la villa numeris

Position paper

RGPD : réviser pour simplifier

Printemps 2026

Sommaire

Remerciements

Nos travaux ont été menés sous la direction de **Jeanne Bossi Malafosse**, avocate au Barreau de Paris, que nous remercions chaleureusement, ainsi que les personnalités qui ont répondu à nos questions dans le cadre d'auditions, **Michel Combot**, ancien directeur des technologies de la CNIL, **Thomas Dautieu**, directeur de l'accompagnement juridique, CNIL, **Thomas Honnet**, délégué à la protection des données, Ville de Marseille, **Patricia Le Large**, déléguée à la protection des données, Orange France, **Fabrice Mattatia**, délégué à la protection des données, Ministère de l'intérieur, **Hugues de Maupeou**, Government Affairs and Public Policy Manager, Google France, **Juliette Rouilloux-Sicre**, Group Data Protection Officer, Thales et **Laurent Teyssandier,** délégué à la protection des données, Criteo, et toutes celles et tous ceux qui ont préféré garder l'anonymat.

Merci à **France Charruyer,** associée fondatrice d'Altij Avocats et présidente de l'association d'intérêt général Data Ring, **Clothilde Hocquard**, Regulatory Affairs and Advocacy Lead, France Digitale, **Nathalie Laneret**, directrice des Affaires publiques, Criteo, **Ariane Thomas**, directrice Tech du développement durable, L'Oréal, et **Olivier Esper**, responsable relations institutionnelles, Google France, pour leur éclairage et contribution, et à **Arthur Brodmann** pour sa relecture attentive.

Le point de vue de Mykaïa

Avant-propos

Percevant, de la part de ses membres et du marché, la nécessité de lancer une réflexion sur l'évolution du Règlement général sur la protection des données (RGPD), La villa numeris avait pris l'initiative dès l'été 2025, de mener des travaux en ce sens, fort de premières publications «RGPD: 5 ans, ça se fête?» en 2023, et de travaux soutenus sur les transferts internationaux de données.

Précision méthodologique

Prenant acte que la Commission européenne a communiqué son projet d'omnibus visant à simplifier les règles européennes applicables aux données en incluant le RGPD dans son périmètre, La villa numeris a réorienté ses travaux pour se livrer à une première analyse du projet d'omnibus sur la base d'auditions de personnalités reconnues pour leur expertise (dirigeants d'entreprises, juristes, DPO d'organisations publiques et privées, régulateurs) et d'un travail de réflexion porté par Jeanne Bossi Malafosse, avocate au Barreau de Paris.

La note de position qui suit repose sur ces entretiens et sur cette réflexion. Les citations entre guillemets sont issues des auditions menées par La villa numeris auprès de dirigeants et d'experts dont la plupart ont souhaité garder l'anonymat pour conserver une liberté de ton avec le souci de ne pas engager publiquement leurs organisations et les exposer à des controverses sur un sujet par nature polémique. De fait, nous avons choisi de n'attribuer aucune citation dans la mesure où celles-ci reflètent un sentiment majoritaire parmi les personnalités que nous avons interrogées.

Nous remercions chaleureusement les représentants d'entreprises et d'institutions publiques qui ont accepté de contribuer ainsi à nos travaux.

Mise en perspective et motivations

Dix années se sont écoulées depuis l'adoption du Règlement général sur la protection des données (RGPD), entré en application en mai 2018 et devenu un des emblèmes de la protection des individus… et d'une certaine complexité administrative.

Malgré les difficultés initiales de mise en œuvre des exigences du texte et la marche forcée pour certains de la mise en conformité, le texte a permis une véritable acculturation à la protection des données et une responsabilisation accrue des acteurs, à saluer comme il se doit.

Toutefois, pour beaucoup d'acteurs aujourd'hui, surtout les plus petites entreprises et les start-ups, qui manquent de ressources juridiques pointues face à des textes jugés « incompréhensibles», la nécessité d'une clarification et d'une simplification est toujours affirmée.

Surtout, on constate que selon les applications qui sont faites du texte, certains juristes, souvent DPO, affichent une position parfois rigide qui ne sert pas la protection des données.

Face à ce constat, notre philosophie nous conduit à promouvoir un modèle où les principes de protection des données n'empêchent pas l'innovation et le développement des actions commerciales mais deviennent au contraire un atout concurrentiel et de confiance tout en réaffirmant la primauté de l'humain.

Contexte de l'Omnibus

L'initiative de la Commission européenne. La proposition de Règlement publiée le 19 novembre 2025 vise notamment à apporter un «soulagement immédiat» aux entreprises et à stimuler la compétitivité via des modifications techniques ciblées. Nous saluons positivement cette initiative.

Elle intervient également dans un paysage législatif saturé par l'entrée en application successive et non coordonnée d'une série de textes européens traitant de la donnée : Data Governance Act, AI Act, Data Act, Espace européen des données de santé pour n'en citer que quelques-uns. Cette situation accentue encore la complexité juridique à laquelle sont confrontées les entreprises et crée nécessairement un climat d'insécurité juridique quand les dispositions de ces textes imposent de nouvelles obligations aux acteurs qui ne s'articulent pas toujours entre elles.

