Renaissance Numérique

SYNTHÈSE SEPTEMBRE 2026

Omnibus numérique : quels enjeux pour la vie privée ?

Synthèse de l'événement

« Omnibus numérique : quels enjeux pour la vie privée ? »

À l'occasion de la publication de son rapport « Repenser le Digital Omnibus : simplification vs. droits, cohérence et méthode » (juin 2026), Renaissance Numérique a réuni, le 24 juin 2026, des représentants d'entreprises, de la société civile, de la recherche et des avocats, pour débattre des enjeux du projet d'omnibus numérique sur la vie privée.

Cette synthèse reprend les principaux éléments abordés lors de cette table ronde, qui a eu lieu chez Hogan Lovells.

Participants

KEMICHE Anissa, Directrice Affaires Publiques Europe et International, Numeum

MARIEZ Jean-Sébastien, Avocat associé, Momentum Avocats

MICHAELSEN Frithjof, Chargé de mission relations institutionnelles Europe & secteur numérique, Que choisir ensemble

ROSSI Julien, Maître de conférences en Sciences de l'information et de la communication à l'UFR « Culture et communication », Université Paris 8

Animateur

DROUARD Étienne, Avocat Associé, Hogan Lovells

Rapporteures

D'ASCIA Adele, Renaissance Numérique

BHOJWANI Tasha, Renaissance Numérique

Contexte

Le 19 novembre 2025, la Commission européenne présentait le paquet « Digital Omnibus » en vue de simplifier le corpus législatif européen relatif au numérique. Ce paquet se décline en deux volets : un premier consacré à l'intelligence artificielle (Omnibus sur l'IA, modifiant notamment l'AI Act), et un second portant sur l'acquis numérique existant, en particulier le RGPD et la directive ePrivacy.

Portée par les conclusions des rapports Draghi et Letta sur la compétitivité européenne, cette initiative s'inscrit dans une logique de réduction de la charge administrative et de renforcement de la compétitivité des organisations opérant sur le marché intérieur.

Au printemps 2026, les négociations sur le Digital Omnibus étaient dans une phase décisive : à l'issue du trilogue du 7 mai 2026, Parlement et Conseil ont trouvé un accord politique sur le volet « Omnibus on AI ». Le 13 mai 2026, les représentants des États membres réunis au sein du Coreper ont approuvé ce compromis, ouvrant la voie aux votes en commission, puis au vote en plénière du Parlement européen le 16 juin 2026. Quelques jours après la tenue de la table ronde organisée par Renaissance Numérique, le Conseil de l'UE a donné son feu vert final le 29 juin 2026, le règlement a été signé le 8 juillet 2026, puis publié au Journal officiel le 24 juillet pour entrée en vigueur le 27 juillet 2026.

Dans ce contexte, Renaissance Numérique s'est attaché à interroger l'apport réel de cette démarche de « simplification », en particulier au regard de la protection de la vie privée et de la cohérence de l'édifice juridique européen. À l'occasion de la publication de son rapport « Repenser le Digital Omnibus : simplification vs. droits, cohérence et méthode » (juin 2026)[1], le think tank a organisé une table ronde dédiée aux enjeux spécifiques de la vie privée dans ce processus. À cette date, alors que le volet dédié à l'IA est en passe d'être définitivement adopté, la seconde partie de la proposition demeure en discussion au Parlement européen et au Conseil, laissant ouvertes de nombreuses questions sur l'équilibre entre simplification, sécurité juridique et garanties offertes aux citoyens, et notamment sur la question relatives aux enjeux sur la vie privée.

Les échanges de cette table ronde se sont donc déroulés à un moment charnière : celui où l'Union européenne discutait du verrouillage possible d'une série de modifications techniques de l'AI Act au nom de la compétitivité et de la mise en œuvre « pragmatique » de la régulation des systèmes d'IA, tandis que les choix à opérer sur la redéfinition de la donnée personnelle, le consentement et le rôle des différents acteurs du numérique restent encore ouverts dans le volet Omnibus consacré à l'acquis RGPD/ePrivacy.

Les débats de cette table ronde ont notamment mis en évidence la fragilité de la démarche de l'Omnibus numérique. Si la volonté d'harmoniser les textes (RGPD, AI Act, Data Act) et d'alléger la charge des entreprises a été saluée dans son principe, la méthode employée a suscité une certaine opposition. Pour les intervenants, la simplification administrative ne doit pas s'opérer au prix d'un recul des droits fondamentaux des citoyens, ni d'une fragilisation des acquis jurisprudentiels qui font la force et l'influence mondiale du modèle européen de

1. Ce rapport s'inscrit dans une suite de travaux menés par le think tank :
- Novembre 2024, publication de la note « Politique numérique de l'UE : l'heure de la cohérence a sonné ».
- Mai 2025 : publication de la note « Numérique : l'urgence d'une interrégulation efficace ».
- Mars 2026 : réponse à la consultation « Digital Fitness Check » de la Commission européenne.

protection des données. Pour l'avenir, les experts s'accordent sur la nécessité de privilégier une harmonisation de l'application pratique des textes plutôt qu'une réécriture législative hâtive, déconnectée des réalités technologiques et opérationnelles de l'écosystème numérique.

