Cartographie des lois européennes du numérique

Stéphane FOSSE
fosse.fr

22 décembre 2024

L'Amérique innove, la Chine copie, l'Europe réglemente.

Résumé

La question d'un cadre législatif adapté au monde numérique prend de l'importance. L'Union européenne a développé plusieurs textes juridiques pour encadrer les activités en ligne. Ces réglementations couvrent divers domaines, de la protection des données à la sécurité des infrastructures, sans oublier la gestion des droits d'auteur dans le marché unique numérique.

Cet article présente une synthèse des principaux textes législatifs européens qui structurent les pratiques numériques actuelles. Nous examinerons tant les régulations établies comme le RGPD, qui a transformé la gestion de la confidentialité des données en Europe après les révélations PRISM et Xkeyscore, que les initiatives récentes telles que le DMA et le DSA, visant à équilibrer les rapports entre grandes plateformes et utilisateurs. Nous aborderons aussi d'autres mesures comme la directive NIS pour la sécurité des réseaux et le Cybersecurity Act, renforçant la résistance des systèmes face aux menaces informatiques.

Table des matières

1 Stratégie européenne pour les données

La stratégie européenne pour les données, formulée par la Commission européenne en 2020, cherche à positionner l'Union comme leader de l'économie des données en exploitant le potentiel des données non personnelles [1]. Cette stratégie naît du constat simple que les données constituent aujourd'hui le carburant de nos économies modernes, une ressource fondamentale pour l'innovation et la croissance. On la retrouve dans notre quotidien,

qu'on le veuille ou non. La Commission reconnaît les bénéfices économiques, sociaux et environnementaux de l'utilisation des données, sans jamais perdre de vue le respect des droits fondamentaux et des valeurs propres à l'Europe.

Dans sa vision, l'Europe a créé un cadre juridique solide favorisant la circulation libre des données non personnelles. L'équité d'accès aux données y occupe une place centrale, tant pour les jeunes pousses que pour les géants industriels. Cette approche garantit que toute collecte ou utilisation de données s'inscrit dans les normes européennes de protection de la vie privée. La stratégie propose par ailleurs un renforcement des capacités européennes dans le traitement des données, avec des investissements ciblés dans les infrastructures et les compétences.

Sa mise en application demande un engagement concret des États membres et des entreprises. Cela touche à plusieurs aspects : gouvernance des données, transparence des processus et interopérabilité des systèmes dans toute l'Union. S'y ajoutent des exigences strictes concernant les normes de sécurité et de cybersécurité, devenues incontournables dans notre monde connecté.

2 Règlement général sur la protection des données (RGPD)

Le Règlement Général sur la Protection des Données, entré en vigueur en 2018, marque un tournant dans l'histoire de la protection des données en Europe [2]. Ce texte central répond aux bouleversements provoqués par les révélations d'Edward Snowden sur la surveillance de masse (affaire PRISM). Il vise à donner aux citoyens européens la maîtrise de leurs données personnelles tout en harmonisant les approches nationales, souvent disparates.

Le champ d'application du RGPD s'étend à tout traitement de données personnelles — qu'il s'agisse de leur collecte, de leur stockage ou de leur utilisation. Sa portée extraterritoriale représente une innovation : même les organisations hors UE doivent s'y conformer si elles traitent des données de résidents européens. Un véritable changement de paradigme dans la régulation numérique mondiale.

Le texte articule un équilibre entre droits des personnes et responsabilités des organisations. Côté obligations, il exige un consentement clair et explicite, une transparence sans faille sur l'usage des données, et des mesures de sécurité adaptées aux risques. Pour certaines structures, la désignation d'un délégué à la protection des données devient obligatoire. Côté droits, les individus peuvent désormais accéder à leurs données, les rectifier, demander leur effacement, ou encore les transférer d'un service à un autre.

Le règlement montre ses dents avec un régime de sanctions dissuasif : jusqu'à 4% du chiffre d'affaires mondial ou 20 millions d'euros pour les infractions graves. Un message clair adressé aux organisations : la protection des données n'est plus une option mais une exigence fondamentale dans notre société numérique.

3 Règlement sur les marchés numériques (DMA)

Le Digital Markets Act, formalisé en 2022 par le règlement (UE) 2022/1925, incarne la réponse européenne à l'hégémonie des géants du numérique [3]. Né d'un constat alarmant — quelques mastodontes contrôlent désormais l'accès au monde digital — ce texte vise à rebattre les cartes. Son ambition est de redonner oxygène et possibilités aux marchés numériques, pour que l'innovation ne reste pas le privilège exclusif des GAFAM.