Il convient également de se garder d'une tendance parfois constatée à la «sur-conformité» de la part de certains acteurs qui multiplient les mesures de conformité: multiplication de fiches de registre inutiles, tendance à effectuer des AIPD pour des traitements qui ne l'exigent pas, recueil du consentement alors qu'il n'est pas nécessaire, etc.

Dès lors, il s'agit d'éviter que l'Europe ne «s'auto-alimente en législations» sans cohérence globale.

Présentation du projet d'omnibus numérique

Le projet a pour ambition de modifier plusieurs législations numériques pour simplifier la lecture de certaines obligations, alléger les charges administratives et clarifier certaines zones grises (notamment sur l'IA et la recherche). Sur ce dernier point en effet, et indépendamment d'une autre proposition de la Commission européenne d'Omnibus IA destinée à revoir certaines dispositions du Règlement sur l'IA adopté le 13 juin 2024, l'Omnibus numérique comporte aussi des dispositions susceptibles d'impacter le Règlement sur l'IA.

Sur le calendrier d'adoption du texte, une adoption rapide - d'ici la fin de l'année 2026 - est espérée.

---

1 | Être ambitieux: favoriser l'ouverture des données et l'innovation

Plusieurs mesures pourraient favoriser l'ouverture des données et l'innovation tout en veillant à des conditions de mise en œuvre adaptées.

1.1 - Définition de la notion de donnée personnelle et des actes d'exécution de la Commission européenne

L'objectif poursuivi par la Commission européenne semble être de sortir des difficultés d'interprétation des notions de pseudonymisation et d'anonymisation en adoptant une nouvelle définition de la donnée personnelle telle qu'elle figure aujourd'hui à l'article 4 du RGPD.

L'exercice est délicat car il s'agit d'intervenir sur la définition socle de la protection des données qui est de considérer que dès lors qu'une personne physique est théoriquement identifiable (directement ou indirectement), la donnée qui la concerne est une donnée personnelle soumise aux principes de protection des données personnelles.

La Commission européenne s'appuie sur le récent arrêt de la CJUE dit « SRB » du 4 septembre 2025, qui considère que pour un responsable du traitement qui conserve la capacité d'identifier les personnes concernées, les données pseudonymisées demeurent pleinement des données à caractère personnel mais qu'en revanche, pour un destinataire qui ne dispose pas de moyens raisonnablement susceptibles d'être utilisés pour ré identifier les personnes, les

mêmes informations cessent d'être qualifiées de données personnelles au sens du RGPD.

C'est donc une clarification importante de la CJUE que la Commission propose d'intégrer dans l'article 4 du RGPD comme suit : «*Les informations relatives à une personne physique ne constituent pas nécessairement des données à caractère personnel pour toute autre personne ou entité, du simple fait qu'une autre entité peut identifier cette personne physique… »* Et dans son considérant 27, l'Omnibus précise ainsi que pour déterminer «*si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement utilisés pour identifier cette personne physique directement ou indirectement*».

Constatons d'abord qu'en pratique et pour certains projets qui associent plusieurs acteurs, il peut être en effet très difficile de respecter les principes de protection des données personnelles, en particulier en cas de réutilisation des données d'une personne physique: comment informer celle-ci de cette nouvelle réutilisation alors que les données pseudonymisées dont on dispose, ne le permettent pas sauf à engager des moyens matériels, financiers et humains déraisonnables.
L'article 11 du RGPD prévoit ainsi que « *Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le présent règlement. »*

Cette clarification de la CJUE est particulièrement importante puisqu'elle touche au concept de la donnée personnelle qui est au cœur du RGPD. Il est donc indispensable qu'elle soit appliquée de façon harmonisée non seulement par les autorités de protection des données personnelles mais également par toutes les juridictions nationales. Seule une codification de cette jurisprudence permettra d'assurer une interprétation identique au sein du marché intérieur et des conditions de concurrence équitables au moment où la donnée est devenu un actif stratégique recherché par les entreprises européennes pour développer de l'intelligence artificielle.

Cette réalité invite donc effectivement à un travail sur le statut de la donnée pseudonymisée qui doit nécessairement conduire à réinterroger la définition de la donnée à caractère personnel.

1.2 - Définition de la recherche scientifique: présomption de compatibilité avec la finalité initiale

Pour lever un frein majeur à l'innovation, l'enjeu consiste à pouvoir réutiliser des données collectées pour des projets de recherche ultérieurs sans avoir à solliciter de nouveau le consentement.

Le Digital Omnibus propose une modification de l'article 5, paragraphe 1 point b du RGPD en indiquant qu'il existe une présomption de compatibilité (là où le texte actuel fait état d'une présomption de non-incompatibilité) entre un traitement ultérieur de données et le traitement initial lorsque le traitement est réalisé à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou

historique ou à des fins statistiques (et dès lors que les dispositions de l'article 89 paragraphe 1 seraient respectées).

