EXPERTISES
DROIT, TECHNOLOGIES & PROSPECTIVES
MARS 2026 - N°521
EXPERTISES DES SYSTÈMES D'INFORMATION

LA PREUVE DE LA MANIPULATION PAR L'ÉCONOMIE COMPORTEMENTALE

EXPERTISES MARS 2026
N°521

EXPERTISES
DROIT, TECHNOLOGIES & PROSPECTIVES

SOMMAIRE

Directeur de la publication :
Philippe THOMAS
Directeur de la rédaction :
Jean ALBERT
Rédactrice en chef :
Sylvie ROZENFELD / sr@expertises.info
Doctrines :
EVA ASPE
FABRICE DEGROOTE
ALEXANDRE FIEVEE
FLORENT GASTAUD
DANIEL GUINIER
ALEXANDRA ITEANU
ETIENNE JABOEUF
ANNE-MAUD LAGARDE
GARANCE MATHIAS
Maquette, conception et couverture
Jérôme VADON / jerome@vadon.fr
Impression : Imprimerie Hiver
156 rue Oberkampf, 75011 Paris
Dépot légal : Mars 2026
ISSN 2824-8775 (digital) / ISSN 2606-037X (imprimé)
Informatique et libertés : Les noms, prénoms et adresses de nos abonnés sont communiqués à nos services internes et aux organismes liés contractuellement avec Expertises, sauf opposition. Dans ce cas, la communication sera limitée au service de l'abonnement. Les informations pourront faire l'objet d'un droit d'accès ou de rectification dans le cadre légal. **Reproduction :** Le Centre français d'exploitation du droit de copie (CFC) n'est pas mandaté par la société Celog Participations, éditrice de la revue Expertises, pour délivrer des autorisations de reproduction de copies payantes. **Formation :** Cette publication peut être utilisée dans le cadre de la formation permanente. **Fondateur :** Daniel Duthil
Publié par APP Solutions : RCS Paris 519 136 170
N° commission paritaire publications et agences de presse : 0523 T 83093. 11 numéros par an.

RGPD

Les codes de conduite : un levier de conformité sectoriel au service des DPO

Analyse du régime juridique des codes de conduite, outils de simplification de mise en conformité aux dispositions applicables en matière de protection des données personnelles pour les acteurs privés et publics : l'exemple du code de conduite CISPE « *Cloud Infrastructure Services Providers in Europe* »

L'entrée en application du Règlement général sur la protection des données (RGPD) le 25 mai 2018 a marqué un changement de paradigme fondamental : le passage d'une logique de formalités administratives préalables à un principe de responsabilité active, l'accountability. Dans ce nouveau cadre, les responsables de traitement et les sous-traitants ne doivent plus seulement respecter la loi, ils doivent être en mesure de démontrer, à tout moment, cette conformité[1].

Pour accompagner les acteurs dans cette démarche, le législateur européen a prévu une panoplie d'outils de responsabilisation. Parmi eux, les codes de conduite occupent une place singulière. Conçus comme des instruments de « *co-réglementation* », ils visent à traduire les principes parfois généraux du RGPD en règles opérationnelles, adaptées aux spécificités de secteurs d'activité donnés. En outre, ils peuvent contribuer à réduire les éventuelles différences d'harmonisation entre les États membres[2]. Pourtant, malgré leur potentiel de sécurisation juridique, force est de constater que l'usage des codes de conduite demeure modeste ; le fonctionnement du dispositif est relativement méconnu des professionnels du secteur et notamment des Data Protection Officer (DPO).

Le code de conduite de l'association CISPE (Cloud Infrastructure Services Providers in Europe), premier code de conduite transnational approuvé dans l'Union par avis de l'EDPB en mai 2021[3] constitue un précieux instrument qui permet de disposer d'un recul de plusieurs années sur le processus de création d'un code de conduite, son approbation par les autorités compétentes et ses apports en matière de conformité. Cet article se propose d'analyser le régime juridique des codes de conduite et d'illustrer, à travers l'exemple de CISPE, comment ils simplifient la mise en conformité d'acteurs privés et publics aux dispositions applicables en matière de protection des données personnelles.

