1

[10] Voir l'article 3 (« Entités essentielles et importantes ») de la Directive (UE) n°2022/2555 du Parlement européen et du Conseil, 14 décembre 2022, préc.

[11] Voir, pour aller plus loin, E. Buisson, *La réglementation relative au risque de cyberattaques au sein des chaînes d'approvisionnement*, Thèse dactyl., Université Bretagne-Sud, Chaire Cyber de l'IHEDN, avril 2025, dir. M. Séjean, 309 pages.

Présentation des quinze textes de législation européenne entre 2016 et 2025

	Nom du texte	Type	Date d'entrée en vigueur	Textes d'application adoptés par l'UE ?
1	Règlement général sur la protection des données (RGPD) (UE 2016/679)	Règlement	24 mai 2016	Aucun règlement d'application spécifique, mais actes délégués/exécution sur points précis
2	Directive sur la sécurité des réseaux et des systèmes d'information (NIS 1) (UE 2016/1148)	Directive	8 août 2016	N/A
3	Règlement sur la cybersécurité (Cybersecurity Act) (UE 2019/881, création de l'ENISA)	Règlement	27 juin 2019	Oui : schémas européens de certification (EUCC, EUCS, etc.)
Début de la Décennie numérique 2020-2030				
4	Règlement sur la gouvernance des données (Data Governance Act) (UE 2022/868)	Règlement	23 juin 2022	Oui : actes d'exécution et délégués sur l'enregistrement, etc.
5	Règlement sur les services numériques (Digital Services Act, DSA) (UE 2022/2065)	Règlement	16 novembre 2022	Oui : actes d'exécution sur rapports de transparence, coopération
6	Directive sur la résilience des entités critiques (REC) (UE 2022/2557)	Directive	16 janvier 2023	N/A
7	Directive sur des mesures destinées à assurer un niveau élevé commun de cybersécurité (NIS 2) (UE 2022/2555)	Directive	16 janvier 2023	N/A

	Nom du texte	Type	Date d'entrée en vigueur	Textes d'application adoptés par l'UE ?
8	Règlement sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2554)	Règlement	16 janvier 2023	Oui : actes délégués, normes techniques (RTS/ITS)
9	Directive sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2556)	Directive	16 janvier 2023	N/A
10	Règlement sur les données (Data Act) (UE 2023/2854)	Règlement	11 janvier 2024	Oui : actes d'exécution attendus, non encore adoptés
11	Règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (UE/Euratom 2023/2841)	Règlement	7 janvier 2024	Oui : actes d'exécution attendus, non encore adoptés
12	Règlement sur l'intelligence artificielle (AI Act) (UE 2024/1689)	Règlement	11 juillet 2024	Oui : actes délégués/exécution prévus, encore en préparation
13	Directive sur la responsabilité du fait des produits défectueux (UE 2024/2853)	Directive	9 décembre 2024	N/A
14	Règlement sur la cyberrésilience (Cyber Resilience Act, CRA) (UE 2024/2847)	Règlement	10 décembre 2024	Oui : actes délégués/exécution attendus, non encore adoptés
15	Règlement sur la solidarité en matière de cybersécurité (Cyber Solidarity Act, CSA)	Règlement	4 février 2025	Oui : actes d'exécution attendus, non encore adoptés

La directive SRI 2 aurait pu s'inspirer du mécanisme mis en place par le règlement DORA sur la cybersécurité des services financiers[12]. Ce règlement comporte, lui aussi, des dispositions spéciales sur les « prestataires tiers de services TIC [Technologies d'Information et de Communication] ». Mais son article 28§1, a) énonce clairement que l'assujetti à DORA est responsable des vulnérabilités de sa chaîne d'approvisionnement : « 1. Les entités financières gèrent les risques liés aux prestataires tiers de services TIC en tant que partie intégrante du risque lié aux TIC dans leur cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, et conformément aux principes suivants : a) les entités financières qui ont conclu des accords contractuels pour l'utilisation de services TIC dans le cadre de leurs activités restent à tout moment pleinement responsables du respect et de l'exécution de toutes les obligations découlant du présent règlement et du droit applicable aux services financiers ». Pourquoi ne pas l'avoir indiqué également dans la directive SRI 2 ? La chaîne d'approvisionnement d'une entité essentielle ou importante – l'on parle de 100 000 entités dans toute l'Union européenne – aurait dû faire l'objet de précisions sur ce point, car si une entreprise ne sait pas qu'elle est concernée par un texte, il y a peu de chances qu'elle s'y conforme. À ces difficultés concernant la qualification juridique des acteurs concernés par la législation de droit de la cybersécurité en Union européenne, il faut ajouter un impensé au niveau du régime juridique.

Un impensé dans le régime juridique applicable aux acteurs concernés

Bien que la France n'ait pas encore transposé dans son droit interne la directive SRI 2, les entreprises ont commencé à s'organiser avec les textes dont elles disposent. Le point d'entrée pour une entité concernée par la directive, c'est l'enregistrement auprès de l'autorité compétente : par exemple, si une entreprise française, établie en France, est une entité essentielle ou importante, elle doit s'enregistrer auprès de l'ANSSI. Mais le texte qui impose cet enregistrement, l'article 26 de la directive SRI 2, n'a pas été pensé pour les multinationales qui opèrent dans plusieurs États membres de l'Union européenne.

Il dispose que : « Les entités relevant du champ d'application de la présente directive sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies, à l'exception des cas suivants : (…) ». Une multinationale ayant des activités dans tous les pays de l'Union européenne doit-elle donc s'enregistrer vingt-sept fois ? Peut-elle centraliser tous les enregistrements auprès de l'ANSSI, si le siège de ses activités est en France ? Oui, elle le peut, mais seulement dans trois séries de cas exceptionnels (art. 26§1 a), b) et c). Or, de nombreuses entreprises de la Base Industrielle et Technologique de Défense (BITD) sont dans une situation administrative difficile : elles remplissent parfois les critères de l'exception qui permettrait de centraliser les enregistrements auprès de l'ANSSI, mais pas pour toutes leurs activités, si bien qu'elles doivent à la fois enregistrer leurs activités auprès des vingt-sept ANSSI européennes, et parfois centraliser certains enregistrements auprès de l'ANSSI française pour les activités qui remplissent les critères des exceptions.

Dans ces conditions, l'Union européenne est en train de créer ce contre quoi elle prétend lutter dans le cadre de ses compétences de protection du marché intérieur (art. 114 TFUE). L'Union européenne était censée protéger les entreprises naissantes de la prédation par les mastodontes qui ont tant de fois racheté leurs concurrents pour neutraliser

[12] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, spéc. Chapitre V « Gestion des risques liés aux prestataires tiers de services TIC ».

les produits qui menaçaient les leurs. Mais avec douze textes gigantesques sur le droit de la cybersécurité entrés en vigueur en trois ans, quel est l'intérêt, pour une entreprise naissante, de croître jusqu'à être assujettie à certains de ces textes européens sur la cybersécurité. Ne vaut-il pas mieux que ces jeunes pousses se fassent racheter par une grande entreprise à la puissance administrative capable de soulever une montagne juridique, en espérant que la montagne n'accouche pas d'une souris économique ?