Rapport

RGPD : 5 ANS, ÇA SE FÊTE ?

PRINTEMPS 2023

la villa numeris

:: remerciements

Merci à **Loïc Rivière**, fondateur d'Hindsight, d'avoir coordonné la rédaction de ce rapport, avec le concours de membres de la Commission Data & IA de La villa numeris, et pour leur contribution à **Mathilde Aubinaud**, journaliste, **Marie-Aude Aufaure**, fondatrice de Datarvest, **Terence Cabot**, avocat, associé de Latournerie Wolfrom Avocats, **Gérard Guinamand**, fondateur de Datascale, **Magali Jalade**, directrice des affaires publiques et juridiques, **Nathalie Laneret**, directrice des Affaires publiques de Criteo, **Jean-Christophe Le Toquin**, président du Cybersecurity Advisors Network (CyAN), **Guy Mamou-Mani**, fondateur du Groupe Open, **Stéphane Martin**, directeur général de l'ARPP, **Paul d'Amécourt, Thara Safi Couplet et Nicolas Rocher** de Lighthouse Europe

Merci aux dirigeants et représentants des entreprises qui ont contribué à nos travaux et dont nous entendons proposer la synthèse la plus juste de leurs analyses et aspirations.

Nous remercions également chaleureusement les personnalités qui ont répondu à nos questions dans le cadre d'auditions, **Eric Bothorel**, député, **Thomas Dautieu**, directeur de l'accompagnement juridique de la CNIL, **Ramy Houssaini**, chief Cyber & Technology Risk de BNP Paribas, **Bertrand Pailhès**, directeur des technologies et de l'innovation de la CNIL, **Yves Poullet**, professeur émérite de la Faculté de droit de Namur, fondateur du Centre de recherches informatique et droit, **Artus de Saint-Seine**, directeur général adjoint d'Isoskele et président de la commission juridique de DMA France, et toutes celles et tous ceux qui ont préféré garder l'anonymat.

Merci à **Arthur Brodmann** pour sa relecture attentive.

David Lacombled, président de La villa numeris

Nouveaux défis, nouvelle régulation

Alors que le Règlement général sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018, La villa numeris entend mettre à profit ces cinq années d'exercice pour se livrer à un premier bilan

Appliqué sur l'ensemble du continent, et parfois au-delà, le RGPD permet à l'Europe de se distinguer dans l'affirmation de ses principes de protection des individus.

Alors que les données constituent désormais le carburant de l'économie, il nous faut veiller néanmoins à ne pas brider pour autant le développement des entreprises. Car nous le savons, l'instabilité n'est jamais propice à la confiance et donc à l'investissement et donc à la croissance.

C'est pourquoi, il nous paraissait important de se livrer à un premier bilan. Si le texte est unanimement loué, son application, et donc son interprétation, ouvrent parfois des interstices dans lesquels doutes et craintes se glissent.

Craignant les sanctions, érigées comme mesure principale du respect du RGPD, les entreprises s'autocensurent parfois plus que de raison. De récentes mises en demeure publiques et de lourdes amendes témoignent d'une application stricte des textes existants. Le sujet est suffisamment sensible pour que de nombreux acteurs aient préféré l'anonymat, comme nous le leur avons proposé, pour partager leurs expériences, leurs aspirations et leurs craintes aussi.

Les régulateurs sont souvent désignés comme des gendarmes de leur marché. Comme tels, ils doivent non seulement manier le bâton mais aussi la carotte en servant de guides à des entreprises dont ils sont en quelque sorte les dépositaires aussi. C'est ce qui fait qu'une autorité est respectée.

Par nature, le sujet est complexe. Rien ne laisse augurer que les choses iront en se simplifiant tant l'Europe, forte du RGPD, semble avoir la tentation de la régulation par défaut, comme un marqueur, avec de nombreux textes, le Digital Service Act (DSA) et le Digital Marketing Act (DMA) pour commencer, les textes sur la Data et l'IA pour continuer, le risque est grand de voir des textes s'empiler sinon s'enchevêtrer.

Alors qu'au cours des dernières années, La villa numeris a publié une contribution au «Artificial Intelligence Act, un rapport puis une note de position sur les transferts transatlantiques de données au service de la souveraineté européenne, nous nous attachons à une approche technologique, économique et juridique afin de proposer des pistes d'évolutions permettant de respecter les droits fondamentaux des individus tout en permettant aux acteurs économiques de sortir de l'insécurité qui pénalise l'innovation.

En résumé

Si le Règlement général de protection des données (RGPD) représente un vrai plus pour renforcer la confiance dans l'espace numérique, il n'a pas pour autant dissipé le climat anxiogène et les incompréhensions.

Devenu une règle de droit européenne à portée internationale, le RGPD demeure en outre, selon les entreprises, interprété différemment et confère une prime certaine au mieux disant. Les entreprises expriment également leur profonde déception face aux lourdeurs administratives qui n'ont pas tenu leurs promesses ou de la mise en place des outils à leur disposition comme les règles d'entreprise contraignantes (Binding Corporate Rules / BCR), ou bien encore les codes de conduite ou les certifications comme outils adéquats.

Face à des obligations concrètes qu'elles estiment trop déconnectées de la réalité et des sanctions élevées et difficilement interprétables, les entreprises souhaitent une révision du RGPD qui irait de pair avec l'adoption en France d'une culture de la régulation plus adaptée à l'innovation et qui offrirait aux autorités de régulation une responsabilité renforcée en matière d'accompagnement des entreprises.

Pour aller plus loin, La villa numeris partage ainsi ses propositions pour un nouveau paradigme de régulation.

