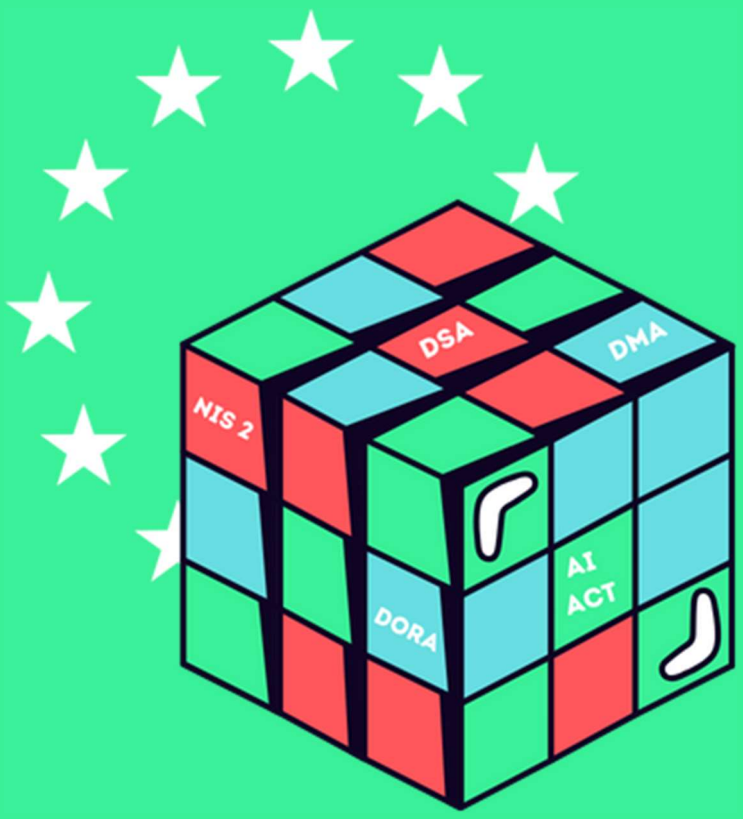
Renaissance Numérique



NOVEMBRE 2024

NOTE

Politique numérique de l’UE : l’heure de la cohérence a sonné

Table des matières

Une politique numérique dépourvue de vision d'ensemble

Dans le tumulte de la transformation numérique de nos sociétés, les cinq dernières années d'activité du Parlement et de la Commission européenne ont été marquées par une succession de réglementations[1] dans la foulée de l'entrée en application du Règlement général sur la protection des données (RGPD)[2] en 2020. Si bien que l'empilement de législations parallèles touchant au numérique[3] [4] laisse désormais entrevoir un paysage juridique aussi complexe que fragmenté.

Il ne fait aucun doute que chaque pièce du puzzle législatif européen avait sa raison d'être sectorielle ou systémique. Il ne s'agit donc pas d'interroger les motivations légitimes de chaque chantier législatif. Elles sont publiques, elles méritaient d'être soutenues, elles ont été débattues puis arbitrées dans le respect des institutions politiques et de leurs missions profondes.

Au demeurant, en matière d'architecture comme en matière de régulation, l'édifice ne tient que par l'imbrication et l'adhérence des éléments qui le composent. Un tas de pierres ne fait pas un bâtiment sans une vision d'ensemble et une gouvernance transverse aux divers corps de métiers. Cette vision, en architecture comme en création en général, n'est pas la somme des objets que l'on juxtapose, mais l'espace laissé par leur juxtaposition. En matière de régulation comme en matière d'architecture, il ne suffit pas que les fondations soient posées et que le bâtiment soit hors d'eau, pour qu'il soit habitable. Une fois la loi votée, des décrets et lignes directrices sont nécessaires pour préciser les détails du texte et pour organiser la coordination avec des normes préexistantes.

Et c'est là que le bât blesse : alors qu'elle n'a pas pris le temps d'effectuer les finitions pour les textes adoptés récemment, la Commission européenne semble être déjà passée au chantier législatif suivant. Cela alors même que des conflits entre régulateurs apparaissent et s'ajoutent aux conflits entre normes, faisant naître des injonctions contradictoires, dont chacune est assortie de sanctions et d'un juge, mais sans règlement d'arbitrage, autre que juridictionnel et répressif.