Le DMA s'attaque frontalement aux « contrôleurs d'accès », ces entreprises qui régissent notre quotidien numérique. Google, Meta, Amazon, Apple... Tous ces acteurs qui, grâce à leurs plateformes essentielles, connectent des millions d'utilisateurs et d'entreprises. Le texte reconnaît le mécanisme implacable des effets de réseau et des économies d'échelle créent des situations de verrouillage où le choix devient illusion.

Dans son arsenal, le règlement prévoit l'interdiction de pratiques commerciales jugées toxiques pour l'écosystème. Fini le blocage de l'interopérabilité qui emprisonne les utilisateurs. Terminée l'exploitation des données récoltées pour écraser la concurrence. Les plateformes devront jouer cartes sur table, avec une transparence accrue tant dans leurs opérations que dans leurs conditions d'accès.

Le bras armé du texte consiste en des sanctions qui parlent d'elles-mêmes : jusqu'à 10% du chiffre d'affaires mondial pour les contrevenants. Un message sans équivoque pour que les marchés numériques redeviennent ce qu'ils n'auraient jamais dû cesser d'être : des espaces ouverts où la concurrence stimule l'innovation au bénéfice de tous.

4 Règlement sur la gouvernance des données (Data Governance Act)

Le Règlement sur la gouvernance des données [4], adopté en 2022, représente un élément clé de la stratégie de l'Union européenne pour exploiter le potentiel des données numériques et renforcer sa souveraineté en matière de données. Ce règlement vise à améliorer les conditions de partage des données au sein du marché intérieur en

créant un cadre harmonisé pour la gouvernance des données non personnelles, facilitant ainsi la coopération entre les États membres et soutenant l'innovation et l'économie des données basées sur la confiance.

Le règlement établit des normes pour les mécanismes de partage des données et introduit de nouvelles structures comme les intermédiaires de données et les espaces communs européens de données dans des secteurs spécifiques tels que la santé, la mobilité et l'énergie. Il définit des obligations pour ces intermédiaires, garantissant qu'ils opèrent de manière transparente et sécurisée, et oblige les États membres à mettre en place des points de contact pour faciliter le partage transfrontalier de données.

Les contraintes imposées par le règlement incluent des exigences strictes en matière de protection des données et de cybersécurité, ainsi que le respect des principes de neutralité et de transparence dans l'accès aux données. Il vise également à prévenir les effets de verrouillage par des plateformes dominantes en assurant la portabilité des données et leur interopérabilité.

Le règlement n'impose pas directement des sanctions pour non-conformité, mais il établit un cadre pour que les États membres assurent la supervision et l'application des règles à travers des mesures nationales, qui doivent être efficaces, proportionnelles et dissuasives. En outre, il renforce le rôle des autorités nationales et de l'ENISA (Agence de l'Union européenne pour la cybersécurité) pour surveiller l'application des dispositions relatives à la cybersécurité dans ce contexte.

5 Règlement sur les services numériques (DSA)

Le Règlement sur les Services Numériques de l'Union européenne [5], promulgué pour répondre aux défis posés par l'utilisation croissante des services numériques, vise à harmoniser les règles pour les services intermédiaires dans le marché intérieur, tout en garantissant un environnement en ligne sûr et prévisible. Ce règlement, essentiel à l'ère numérique, s'attaque principalement à la gestion des contenus illicites en ligne et impose des obligations rigoureuses aux fournisseurs de services intermédiaires, y compris les plateformes en ligne.

Le DSA impose à ces fournisseurs la responsabilité de surveiller activement et de retirer les contenus illégaux, tout en respectant les droits fondamentaux tels que la liberté d'expression. Il instaure des mesures pour garantir que les informations sur les biens et services en ligne soient transparentes et fiables, contribuant ainsi à une meilleure protection des consommateurs. De plus, il exige des fournisseurs de services intermédiaires qu'ils assurent une plus grande transparence sur leurs algorithmes et facilitent l'accès des autorités nationales aux informations nécessaires pour superviser et appliquer la loi.

En cas de non-conformité, le DSA prévoit des sanctions significatives pour les entreprises, incluant des amendes pouvant atteindre des pourcentages élevés du chiffre d'affaires global. Ces sanctions visent à s'assurer que les règles ne sont pas simplement des recommandations mais des exigences strictes qui influencent la manière dont les services numériques opèrent au sein de l'UE. Le but ultime est de créer un marché numérique plus sûr et plus équitable, où les droits des utilisateurs sont protégés et les acteurs malveillants sont tenus responsables.