Méthodologie

Ecouter, comprendre, partager. Nos travaux sont principalement nourris par :

- Deux tables rondes publiques à Bercy, dans le cadre des Assises Data Transformation, le 26 janvier 2023, et au Palais du Luxembourg, dans le cadre de notre Observatoire des enjeux législatifs #DigiLex, le 13 avril 2023 ;
- Une consultation publique et transparente de professionnels et d'experts, dont 50 ont répondu, sous forme d'un questionnaire auto-administré avec l'outil Synapscore entre les 26 janvier et 7 mars 2023 ;
- Une série d'auditions de délégués à la protection des données (DPO) ou de dirigeants de grandes entreprises (Banque, Services, Mobilité, Publicité) sous couvert d'anonymat, d'experts et d'élus;
- Un travail de documentation et une analyse juridique

1. Un bilan plus que contrasté

Si le Règlement général de protection des données (RGPD) représente un vrai plus pour renforcer la confiance dans l'espace numérique, il n'a pas pour autant dissipé le climat anxiogène et les incompréhensions

L'adoption d'un cadre juridique harmonisé au niveau européen susceptible de renforcer la confiance numérique a de fait été accueillie favorablement tant par les entreprises que par les individus. Les premières y percevant l'opportunité d'un développement facilité de l'économie numérique, les seconds l'assurance d'une meilleure protection de leurs données personnelles, confirmant ainsi l'Europe comme territoire protecteur des droits fondamentaux.

Pour toutes les entreprises traitant des données personnelles, avec le renforcement de leurs droits, il a donc fallu consentir à des investissements importants en matière de sécurité et de mise en œuvre de la conformité pour répondre aux exigences du texte et mettre en œuvre plus largement une politique de confidentialité avec des mécanismes et procédure internes permettant démontrer le respect des règles relatives à la protection des données (accountability) voire l'embauche d'un délégué à la protection des données (DPO). Mais il a fallu également depuis 2018 naviguer à vue entre les interprétations fluctuantes et les jurisprudences nouvelles pour adapter en conséquence leurs traitements, voire même leurs modèles d'affaires.

Cinq ans plus tard et alors que le cadre réglementaire n'est pas encore stabilisé, la déception est donc immense quant au constat qu'à l'inverse de ce qui était visé, un véritable climat de défiance s'est progressivement installé. Ce climat ne s'explique qu'en partie par des incidents de fuites de données qui, bien que très médiatisés, furent au final assez rares et principalement le fait d'actes malveillants.

Au-delà de ces actes de malveillance (hacking, phishing, spoofing…), ce climat s'explique donc surtout d'une part par une expérience utilisateur pour le moins déroutante qu'illustre parfaitement l'évolution du recueil de consentement aux cookies par exemple, entre incompréhension des enjeux et fatigue du consentement.

Il s'explique d'autre part par l'insécurité juridique dans laquelle évoluent les entreprises, comme par exemple sur la question du transfert hors de l'Union européenne des données avec l'invalidation du Privacy Shield qui les a laissées jusqu'à aujourd'hui sans solution satisfaisante pour accomplir les transferts qui restent pour elles nécessaires. Elles doivent encore attendre que les négociations entre les autorités européennes et américaines aboutissent

avec l'adoption d'un accord qui sera très probablement attaqué en justice....

Il s'explique également par le rythme effréné des mises en demeure et des sanctions prononcées, toujours plus fortes, largement communiquées par les Autorités de régulation - qui en font les seuls indicateurs de l'efficacité de leurs interventions. Les sanctions et sujets en cause visent souvent des services devenus des quasi-commodités numériques, mais qui demeurent pour autant souvent inintelligibles pour le commun des mortels… Voire pour l'industrie numérique dans son ensemble qui tremble à l'idée qu'une décision fasse nouvelle jurisprudence et déstabilise les modèles économiques mis en place, comme nous l'ont témoigné la quasi intégralité des entreprises auditionnées.

Il s'explique enfin par la stigmatisation constante, par certains activistes, des modèles économiques reposant sur la gratuité (modèle publicitaire notamment) et l'échange de données, activistes qui sous couvert d'une attention spécifique portée à la protection des données personnelles, confessent viser en réalité à interdire purement et simplement ces modèles.

5 ans après, des utilisateurs méfiants et des entreprises tétanisées

Selon le baromètre de la confiance numérique (Acsel) de novembre 2022, même si le résultat est en hausse, les Français sont encore légèrement plus nombreux à ne pas faire confiance au numérique (47%) qu'à lui faire confiance (46%). Les jeunes sont en outre plus méfiants que la moyenne quant à la capacité des réseaux sociaux à garantir la protection de leurs données personnelles (54% pour les 15-24 ans, soit -6 points par rapport à 2021). Réalisé par Data Legal Drive en partenariat avec l'AFJE et Lefebvre Dalloz, le baromètre RGPD 2022 révèle quant à lui que 53% des entreprises disent redouter un contrôle de la CNIL et le prononcé de sanctions avec la procédure de sanction simplifiée pour les cas les moins complexes et les manquements les plus courants.

Accountability : une approche finalement très pénalisante pour les entreprises

Le RGPD portait en lui la promesse d'une plus grande fluidité de la gestion de la conformité, avec la fin des formalités préalables remplacées par le principe d'accountability (à savoir l'obligation de "rendre des comptes") inspiré des mécanismes de co-régulation expérimentés de longue date outre-Atlantique. Une forme de co-régulation associant responsables de traitement et autorités avec l'aide de codes de conduite et de certifications devait ainsi se mettre en place sous le signe de la conformité et de la transparence. En contrepartie cependant, si la mise en œuvre de l'accountability devait in fine réduire les amendes, une augmentation des sanctions

maximum pouvant atteindre 4% du chiffre d'affaires mondial devait servir d'épée de Damoclès.

Loin de la théorie, en réalité, le dossier de documentation pour la conformité attendu des autorités peut représenter, selon le contexte, une véritable somme à produire ! Si bien que les entreprises auditionnées nous ont souvent indiqué faire face à un processus de documentation sans fin.