Les conséquences délétères de ce foisonnement réglementaire non-abouti commencent à se faire sentir, préfigurant des difficultés dans la mise en œuvre et l'articulation des

[1] Bruegel, "Overview of EU Legislations in the Digital Sector", November 2023: https://www.bruegel.org/sites/default/files/private/2023-11/Bruegel_factsheet.pdf

[2] 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

[3] "Pause réglementaire dans la tech ? Pas avec tous ces textes européens à rouvrir", *Contexte*, 7 juin 2024 : https://www.contexte.com/article/tech/les-clauses-de-rendez-vous-deja-connues_188238.html

[4] IAAP, Organizational Digital Governance Report 2024 p. 17: https://iapp.org/media/pdf/resource_center/organizational_digital_governance_report.pdf

textes adoptés ces dernières années. Les entreprises et les acteurs publics se retrouvent parfois désemparés, confrontés à une myriade de législations dont l'applicabilité et la conformité sont devenues des défis (notamment du fait de leur coût financier, en particulier pour les plus petites entreprises[5]). En outre, l'identification du régulateur compétent se conjugue de plus en plus au pluriel, et l'arbitrage entre les différents textes relève davantage de l'espérance que d'un mécanisme établi.

La genèse d'un mille-feuille législatif

Avant 2020

L'actualité réglementaire de ces dernières années a été largement dominée par les travaux relatifs à deux textes majeurs.

D'une part, le RGPD. Adopté le 27 avril 2016 après quatre années de débat, il a fait l'objet de plus d'amendements qu'il n'y en eut durant 25 années de construction de la Politique agricole commune. Entré en application le 25 mai 2018, il a remplacé la Directive 95/46 du 24 octobre 1995[6], qui était jusqu'alors le socle commun européen en matière de protection et de circulation des données à caractère personnel. Le RGPD promettait aux citoyens européens et au reste du monde d'offrir une vision et une interprétation commune et homogène de la protection des données telle que les valeurs de l'Union européenne l'envisagent.

D'autre part, le projet de Règlement e-Privacy[7], qui est immobilisé depuis sept ans en raison de divergences entre les États membres, a vocation à établir des règles spécifiques pour la fourniture et l'utilisation de services de communications électroniques – en somme, l'internet en général. Ce projet de règlement a eu pour vocation de mettre à jour, une fois le RGPD nouvellement adopté, la directive 2002/58/CE, dite directive "e-Privacy"[8]. En novembre 2024, il se fait encore attendre, laissant des lacunes d'interprétation à un ensemble de régulateurs qui ne sont pas

[5] Une analyse d'impact produite par la Commission européenne dans le cadre de l'AI Act montre que, pour une entreprise de 50 employés, la mise sur le marché d'un seul produit doté d'IA pourrait entraîner des coûts de mise en conformité allant de 216 000 à 319 000 euros. Commission européenne (2021), "Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe", Final Report (D5): https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1

[6] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31995L0046

[7] Règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017PC0010

[8] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32002L0058

toujours ceux du RGPD, ou qui n'ont aucune obligation de s'accorder sur des interprétations communes aux défis d'aujourd'hui : géolocalisation, publicité ciblée, exploitation des données de trafic, prospection électronique, etc.

Parallèlement à l'adoption progressive de ces deux textes majeurs, Thierry Breton, le Commissaire européen chargé du marché intérieur de 2019 à 2024, a orchestré un vaste mouvement législatif visant tantôt à compléter des réglementations existantes, tantôt à adopter de nouvelles réglementations, ajoutant ainsi des couches de régulation dans des domaines en perpétuelle évolution.

