NOTE D'INFORMATION
ET D'ACTUALITÉ

Panorama des règlements européens sur le numérique

> COMPRENDRE LES RÉGLEMENTATIONS APPLICABLES

CIGREF
20 SEPTEMBRE 2023

Cigref
RÉUSSIR
LE NUMÉRIQUE

Cigref

Panorama des règlements européens sur le numérique

Comprendre les réglementations applicables

Septembre 2023

AVANT-PROPOS

Depuis l'irruption du RGPD dans le paysage réglementaire européen, et à l'occasion des travaux pilotés par le Cigref entre juin 2016 et novembre 2017 pour préparer au profit de nos adhérents son entrée en vigueur le 25 mai 2018, notre association et son Conseil d'administration ont acquis la conviction de l'importance d'une implication de notre part en amont de l'élaboration des textes législatifs européens. En effet, ce travail en amont doit permettre de se prémunir, d'une part, des excès de zèle réglementaires des institutions européennes, et, d'autre part, des moyens de lobbying exorbitants et asymétriques que les géants technologiques non européens savent déployer pour orienter les processus législatifs à leur profit. C'est dans ce contexte que le Cigref s'est doté d'une capacité d'appréciation, de décision et d'action en matière d'influence auprès de la Commission, du Conseil et du Parlement européens, afin de ne pas laisser ces processus législatifs, qui pourraient avoir un impact sur nos adhérents, à la seule main de leurs principaux fournisseurs de produits et services numériques.

La partie reste inégale, certes, et nous l'avons encore observé avec le refus de la Commission européenne de désigner AWS, Google Cloud et Microsoft comme gatekeepers au titre des cloud services, pourtant bien identifiés dans le Digital Markets Act. Nous n'avons aucun doute sur l'intensité du lobbying que ces acteurs ont dû déployer pour parvenir à ce résultat. Nous l'avons encore observé à propos des négociations en cours sur un schéma européen de certification du cloud, l'EUCS. Les principales organisations représentatives de l'industrie de la tech aux États-Unis ont appelé, dans une lettre ouverte adressée au plus haut niveau de l'administration américaine, à agir contre ce projet de schéma de certification européen au prétexte que celui-ci « menace potentiellement les intérêts économiques et la sécurité nationale des États-Unis ».

Si, ces dernières années, nous n'avons pas recueilli que des succès auprès des institutions européennes, celles-ci savent désormais qu'elles peuvent compter sur nos associations représentatives des utilisateurs professionnels de produits et services numériques. Et elles n'hésitent d'ailleurs plus à nous solliciter et à nous écouter. Dans ce contexte, il est essentiel que nos adhérents maintiennent leur mobilisation sur les différents textes législatifs qui sont encore en cours de négociation et d'adoption au sein des institutions européennes, et qui sont présentés dans cette note d'information et d'actualité du Cigref.

C'est donc en priorité à l'intention de nos adhérents que nous publions ce panorama des règlements européens portant sur le numérique. Il a été réalisé après un excellent travail de synthèse de notre stagiaire juriste, Aliette Diéval, dont je salue ici les qualités professionnelles et que je remercie très vivement.

Henri d'Agrain,
Délégué général du Cigref

TABLE DES MATIÈRES

1 INTRODUCTION

En réponse à l'évolution et au développement constant des technologies numériques, l'Union européenne s'est dotée d'une « Stratégie numérique pour l'Europe pour la décennie 2020-2030 ».

C'est dans le cadre de cette Stratégie que la Commission européenne a proposé différents règlements ayant pour finalité d'encadrer le rôle des services et marchés numériques et de faciliter les transferts des données tout en s'assurant de la confiance et la sécurité des entreprises et citoyens européens.

2 DIGITAL MARKETS ACT

Le « règlement sur les marchés numériques » a pour objectif d'établir des conditions de concurrence équitables et loyales afin de favoriser l'innovation, la croissance et la compétitivité, tant dans le marché unique qu'à l'échelle internationale, ainsi que de renforcer la liberté de choix des consommateurs européens.