Surtout, le Digital Omnibus, à l'inverse de la rédaction actuelle du RGPD, précise que cette compatibilité s'apprécie indépendamment de l'article 6 paragraphe 4 du RGPD.

En d'autres termes, il ne serait plus nécessaire pour ces traitements de données de mettre en œuvre un test de compatibilité entre le traitement initial et le traitement ultérieur.

Pour rappel, ce test de compatibilité impose au responsable de traitement de vérifier:

- l'existence d'un lien entre les finalités pour lesquelles les données ont été collectées et les finalités du traitement ultérieur;
- le contexte dans lequel les données ont été collectées et en particulier la relation entre les personnes concernées et le responsable de traitement;
- la nature des données traitées, et en particulier la présence de données sensibles ;
- les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;
- l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Il s'agit donc ici d'une évolution importante, permettant une plus grande liberté dans la réutilisation des données pour un traitement ultérieur, sans pour autant abaisser le niveau de protection pour les droits et libertés des personnes concernées.

La présomption de compatibilité avec la finalité initiale doit être affirmée. Ainsi la proposition «Un levier pour la donnée» va dans un sens à saluer et à affirmer.

Cependant, l'efficacité de cette mesure repose sur une clarification nécessaire de la définition même de la «recherche scientifique» proposée par l'omnibus numérique à l'article 4(38). Afin d'apporter une pleine sécurité juridique aux investisseurs, le législateur devrait explicitement indiquer dans le texte qu'indépendamment de la poursuite d'un but commercial, la recherche peut être financée par des fonds privés ou publics. Sans cette précision, le flou sur le champ d'application de cette présomption risque de pérenniser une incertitude préjudiciable à la R&D européenne.

1.3 - Assouplissement pour l'IA: nouvelle base légale et possibilités de traiter des données sensibles

L'Omnibus propose de prévoir de manière explicite que l'intérêt légitime peut servir de base légale pour l'entraînement des modèles de langage d'IA et répondre ainsi à une demande forte de l'industrie pour sécuriser ses investissements.

1.3.1 Article 88ter: Sécuriser l'intérêt légitime pour l'entraînement de l'IA

Nous saluons cette ambition de l'Omnibus de confirmer de manière explicite que l'intérêt légitime constitue une base légale valide pour le développement et l'exploitation des

modèles d'IA. C'est une condition *sine qua non* pour répondre à la demande de l'industrie et sécuriser les investissements européens. Toutefois, pour que cette reconnaissance soit effective, le texte doit garantir une harmonisation totale du Marché Unique: il faut supprimer la disposition permettant aux lois nationales de contourner le RGPD en exigeant le consentement au niveau national, sous peine de créer une fragmentation réglementaire ingérable. Il en va de même quant aux modalités d'application de l'intérêt légitime.
De manière surprenante, la rédaction actuelle de l'article 88ter restreint l'usage de l'intérêt légitime en limitant le test de mise en balance aux seuls intérêts du responsable de traitement, excluant de fait ceux des tiers. Cette approche constitue non seulement une rupture juridique avec l'article 6(1)(f) du RGPD et la jurisprudence établie, qui permettent expressément de prendre en compte les intérêts légitimes poursuivis par un tiers, mais également s'apparente à un non-sens technologique. En effet, l'intelligence artificielle est par essence une technologie dont les bénéfices économiques et sociétaux s'étendent bien au-delà de la seule entreprise qui développe ou améliore un modèle. Afin de refléter la réalité de cette technologie et de ne pas brider l'innovation européenne, le législateur doit impérativement modifier le texte pour y inclure expressément les intérêts des tiers dans ce test de mise en balance.

1.3.2 Article 9(5): Adopter une approche par les risques pour les données sensibles

Autoriser le traitement de catégories particulières de données (sensibles) s'avère crucial pour la détection et la correction des biais dans les algorithmes d'IA. Il s'agit là d'une avancée pragmatique que la plupart des acteurs salue.

En effet, le Digital Omnibus propose notamment d'ajouter une nouvelle exception à l'interdiction de traiter des données sensibles, complétant ainsi la liste de l'article 9 du RGPD.

Il propose de prévoir la possibilité de traiter des données sensibles dans le cadre du développement et de l'exploitation d'un système ou d'un modèle d'IA, sous réserve de respecter les principes relatifs au traitement de données à caractère personnel (article 5 du RGPD).

Cette nouvelle exception vise à stimuler le développement de systèmes ou de modèles d'intelligence artificielle dans l'Union européenne en permettant la collecte de données sensibles pour l'entraînement de ces systèmes ou modèles.

Le Digital Omnibus prévoirait toutefois un cadre strict en imposant la mise en œuvre de mesures techniques et organisationnelles appropriées afin d'éviter la collecte de données sensibles. Si toutefois ces mesures n'empêchent pas le traitement de telles données, alors le responsable de traitement devra faire en sorte de supprimer ces données. Si cette suppression s'avère toutefois impossible, alors le responsable de traitement devra protéger les données contre toute utilisation de ces données pour produire des résultats et contre toute divulgation ou toute autre forme de mise à disposition des données à des tiers.