Depuis 2020

Depuis 2020, deux grandes séries de textes ont été promulguées. La première met à jour des textes existants, renforçant ou redistribuant les pouvoirs des régulateurs déjà en place. C'est le cas par exemple des nouveaux pouvoirs – notamment de sanction – conférés en France à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) par la Directive sur la sécurité des réseaux et des systèmes d'information[9], dite "NIS 2"[10]. La seconde série de textes concerne de nouvelles réglementations dépourvues de régulateurs attitrés, laissant aux États membres la responsabilité de la mise en œuvre et de l'interprétation de ces textes, au gré de dynamiques nationales, accroissant les pouvoirs de certains régulateurs, privant d'autres d'une partie de leurs prérogatives ou créant de nouveaux entrants sur ce marché en pleine effervescence de la régulation numérique.

On doit cette plasticité au programme lancé en 2019 par Thierry Breton, le *Digital Decade 2020-2030*, ou "décennie numérique de l'Europe"[11], qui établit de grands axes de développement numérique. Traditionnellement, de telles annonces définissent le mandat législatif de chaque nouvelle Commission, à la suite des élections du Parlement européen. En l'espèce, Thierry Breton a pris le soin d'éviter d'articuler entre eux les grands principes et textes antérieurs, afin d'éviter des blocages politiques et institutionnels. En abordant des thématiques diverses de façon concomitante, la Commission européenne a ainsi pu repousser à plus tard, au stade de l'application des textes, le « combat des chefs », entre des régulateurs complémentaires ou antagonistes,

[9] Renaissance Numérique, "7 recommandations sur le projet de loi de transposition de la Directive NIS2", avril 2024 : https://www.renaissancenumerique.org/publications/directive-nis2/

[10] La Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau commun élevé de cybersécurité dans l'Union, dite "NIS2", est la révision de la directive NIS de 2016. Elle vise à harmoniser les exigences en matière de cybersécurité pour les États membres et les entreprises, en tenant compte de nouveaux défis dans le domaine de la sécurité des réseaux et des systèmes d'information.

[11] Commission européenne, Décennie numérique de l'Europe : objectifs numériques pour 2030 : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

chargés des données personnelles et des libertés individuelles, des médias et des contenus, de la protection des consommateurs ou des mineurs, de la concurrence, de la cybersécurité, de la résilience opérationnelle, des plateformes et des acteurs systémiques, de l'intelligence artificielle, de la souveraineté technologique, etc.

À titre d'exemple, il est d'usage d'entendre parler du couple « DMA/DSA »[12] alors même que ces textes n'ont pas le même champ d'application. Ou d'associer le Digital Governance Act et le Data Act pour les aborder dans leur globalité, comme deux instruments convergents de régulation. Et d'employer des concepts dans différents contextes pour tracer de nouvelles pistes de régulation, comme c'est le cas avec la notion de *"very large online platform"* (« très grande plateforme en ligne ») tirée du DSA, qui est parfois reprise dans le contexte de la liberté du consentement au sens du RGPD. Tout cela pose la question de la coordination réglementaire et de la vision d'ensemble en cas de conflits de normes.

Quatre grands secteurs objets de régulations spécifiques

Les plateformes et les services d'intermédiation

- Le Règlement sur les marchés numériques (Digital Markets Act[13] ou DMA en anglais) du 14 septembre 2022, vise à lutter contre les pratiques anticoncurrentielles des géants du numérique et à corriger les déséquilibres de leur domination sur le marché européen tout en renforçant la protection des utilisateurs en ligne. Progressivement applicable depuis le 2 mai 2023, il est entièrement entré en vigueur le 6 mars 2024, date depuis laquelle les géants du numérique doivent respecter de nouvelles obligations et interdictions sous peine de lourdes amendes.
- Le Règlement sur les services numériques (Digital Services Act[14] ou DSA en anglais) du 19 octobre 2022, décline le principe selon lequel ce qui est illégal hors ligne est illégal en ligne. Il fixe un ensemble de règles pour responsabiliser les plateformes numériques dans la lutte contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux (images pédopornographiques, attaques racistes, désinformation, vente de drogues ou de contrefaçons).