Outil de régulation ex-ante du marché, le règlement tend à mettre fin à la domination des « contrôleurs d'accès » à l'entrée d'internet, aussi appelés « *gatekeepers* ». Ces entreprises, ayant au moins 7.5 milliards d'euros de chiffre d'affaires annuel au sein de l'Union européenne et plus de 45 millions d'utilisateurs mensuels, sont soumises à différentes obligations et interdictions :

- Les *gatekeepers* ont l'obligation de :
    - Permettre aux utilisateurs de désinstaller les applications déjà préinstallées sur leurs smartphones ;
    - Rendre les services de messagerie instantanée interopérables ;
    - Permettre aux développeurs d'applications d'accéder, dans des conditions équitables, aux fonctionnalités auxiliaires et aux matériels informatiques des smartphones.
- Les *gatekeepers* ont l'interdiction de :
    - Classer leurs propres produits ou services de façon plus favorable que ceux de leurs concurrents : il s'agit donc de la fin du principe de l'auto-préférence ;
    - Utiliser, sans le consentement des utilisateurs, leurs données personnelles collectées entre différents services ;
    - Empêcher les entreprises utilisatrices de proposer, à des conditions différentes, leurs produits ou services sur d'autres plateformes ou canaux de distribution.

2.1 CHRONOLOGIE INSTITUTIONNELLE

- **15 décembre 2020** : proposition de la Commission ;
- **5 juillet 2022** : position du Parlement ;
- **18 juillet 2022** : orientation générale du Conseil ;
- **12 octobre 2022** : publication au JOUE (Journal Officiel de l'Union Européenne) ;
- **1er novembre 2022** : entrée en vigueur ;
- **Mai 2023** : entrée en application ;
- **6 septembre 2023** : la Commission a désigné les « *gatekeepers* ».

2.2 POSITIONNEMENT DU CIGREF

- Appel à revoir les critères qualitatifs et quantitatifs de la définition des « *gatekeepers* » afin :

  - D'adopter une approche par la taille des marchés et des marchés de niche et non en fonction de seuils ;
  - D’éviter les effets collatéraux indésirables en considérant uniquement la part provenant de la vente de services numériques.
- Appel à inclure des mesures directement applicables afin d’interdire plus de pratiques déloyales et préjudiciables aux utilisateurs ;
- Appel à élargir la liste de ces pratiques déloyales, à la rendre évolutive ;
- Appel à renforcer la mise en œuvre effective des règles par les autorités nationales dotées de pouvoirs d’exécution étendus ;
- La désignation des « *gatekeepers* » par la Commission le 6 Septembre 2023 n’ayant pas inclus au titre du DMA les 3 principaux fournisseurs de cloud, le Cigref a fait parvenir un courrier de protestation et de demande de clarification à la présidence de la Commission européenne, co-signé par ses partenaires belges, néerlandais et allemands.

2.3 ADAPTATION DU DROIT NATIONAL

Projet de loi sur l’Espace Numérique : Vise à interdire aux géants du numérique de privilégier leurs services sur leurs plateformes. L’application directe du DMA au niveau européen renforcera la capacité des entreprises européennes à pénétrer les marchés de l’économie numérique.

3 DIGITAL SERVICES ACT

Le « Règlement sur les services numériques » tend à garantir un environnement en ligne sûr en responsabilisant les « fournisseurs de services intermédiaires », à savoir les plateformes et moteurs de recherche, afin d'assurer la protection des droits fondamentaux, tels que la liberté d'expression ou la protection des consommateurs. Pour cela, le règlement prévoit des mesures visant à lutter contre la diffusion de contenus illicites et préjudiciables ainsi que les produits et services illégaux en ligne.

Remplaçant la directive e-commerce du 8 juin 2008, le règlement met en pratique le principe de « ce qui est illégal hors ligne est illégal en ligne ». Pour cela, les très grandes plateformes et très grands moteurs de recherche, donc les services rassemblant *a minima* 45 millions d'utilisateurs mensuels, sont soumises à deux obligations :

- **Obligation de transparence en ligne** : prévoir un système interne de traitement des réclamations, expliquer le fonctionnement des algorithmes, interdiction de la publicité ciblée pour les mineurs et du profilage fondé sur des données sensibles ;
- **Obligation d'atténuation des risques et de réponse aux crises** : analyser les risques systémiques générés, effectuer des audits indépendants de réduction des risques et accorder l'accès aux données clés de leur interface aux chercheurs.