Annexe ⏭ Le dossier de conformité : une véritable somme à produire

---

RGPD : une règle de droit européenne à portée internationale certes mais interprétée différemment et donnant la prime au mieux disant

D'aucuns reconnaissent aujourd'hui que le RGPD est devenu une règle de droit internationale en ce qu'il inspire la rédaction de réglementations semblables dans le monde. En réalité, c'est moins sa qualité intrinsèque que sa portée extra-territoriale (art. 3) qui a contraint les autres territoires à un alignement de fait. Il est d'ailleurs à craindre que dans d'autres zones géographiques s'élaborent également des réglementations relatives à l'accès aux données, suscitant alors des conflits de loi (comme dans le cas du Cloud Act).

En tant que règlement, norme d'application directe, le RGPD laissait pour autant entrevoir au moins une homogénéité dans sa mise en œuvre à l'intérieur de l'Union européenne. Avec la procédure dite du «guichet unique», il laissait accroire également à une relation centralisée avec l'autorité de contrôle de référence pour les groupes opérant sur plusieurs territoires européens. Il en fut en réalité tout autrement…

La question des bases légales a ainsi été l'objet d'interprétations diverses selon les autorités, jusqu'à susciter en 2022 une controverse entre la Commission européenne et l'autorité néerlandaise de protection des données (Autoriteit Persoonsgegevens) au sujet de leurs interprétations divergentes des situations dans lesquelles le traitement peut reposer sur l'intérêt légitime de l'entreprise. L'autorité irlandaise (DPC), qui accueille le siège de nombreux fournisseurs de services numériques en Europe, a vu son interprétation des bases légales (ici le contrat) également contestée cette fois par ses consoeurs allemandes et françaises, au point de susciter une décision contraignante du Comité européen de la protection des données (CEPD).

De même, le principe de coopération entre autorités en cas de traitement de données transfrontalier a conduit les autorités nationales à se prévaloir régulièrement d'une compétence propre pour ester en justice. Ainsi, pour tout sujet relatif aux cookies, la directive E-privacy motive une compétence nationale pour juger de problématiques relevant, elles, du consentement au traitement des données personnelles, c'est-à-dire du RGPD.

En outre, les voies de recours contre les décisions des autorités nationales diffèrent sensiblement selon les pays. Et l'interprétation licite du texte s'est en réalité précisée au gré des nombreuses jurisprudences issues des décisions de la CNIL, du Conseil d'Etat ou encore de la CJUE : des typologies de données aux transferts hors UE en passant par le consentement, la notion de responsable de traitement ou de sous-traitant. Des notions tout simplement décisives pour la définition du cadre légal dans lequel opèrent les entreprises !

RGPD, ePrivacy, Data/IA : à quel(s) saint(s) se vouer et… comment innover ?

Si la prévalence du RGPD a été affirmée par les co-législateurs européens, elle n'écarte pas les risques d'incohérence avec les autres textes en cours d'élaboration dans le domaine de la donnée. Le RGPD prévoit dans sa lettre l'application du principe de proportionnalité entre le droit à la protection des données à caractère personnel et les autres libertés et droits fondamentaux. En outre, il est précisé que le droit à la protection des données à caractère personnel n'est pas un droit absolu. En pratique, le RGPD entre directement en contradiction avec le développement de nombreuses technologies innovantes qui font l'objet de l'élaboration de nouvelles régulations.

Le Data Act crée un certain nombre d'obligations qui semblent pouvoir entrer en contradiction avec le RGPD. Le partage des données pour créer de la valeur économique se heurte au RGPD dont le principe est de minimiser des données en veillant à ne pas les partager avec des tiers non autorisés. De fait, le Data Act amplifie les exigences de portabilité du RGPD pour les détenteurs de données en visant aussi bien les données personnelles que les données non personnelles, sans clarifier son articulation avec le RGPD dans le cas des données personnelles et en renvoyant la définition de données non-personnelles à tout ce qui ne relève pas du RGPD. Un vrai labyrinthe pour qui veut se lancer dans des projets d'innovation par l'utilisation de la donnée !

Si le futur règlement E-privacy - s'il voit le jour - sera de fait Lex specialis par rapport au RGPD, nous pourrions nous retrouver dans une situation où la mise en œuvre d'un traitement nécessite la collecte de deux consentements distincts aux mêmes conditions de validité. Or les consentements requis par exemple pour le dépôt de cookies de mesure d'audience ou de détection de la fraude entrent en contradiction, sauf exemption justifiée, avec les obligations croissantes de transparence et de sécurité imposées aux responsables de traitement et qui requièrent de traiter des données personnelles pour s'y conformer ! On fait ainsi dépendre des traitements de données qui bénéficient à l'entreprise (mesure d'audience) ou à l'ensemble des utilisateurs (lutte contre la fraude) du bon vouloir des internautes de consentir ou non

individuellement au traitement de leurs données !

Alors que s'élabore l'IA Act, il apparaît évident que les principes de minimisation de la collecte de données personnelles et des finalités du RGPD entrent aussi en contradiction, même avec les principes d'innovation (machine learning) en intelligence artificielle qui reposent sur une collecte massive et une démarche heuristique. Il en va de même avec l'information et l'explicabilité requises dans des systèmes complexes fonctionnant comme des boîtes noires, ou encore avec la notion de prise de décision automatisée dont les exigences (article 22) semblent également incompatibles avec ce type de développements. A ce titre la liste des contraintes ou précautions soulevées par la CNIL ne semble pas compatible avec la plupart des scénarios de ce type d'innovations.