Ainsi, si le Digital Omnibus apporte une tolérance pour l'entraînement des systèmes et modèles d'intelligence artificielle, cette proposition s'attache à faire en sorte qu'aucune donnée sensible ne soit divulguée dans les données de résultat des intelligences artificielles.

La pratique des «Bacs à sable» réglementaires doit également être encouragée afin de tester l'innovation sans risque de sanction immédiate. Les autorités de protection des données devaient consacrer à cet égard plus de moyens à cette pratique qui correspond davantage aujourd'hui à la réalité des traitements concernés mis en œuvre plutôt qu'à leur examen souvent très théorique et doctrinal des dossiers de formalités qui leur sont soumis.

---

2 | Être concret

Plusieurs mesures concrètes pourraient alléger les obligations des acteurs économiques sans remettre en question les principes de protection des données personnelles.

2.1 - Les droits des personnes

Simplifier pour informer. Trop longues ou trop répétées, les notes d'information ne sont plus, ni lues, ni comprises. La surcharge d'information actuelle, avec notamment des mentions légales interminables, nuit à la confiance et à la compréhension réelle par l'utilisateur. Une information plus concise et lisible doit être mise en œuvre.

A cet égard, la proposition Digital Omnibus vise à simplifier les obligations relatives à l'information qui doit être fournie aux personnes concernées.

D'une part, il précise l'étendue de l'exception actuelle du RGPD visée à l'article 13.4 qui prévoit que la personne qui dispose déjà des informations visées par le texte n'a pas à être de nouveau informée tout en précisant que cette exception s'applique s'il existe *« des motifs raisonnables permettant de supposer que la personne concernée a déjà connaissance de l'identité du responsable de traitement et des finalités du traitement. »*
D'autre part, il prévoit d'autres exceptions à l'obligation d'information lorsque les données ont été collectées dans le cadre d'une relation claire et circonscrite entre les personnes concernées et que le responsable de traitement exerce une activité qui n'est pas intensive en données.

Toutefois, le Digital Omnibus tempère immédiatement cette volonté de simplification pour les acteurs en indiquant que ces exceptions ne peuvent être invoquées si le responsable de traitement:

- transmet les données à d'autres destinataires;
- transfère les données vers un pays tiers;

- procède à une prise de décision automatisée, y compris le profilage;
- ou que le traitement soit susceptible d'engendrer un risque élevé pour les personnes concernées.

Cette évolution peut être bienvenue pour les responsables de traitement dans la mesure où elle simplifie cette obligation d'information pour des traitements présentant peu de risque pour les personnes concernées. Par exemple, cette exception évitera d'introduire, dans certains contrats ou dans certaines politiques de confidentialité des mentions d'information qui avaient pour seul but de se conformer à la réglementation mais qui ne répondaient à aucun enjeu en matière de protection des données personnelles.

Il conviendra toutefois de préciser ce qu'est une activité non intensive en données.

Il peut être regretté que le texte ne reprenne pas l'exception actuellement prévue par l'article 13 du RGPD (connaissance préalable des informations par les personnes concernées). Ainsi, une interprétation restrictive de la notion de «relation claire et circonscrite» pourrait être de nature à réduire les exceptions à l'obligation d'information dans la mesure où le bénéfice de l'exception actuelle serait soumis à toutes les nouvelles conditions (relation claire et circonscrite notamment).

Il est donc indispensable d'obtenir des précisions sur l'interprétation à retenir afin d'être certain que ce texte constitue bien une mesure de simplification.

En outre, la proposition de Digital Omnibus ajoute une exception à l'obligation d'information lorsque le traitement est effectué à des fins de recherche scientifique et que la fourniture de ces informations s'avère impossible ou impliquerait un effort disproportionné de la part des responsables de traitement ou que le respect de cette obligation serait susceptible de rendre impossible ou de compromettre gravement la réalisation de la recherche elle-même.

Si cette exception est intéressante pour un responsable de traitement qui souhaite réutiliser, à des fins de recherche scientifique, des données déjà collectées auprès des personnes concernées et qui ne disposent pas ou plus des coordonnées des personnes concernées, elle n'aura d'effet que si les conditions de son application sont définies précisément.

Elle serait pourtant utile dans certains cas, en particulier dans le secteur de la recherche médicale où le lien entre le chercheur qui souhaite réutiliser des données collectées initialement pour une autre finalité se heurte régulièrement à des difficultés pratiques importantes pour respecter l'obligation individuelle d'information.

Elle devra également s'accorder avec les droits nationaux.

Mais au-delà de ces simplifications, n'est-il pas opportun de se poser la question du maintien par principe de l'information préalable et individuelle dans tous les cas? Alors que dans sa vie quotidienne, le citoyen connecté accède en permanence à l'information, ne pourrait-on envisager que l'obligation d'information soit satisfaite dans de nombreux cas par une information

générale avec toujours la possibilité de s'opposer dans un délai défini ?