3.1 CHRONOLOGIE INSTITUTIONNELLE

- **15 décembre 2020** : proposition de la Commission ;
- **Juillet 2022** : position du Parlement ;
- **Octobre 2022** : orientation générale du Conseil ;
- **27 octobre 2022** : publication au JOUE ;
- **16 novembre 2022** : entrée en vigueur ;
- **25 août 2023** : entrée en application pour les très grandes plateformes et moteurs de recherche ;
- **1er janvier 2024** : entrée en application.

3.2 ADAPTATION DU DROIT NATIONAL

Projet de loi "Sécuriser et Réguler l'Espace Numérique" (loi SREN) :

- Interdire la publicité ciblée sur les mineurs ou utilisant des données sensibles ;
- Pouvoir choisir librement son moteur de recherche, son navigateur, sa messagerie : en application directe du DSA au niveau européen, les Français ne pourront plus se voir dicter le choix des outils qu'ils utilisent en ligne.

4 DATA GOVERNANCE ACT

Dans le cadre de la Stratégie européenne des données, le « Règlement sur la gouvernance des données » tend à favoriser le partage des données personnelles et industrielles par la mise en place de **structures d'intermédiation**. Le règlement vise également à renforcer la confiance dans le partage des données (relatives à la santé, de mobilité, environnementales, agricoles…) en rendant ce dernier plus sûr, facile et conforme à la législation sur la protection des données.

Quatre ensembles de mesures permettent de stimuler le développement de systèmes de partage de données fiables :

- Mettre en place des mécanismes facilitant la réutilisation de certaines données du secteur public qui ne peuvent être mises à disposition en tant que données ouvertes (ex : les données de santé pour la recherche) ;
- Garantir la fiabilité des intermédiaires dans le partage et la mise en commun des données au sein des espaces européens communs de données dans les domaines stratégiques (la santé, l'environnement, l'énergie, les finances, etc.) ;
- Renforcer l'altruisme des données : le partage des données au profit de la société (pour la recherche médicale, le réchauffement climatique, etc.) ;
- Faciliter le partage transfrontière des données.

Enfin, le règlement a créé le Comité européen de l'innovation en matière de données afin de faciliter le partage des bonnes pratiques.

4.1 CHRONOLOGIE INSTITUTIONNELLE

- **25 novembre 2020** : proposition de la Commission ;
- **avril 2022** : position du Parlement ;
- **16 mai 2022** : orientation générale du Conseil ;
- **3 juin 2022** : publication au JOUE ;
- **13 juin 2022** : entrée en vigueur ;
- **Septembre 2023** : entrée en application.

4.2 ADAPTATION DU DROIT NATIONAL

Projet de loi "Sécuriser et Réguler l'Espace Numérique" : stimuler l'économie de la donnée européenne.

5 DATA ACT

Dans le cadre de la Stratégie européenne des données, le « Règlement sur les données » tend à maximiser la valeur des données dans l'économie en facilitant la disponibilité et le partage des données entre les entreprises, les consommateurs et les organismes publics. Complétant le DGA, il précise qui peut créer de la valeur à partir des données et dans quelles conditions.

Il comporte une obligation de partage des données aux utilisateurs pour les « détenteurs de données », à savoir les fabricants de produits connectés et fournisseurs de services connexes. Cependant, depuis le RGPD et les arrêts Schrems et Schrems II (invalidant les décisions d'adéquation UE-USA), les services du cloud doivent empêcher les transferts internationaux de données industrielles, ou leur accès par un gouvernement tiers, qui ne seraient pas compatibles avec les législations européenne et nationale.

5.1 CHRONOLOGIE INSTITUTIONNELLE

- **23 février 2022** : proposition de la Commission ;
- **14 mars 2023** : position du Parlement ;
- **17 mars 2023** : orientation générale du Conseil.

5.2 POSITIONNEMENT DU CIGREF

- Les clauses contractuelles abusives doivent cesser pour tous les types d'entreprises et pas seulement les plus petites ;
- Des définitions claires sont essentielles pour garantir la sécurité juridique, notamment sur les acteurs de la chaîne des données et la définition des données couvertes par le règlement, dans le respect des secrets commerciaux ;
- Le règlement est un vecteur pertinent pour interdire les comportements anticoncurrentiels et l'utilisation abusive des données en complément du DMA ;
- Des ambitions plus élevées sont possibles en termes de changement des fournisseurs de service de traitement des données ;
- Des limites claires à la disponibilité des données et des systèmes de compensation équitables sont essentielles pour soutenir l'innovation ;
- Des règles claires et des sanctions élevées pour les transferts internationaux de données doivent être mises en place.