De gauche à droite : Julien Rossi, Anissa Kemiche, Jean-Sébastien Mariez et Frithjof Michaelsen.

↘ Redéfinir la donnée personnelle : clarification ou fragilisation du RGPD ?

Au cœur des échanges qui ont eu lieu lors de cet événement figure la proposition de la Commission européenne de réviser l'article 4 du RGPD afin de redéfinir la notion de « donnée à caractère personnel ».
En effet, le texte propose qu'une donnée ne soit qualifiée de personnelle au sens du RGPD qu'au regard d'une « entité » (qui reste à définir) qui dispose, par elle-même et avec les ressources raisonnablement à sa disposition, des moyens d'identifier directement ou indirectement la personne concernée. Cette réécriture montre une méconnaissance manifeste du fait que les obligations du RGPD s'appliquent aux responsables du traitement, définis non pas par leur capacité d'accéder à des données, mais à celle de définir les modalités et finalités de leur traitement.

Anissa Kemiche (Numeum) a exprimé le soulagement d'une grande partie des entreprises du numérique face à ce qu'elle qualifie de retour au pragmatisme. Selon elle, le flou qui entoure cette définition engendre une incertitude systémique. Par exemple, une entreprise qui publie des statistiques agrégées sur la fréquentation de ses points de vente physiques reste suspendue à l'interprétation des autorités nationales de contrôle (comme la CNIL en France), qui adoptent souvent des positions extensives et divergentes sur la possibilité de réidentification. Pour Numeum, les acteurs économiques ne réclament pas une pure dérégulation, mais des « règles praticables et précises », cohérentes avec le corpus législatif européen du numérique. Le recentrage proposé par la Commission européenne permettrait d'encourager l'innovation en offrant, selon Numeum, un cadre prévisible et sécurisant, adapté au responsable de traitement.

En revanche, **Julien Rossi** (Université Paris 8) a mis en garde contre le risque de contournement systématique des obligations du RGPD que cette nouvelle formulation pourrait favoriser. En limitant la responsabilité aux seuls moyens immédiats du responsable de traitement, cela peut ouvrir la voie à des déclarations d'opportunité. Ainsi, de nombreuses entités pourraient unilatéralement qualifier leurs données comme « étant sous pseudonyme » ou « anonymes » pour tenter de s'exclure du champ protecteur du règlement. Cette porosité de la qualification se ferait au détriment direct des citoyens, qui perdraient le contrôle sur l'exploitation de leurs informations dans des chaînes de sous-traitance complexes où la réidentification reste techniquement possible par le croisement de bases de données tierces. L'exercice de leurs droits pourrait alors devenir plus difficile. En outre, les responsables du traitement se retrouveraient confrontés à une forte insécurité juridique, puisqu'ils couraient le risque que les partenaires avec qui ils partagent la responsabilité du traitement de données personnelles se prévalent à tort de cette nouvelle possibilité.

Cette redéfinition achoppe également sur l'évolution rapide de l'état de l'art technologique. **Jean-Sébastien Mariez** (Momentum Avocats) relève ainsi que la ligne de démarcation entre donnée personnelle et donnée non personnelle est devenue quasi impossible à tracer. Cette définition nécessitera l'adoption de lignes directrices du CEPD (Comité européen de la protection des données) en vue de redéfinir les notions d'anonymisation et de pseudonymisation. En outre, l'avocat déplore l'absence de prise en compte de l'évolution profonde des technologies renforçant la protection de la vie privée (dites "*Privacy Enhancing Technologies*")[2] depuis la rédaction du RGPD en 2016. Plutôt que de s'enfermer dans des débats doctrinaux déconnectés de la pratique, le régulateur européen devrait, selon lui, s'appuyer sur des critères techniques, fonctionnels et factuels, qui ont grandement évolué depuis la rédaction de la directive ePrivacy ; les technologies contemporaines (dont les nouvelles techniques de chiffrement par exemple) étant aujourd'hui capables de traduire en pratique les principes du RGPD.

2. Privacy enhancing technologies, OCDE : https://www.oecd.org/en/topics/privacy-enhancing-technologies.html

Pour **Frithjof Michaelsen** (Que choisir ensemble), tout ceci doit être envisagé sous l'angle de l'importance capitale du RGPD. En ce sens, s'il estime que le RGPD n'est pas, à proprement parler, un texte de cybersécurité, il n'en reste pas moins le berceau. Selon lui, il faut donc s'accorder sur une définition des données personnelles permettant d'avoir l'expérience la plus sécurisée possible.