Il est intéressant de noter que le texte de l'Omnibus fait référence à la possibilité de rendre accessibles au public les informations exigées au titre de l'information individuelle dès lors que celle-ci serait impossible. A condition de définir beaucoup plus largement qu'aujourd'hui l'appréciation de cette impossibilité.
Lutter contre les abus en cas de demandes excessives. Le droit d'accès par les citoyens est souvent détourné de sa finalité, visant à vérifier la licéité du traitement, pour servir de levier dans des litiges commerciaux, de consommateurs mécontents par exemple, ou concurrentiels. Dès lors, un principe de proportionnalité doit pouvoir s'appliquer. Ainsi les entreprises devraient pouvoir refuser des demandes manifestement abusives ou répétitives, et ce sans risque juridique disproportionné.

En ce qui concerne le droit d'accès des personnes concernées, l'article 12 du RGPD permet déjà, au responsable de traitement, de refuser ou de facturer les coûts supportés en cas de demande considérée comme «*manifestement infondée ou excessive*» notamment en raison de son caractère répétitif.

Le texte proposé par projet de Règlement Digital Omnibus va plus loin, en ajoutant la possibilité pour le responsable de traitement de refuser la demande ou de facturer les coûts supportés, dans le cadre d'une demande de droit d'accès fondée sur l'article 15 du RGPD lorsque la personne concernée abuse des droits conférés par le RGPD à des fins autres que la protection de ses données.

Il sera intéressant de suivre cette notion d'abus de droit afin de savoir ce qu'elle recouvre exactement.

Cette modification induite par le Digital Omnibus constitue sans doute une réaction à la jurisprudence de la CJUE, qui jusqu'à présent a jugé à plusieurs reprises que ce droit peut être exercé à toute fin, y compris en matière de litige ou pour la production de preuves. Toutefois le récent arrêt de la même Cour rendu public le 19 mars 2026 (affaire C-526/24) semble revenir sur cette position puisqu'il précise qu'une première demande d'accès peut, dans certaines circonstances, être considérée comme excessive et donc abusive, notamment si elle est introduite dans le seul but de demander ensuite une réparation pour une prétendue violation du RGPD.

En effet, il est par exemple devenu pratique courante que des salariés, dans le cadre de pré-contentieux prud'homaux, exercent leur droit d'accès afin de se constituer les preuves nécessaires dans le cadre du litige à venir.

Certaines organisations se retrouvent alors à supporter un important travail d'analyse et de compilation de données afin de pouvoir répondre à une demande de droit d'accès, dans un délai particulièrement contraint (1 mois), ces demandes n'étant aucunement liées à la protection de leurs données personnelles mais plutôt par la constitution d'éléments de preuve en leur faveur ou la volonté de nuire à leur ex employeur.

La rédaction du Digital Omnibus est donc bienvenue, dès lors que l'abus de droit sera défini en l'espèce, et ne remettra pas en cause l'équilibre qui doit toujours être

maintenu entre la préservation des droits des personnes concernées et la préservation des intérêts des entreprises.

2.2 - Les assouplissements annoncés qui ne doivent pas remettre en question la responsabilité des acteurs

2.2.1 - Liste des traitements soumis à une analyse d'impact
Aujourd'hui, la liste des traitements de données soumis à une analyse d'impact relative à la protection des données (AIPD) dépend de la doctrine de chaque autorité de protection des données alors même que le RGPD en définit les grandes catégories.

Le projet de Digital Omnibus propose de renvoyer au Comité Européen de Protection des Données (CEPD) le soin de définir une liste de traitements pour lesquels une analyse d'impact est requise, et une liste pour lesquels cette analyse n'est pas requise.

Le Comité transmet ensuite ces listes à la Commission.

Attribuer cette compétence au CEPD vise donc certainement à avoir une position commune à l'ensemble des pays européens en réduisant les écarts d'interprétation entre les pays membres de l'UE, ce qui sera de nature à être bien accueilli par les acteurs.

En outre, le Digital Omnibus prévoit que le CEPD élabore une méthodologie commune pour la réalisation des analyses d'impact, évolution au niveau européen qui serait effectivement bienvenue.

Dans une approche par les risques souhaitables, il faut réaffirmer que l'AIPD doit se concentrer sur les «hauts risques» réels et ne pas devenir une formalité bureaucratique systématique.

2.2.2 - Conditions de notification d'une violation de données

Eviter la sur-notification s'avère plus que jamais nécessaire. Le projet d'aligner les régimes de notification (à l'autorité) et de communication (aux personnes) risque de diluer l'effet d'alerte et d'alourdir inutilement la charge pour des incidents mineurs.

Ainsi, les critères de gravité gagneraient à être énoncés de manière plus claire pour ne notifier que ce qui présente un risque réel pour les droits et libertés, afin de ne pas submerger les DPO et les autorités.

Le projet de Digital Omnibus propose plusieurs mesures qui visent à alléger et à simplifier les obligations de notification en cas de violation de données et à rendre à cette disposition sa vraie signification.