Dans le domaine de la mobilité, la CNIL a condamné à plusieurs reprises la collecte "disproportionnée" de données de géolocalisation de la part de sociétés de location de véhicules cherchant pourtant à assurer la maintenance et l'assistance ou à se prémunir contre les vols ou les infractions au code de la route, en relevant ces positions tous les 500 m ou toutes les 30 secondes… On comprend bien que c'est une approche formaliste du RPGD qui est privilégiée en lieu et place d'une approche par les risques qui serait plus à même de garantir l'équilibre avec les droits et libertés fondamentaux, parmi lesquels la liberté d'entreprise ou la fourniture de meilleurs services et prestations ou encore le respect du droit de propriété.

2. Le risque d'une déconnexion du réel

Les obligations concrètes sont trop déconnectées de la réalité réelle et laissent planer le doute sur les entreprises

Au sujet des contrats de traitement de données (Data Processing Agreements, DPA) à conclure entre le responsable de traitement et sous-traitant de données personnelles, les entreprises auditionnées ont toutes convergé : elles émettent un doute certain sur leur capacité à être strictement conformes au RGPD. Au gré des sanctions prononcées par la CNIL en France et des motivations présentées, ce sentiment ne fait que se renforcer…

La CNIL avait prévenu dès 2018 en évoquant "une montagne" à gravir et confirmé qu'aucune période de grâce ne serait accordée - même si une phase d'apprentissage serait en revanche nécessaire. Cette phase a été plus longue que prévue… Est-elle vraiment terminée cinq ans après l'entrée en vigueur du texte ? Un an après, le constat était que seule une entreprise sur trois était conforme selon une étude de Capgemini. Les premières plaintes furent déposées dès le lendemain de l'entrée en vigueur du texte et les premières sanctions ne tardèrent pas non plus.

Il faut toutefois reconnaître la logique de certaines décisions qui ont sanctionné les déficiences ou carences de certains responsables du traitement par exemple en matière de sécurité des données personnelles, comme ce fut le cas pour British Airways et le groupe Marriott sanctionnés en 2020 par l'ICO, l'autorité britannique compétente, en 2020 ou plus récemment par la CNIL de Slimpay (2021) et Free (2022) et Doctissimo (2023). C'est d'ailleurs un élément structurant à mettre au crédit du RGPD que celui d'imposer des bonnes pratiques en matière de cybersécurité à même de protéger les données personnelles des utilisateurs..

Les sanctions ultérieures ont néanmoins mis en exergue les difficultés auxquelles se trouvent confrontées les entreprises pour mettre en œuvre strictement les obligations découlant du RGPD. C'est le cas notamment de la durée de conservation des données, qui impose de fait de mettre en œuvre des procédures de suppression (purges) continues des données stockées.

Ces procédures peuvent se révéler être un casse-tête pour les entreprises tant le champ des données personnelles est large et imprécis et les données collectées de différentes formes par différentes sources au sein de l'entreprise. Ainsi, un simple e-mail archivé contenant un fichier de données reçu peut être la cause d'une conservation excessive… Le relèvement des exigences de sécurité peut aussi être un casse-tête lorsqu'il implique une mise en œuvre conjointe avec l'utilisateur. Ainsi, la mise en

œuvre de mots de passe de 12 caractères suppose une adoption réciproque et systémique de la part de tous les utilisateurs/clients et à défaut entraîne une sanction (Cf. Décision CNIL sanctionnant Infogreffe pour manquement à son obligation de sécurité en plus du manquement à son obligation de conservation pour une durée proportionnée à la finalité du traitement).

De même certains principes du RGPD comme la minimisation de la collecte se heurtent à une appréciation relativement subjective de la proportionnalité requise. Enfin, des sanctions prises à l’encontre d'un seul acteur ou bien certaines décisions de la CJUE ont un effet systémique et mettent immédiatement de nombreuses entreprises dans une situation de non-conformité. C’est le cas qu’illustre parfaitement l'invalidation du Privacy Shield ou encore de façon contiguë celle visant la solution de mesure d'audience Google Analytics.

De nombreuses entreprises nous ont ainsi indiqué se trouver démunies par rapport à ces décisions qui devraient selon elles faire davantage l’objet d’une approche par les risques. Or précisément la solution Google Analytics n’a jamais fait l’objet d’aucune demande de communication de données de la part des autorités américaines.

Autorités de contrôle : un agenda stratégique sous contrainte ?

Il est un fait indiscutable : ce sont en priorité les plaintes qui fixent l’agenda des Autorités de régulation. Pourquoi ? D’une part parce que leurs moyens sont réduits. Parce que ces plaintes suivent un rythme effréné depuis 2018 et qu’elles sont massives ! Et enfin parce que le RGPD impose aux autorités de traiter toutes les plaintes qu’elles reçoivent. Une association bien connue bat le fer depuis 2018 et fixe de fait le rythme des contrôles et des sanctions : None Of Your Business (NOYB) fondée par Max Schrems. Dédiée à la protection de la vie privée, elle confesse sans ambiguïté par l'intermédiaire de ses représentants s'opposer philosophiquement et radicalement aux modèles économiques reposant sur la monétisation des données personnelles et donc avoir l’industrie publicitaire en ligne de mire.