Le mécanisme réglementaire des codes de conduite : un outil de "co-réglementation"

Le régime des codes de conduite est principalement régi par les articles 40 et 41 du RGPD, complétés par les lignes directrices 1/2019 du Comité Européen de la Protection des Données (EDPB).

Nature et objectifs d'un code de conduite

Le code de conduite est un instrument de responsabilisation volontaire. Contrairement à la loi qui s'impose par nature, la création d'un code de conduite ainsi que l'adhésion ultérieure à celui-ci résultent d'actes volontaires. La vocation première des codes de conduite est de préciser l'application du RGPD en intégrant les particularités d'un secteur spécifique et/ou de ses activités de traitement. Comme le souligne l'EDPB[4], un code ne doit pas se contenter de paraphraser le texte légal ; il doit apporter une « *valeur ajoutée* » en proposant des solutions concrètes aux problématiques propres à un secteur.

Un processus de création exigeant

La faculté de rédiger et de présenter un code est réservée aux associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants[5]. Les « *propriétaires du code* » (porteurs du projet) doivent démontrer leur capacité à comprendre et à porter les intérêts de leur secteur. Selon l'EDPB, cette représentativité s'évalue au regard du nombre de membres représentés ou de l'expérience de l'organisme dans les activités de traitement concernées. Il peut s'agir de fédérations professionnelles, de syndicats sectoriels ou d'associations ayant pour membres des sociétés généralement concurrentes intervenant dans un secteur d'activité donné (ce qui est par exemple le cas pour l'association CISPE, qui regroupe des acteurs concurrents comme AWS, OVH, ARUBA, etc.). Dans ce dernier cas, la rédaction d'un code de conduite nécessite donc un important travail de collaboration, entre des acteurs traditionnellement concurrents, aux visions parfois divergentes.

Une procédure d'approbation rigoureuse

L'approbation d'un code de conduite suit une procédure stricte. Pour les codes nationaux, l'autorité de contrôle (comme la Cnil en France) valide le texte. Pour les codes transnationaux, qui couvrent des activités dans plusieurs États membres, le mécanisme de contrôle de la cohérence s'applique : l'autorité chef de file soumet le projet à l'EDPB qui rend un avis contraignant[6]. Une fois l'avis favorable rendu, l'autorité nationale cheffe de file approuve officiellement le code. Il est ensuite inscrit dans le registre public de l'Union européenne. Ces mécanismes permettent de garantir le sérieux et la conformité des codes de conduite approuvés eu égard aux dispositions réglementaires.

Le rôle central des "Monitoring Bodies"

Un code de conduite ne peut être validé s'il ne prévoit pas de mécanisme de contrôle. En pratique, ce sont les "Monitoring Bodies" qui jouent ce rôle. Ces organismes doivent être accrédités par l'autorité de contrôle compétente.

Pour être agréés par une autorité nationale comme la Cnil, ils doivent justifier d'une indépendance totale, d'une expertise technique sectorielle et de l'absence de conflit d'intérêts. En pratique, leurs missions consistent à évaluer l'éligibilité des candidats à un code de conduite (i.e. une société souhaitant déclarer qu'elle respecte les exigences d'un Code de Conduite à titre d'exemple), à réaliser des audits périodiques et à traiter les réclamations de manière transparente. En tant qu'organes de régulation, ils disposent de pouvoirs de sanction gradués, allant de l'avertissement à l'exclusion définitive d'un code de conduite.

Les "Monitoring Bodies" sont la garantie d'une conformité supervisée par un tiers, sécurisant ainsi l'analyse de risques et simplifiant les processus de vérification des exigences d'un code de conduite.

Un usage modeste des codes de conduite face aux ambitions des régulateurs

Alors que les codes de conduite sont présentés comme une « *méthode pratique, potentiellement rentable et pertinente* » pour harmoniser la protection des données au sein de l'Union européenne[7], leur nombre et leurs usages restent limités plusieurs années après l'entrée en vigueur du RGPD.