[12] Commission européenne, En avant-première : comment la Commission appliquera la DSA et la DMA - Blog du Commissaire Thierry Breton : https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_4327
[13] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
[14] Règlement (UE) 2022/2065 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

La stratégie européenne pour les données[15]

- Le Data Governance Act[16], applicable à compter du 24 septembre 2024, vise à garantir l'accès à de grands volumes de données au profit de l'économie européenne. Il organise également un contrôle afin de préserver la souveraineté numérique de l'Union européenne. En outre, cette réglementation permet d'articuler l'accès ouvert aux données avec le RGPD.
- Le Data Act[17] s'appliquera à compter du 12 septembre 2025. Ce texte vise à favoriser l'ouverture accrue des données provenant de l'internet des objets, afin de stimuler le développement d'une économie de la donnée compétitive, bénéfique tant aux utilisateurs qu'aux entreprises européennes.

Enfin, il est envisagé de créer des espaces européens communs de données spécifiques à certains domaines, en débutant avec un espace européen de données de santé (European Health Data Space ou EHDS, en anglais)[18].

L'intelligence artificielle

L'intelligence artificielle (IA) fait l'objet d'une régulation spécifique : le Règlement sur l'intelligence artificielle[19] (AI Act en anglais), dont l'ambition est de veiller à ce que les systèmes d'IA mis sur le marché européen et utilisés au sein de l'UE soient fiables et respectent les droits fondamentaux et les valeurs de l'UE. Pour cela, le texte met l'accent sur la transparence, la responsabilité et la sécurité des systèmes d'IA. La Directive sur la responsabilité de l'IA[20], proposée le même jour que l'AI Act, a pour sa part l'objectif de définir les règles de responsabilité civile applicables aux systèmes d'intelligence artificielle, afin de garantir la sécurité et la protection des droits des citoyens européens.

Les responsables politiques de l'Union européenne se sont félicités du calendrier rapide d'adoption du Règlement sur l'IA, montrant que l'Union européenne était à la pointe de la régulation. Cependant, il est à craindre que le temps passé à organiser de façon

---

[15] Commission européenne, "Stratégie européenne pour les données" : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_fr

[16] Règlement (UE) 2022/868 du Parlement européen et du Conseil portant sur la gouvernance européenne des données : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

[17] Règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

[18] Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197

[19] Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0206

[20] Directive du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52022PC0496

cohérente cette régulation et son interprétation sera très long, pour plusieurs raisons structurelles.

En premier lieu, chaque État membre désignera son régulateur de l'IA, soit nouveau, soit parmi des régulateurs existants. Durant les premières années d'application de l'AI Act, chacun devra également arbitrer – ou laisser perdurer – des conflits de compétences entre régulateurs (protection des données personnelles, sécurité, concurrence et protection des consommateurs) et avec les autorités judiciaires qui auront la tâche de mettre en œuvre un mécanisme européen de responsabilité civile – qui reste encore à définir.

En second lieu, cette division en deux textes, régissant d'une part, les principes et les obligations mais pas les régulateurs et d'autre part, un régime harmonisé de responsabilité civile au sein de l'Union européenne, ne deviendra lisible qu'à l'issue d'une multitude de décisions de la Cour de Justice de l'Union européenne, c'est-à-dire… pas avant quelques années.

La cybersécurité et la cyber-résilience

La cybersécurité et la cyber-résilience font l'objet de plusieurs textes :

- La Directive sur la sécurité des réseaux et des systèmes d'information (dite « Directive NIS 2 »), adoptée le 27 juin 2021, s'appuie sur les acquis de la Directive NIS 1. Ses objectifs sont le renforcement du niveau de sécurité des sous-traitants en contact avec des infrastructures critiques, l'intégration des collectivités territoriales dans le périmètre de la directive et l'élargissement des secteurs concernés, passant de 19 à 35 (dont la gestion des déchets, les services postaux ou l'agroalimentaire).
- Le Cyber Resilience Act[21], élaboré sur la base de la stratégie de cybersécurité de l'UE de 2020[22], introduit également des règles communes en matière de cybersécurité pour les fabricants et les développeurs de produits comportant des éléments numériques, couvrant à la fois le matériel et les logiciels. L'objectif de ce texte est de protéger les consommateurs et les entreprises des risques en matière de cybersécurité dans leur utilisation des matériels filaires et connectés, ainsi que des logiciels.