En mesure de déposer simultanément des plaintes dans les 27 Etats membres de l’Union européenne pour viser les entreprises qui y ont une activité, NOYB impose de fait aux autorités de travailler en concertation pour traiter prioritairement de ces plaintes en créant des groupes de travail ad hoc. Visant spécifiquement mais pas exclusivement les entreprises tech américaines dont le siège européen est en Irlande, NOYB dépose de nombreuses plaintes auprès de l'autorité irlandaise, qui a enregistré pas moins de 3 419 plaintes rien qu’en 2021. Mais sur des sujets relevant également de la directive E-privacy (les cookies par exemple), NOYB dépose volontiers ses plaintes auprès des différentes autorités nationales compétentes sur ce texte, en particulier celles réputées les plus strictes dans leur interprétation du droit. Or le caractère systémique des sanctions

visant les multinationales adtech (Cookies, Google Analytics) fait évidemment que c'est tout un écosystème d'entreprises qui est à chaque fois directement concerné.
Dans ce contexte, l'adéquation entre l'agenda de NOYB et des autorités de contrôle laisse parfois dubitatif… Comme en 2022 lorsque la CNIL annonçait le 24 novembre un plan d'action visant les applications mobiles et "qu'elle pourrait décider de mettre en œuvre un plan de contrôle de grande ampleur, comme cela avait été réalisé dans le cadre des actions liées aux cookies et autres traceurs." Et que 5 jours plus tard, le représentant de NOYB en France confiait de son côté au JDN "Nous travaillons sur l'élaboration de plaintes visant les applications mobiles qui collectent les données des utilisateurs à leur insu, via leur SDK, soit pour manque d'information aux utilisateurs, soit pour violation de leur consentement".

Co-régulation : des outils et démarches non fonctionnels

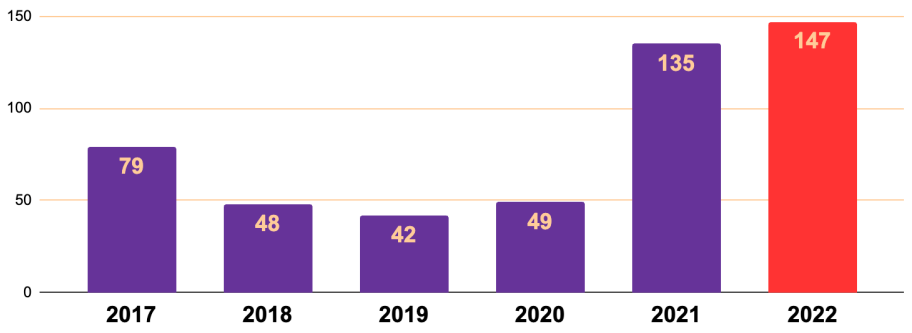
Afin de mettre en œuvre le transfert de données, hors Union européenne, des moyens sont mis à disposition des entreprises : il peut s'agir soit des codes de conduite ou des certifications ou bien encore des clauses contractuelles types (CCT) et des Binding Corporate Rules (Règles d'entreprise contraignantes, BCR) en ce qui concerne plus spécifiquement les transferts de données hors UE.

Les clauses contractuelles sont conclues au cas par cas et donc potentiellement très nombreuses pour les entreprises mondialisées. Ces clauses sont souvent standardisées sous la forme de « clauses types » validées par la Commission européenne. Mais elles ont été mises à jour en 2021, ce qui contraint les entreprises à renégocier les contrats en cours pour y intégrer ces nouvelles clauses ou à utiliser un autre outil de transfert. Conçues en concertation avec les autorités de régulation, les BCR doivent permettre aux multinationales d'organiser de façon systématique les transferts intra-groupes dans le respect du RGPD. Mais elles impliquent la mise en conformité de toutes les filiales y compris situées dans des pays sans législation de protection des données. En théorie, l'élaboration des BCR prend plusieurs mois et peut impliquer plusieurs Autorités de régulation de plusieurs pays. Mais plusieurs entreprises auditionnées nous ont évoqué en réalité plusieurs années avant d'obtenir la validation de leur BCR… Des délais de nature à rendre ces dispositifs in fine inopérants et à dissuader de s'engager dans la démarche…

Cadre général coiffant tous ces dispositifs pour le transfert outre-Atlantique de données, le Privacy Shield a été, on le sait, invalidé par la CJUE. Du jour au lendemain, les entreprises concernées se sont trouvées en défaut potentiel de conformité et sans autre recommandation que d'assumer seules une analyse des risques en fonction des législations locales et d'engager les mesures complémentaires nécessaires…

Quant aux codes de conduite qui permettent à un secteur d'activité, via une fédération professionnelle, d'accompagner cette mise en conformité à travers la diffusion de bonnes pratiques et de spécifier l'application du RGPD à un secteur donné, ils n'ont pas du tout rencontré le succès escompté. Seuls deux codes de conduite européens ont vu le jour depuis l'entrée en vigueur du RGPD : le code de conduite des fournisseurs d'infrastructures cloud relatif à la protection des données mis en œuvre par le CISPE (Cloud Infrastructure Services Providers in Europe) et le code de conduite européen pour les prestataires de Cloud !

Le prix de la sanction
Mises en demeure de la CNIL en 2022



Depuis l'entrée en application du RGPD, les amendes prononcées par les autorités européennes de protection des données dépassent le montant total de 2,5 milliards d'euros. La CNIL a de son côté prononcé des sanctions pour un montant global d'un peu plus d'un demi-milliard d'euros (RGPD & ePrivacy).

Certaines autorités communiquent chaque année sur les montants des sanctions prononcées et produisent des graphiques dynamiques qui n'ont rien à envier à ceux que produisent les entreprises pour décrire leurs résultats économiques et financiers….

Pourtant le nombre et les montants des sanctions sont davantage le reflet du nombre de plaintes, de leur aboutissement et des entreprises ciblées que d'un climat particulier garantissant la protection de données personnelles.

En outre, les entreprises s'interrogent sur le calcul de ces montants en l'absence d'explication motivée ou d'un quelconque barème. Ce qui crée un climat très anxiogène au sein duquel les départements concernés des entreprises se trouvent dans l'incapacité de fournir une évaluation pertinente des risques financiers associés - cela relève pourtant de leur responsabilité. Cela alors qu'il serait envisageable de publier une échelle indicative comme le fait l'autorité néerlandaise. Enfin, il apparaît que certaines sanctions peuvent représenter des montants considérables au regard de l'activité économique de l'entreprise : 3% ou 4% du chiffre d'affaires, cela peut représenter 100% de la profitabilité pour certaines activités ! Pour renforcer les protections en ligne, cette politique du chiffre devrait être remplacée par une politique de la co-construction ou a minima du dialogue entre l'autorité compétente et les acteurs soumis au RGPD.