Les causes de la frilosité des acteurs

Plusieurs facteurs peuvent expliquer un usage modeste de cet instrument juridique :

- D'abord, le nombre limité de structures pouvant prétendre initier la rédaction d'un code de conduite : l'exigence de représentativité d'un secteur pouvant être difficile à atteindre ;
- Ensuite, les moyens étant nécessaires pour déployer un tel projet et le maintenir dans le temps. Les processus de création, de concertation et d'approbation d'un code de conduite étant souvent longs et chronophages. En outre, la rigueur des critères d'approbation fixés par l'EDPB a certainement pu décourager certains groupements ;
- Enfin, cet instrument a finalement fait l'objet de peu de communication de la part des autorités de contrôle, ce qui n'a pas contribué, à date, à sa démocratisation.

Pourtant, la rareté des codes validés et leur usage modeste par les acteurs économiques sont certainement préjudiciables aux entreprises, en particulier aux PME. Pour ces dernières, un code de conduite constitue un « *recueil de règles* » clés en main, leur évitant de mener individuellement des analyses de conformité exhaustives et coûteuses, notamment pour la sélection de leurs sous-traitants.

Les intérêts d'un code de conduite, à l'instar du code CISPE

Dans ce paysage encore clairsemé, le code de conduite CISPE fut le premier à faire l'objet d'un avis favorable de l'EDPB en mai 2021 et d'une approbation formelle de la part de la Cnil[8]. Il se concentre, à ce jour, exclusivement sur les fournisseurs d'Infrastructure As a Service (IaaS).

Une délimitation claire des responsabilités du fournisseur d'IaaS

L'un des apports majeurs du code CISPE est la clarification de la répartition des responsabilités entre le fournisseur d'Infrastructure-as-a-Service (IaaS) et son client, utilisateur du service. À la différence du SaaS (Software as a Service), où le fournisseur dispose d'un contrôle sur l'application, le fournisseur d'IaaS fournit un « *matériel virtualisé* » dont il ignore, par essence, le contenu. À ce titre, il ne peut, en qualité de sous-traitant, disposer du même niveau d'intervention qu'un fournisseur de SaaS, notamment en matière d'assistance d'un responsable de traitement quant à l'exercice du droit des personnes ou encore dans la mise en œuvre de mesures de purges des données.

L'un des intérêts d'un code de conduite sectoriel est alors de fixer des obligations à charge des parties, en cohérence avec les particularités sectorielles concernées ; tout en permettant le respect des exigences du RGPD.

La mise en œuvre d'obligations allant au-delà des dispositions du RGPD

Le code de conduite CISPE vise également à fournir des garanties pouvant aller au-delà des simples exigences du RGPD. À titre d'exemple, les fournisseurs d'IaaS souhaitant respecter les exigences du code doivent prendre des mesures particulièrement protectrices. C'est notamment le cas :

- en matière de sécurité. Alors même que l'article 32 du RGPD fixe des obligations de sécurité très générales, le code de conduite CISPE impose aux fournisseurs d'IaaS la mise en œuvre de nombreuses obligations concrètes en matière de sécurité, qui sont listées de manière très précise en Annexe A du code. Pour certaines de ces exigences, un mécanisme "d'équivalence" est mis en œuvre avec certaines normes internationales (comme l'ISO 27001 par exemple), afin qu'un fournisseur d'IaaS certifié selon ces normes équivalentes puisse accélérer et faciliter son processus de vérification des exigences du code de conduite CISPE par un Monitoring Body ;
- en matière de localisation des données. Une caractéristique distinctive du code CISPE est l'obligation pour chaque service conforme d'offrir à ses clients la possibilité de stocker et traiter ses données exclusivement dans l'Espace Économique Européen ;
- en matière de contrôle de la sous-traitance ultérieur. Tout en prévoyant des mécanismes de conformité compatibles à ceux prévus par le RGPD, le code de conduite CISPE apporte plus de sécurité et de transparence sur certains aspects. À titre d'exemple, dans le cadre d'une «*autorisation générale*», l'article 28-2) du RGPD prévoit que le sous-traitant «*informe le responsable du traitement de tout changement*» ; sans autres précisions. Aussi dans le cadre d'une «*autorisation générale*», le code de conduite CISPE impose aux fournisseurs d'IaaS «*d'informer par écrit (y compris par voie électronique)*» ses clients.