6 Règlement eIDAS

Le règlement eIDAS (Règlement UE N° 910/2014) établit un cadre juridique pour l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur de l'Union européenne [6]. Son objectif principal est de renforcer la confiance dans l'environnement numérique en facilitant l'utilisation transfrontalière et interopérable de l'identification électronique et en standardisant les services de confiance, comme les signatures électroniques, pour sécuriser les échanges électroniques.

Ce règlement répond à plusieurs besoins : la fragmentation du marché numérique, le manque d'interopérabilité entre les systèmes d'identification électronique des États membres et l'augmentation de la cybercriminalité. Il remplace la directive précédente qui traitait des signatures électroniques sans fournir de cadre complet et transfrontalier pour les transactions électroniques sécurisées.

Le règlement impose des obligations claires aux prestataires de services de confiance et aux États membres, notamment la reconnaissance mutuelle des moyens d'identification électronique notifiés, garantissant ainsi que les citoyens et entreprises peuvent utiliser leurs propres systèmes nationaux d'identification électronique partout dans l'UE. Cela comprend l'authentification et la signature électroniques sécurisées qui doivent être reconnues par tous les États membres.

En cas de non-conformité, le règlement prévoit des sanctions, notamment des amendes et autres mesures répressives pour garantir l'application des règles établies. Les sanctions visent à garantir que les prestataires de services de confiance et les autorités nationales prennent les mesures nécessaires pour respecter les exigences en matière de sécurité, de fiabilité et de reconnaissance mutuelle des services et identités numériques.

7 Directive NIS2

La directive NIS2 [7], adoptée en 2022, marque un tournant dans l'arsenal cybersécuritaire européen [7]. Succédant à une première version jugée trop timide, ce texte musclé répond aux cyberattaques de plus en plus sophistiquées qui menacent nos infrastructures critiques. Colonial Pipeline, SolarWinds, NotPetya... Ces incidents ont démontré notre vulnérabilité collective et la nécessité d'une riposte à l'échelle européenne.

NIS2 élargit considérablement son filet protecteur. Là où sa devancière se limitait à quelques secteurs essentiels, cette nouvelle mouture englobe désormais un spectre bien plus large d'entités, des fournisseurs d'énergie aux fabricants de dispositifs médicaux, en passant par les services numériques. Cette approche témoigne d'une prise de conscience : dans un monde hyperconnecté, la chaîne n'est solide que si tous ses maillons le sont.

La directive dessine une architecture de défense à plusieurs niveaux. Au sommet, les États membres doivent élaborer des stratégies nationales cohérentes et mettre sur pied des équipes de réponse aux incidents (CSIRTs). À l'échelon opérationnel, les organisations concernées doivent adopter des mesures de sécurité proportionnées à leurs risques et signaler rapidement tout incident significatif. Innovation notable : la directive établit des canaux pour le partage d'informations entre entités publiques et privées, brisant ainsi les silos traditionnels qui freinent la réponse collective.

Côté sanctions, NIS2 laisse aux États membres le soin de définir les pénalités, avec une exigence : elles doivent être « effectives, proportionnées et dissuasives ». Cette flexibilité permet une adaptation aux spécificités nationales tout en maintenant une pression suffisante pour garantir l'application du texte.

Cette directive incarne la conviction européenne qu'en matière de cybersécurité, aucun pays ne peut faire cavalier seul. Seule une approche coordonnée peut protéger efficacement notre tissu économique et social contre des menaces qui ignorent les frontières.

8 Règlement sur la cybersécurité (Cybersecurity Act)

Le Cybersecurity Act [8], règlement de l'Union européenne, renforce la confiance dans le marché numérique par le biais de la certification de cybersécurité des technologies de l'information et des communications. Il répond au besoin d'améliorer la cybersécurité à travers l'UE, face à l'augmentation des risques liés à une connectivité et numérisation accrues, particulièrement avec l'avènement de l'internet des objets.

Le règlement consolide l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, en lui donnant un mandat permanent pour aider au développement et à la mise en œuvre de politiques de cybersécurité. L'ENISA joue un rôle clé dans l'établissement d'un cadre de certification européen, visant à assurer que les produits, services et processus TIC respectent des normes de sécurité uniformes.