Ainsi, le délai de notification auprès de l'autorité de contrôle en cas de violation de données s'étend à 96 heures à compter de sa découverte, contre 72 heures actuellement, ce qui évitera sans doute des notifications complémentaires qui alourdissent la procédure.

Le projet de Digital Omnibus fait également référence à la mise en place du point d'entrée unique pour notifier les violations, introduit par la directive (UE) 2022/2555 et toujours attendu en pratique pour répondre aux différentes obligations de notification imposées par les textes européens (RGPD, directive NIS 2 notamment).

Enfin, il renvoie au comité européen de protection des données (CEPD) pour l'élaboration d'un modèle commun de notification ainsi qu'une liste des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés d'une personne, modèle qui devra être adopté par la Commission au moyen d'un acte d'exécution.

Ce point sera particulièrement attendu dans la mesure où cette notion de risque élevé est peu claire pour le moment et engendre toujours un questionnement sur la nécessité de notifier la violation de données aux personnes concernées ou non, bien que les exemples déjà développés par le CEPD soient déjà utiles en la matière.

---

3 | Opportunités manquées

3.1 - Gouvernance: rôle et conditions d'intervention du CEPD et actes d'exécution de la Commission

Le CEPD - Même si ce sujet n'est pas traité directement dans le projet de texte, les acteurs souhaitent que le fonctionnement du Comité européen de la protection des données (CEPD) soit réformé. Celui-ci reste perçu comme trop «opaque» produisant des lignes directrices déconnectées de la réalité opérationnelle.

Pour y remédier, il serait opportun de prévoir une consultation des parties prenantes avant et non après la rédaction des lignes directrices (guidelines). Cela éviterait les postures et les positions dogmatiques ou maximalistes en privilégiant le dialogue.

Par exemple, le CEPD pourrait avoir une démarche plus constructive vis-à-vis du monde industriel en acceptant de recevoir les représentants des secteurs concernés.

Imposer également des règles de vote plus transparentes au CEPD dans le cadre de ses prises de position et des délais de production des guidelines permettrait de renforcer son autorité.

Par exemple, la production plus rapide de ses guidelines actualisées sur l'anonymisation aurait peut-être permis d'éviter des positions plus radicales sur la définition de la donnée à caractère personnel telle qu'elle est proposée aujourd'hui par la Commission dans l'Omnibus numérique.

Il est nécessaire de disposer au niveau européen d'un organe de gouvernance beaucoup plus efficace et à l'écoute des acteurs et dont l'autorité sera ainsi plus reconnue.

Vers une harmonisation réelle: il conviendrait de renforcer le pouvoir du CEPD pour unifier la doctrine, ce qui éloignerait le morcellement des approches et interprétations des autorités nationales, comme la CNIL, à

ajouter des «surcouches» ou des exigences supplémentaires. Ceci vient, par nature, fragmenter le marché unique.

La Commission - Le projet d'article 41 bis prévoit que la Commission peut adopter des actes d'exécution pour préciser les moyens et les critères permettant de déterminer si une donnée pseudonymisée constitue toujours une donnée à caractère personnel pour certaines entités.

Il serait plus constructif également d'inclure dans ces actes d'exécution la définition du champ de l'anonymisation, les travaux tant annoncés du CEPD sur l'anonymisation et la pseudonymisation n'étant toujours pas adoptés. Attendre sur ce sujet l'avis des autorités de contrôle qui aujourd'hui ne partagent pas la même opinion sur l'évolution de la définition de donnée à caractère personnel et qui ne comptent pas manifestement prendre en compte l'arrêt de la CJUE du 4 septembre dernier invitent en effet plutôt à favoriser des actes d'exécution interprétatifs du texte.

Il pourrait aussi être opportun de pouvoir reconnaître la valeur des Privacy Enhancing Technologies (PETs) qui constituent un bon moyen d'implémentation concrète des principes de protection des données personnelles. En effet, les procédures actuelles d'adoption des codes de bonne conduite restent très compliquées et chronophages.

3.1 - La pratique des «Bacs à sable» réglementaires

Elle devrait être encouragée afin de tester l'innovation sans risque de sanction immédiate. Les autorités de protection des données devaient consacrer à cet égard plus de moyens à cette pratique qui correspond davantage aujourd'hui à la réalité des traitements concernés mis en œuvre plutôt qu'à leur examen souvent très théorique et doctrinal des dossiers de formalités qui leur sont soumis.

Il serait logique que le projet d'Omnibus numérique reconnaisse cette pratique alors que le Règlement sur l'Intelligence artificielle la consacre dans ses articles 58 et 59.