3. Refonder la régulation

Faut-il envisager de réviser le RGPD ?

Cinq ans après l'entrée en vigueur du RGPD, le constat est amer pour les entreprises. Esseulées dans leurs démarches de conformité, découragées par l'empilement successif des recommandations et autres opinions des autorités de régulation ainsi que par des réglementations s'ajoutant au RGPD et visant leur activité numérique, bridées dans leur capacité d'innovation, se sentant évoluer sous une épée de Damoclès, voire tétanisées à l'idée même d'un contrôle, elles nous ont confié leur souhait commun d'une révision du RGPD.

Le constat est unanime : la CNIL a adopté une approche qui fait prévaloir la protection des données personnelles sur les autres droits ou libertés alors qu'elle devrait concilier les différents droits fondamentaux et mieux tenir compte du principe de proportionnalité pourtant prévu par le texte sous le contrôle du juge si nécessaire.

Le constat est unanime : la CNIL a adopté une approche qui fait de la protection des données personnelles un quasi droit absolu qui prévaut sur tous les autres droits ou libertés. Cette approche entre en conflit avec le principe général de conciliation entre les différents droits fondamentaux et avec celui de proportionnalité pourtant prévus par le texte. Le RGPD devrait donc être révisé afin de contraindre davantage les autorités à mettre en œuvre ces principes.

En outre, il est constaté que la mission d'accompagnement des entreprises par la co-régulation dévolue aux autorités de régulation est in fine délaissée au profit du traitement des plaintes. Il est dès lors logique que, moins bien accompagnées et laissées dans l'incertitude juridique, sans possibilité d'expliquer aux autorités leurs activités et les traitements de données personnelles en découlant, les entreprises soient davantage sanctionnées. Au-delà des rares cas de violations délibérées, ce sont souvent une mauvaise communication avec une divergence dans l'interprétation de la mise en œuvre des dispositions du RGPD et de l'évaluation des risques qui génèrent une sanction de l'autorité de contrôle.

Des entreprises auditionnées et qui ont fait l'objet de contrôles, nous ont indiqué une difficulté à établir un dialogue constructif. D'autres ont reconnu ne pas chercher à l'engager en amont, ne pas vouloir prendre le risque d'affronter une possible hostilité de principe et préférer plutôt envisager de "passer sous le radar"...

L'accompagnement, ce n'est pas seulement celui de la mise en conformité mais c'est aussi celui du processus d'innovation. Or de nombreuses décisions ont visé des domaines très innovants, semblant mettre en cause certains modèles, comme dans le domaine de la mobilité. Ce qui démontre l'intérêt

d'avoir davantage recours aux bacs à sable réglementaires.

L'accompagnement de l'innovation est en effet décisif pour permettre aux entreprises concernées de développer leurs produits et services dans un cadre protecteur pour les utilisateurs. Les entreprises françaises et européennes ont le sentiment d'avancer avec de véritables "boulets réglementaires" aux pieds en comparaison de leurs homologues américaines ou asiatiques.

Pourtant l'effectivité d'un droit ne se mesure pas qu'à l'aune de la sanction, mais aussi à celle de sa mise en œuvre pratique. Comment être Privacy by design sans être accompagné, sans une régulation pro-innovation, sans évaluation de l'innovation au regard du risque? Il est des domaines où le "y'a qu'à faut qu'on" ne suffit pas.

Les restrictions du RGPD à la circulation des données en dehors de l'Union européenne créent également une situation de blocage avec certains territoires pour les transferts de données qui sont pourtant le propre de l'économie numérique, voire de toute multinationale effectuant des transferts intra-groupe. Blocage insoluble et très préjudiciable pour les entreprises européennes : 80% des organisations européennes utilisent par exemple Google Analytics et se sont retrouvées du jour au lendemain sans solution alternative et avec la peur d'être sanctionnées par la CNIL.

La récente décision de la CNIL concernant l'entreprise Lusha démontre enfin qu'une société non établie en Europe peut exercer une activité de scraping et de monétisation des données qu'une société établie en Europe ne peut licitement effectuer… Faut-il y déceler une incitation à s'expatrier pour toutes les sociétés de datamarketing qui exercent leur métier avec de plus en plus de difficultés face aux contraintes de conformité.

Changer la culture de la régulation en particulier en France

Les entreprises auditionnées ont également convergé, lorsqu'elles opèrent dans plusieurs territoires, pour soulever une différence de culture de la régulation entre les autorités des différents Etats européens. En question, premièrement, la culture du dialogue…

La CNIL a il est vrai publié de nombreuses recommandations sectorielles qui veulent traduire indéniablement une démarche d'accompagnement des entreprises. Mais ces recommandations n'ont pas toujours fait l'objet de concertations préalables ou bien les entreprises concernées ont eu le sentiment que leur voix n'était pas prise en compte selon une approche qui aurait pu être ainsi plus pragmatique, comme dans le cas des lignes directrices visant les cookies publicitaires par exemple.

Codes de conduite, bacs à sable réglementaires : les autorités de protection des données devraient favoriser ces échanges en particulier en amont de l'adoption de ces recommandations - voire les tester avec quelques entreprises avant leur publication (“policy prototyping”)... Les autorités ont eu aussi tendance à refuser de travailler sur des codes de conduite avec les secteurs dans lesquels des plaintes ont été déposées. Pourtant rien ne l'interdit dans le RGPD. Cela indique, selon les entreprises auditionnées, une absence de volonté d'accompagner certains secteurs pour les aider à identifier les solutions conformes au RGPD, mais en revanche une volonté de sanctionner. Certaines entreprises soulignent aussi que cela traduit en creux une condamnation sans équivoque de business models ou de secteurs dont les modèles reposent en effet sur l'utilisation de la donnée.