- en matière de gestion de violations de données. Tout en prévoyant des mécanismes de conformité compatibles à ceux prévus par le RGPD, le code de conduite CISPE comporte là encore des mesures plus protectrices pour les clients des fournisseurs d'IaaS. À titre d'exemple, conformément à l'article 33 du RGPD «*Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance*». Le code de conduite CISPE impose quant à lui aux fournisseurs d'IaaS de «*notifier le client sans délai dès lors qu'un CISP a obtenu l'assurance qu'une violation de données a eu lieu en rapport (...)*».

Au-delà de fournir un cadre adapté à un secteur d'activité donné, un code de conduite peut également s'avérer vertueux pour les droits et libertés des personnes concernées et/ou -comme dans le cadre de CISPE- des responsables de traitement ; en visant des objectifs de sécurité et de conformité allant au-delà des exigences réglementaires.

La simplification de la due diligence pour les DPO

Pour un DPO, la sélection d'un sous-traitant informatique est souvent une source de complexité majeure. L'article 28.1 du RGPD impose de ne faire appel qu'à des sous-traitants présentant des « *garanties suffisantes* ». En pratique, cette obligation de vérification est souvent matérialisée par des questionnaires de sécurité interminables adressés aux prestataires informatiques ; en vue d'évaluer leurs mesures de sécurité et de conformité. Ces vérifications doivent être réalisées fournisseur par fournisseur ; ce qui est souvent extrêmement chronophage.

Le mécanisme des codes de conduite vise à faciliter ces mesures de vérification en externalisant ces vérifications à une autorité indépendante tierce -les Monitoring Bodies- qui fonde ses évaluations selon un référentiel clair, déterminé, et approuvé par les autorités de contrôle.

Pour les DPO, les codes de conduite peuvent donc devenir un allié de taille, apportant une réponse précieuse aux exigences de l'article 28 du RGPD et facilitant leur travail d'appréciation de la conformité de leurs partenaires.

À l'instar d'une certification ISO 27001 en matière de SMS (Système de Management de la Sécurité de l'Information), le respect des exigences du code de conduite CISPE par un fournisseur d'IaaS constitue un marqueur, facilement identifiable, garantissant le respect de nombreuses exigences de conformité et de sécurité.

Conclusion

Le mécanisme des codes de conduite, bien qu'encore sous-utilisé, représente certainement une partie de l'avenir de la conformité au RGPD. En transformant des principes juridiques en exigences techniques et opérationnelles, ils réconcilient le droit et la technologie. L'exemple du code CISPE démontre qu'il est possible de déployer, en pratique, ce type d'instrument juridique, y compris dans un secteur d'activité fortement concurrentiel et au sein duquel ses acteurs disposent de visions parfois très éloignées, notamment sur les enjeux de transferts de données et de souveraineté numérique.

Le mécanisme des code de conduite réduit l'insécurité juridique, allège les processus de conformité et participe à renforcer la confiance dans l'écosystème numérique européen.

Il est désormais de la responsabilité des professionnels du droit d'encourager le recours à ces standards sectoriels et de privilégier, dans leurs recommandations, les prestataires ayant fait le choix de cette transparence supervisée.

Florent GASTAUD
DPO externalisé
Fondateur de Mon DPO externe
Membre du CCTF (Code of Conduct Task Force) de CISPE

Notes

(1) Article 5-2 du Règlement (UE) 2016/679 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

(2) Lignes directrices 1/2019 de l'EPDB, 4 juin 2019, relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679

(3) Avis 17/2021 de l'EPDB sur le projet de décision de l'autorité de contrôle française concernant le code de conduite européen soumis par les prestataires de services d'infrastructure en nuage (CISPE), 19 mai 2021

(4) Lignes directrices 1/2019 de l'EPDB, 4 juin 2019, relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679

(5) Article 40-2 du Règlement (UE) 2016/679 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

(6) Article 40-7 du Règlement (UE) 2016/679 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

(7) Lignes directrices 1/2019 de l'EPDB, 4 juin 2019, relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679

(8) Délibération n°2021-065 du 3 juin 2021 portant approbation du code de conduite européen porté par Cloud Infrastructure Service Providers Europe (CISPE)

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info