↘ Le consentement à bout de souffle

L'échange s'est également intéressé aux fondements de la licéité des traitements de données, bousculés par l'intégration croissante de l'intelligence artificielle. Le RGPD pose le principe d'un consentement libre, spécifique et éclairé.

Julien Rossi qualifie ce cadre de théorique et d'inadapté aux usages algorithmiques modernes. En vertu des articles 5(1) et 12 du RGPD, un traitement doit être transparent et intelligible pour l'utilisateur. Cependant, s'interroge-t-il, comment un citoyen peut-il consentir de façon éclairée à un traitement dont la complexité sous-jacente échappe parfois aux concepteurs mêmes du système ? Il estime que cette opacité intrinsèque rend le recueil du consentement artificiel, voire hypocrite. Face à cette impasse, le chercheur appelle à dépasser la simple injonction légale pour stimuler l'innovation au sein même de l'écosystème technologique, afin de concevoir des architectures applicatives nativement intelligibles et transparentes, conformément au principe de "*privacy by design*" prévu par le RGPD.

Jean-Sébastien Mariez a pointé du doigt ce qu'il considère être un acharnement des autorités de régulation sur le recueil du consentement, au détriment des autres bases légales prévues par le texte européen, notamment l'intérêt légitime. Selon lui, en restreignant de manière excessive l'usage de cette base légale, les régulateurs ont acculé l'industrie à un usage systématique, et souvent dévoyé, des bannières cookies. Cette sur-sollicitation permanente engendre une fatigue cognitive généralisée des internautes, qui cliquent pour faire disparaître les bandeaux de cookies sans plus aucune considération pour la protection de leur vie privée.

À l'inverse, **Julien Rossi** rappelle que l'intérêt légitime ne saurait être un laissez-passer absolu pour l'industrie publicitaire et le ciblage comportemental. Dans le cadre du tracking en ligne, notamment sur les sites d'information, s'en remettre à l'intérêt légitime de l'éditeur pour profiler politiquement un internaute est problématique. Cela reporte l'entière responsabilité de la protection sur l'utilisateur, contraint d'entamer des démarches complexes d'*opt-out* (ou droit de refus) auprès de dizaines de partenaires commerciaux dont il ignore souvent jusqu'à l'existence.
La mise en œuvre des signaux de consentement illustre cette impasse technique. L'écosystème a vu proliférer des protocoles concurrents (Do Not Track, Global Privacy Control, Transparency and Consent Framework de l'IAB, etc.). Néanmoins, comme l'explique Julien Rossi, aucun texte ne tranche la question de la hiérarchie de ces signaux en cas de contradiction (par exemple, entre navigateur et les cookies). Pour lui, cette incertitude opérationnelle se double d'une anxiété technique pour les responsables de traitement. À titre d'illustration, le déploiement de technologies de pointe comme le chiffrement homomorphe[3] ou la cryptographie post-quantique soulève des questions de conformité abyssales. Les gestionnaires craignent que des autorités de contrôle déconnectées des réalités techniques finissent par leur imposer des choix d'algorithmes ultra-spécifiques, transformant la conformité RGPD en un exercice de micro-gestion technologique hors de portée des structures de taille intermédiaire. De plus, les choix des autorités sont susceptibles d'être contredits par

3. « Le chiffrement homomorphe est une technique de cryptographie permettant de réaliser des opérations sur des données chiffrées sans que celles-ci aient à être déchiffrées. Le résultat de ces opérations reste sous forme chiffrée et ne peut être déchiffré que par les destinataires autorisés (détenant la clé de déchiffrement). Cette technique permet ainsi aux participants d'un calcul de garder leurs données confidentielles au cours d'un calcul ». Source : https://www.cnil.fr/fr/definition/chiffrement-homomorphe

la suite par les juges. Le régulateur semble ne pas être l'acteur le mieux placé pour se prononcer sur l'algorithme standard à utiliser, sans tenir compte des considérations techniques, fonctionnelles, et de sécurité. Le flou de certaines dispositions du RGPD peut alors s'avérer pour partie une force pour les acteurs innovants, qui ont certes la responsabilité, mais aussi la liberté de définir de quelle manière opérationnellement réaliste et technologiquement pertinente ils protègent les données personnelles.

↘ Entre souveraineté et fragmentation : les limites de l'approche Omnibus

Traiter ces frictions autour de la vie privée numérique au niveau européen ajoute une multiplicité d'acteurs, donc de potentielles complications au processus de simplification. Par exemple, pour remédier à la lassitude des utilisateurs face aux bannières cookies, le projet d'Omnibus introduit l'idée d'une centralisation du refus de consentement au niveau des navigateurs et des systèmes d'exploitation.