Les obligations imposées par ce règlement incluent la nécessité pour les États membres de reconnaître les certifications de cybersécurité issues de n'importe quel autre État membre, encourageant ainsi la coopération transfrontalière et la mutualisation des ressources et des informations. Les entités privées sont encouragées à adhérer volontairement à ces normes pour renforcer la confiance des consommateurs dans leurs produits et services.

En termes de sanctions, le Cybersecurity Act ne précise pas directement des pénalités pour non-conformité avec les normes de certification ; cependant, il instaure un système où le non-respect peut affecter la réputation et la crédibilité des entreprises sur le marché, mettant ainsi un accent sur le respect volontaire et la responsabilité des acteurs du marché.

9 Règlement sur la cyber-résilience (Cyber Resilience Act)

Le Cyber Resilience Act [9], proposé par la Commission européenne en 2022, s'attaque à un angle mort de la cybersécurité européenne : les produits connectés [9]. Avec la multiplication des objets intelligents dans notre quotidien, du réfrigérateur au thermostat, la surface d'attaque s'est démultipliée. Le coût mondial des cyberattaques a atteint le chiffre vertigineux de 5 500 milliards d'euros en 2021 — plus que le PIB de nombreux pays.

Ce texte novateur couvre tous les produits avec une dimension numérique, du grille-pain connecté aux routeurs en passant par les caméras de surveillance. Quelques secteurs échappent à son emprise, comme les dispositifs médicaux ou l'automobile, qui disposent déjà de leurs propres réglementations sectorielles.

Pour les fabricants, le message est clair : la sécurité doit être intégrée dès la conception (*security by design*), non comme une réflexion tardive. Fini les mots de passe par défaut identiques sur des millions d'appareils. Terminés les produits lancés avec des failles connues. Le texte impose des obligations concrètes : absence de vulnérabilités exploitables connues, processus de gestion des vulnérabilités, et fourniture de mises à jour de sécurité pendant au moins 5 ans. Toute vulnérabilité découverte devra être signalée à l'ENISA dans un délai de 24 heures.

Le règlement introduit une classification binaire selon le niveau de risque. Les produits critiques (classe II) comme les systèmes d'exploitation ou les microprocesseurs devront passer sous les fourches caudines d'organismes tiers notifiés pour obtenir leur certification.

La force de frappe du texte se mesure à ses sanctions : jusqu'à 15 millions d'euros ou 2,5% du chiffre d'affaires mondial pour les infractions graves. Une période transitoire de 24 mois laissera le temps à l'industrie de s'adapter, sauf pour les obligations de notification, applicables dès 12 mois après l'entrée en vigueur.

Cette législation pionnière cherche à établir un cadre harmonisé pour toute l'Union, évitant ainsi une fragmentation réglementaire qui nuirait autant à la sécurité qu'au marché unique.

10 Règlement sur l'intelligence artificielle (IA Act)

L'AI Act, adopté en 2024, représente le premier cadre réglementaire complet au monde sur l'intelligence artificielle [10]. Face à l'explosion des systèmes comme ChatGPT ou Midjourney, l'Europe a choisi de ne pas attendre les dérives pour agir. Ce texte pionnier vise un équilibre délicat : encadrer sans étouffer, protéger sans freiner l'innovation.

La philosophie du règlement repose sur une approche graduée selon les risques. Au sommet de la pyramide, certaines pratiques jugées inacceptables sont purement interdites : manipulation, notation sociale, identification biométrique en temps réel dans l'espace public (sauf exceptions strictement encadrées). Viennent ensuite les systèmes à haut risque dans des secteurs sensibles comme l'éducation ou la santé, soumis à des exigences draconiennes. Enfin, pour les systèmes interagissant avec les humains ou générant du contenu, la transparence devient maître-mot.

L'architecture des responsabilités dessine un écosystème où chaque acteur joue sa partition. Les fournisseurs doivent déployer des systèmes de gestion des risques, documenter leurs choix techniques, garantir la qualité des données et se plier à des évaluations indépendantes. Les utilisateurs professionnels, quant à eux, doivent rester vigilants et signaler tout incident grave. Un registre européen recensera tous les systèmes à haut risque.

L'innovation du texte porte sur l'encadrement spécifique des modèles d'IA fondamentaux comme GPT-4 ou Claude. Pour les modèles présentant des risques systémiques, des obligations renforcées s'appliquent : évaluations poussées, documentation des jeux d'entraînement, mesures d'atténuation des risques.