[21] Règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

[22] Commission européenne, "La stratégie de cybersécurité" : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

- Enfin, le 16 janvier 2023, le Règlement sur la résilience opérationnelle numérique (dit « Règlement DORA »)[23] est entré en vigueur, après son adoption par le Conseil de l'Union européenne en novembre 2022. Il s'agit d'un cadre réglementaire innovant, qui s'attaque aux risques posés par la profonde transformation numérique des services financiers, l'interconnexion croissante des réseaux et des infrastructures critiques, ainsi que par la multiplication des cyberattaques, de plus en plus sophistiquées, à l'encontre des acteurs du secteur financier. Le Règlement DORA apporte, dans un seul acte législatif et pour la première fois de l'histoire de l'Union européenne, un cadre détaillé et complet sur la résilience opérationnelle numérique pour les entités financières – pour le moment. Il prévoit également la mise en place d'un mécanisme de surveillance directe des prestataires de services informatiques au niveau de l'UE.

La cohésion législative : grand impensé de la politique numérique européenne

À la suite de cette période de foisonnement réglementaire, le Commissaire européen Thierry Breton a démissionné et été remplacé. Dans un rapport intitulé *The future of European competitiveness*, l'ancien président de la Banque centrale européenne, Mario Draghi, identifie la lourdeur réglementaire européenne comme un obstacle au passage à l'échelle de jeunes pousses dans le secteur de la tech[24]. L'Union européenne semble en difficulté lorsqu'il s'agit d'appliquer ses propres règles, à elle-même comme à l'égard d'acteurs extra-européens. Il est donc nécessaire d'évaluer le bilan du paysage réglementaire dans lequel l'Union européenne a choisi de vivre son avenir numérique.

Il semble d'abord indispensable de le contextualiser : la promulgation de ces textes est intervenue alors que l'Union européenne se trouve à un tournant électoral et géopolitique, engagée dans des débats existentiels portant sur divers sujets tels que la réforme de la Politique agricole commune, les dépendances sanitaires, l'énergie, les infrastructures informatiques d'hébergement et de calcul, exacerbés par les bouleversements climatiques et les tensions géopolitiques accentuées par la guerre en Ukraine et l'embrasement du Moyen-Orient.

---

[23] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2554

[24] Mario Draghi, "The future of European competitiveness. Part A: A competitiveness strategy for Europe", September 2024 : https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

Par ailleurs, l'Union européenne superpose des obligations réglementaires susceptibles d'entraîner de nombreux conflits de compétences entre régulateurs anciens et nouveaux, puisque plusieurs d'entre eux seront immanquablement chargés d'un même objectif législatif ou d'objectifs divergents nécessitant des arbitrages. Le tout sans arbitre ni procédures d'arbitrage. À titre d'exemple, la question du profilage des personnes n'est pas abordée de la même manière dans le RGPD que dans le Règlement sur l'intelligence artificielle, dont l'Union européenne se targue de la vitesse d'élaboration. Or, la régulation de l'IA agite la plupart des États du monde et, dans chaque État, de nombreux régulateurs existants ou en devenir pour la réguler. La superposition des règles et des compétences liées à la conception ou à l'utilisation de l'IA est déjà, en 2024, un millefeuille de normes et de compétences réglementaires dont le simple inventaire est fastidieux et la priorisation hypothétique.

Lorsque les plus grands acteurs de l'IA renoncent à déployer leurs services dans certaines régions dont l'insécurité juridique leur paraît trop élevée, leur recul face au défi réglementaire européen doit nous interroger. Si l'Europe leur fait peur, doit-on s'en réjouir ou s'en inquiéter pour nos propres entreprises ? Mesure-t-on ce que cela dit du poids de cette insécurité réglementaire pour une entreprise d'origine européenne ?

Dans un autre secteur, lorsqu'une entreprise est à la fois un opérateur d'importance vitale et une banque ou un assureur, se pose la question de savoir si elle doit appliquer le Règlement DORA ou la Directive NIS 2, et si elle doit se concevoir comme un organisme financier régulé ou comme un prestataire informatique. De telles interrogations n'ont pas été envisagées par le législateur européen. Elles sont apparues une fois les textes juxtaposés et soumis à l'analyse de régulateurs provenant d'horizons différents : ici, la cybersécurité et la régulation financière.