3.2 - L'intégration inachevée de la directive e-Privacy et la fatigue du consentement

L'ambition du Digital Omnibus de rapprocher ces règles du RGPD (via le nouvel article 88a) partait d'une excellente intention: unifier le cadre juridique pour assurer une régulation plus cohérente sous l'égide unique des autorités de protection des données et via le mécanisme du guichet unique. Malheureusement, il s'agit d'une occasion manquée. Alors que la Commission a affiché sa volonté de démanteler progressivement la directive ePrivacy, le projet d'Omnibus n'y répond pas. En maintenant une dichotomie où les données à caractère personnel basculent dans le RGPD tandis que les données non personnelles liées au même équipement terminal restent sous l'égide de la directive ePrivacy, le texte va imposer aux entreprises de répondre à de multiples régulateurs pour un seul et même cookie. Loin de simplifier le droit, ce maintien en l'état va paradoxalement créer davantage de conflits de juridiction, d'insécurité juridique et de complexité d'application que la situation actuelle.

Adoptée en 2002, il y a près de 25 ans, la Directive vie privée et communications électroniques (e-Privacy) apparaît comme «complètement dépassée».

Si le projet d'Omnibus numérique évoque le sujet, il ne se risque pas à vouloir régler le problème de fond que constitue une «fatigue du consentement» grandissante des utilisateurs pour accéder aux sites Web et face aux bannières publicitaires.

Un nouvel article 88 bis serait intégré au RGPD et prévoirait l'exigence de consentement pour le stockage de données à caractère personnel ou pour l'accès à des données déjà stockées sur les équipements terminaux des personnes physiques, intégrant dans le RGPD les dispositions de la Directive 2002/58 (e-privacy).

Plutôt que de simplement fusionner les règles, la Commission s'est contentée de dupliquer les règles applicables aux cookies (article 5(3) de la directive e-Privacy) dans le RGPD (nouvel article 88a). Ainsi, (1) les règles de la directive e-Privacy continueraient à s'appliquer au traitement des données non personnelles, et (2) elles continueraient également à s'appliquer au traitement des données personnelles des personnes morales, car ces données ne relèvent pas du champ d'application du RGPD. La proposition créerait une asymétrie entre les exceptions à l'obtention du consentement en fonction des règles de e-Privacy et du RGPD, avec davantage d'exemptions prévues pour l'utilisation des données personnelles que pour les données non personnelles. Par exemple, l'accès aux données non personnelles à des fins de mesure d'audience serait soumis au consentement des utilisateurs, alors que le traitement de leurs données personnelles à cette même fin ne le serait pas. L'approche hybride qui en résulte risque de maintenir, voire d'amplifier, les incohérences et la charge de conformité que l'Omnibus était censé simplifier.

Dans tous les cas, une réflexion plus large devrait être menée afin d'évaluer la nécessité de maintenir un cadre juridique distinct pour l'accès et le stockage des données sur les équipements terminaux. Elle implique également une approche unifiée des autorités compétentes.

Le projet d'article 88 ter concernerait lui les indications automatisées et lisibles par machine des choix individuels, ainsi que le respect de ces indications par les fournisseurs de sites web.

Mais des mesures plus audacieuses devraient être envisagées tout en préservant le modèle économique du Web financé majoritairement par la publicité car l'obligation de centraliser les signaux des navigateurs ne résout pas concrètement la lassitude des utilisateurs.

La proposition de la Commission d'introduire une nouvelle disposition dans le RGPD (article 88b) imposant le respect de signaux standardisés, automatisés et lisibles par machine exprimant les choix des utilisateurs, ajoutera une nouvelle couche de complexité.

En France, l'Autorité de la Concurrence a démontré que la centralisation du consentement au niveau du navigateur renforcerait considérablement la position des contrôleurs d'accès (*gatekeepers)*.

D'un point de vue technique, le mécanisme proposé par la Commission est inapplicable en pratique : les utilisateurs interagissent avec les services numériques à partir d'une grande diversité d'appareils et de points d'entrée (navigateurs, *app stores*, les agents IA, etc.) Obliger tous les fournisseurs de services à se conformer à des choix universels est donc techniquement irréalisable. La définition de ces choix pourrait donner lieu à des débats insolubles sur le niveau de granularité nécessaire pour l'interface de consentement, les différentes finalités, la définition de la validité du consentement qui devrait être valable pour l'ensemble de la chaîne de valeur, ou la gestion des conflits de consentement (un utilisateur refuse la collecte sur son appareil connecté mais pas sur son ordinateur).

Les utilisateurs préfèrent en général faire des choix pour chaque service individuel plutôt que par le biais de mécanismes au niveau du navigateur. Cela permet un contexte plus clair, une plus grande transparence, un meilleur contrôle et au final plus de confiance. Au contraire, les mécanismes de consentement centralisés apportent moins de visibilité et de contrôle sur les organisations qui peuvent traiter les données.

Enfin, le consentement centralisé serait en contradiction avec le principe selon lequel un consentement valable doit être spécifique, lié à une finalité et associé à des opérations de traitement clairement identifiées afin de permettre aux utilisateurs de faire des choix éclairés et autonomes pour chaque finalité de traitement.
Plutôt que de modifier la façon dont le consentement peut être donné, une meilleure approche serait de demander le consentement aux utilisateurs uniquement pour les activités les plus intrusives.