Frithjof Michaelsen a souligné l'ironie et le danger systémique de cette proposition. Il fait le constat que les outils de navigation et les systèmes d'exploitation dominants sur le marché européen sont développés et contrôlés par les GAFAM (Google, Apple, Microsoft, Meta). En confiant la centralisation du consentement à ces acteurs, dont les revenus dépendent directement de l'exploitation publicitaire des données personnelles, l'Union européenne pourrait créer un conflit d'intérêts majeur. Le représentant de l'association de consommateurs craint que ces entreprises n'utilisent ce rôle d'intermédiaire pour asseoir leur position dominante, au détriment des éditeurs de presse indépendants et des alternatives technologiques européennes.
Il pose également la question du consentement granulaire en fonction des différents types de traitements. Cette initiative semble en théorie idéale, mais cela amène en pratique une complexité supplémentaire à l'échelle de l'utilisateur.

Pour **Anissa Kemiche**, l'application territoriale de la réglementation numérique en Europe reste marquée par de profonds clivages nationaux, qui nuisent à l'équité économique. Elle a ainsi évoqué la divergence de doctrine entre les deux moteurs de l'Union :

- → La France, alignée sur une tradition de protection stricte et d'indépendance de son régulateur (la CNIL), défend une application rigoureuse de l'acquis communautaire.
- → L'Allemagne, plus attentive aux impératifs industriels et à la compétitivité de ses entreprises, plaide pour des approches assouplies, notamment sur la définition des données personnelles et les transferts de données.

Elle estime que cette divergence est amplifiée par des structures institutionnelles asymétriques. Tandis que la France s'appuie sur une autorité unique et centralisée, l'Allemagne souffre d'un morcellement avec ses 18 autorités de contrôle.[4] Pour un acteur économique opérant à l'échelle européenne, ce mille-feuille administratif crée une insécurité chronique.

Jean-Sébastien Mariez a rapporté des cas de blocages opérationnels où, pour un même dossier d'accord de transfert de données (*Binding Corporate Rules* - BCR), deux autorités nationales ne soulevaient aucune objection tandis qu'une troisième paralysait l'ensemble de la procédure, ruinant ainsi l'ambition d'un guichet unique européen.

À ce titre, plusieurs questions et interventions du public présent lors de cette table ronde ont convergé vers une critique de la méthode législative bruxelloise. Une personne du public

4. L'Allemagne compte une autorité par Land (16), excepté pour la Bavière qui en compte deux, ainsi qu'une autorité au niveau fédéral.

a ainsi fait un parallèle entre les projets de simplification européens et les lois de simplification françaises qui, par le jeu des amendements, finissent par complexifier la règle de droit. L'absence d'études d'impact rigoureuses et transparentes a été condamnée par une autre personne présente. **Anissa Kemiche** et **Frithjof Michaelsen** ont également dénoncé des documents d'évaluation d'impact « vides », incapables d'appréhender les coûts réels de mise en conformité pour l'écosystème et le risque de distorsion de concurrence par rapport à d'autres zones géographiques.

Cette déconnexion s'explique également par l'absence de dialogue horizontal au sein même de la Commission européenne. **Julien Rossi** a pointé du doigt les « querelles de chapelles » entre la direction générale des réseaux de communication, du contenu et des technologies (DG CONNECT) de la Commission européenne, guidée par une logique d'optimisation du marché de la donnée (concept de *data holder* propre au Data Act)[5], et la DG Justice, gardienne de la doctrine des droits fondamentaux (concept de *data controller* propre au RGPD). Le chercheur illustre cette incohérence par l'impasse réglementaire entourant les objets connectés ou les automobiles intelligentes. Ces technologies, qui captent des données dans l'intimité des individus, relèvent historiquement de la logique d'accès au terminal de la directive ePrivacy, qui n'est pas tout à fait la même que le régime prévu par le RGPD qu'elle complète.

Enfin, **Jean-Sébastien Mariez** a conclu en alertant sur l'illusion d'une réécriture des textes fondamentaux. Réformer la définition de la donnée personnelle pour répondre à une urgence politique revient à fragiliser des années de jurisprudence constante et protectrice de la Cour de justice de l'Union européenne (notamment l'arrêt historique Breyer de 2016 ainsi que la récente jurisprudence sur le droit d'accès dont l'arrêt Brillen Rottler de la CJUE). En ouvrant la boîte de Pandore de la révision textuelle, l'Europe risque d'affaiblir l'attractivité de son marché intérieur en y substituant une instabilité juridique permanente.

5. Détenteur de données en français, le fabricant du produit connecté ou le fournisseur du service connexe qui dispose des données. https://www.donneespersonnelles.fr/data-act-rgpd-differences

Renaissance Numérique
www.renaissancenumerique.org
Septembre 2026