Les régulateurs chargés de la protection des consommateurs, de la liberté de communication et de la protection des mineurs, sont différents, ce qui rend la clarification de leurs prérogatives difficile, voire impossible à anticiper, lorsqu'il s'agit de déterminer dans quelle mesure ils doivent s'appuyer sur le DSA, sur le RGPD, sur le droit de la consommation ou sur le droit de la concurrence, pour exercer leurs leviers d'action. Le secteur de l'audiovisuel s'interroge, de son côté, sur l'articulation entre le DSA et la directive Services de médias audiovisuels (SMA).

Sur la cybersécurité, le règlement DORA donne une place aux régulateurs financiers, les amenant loin de leurs métiers de base. Malheureusement, ils n'ont pas – et n'auront jamais – en interne le niveau de compétence des régulateurs dédiés à la cybersécurité, avec lesquels ils devront nécessairement s'articuler. Les modalités de la coopération sont pour l'instant floues, et la question ne pourra que difficilement être tranchée par une juridiction, dont ce n'est pas le rôle de gérer la coopération technique entre autorités administratives indépendantes.

Face à ces complexités exacerbées, le contentieux réglementaire et judiciaire risque de précéder la clarté de la norme et la prévisibilité de sa régulation. Pour éviter d'en arriver là, il est plus que jamais indispensable de combler le travail incomplet de la législature européenne précédente : une fois qu'une obligation est posée, qui la fait appliquer, avec quelle cohérence, quels arbitrages en cas de conflits de compétences, et à quelle vitesse ?

La recherche de solutions d'harmonisation et de rationalisation du puzzle législatif du numérique européen est une urgence. Elle est indispensable pour assurer une application cohérente et efficace des règles, et éviter des conflits entre les autorités compétentes. C'est une mission qui incombe aux politiques, pas aux juridictions, et encore moins à des arrangements entre régulateurs.

En substance, à force de combler des poches dites de « non-droit », le droit européen du numérique comporte des zones de « sur-droits » ou de « plusieurs droits ». Non par oubli de désigner des régulateurs, mais par leur superposition, sans mécanisme de cohérence transverse. Tous ces régulateurs seront légitimes. Tous seront attachés à leur pré-carré. Aucun ne cèdera un pouce de prérogatives à un autre, à moins d'y être forcé. Mais aucun n'y est forcé. Aucun n'a pour mission d'avoir une vision globale d'une activité, d'un socle d'obligations compatibles et d'une efficacité sociétale pour garantir le respect de l'ensemble des règles – toutes légitimes – qui s'amoncèlent.

Le pouvoir judiciaire : solution au manque de cohésion règlementaire ?

Cette vague d'adoption de textes législatifs a coïncidé avec les premières années de mise en œuvre du RGPD, qui ont bénéficié de deux sources de clarification principales : le Comité Européen pour la Protection des Données (CEPD), instauré par le RGPD, et la Cour de Justice de l'Union européenne (CJUE), y compris dans des domaines non prévus par les législateurs.

Par exemple, en 2016, l'adoption de deux textes – le RGPD et la Directive « Police-Justice »[25] – le même jour, semblait distinguer les enjeux de sécurité publique et de justice d'une part, et la vie privée dans les activités commerciales et privées d'autre part. Cependant, la CJUE a décidé d'appliquer la Charte européenne des droits de l'homme pour articuler les enjeux de sécurité nationale avec les principes du RGPD, alors même

[25] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L0680

que l'Union européenne n'avait jamais défini ni adopté de notion de « sécurité nationale » auparavant, puisqu'aucun État membre n'est habilité à céder ce pan de sa souveraineté à des arbitrages communautaires.

Ainsi, il devient évident que le pouvoir administratif et judiciaire, délégué à des autorités et des juges indépendants sur lesquels les pouvoirs exécutifs et les parlements nationaux ou européens n'ont aucune prise, sera chargé d'articuler ces textes entre eux. Cependant, les régulateurs et les juridictions n'en ont ni la prérogative, ni la culture, ni le mandat institutionnel. Qui plus est, dans chaque État, la séparation des pouvoirs se manifeste par une véritable articulation entre eux. Lorsque le législatif se réduit, l'exécutif peut accroître sa sphère de compétence, ce qui peut entraîner des arbitrages, souvent d'ordre constitutionnel.