Centraliser le choix des utilisateurs au niveau du navigateur est donc une fausse bonne idée et ferait peser un double risque sur l'écosystème européen: en automatisant les choix de l'utilisateur à l'échelle du système, cette mécanique va inévitablement assécher les revenus publicitaires qui financent la presse et les éditeurs de contenus gratuits. La conséquence directe et rapide sera la multiplication de paywalls sur l'ensemble des sites Internet qui n'auront pas d'autres choix pour se financer. Par ricochet, le mécanisme proposé va lourdement impacter le tissu économique européen – en particulier les PME et les e-commerçants – dont la croissance, la visibilité et l'acquisition de clients reposent de façon importante et croissante sur la publicité en ligne.

Par ailleurs, l'article 88ter va mécaniquement forcer la fuite et la concentration des budgets publicitaires vers les environnements fermés (*walled gardens*). Ces plateformes, qui s'appuient sur des écosystèmes d'utilisateurs connectés (log-in), seront immunisées contre ces signaux, faussant ainsi totalement le jeu de la concurrence au détriment de l'Internet ouvert.

Plutôt que de s'obstiner sur le contenant (la *manière* dont on recueille le choix centralisé), le législateur doit changer de paradigme et s'interroger sur le contenu (*ce à quoi* l'on consent). Il faut sortir de la logique binaire actuelle en adoptant une véritable approche par les risques, consistant à exempter de consentement les traitements peu intrusifs. L'intégration d'exemptions claires pour la publicité contextuelle et ses opérations

techniques indispensables (mesure d'audience, plafonnement de la fréquence d'affichage ou « capping », prévention de la fraude) permettrait d'atteindre un double objectif: réduire drastiquement l'affichage des bannières au quotidien tout en incitant activement les entreprises à basculer vers ces modèles respectueux de la vie privée. Cette approche pragmatique est d'ailleurs la solution formellement soutenue et recommandée par l'avis conjoint des régulateurs européens de la vie privée (EDPB/CEPD).

3.3 - Harmonisation des procédures administratives

Absente, l'unification du droit procédural administratif serait un véritable progrès. Aujourd'hui, les entreprises doivent gérer 27 procédures contentieuses différentes. Cette géométrie variable est un frein sérieux pour les acteurs paneuropéens et n'est pas de nature à favoriser l'émergence d'acteurs européens capables de répondre aux acteurs américains ou chinois.

3.4 - Gouvernance centralisée

L'absence d'un véritable régulateur unique européen fort pour les acteurs transfrontaliers laisse subsister un système complexe de «guichet unique» qui montre ses limites. Avec le renforcement des pouvoirs du CEPD, «une base partagée commune à toutes les organisations» devrait être envisagée.

Ce point doit être apprécié avec celui développé plus haut sur le CEPD.

Conclusion

La tentative de la Commission européenne de modifier le RGPD tel qu'il a été adopté en 2016 et mis en application en 2018 pour en simplifier certaines dispositions ou pour clarifier et alléger certaines obligations et prendre en compte une réalité numérique très mouvante, est une initiative saluée par les acteurs et en particulier les entreprises qui ont besoin pour travailler de données à caractère personnel.

Ces acteurs ne souhaitent pas à cet égard revenir sur certaines des obligations posées par le RGPD alors qu'ils ont mis en place des procédures, revu leurs contrats et organisé la conformité au texte. Par exemple, vouloir limiter la tenue d'un registre des traitements à un seuil déterminé de salariés paraît inutile alors que c'est un outil de contrôle de la conformité d'un responsable de traitement vis-à-vis de la chaîne de ses sous-traitants.

En revanche, ils souhaitent que certaines mesures qui s'apparentent davantage lors de leur implémentation à des procédures très administratives ou à des obligations qui s'avèrent dans certains cas très difficiles, voire impossibles à respecter, soient

réexaminées à la lumière d'un contexte international très compétitif et désormais marqué par la numérisation généralisée et le recours aux outils d'intelligence artificielle. Certes, il peut paraître audacieux de vouloir modifier la définition de la donnée à caractère personnel tant celle-ci commande l'application des principes de protection des données personnelles. Mais comment avancer sur ce sujet alors que d'autre part, ni le CEPD, ni les autorités de protection des données ne proposent de solutions pratiques, efficaces dans des délais qui soient compatibles avec la réalité d'un temps économique, concurrentiel qui s'accélère en permanence.

Et l'argument souvent opposé de la nécessité de conserver un modèle européen respectueux des droits et libertés individuels ne tient plus forcément quand on voit en pratique l'acharnement à exiger des acteurs, sauf à bloquer leur projet, des conditions de respect de mesures de protection des données impossibles à mettre en place et dès lors dénuées de sens.

Le sens justement de la protection des données personnelles doit être repensé (retrouvé?) pour en conserver l'esprit et l'adapter. Ce projet de texte d'omnibus numérique est une occasion à saisir pour avancer. ❐

la vi//a .
numeris

*unlock the future, make it human**

hello@lavillanumeris.com
+33 7 80 96 11 11
http://www.lavillanumeris.com

**libérez l'avenir, rendez-le plus humain*