Avec ce texte, l'Europe trace une voie originale entre le laisser-faire américain et le contrôle étatique chinois. Une approche qui pourrait, comme jadis le RGPD, devenir un standard mondial par effet domino.

11 Directive droit d'auteur

La Directive sur le droit d'auteur dans le marché unique numérique, promulguée par l'Union européenne, vise à adapter le cadre législatif de la propriété intellectuelle aux nouvelles réalités du numérique [11]. Cette directive reconnaît la nécessité de moderniser la législation sur le droit d'auteur pour mieux refléter l'utilisation des œuvres protégées sur les plateformes numériques, garantissant ainsi une rémunération équitable des créateurs et des titulaires de droits dans l'environnement numérique.

Elle encadre plusieurs aspects, notamment les responsabilités des fournisseurs de services de partage de contenus et des agrégateurs de nouvelles, les exceptions au droit d'auteur pour l'enseignement et la préservation du patrimoine culturel, ainsi que la mise en place de mécanismes plus efficaces pour le contrôle et la rémunération des œuvres utilisées en ligne.

Les obligations incluent pour les plateformes et agrégateurs l'obligation de conclure des accords de licence avec les ayants droit pour l'utilisation de leurs contenus. Ces entités doivent aussi mettre en place des technologies de reconnaissance de contenus et assurer des mécanismes de plainte et de recours rapides et efficaces pour les utilisateurs et les titulaires de droits.

En cas de non-respect de ces directives, des sanctions peuvent être appliquées par les autorités nationales compétentes, allant jusqu'à des amendes substantielles déterminées par le cadre législatif de chaque État membre de l'UE, assurant ainsi le respect des droits d'auteur dans le marché unique numérique.

12 Règlement sur le libre flux des données à caractère non personnel

Le règlement (UE) 2018/1807, aussi appelé règlement sur le libre flux des données à caractère non personnel, a été établi pour répondre à la nécessité de faciliter la libre circulation des données non personnelles à travers l'Union européenne [12]. Ce règlement vise à supprimer les obstacles au stockage et au traitement des données à travers les frontières de l'UE, contribuant ainsi à l'achèvement du marché unique numérique et à la compétitivité économique de l'Europe.

Ce cadre législatif s'adresse principalement à la suppression des exigences de localisation des données imposées par les États membres, qui limitent où les données peuvent être stockées et traitées. Il rend illégales les restrictions

imposées par les gouvernements des États membres qui exigent que les données soient stockées ou traitées sur leur territoire national, sauf pour des raisons de sécurité publique. Le règlement souligne également la nécessité de supprimer les obstacles liés aux pratiques de marché qui limitent la mobilité des données non personnelles.

Concernant les obligations, le règlement exige que les États membres, ainsi que les fournisseurs de services de traitement de données, facilitent la libre circulation des données non personnelles. Les entreprises sont encouragées à adopter des pratiques qui ne restreignent pas la localisation des données, à l'exception de celles qui sont nécessaires pour des raisons de sécurité publique.

Les sanctions en cas de non-respect de ce règlement ne sont pas explicitement détaillées dans le texte lui-même mais sont laissées à la discrétion des États membres. Ces derniers doivent établir des mesures punitives qui sont effectives, proportionnelles et dissuasives pour garantir le respect du règlement.

Ce règlement est essentiel pour garantir que les données non personnelles puissent circuler librement à travers l'Union européenne sans être injustement restreintes par des localisations spécifiques, facilitant ainsi une plus grande innovation et une meilleure efficacité économique au sein du marché unique numérique.

Références

[1] Stratégie européenne pour les données, Commission européenne, 2020.

[2] Règlement général sur la protection des données, Union européenne, 2016.

[3] Règlement sur les marchés numériques, Union européenne, 2022.

[4] Règlement sur la gouvernance des données, Union européenne, 2022.

[5] Règlement sur les services numériques, Union européenne, 2022.

[6] Règlement sur l'identification électronique et les services de confiance, Union européenne, 2014.

[7] Directive sur la sécurité des réseaux et des systèmes d'information (NIS2), Union européenne, 2022.

[8] Règlement sur la cybersécurité (Cybersecurity Act), Union européenne, 2019.

[9] Règlement sur la cyberrésilience (Cyber Resilience Act), Commission européenne, 2022.

[10] Règlement sur l'intelligence artificielle (IA Act), Union européenne, 2024.

[11] Directive sur le droit d'auteur dans le marché unique numérique, Union européenne, 2019.

[12] Règlement sur le libre flux des données à caractère non personnel, Union européenne, 2018.