Dans le droit européen, ce qu'on appelle le « principe de subsidiarité » constitue une stratification des compétences respectives de l'UE et des États membres, mais ne garantit pas leur articulation. Lorsque le législateur européen adopte des droits ou des principes qui confèrent des prérogatives à des justiciables européens, qui instituent des sanctions et qui laissent aux États membres le soin de désigner des régulateurs compétents, l'absence d'articulation entre l'échelon national et l'échelon européen estompe mécaniquement la chaîne d'interprétation et incite à recourir au juge.

Or, aucun recours juridictionnel devant la CJUE ne permettrait à un même justiciable d'interroger en une seule fois des décisions divergentes émises par plusieurs régulateurs chargés d'appliquer des textes différents. L'office du juge consiste à examiner si chaque régulateur a ou non commis une erreur d'interprétation du texte dont il a la charge. Il ne consiste pas à arbitrer des strates législatives à la place du législateur, ni à se prononcer sur l'opportunité ou la priorité à appliquer un texte plutôt qu'un autre. Cet exercice est réservé aux Cours constitutionnelles des États membres ou, lorsque la Convention européenne de Sauvegarde des Droits de l'Homme est concernée, à la Cour européenne des droits de l'homme (CEDH). Stratégiquement, pour éviter un tel arbitrage de principes et d'interprétations antagonistes, il suffit de ne pas saisir la CEDH, ou de ne pas être habilité à la saisir.

Lorsque les adversaires d'un texte ne parviennent pas à l'empêcher devant le législateur européen, ils peuvent ainsi compter sur le désintérêt européen pour la mise en œuvre effective des textes adoptés. Ce désintérêt se traduit souvent par l'absence d'ambition concernant leur exécution, au motif que les institutions européennes s'en remettront à la (mauvaise, variable, incohérente) volonté des États membres.

Il est alors légitime de se demander si nous n'assistons pas à un glissement allant de la séparation des pouvoirs à l'isolement des pouvoirs. Lorsque les États membres

délèguent eux-mêmes la compétence d'exécution (réglementaire) à des régulateurs indépendants, ils s'en remettent à des administrations, certes indépendantes, mais dépourvues de tout pouvoir d'articulation de leurs compétences respectives. La démocratie fédérale nous a appris que des lois sans pouvoir fédéral génèrent des conflits de compétences et une inefficacité réglementaire. *In fine*, nous pouvons alors nous demander si l'isolement des pouvoirs ne mène pas à l'inefficacité du droit…

Faut-il autant légiférer quand on n'envisage pas le risque du cumul d'injonctions parfois contradictoires ? La question est légitime quand, faute de penser à se doter des moyens de l'exécution des lois, on n'envisage plus que de sanctionner leur inexécution. L'Union européenne s'illusionne parfois du montant des sanctions que prononcent ses autorités juridictionnelles, alors que :

- des sanctions de la violation de la loi ne rétablissent aucun équilibre concurrentiel ou économique : elles ne ressuscitent pas les entreprises mortes d'injustices concurrentielles ou du trop-plein législatif. Elles constatent seulement l'échec à faire respecter la loi ;
- des sanctions exemplaires n'imposent pas une règle à des acteurs capables de la contourner ou d'y survivre. Elles effraient les concurrents – européens – des acteurs dominants, incapables d'accéder à la sophistication du droit et à la complexité de son articulation dans la prise de décisions et de risques stratégiques.

Quelles priorités pour la nouvelle mandature européenne ?

Afin de dépasser cette situation, il est impératif que la nouvelle mandature européenne œuvre à la mise en place de textes de procédure et d'interprétation afin de garantir une articulation efficace entre les grands textes législatifs européens.