Une mise en oeuvre de la régulation qui doit également innover dans son approche

En cause également durant les auditions, un fonctionnement de l’autorité de régulation en silos qui néglige les effets de ses décisions sur les autres équilibres, quitte à corriger un dysfonctionnement et de fait à en susciter un autre dans le domaine de compétence d’une autre autorité de régulation !

C’est pourtant précisément un domaine où il est tout à fait possible d’innover. Le modèle mis en place dans le domaine de la publicité peut ainsi inspirer. L’ARCOM a confié à l’autorégulation au sein de l’ARPP des compétences étendues d’intervention et de contrôle. L'exemple espagnol est également intéressant en ce qu'il confie des responsabilités concernant le traitement des plaintes à une association professionnelle dont le code de conduite a été préalablement validé.

La coopération entre organisations est clé pour assurer d’une part une application plus pragmatique du RGPD et d’autre part un accompagnement plus pertinent des entreprises. A ce titre, au Royaume-Uni, l'autorité de la concurrence (CMA), l'autorité de protection des données (ICO) et le régulateur financier ont créé un forum de coopération : le Digital Regulatory Cooperation Forum. En France, une consultation du PEReN (Pôle d’Expertise de la Régulation Numérique, service à compétence nationale, qui mobilise une équipe d’experts data scientists, docteurs ou ingénieurs compétents en matière d’analyse de données) est certes possible mais demeure facultative.

Ces bonnes pratiques doivent être systématisées et organisées. Elles contribueront à mettre en place une régulation en phase avec la transversalité de l’économie numérique et la réalité des entreprises.

4. Nos propositions

4.1 - Changer de cap / de paradigme dans l'interprétation du RGPD

- Appliquer l'approche par les risques prévue par le RGPD reposant sur l'évaluation de la probabilité et de la sévérité des risques pour les droits et libertés des personnes

- Baser davantage les décisions sur le considérant 4 du RGPD selon lequel le droit à la protection des données à caractère personnel n'est pas un droit absolu et qu'il doit être mis en balance avec les autres droits fondamentaux, conformément au principe de proportionnalité, notamment avec la liberté d'entreprise ;

- Mieux équilibrer les bénéfices et les risques des traitements de données personnelles

- Adopter une approche pragmatique et raisonnable dans la mise en œuvre des droits des personnes pour éviter les abus de droit

- Reconnaître que le risque zéro n'existe pas et que les obligations du RGPD sont généralement davantage des obligations de moyens que de résultat qui se traduisent dans la mise en place d'un programme d'amélioration continue

---

4.2 - Avoir une approche raisonnable dans la mise en oeuvre des sanctions

- Prévoir la possibilité pour la CNIL de classer sans suite des plaintes formulées par des requérants

- Créer une possibilité de confrontation d'une décision de la CNIL au regard d'une autre autorité de régulation au profit de l'entreprise mise en cause

- Créer une obligation de motiver de façon explicite le montant des sanctions en relation avec les infractions constatées et la jurisprudence, avec la communication d'une échelle indicative des sanctions possibles

- Reconnaître les investissements des entreprises dans les techniques d'anonymisation et de pseudonymisation comme des mesures de réduction des risques qui doivent être prises en compte dans la détermination de la sanction

4.3 - Avoir une approche plus constructive dans la production de droit souple

- Solliciter l'opinion des différentes parties prenantes dans une phase de pré-consultation avant de rédiger le premier projet de recommandation/avis

- Dans le cadre des consultations publiques, être transparent sur les commentaires reçus et expliquer pourquoi telle ou telle proposition de modification a été rejetée

- Effectuer une analyse d'impact économique en amont de l'adoption d'une recommandation ou d'un avis

- Adopter des recommandations/avis nuancés qui proposent des solutions sans être trop prescriptifs et en laissant une marge de manœuvre aux organisations pour atteindre l'objectif recherché par le texte

- Faire tester les recommandations/avis par une sélection d'entreprises/un comité consultatif d'experts pour tester la faisabilité de leur mise en oeuvre en amont de leur publication finale

---

4.4 - Accélérer l'accompagnement des entreprises

- Organiser un cadre pérenne et adapté aux besoins des entreprises pour les expérimentations (bacs à sable réglementaires) et l'innovation en collaboration avec les autres régulateurs

---

4.5 - Modifier la composition de la CNIL

- Modifier la composition du Collège de la CNIL pour permettre à des représentants du monde économique et des acteurs de l'innovation d'y siéger

- Renforcer les ressources de la CNIL avec davantage de profils ayant une expérience significative dans la mise en oeuvre concrète des règles

- Améliorer l'information et la transparence du mécanisme de consultation pour avis des CNIL européennes

---

4.6 - Faire de la CNIL le moteur d'une inter-régulation effective

Promouvoir les mécanismes d'inter-régulation et la coopération entre les autorités de régulation sur les sujets concernant le numérique

- Créer une instance de coopération entre autorités de régulation où les différents enjeux de compétitivité, de protection de données, de protection de l'ordre public,... seraient considérées, dans une approche d'inter-régulation de l'économie de la donnée

- Prévoir un renforcement de l'inter-régulation et des saisines pour avis entre les autorités de régulation selon les sujets examinés ;

    - Possibilité de prévoir des obligations de demande d'avis ou de saisines dans la loi ;
-
    - Exemple : l'article R 463-9 du Code de Commerce qui impose au rapporteur de l'Autorité de la Concurrence de communiquer à un certain nombre d'autorités toute saisine relative à des secteurs entrant dans leur champ de compétences afin de leur permettre de faire part de leurs observations

- Adopter le principe de confier la mise en oeuvre des textes à l'autorité de régulation la plus à même d'en atteindre les objectifs

Pour aller plus loin

CNIL

Le règlement général sur la protection des données - RGP

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, et abrogeant la directive 95/46/CE.