Selon la célèbre formule de Jean-Claude Junker, *"Nous savons tous ce qu'il faut faire, mais nous ne savons pas comment être réélus après l'avoir fait"*. Certes, écrire des procédures est fastidieux et n'a jamais fait élire ou réélire personne. Mais c'est ce qui fait l'efficacité ou l'inefficacité d'une norme et, par conséquent, d'une volonté politique. Cette mesure de rationalisation réglementaire, bien que susceptible de donner l'impression de ralentir les processus, vise en réalité à assurer une efficacité transverse du droit européen du numérique.

Dans cette optique, et dans la continuité des lignes directrices du CEPD du 14 mars 2022 relatives à l'application de l'article 60 du RGPD sur la « coopération entre l'autorité de

contrôle chef de file et les autres autorités de contrôle concernées »[26], le CEPD a déjà affirmé sa volonté de renforcer la coopération transfrontalière entre les autorités de protection des données des États membres de l'UE, afin de garantir l'application efficace et cohérente du RGPD[27].

De même, il est crucial de créer des mécanismes permettant de coordonner les différents textes législatifs, en particulier les textes qui sont, à tort ou à raison, souvent couplés tels que le DMA/DSA, la Directive NIS 2/le Règlement DORA, ou encore le RGPD/le Règlement sur l'intelligence artificielle/le Data Act et le Data Governance Act. Un tel regroupement réglementaire n'est pas envisageable sans prendre en compte les niveaux nationaux : les régulateurs compétents peuvent être nouveaux ou existants, mais leur collaboration n'a parfois pas été prévue par le législateur européen.

En complément, il devient urgent de réaliser, pour l'ensemble des textes évoqués, des analyses d'impact qui ne soient pas uniquement des analyses de mise en œuvre. Certes, ces dernières doivent permettre de constater si les législations en question ont porté leurs fruits. Mais elles doivent également permettre d'interroger leurs potentiels effets négatifs, leur pertinence a posteriori, d'éventuels manquements, le coût de la mise en conformité pour les différents acteurs concernés, ou encore de potentielles contradictions avec d'autres textes.

Enfin, il est essentiel d'agir rapidement, car les conflits de compétences et les défis d'articulation engendrent non seulement de l'inefficacité, mais aussi et peut-être surtout de l'injustice et de l'insécurité. En d'autres termes, lorsque plusieurs objectifs louables sont juxtaposés sans se soucier de leur articulation, toutes les protections et garanties espérées peuvent produire des effets inverses et, a minima, aucun effet espéré.

[26] CEPD, Lignes directrices 02/2022 relatives à l'application de l'article 60 du RGPD : https://www.edpb.europa.eu/system/files/2022-10/guidelines_202202_on_the_application_of_article_60_gdpr_fr.pdf

[27] CEPD, Propositions pour une meilleure harmonisation de l'application du RGPD : https://www.edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

Auteur

Etienne DROUARD
Avocat associé, Hogan Lovells (Paris)

Contributeurs

Jessica GALISSAIRE
Responsable des études et des partenariats, Renaissance Numérique

Anissa KEMICHE
Déléguée aux Affaires européennes, Numeum

Samuel LE GOFF
Président, Renaissance Numérique

Jean-Luc SAURON
Haut fonctionnaire et Professeur, Université Paris Dauphine - PSL

Rayna STAMBOLIYSKA
Présidente, RS Strategy

Directeur de la publication

Jean-François LUCAS
Délégué général, Renaissance Numérique

À propos

Créé en 2007, Renaissance Numérique est un think tank indépendant dédié à la transformation numérique de la société. Il œuvre à éclairer les évolutions que cette transformation entraîne et à donner à chacun les clés de sa maîtrise.

Renaissance Numérique est un lieu de débat et de confrontation positive d'expertises et d'idées. Il réunit des universitaires, des personnalités, des organisations non gouvernementales ou encore des entreprises. Ses réflexions, largement diffusées via des contributions, publications et des événements, sont portées auprès d'acteurs publics comme privés, au niveau français, européen et international.

Renaissance Numérique est membre de l'Observatoire de la haine en ligne porté par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et du comité d'organisation du Forum sur la Gouvernance de l'Internet (FGI) France.

Renaissance Numérique

Koburo, 35 rue Chanzy – 75011 Paris
www.renaissancenumerique.org

Novembre 2024