>> Lire

Le rapport annuel 2022 de la CNIL

Renforcement de l'accompagnement des entreprises et administrations, campagnes d'information du public et éducation au numérique des plus jeunes, plaintes et action répressive, future réglementation européenne sur la donnée : dans ce nouveau rapport, la CNIL revient sur les temps forts de l'année 2022.

>> Lire

Table-ronde des Assises Data Transformation du 26 janvier 2023

RGPD: au défi de la souveraineté et de la compétitivité

A la faveur des Assises Data Transformation dont elle est partenaire, La villa numeris initie ses travaux sur le RGPD qui s'imposent à tous les acteurs économiques depuis cinq ans. Avec la participation de Juliette Rouilloux-Sicre, vice-présidente Data, Propriété intellectuelle et Cyber du groupe Thales, et Nicolas Rieul, vice-président d'Europe de l'Ouest de Criteo.

>> Lire et regarder

#DigiLex Observatoire des enjeux législatifs de la transformation du 13 avril 2023

L'économie numérique au défi de la régulation

Alors que les lois et règlements s'empilent et se chevauchent, focus sur des autorités indépendantes devant réguler des acteurs sur des marchés en évolution constante. Avec la participation de Jean Hingray, sénateur, Laure de La Raudière, présidente de l'ARCEP, Thaima Samman, avocate spécialisée en affaires publiques et réglementation, et Laurent Benzoni, économiste, professeur d'économie à l'Université Panthéon-Assas.

>> Lire

Le dossier de conformité : une véritable somme à produire

Selon le contexte (nature et volume des données traitées notamment), le dossier d'accountability permettant à l'entreprise de démontrer sa conformité au RGPD, en cas de demande de l'autorité de contrôle, devra comporter les documents suivants régulièrement actualisés, classés par thèmes:

Les fondamentaux de la conformité :

- Code d'éthique sur les principes fondamentaux appliqués par l'organisme
- Documentation relative à la nomination du DPO et ses relais locaux
- Cartographie des traitements et schémas des flux de données
- Registre des traitements
- Fiches par traitement (précisions et justifications détaillées des choix et prises de position effectués)
- Evaluation des risques du traitement et analyse d'impact relative à la protection des données

Transparence et information des personnes :

- Procédure sur la gestion des demandes de droits d'accès RGPD par les salariés (suppression, opposition, portabilité, etc.)
- Procédure sur la gestion des demandes de droits d'accès RGPD par les clients
- Politique de confidentialité interne destinée aux salariés de l'organisme
- Politique de confidentialité externe destinée aux candidats au recrutement
- Politique de confidentialité externe destinée aux clients de l'organisme
- Politique de confidentialité externe destinée aux partenaires/fournisseurs
- Politique de confidentialité du site web et gestion des cookies
- Formulaires de consentement
- Modalités de gestion des preuves des recueils de consentements (traçabilité)
- Formulaires types permettant l'exercice des droits RGPD par les salariés et clients
- Traçabilité des traitements effectués en réponse aux demandes d'exercice des droits RGPD

Sécurité, intégrité et confidentialité :

- Politique de Sécurité des Systèmes d'Informations (PSSI)
- Procédure sur les durées de conservation des données, l'archivage et la suppression
- Procédure sur la gestion et la notification des violations de données (data breach)
- Procédure sur la gestion et la conduite des analyses d'impact
- Procédure d'anonymisation/de pseudonymisation des données
- Procédure sur la gestion des projets impliquant les principes de privacy by design/ by default

- Codes de conduite par métier sur les conditions de traitement des données personnelles (DSI, RH, marketing, innovation)
- Charte informatique
- Règlement intérieur
- Rapports des tests d'intrusion et plans d'actions de régularisation
- Rapports des analyses d'impact effectuées sur les traitements à risque
- Traçabilité des violations de données personnelles et conditions de traitement des incidents rencontrés
- PCA - PRA
- Support de sensibilisation/formation RGPD des salariés, feuilles de présence et thèmes abordés
- Certification ISO

Aspects contractuels :

- Politique d'éthique du choix des fournisseurs et partenaires (sous-traitants)
- Liste exhaustive des sous-traitants RGPD, localisation et périmètre d'activité
- Procédure sur le transfert des données personnelles hors UE
- Convention intragroupe, BCR
- Contrats sous-traitants / avenants RGPD
- Contrats de travail des salariés (RH, DSI, marketing, etc.) traitant les données (clause sur obligation de confidentialité spécifique)

Contrôle et audit de l'efficacité des mesures déployées :

- Politique d'audit interne (périodicité, périmètre contrôlé, plan d'audit, tests sur échantillons aléatoires)

//. La villa numeris

Penser digital, rendre réel. La villa numeris est un think tank indépendant qui promeut un modèle européen et ouvert du digital affirmant la primauté de l'humain.

Notre mission : permettre aux décideurs de comprendre et d'anticiper les transformations sociétales et économiques, d'agir en conséquence, de sensibiliser et de mobiliser pour donner du sens aux organisations et réussir leur mutation.

La villa numeris est une association de Loi 1901 présidée par David Lacombled.

Nos travaux :

:: Une approche généraliste sur de grandes thématiques : IA, data, tech, nouvelles formes de travail, santé, territoires connectés, lutte contre les fake news, ...

:: Des rencontres exclusives : 3 cycles de rencontres exigeants et conviviaux avec des dirigeants, acteurs de la révolution digitale : les tendances du marché, les enjeux citoyens et la géostratégie

:: Une plateforme dédiée : centre de ressources, de services et de partage

:: Des opérations spéciales et exclusives : assises de la Data transformation en janvier à Bercy, Observatoire de la Souveraineté numérique

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