6 CYBERSECURITY ACT

Précisant la directive NIS2 du 14 décembre 2022, le « Règlement sur la cybersécurité » a pour objectif d'assurer un niveau élevé de cybersécurité au sein de l'Union en prévoyant dans un premier temps l'attribution un nouveau mandat à l'ENISA : l'Agence de l'Union européenne pour la cybersécurité consolide la coopération au sein de l'Union, en ayant notamment recours à un réseau d'équipe de réponse aux incidents cyber, aide les États-membres dans leurs efforts de renforcement de leurs capacités et s'assurer de la confiance des citoyens à l'égard de l'Europe numérique.

Dans un second temps, le règlement instaure un cadre européen de certifications de cybersécurité à l'échelle de l'Union pour les produits, services et processus TIC. Il s'agit d'harmoniser les méthodes d'évaluation entre les États membres en créant trois niveaux communs de cybercertification afin d'aboutir à une reconnaissance mutuelle des certificats entre les États membres. Ces trois niveaux d'assurance de cybersécurité sont proportionnés au cyber risque, associé à l'utilisation du produit, service ou processus TIC :

- Niveau d'assurance élémentaire : pour les objets destinés au grand public ;
- Niveau d'assurance substantiel : pour les objets ayant passé des tests de conformité par les organismes d'évaluation de la conformité ;
- Niveau d'assurance élevé : si les objets ont passé tests approfondis.

6.1 CHRONOLOGIE INSTITUTIONNELLE

- **13 septembre 2017** : proposition de la Commission ;
- **12 mars 2019** : position du Parlement ;
- **9 avril 2019** : orientation générale du Conseil ;
- **17 avril 2019** : publication au JOUE ;
- **28 juin 2021** : entrée en application.

7 CYBER RESILIENCE ACT

Complétant la directive NIS2 du 14 décembre 2022, le « Règlement sur la cyber résilience » a pour objectif de garantir une plus grande sécurité des logiciels et produits matériels afin de pallier deux problèmes : le faible niveau de cybersécurité ainsi que le manque de clarté des informations liées à la sécurité des produits.

Ce règlement instaure une obligation de sécurité des produits comportant un élément numérique dès leur conception pour les fabricants de ces produits connectés : il s'agit d'un devoir de vigilance pour le cycle de vie du produit. Les fabricants ont également l'interdiction de livrer des produits comportant des failles de sécurité connues.

7.1 CHRONOLOGIE INSTITUTIONNELLE

- **15 septembre 2022** : proposition de la Commission.

7.2 POSITIONNEMENT DU CIGREF

- Adopter une approche cohérente avec les autres instruments juridiques de l'Union européenne en matière de cybersécurité notamment la directive NIS2 ;
- Concevoir une évaluation de la conformité sur les vulnérabilités plus alignée sur les pratiques et les contraintes opérationnelles, notamment en matière de *reporting* des vulnérabilités et de leur traitement ;
- Renforcer les dispositions relatives aux logiciels et éléments open source ;
- Couvrir les technologies numériques dans les produits, services et processus indépendamment de leur utilisation par les consommateurs individuels ou les utilisateurs professionnels.

8 CYBER SOLIDARITY ACT

Le « Règlement sur la cyber solidarité » a été proposé en mars 2022 en réaction à l'invasion de l'Ukraine par la Russie : il s'agit de renforcer la coopération à l'échelle de l'Union européenne en matière de préparation, détection et réaction aux cyberattaques de grande ampleur ainsi que de stimuler la coordination tant transfrontalière qu'entre les secteurs public et privé au sein d'un même État membre.

Pour cela, le règlement prévoit la création de différentes structures :

- **Cyberbouclier européen** composé de centres d'opérations de sécurité (SOC) nationaux et transfrontaliers répartis dans toute l'Union. Ces pôles régionaux de cybercoopération vont détecter les menaces, les atténuer et y réagir (en ayant notamment recours à l'IA). Ce bouclier ne remplacera pas les centres d'opérations de cybersécurité actuels des États membres et devra coopérer avec ces derniers ;
- **Réserve de cybersécurité** comprenant des entreprises privées certifiées et de confiance (les « fournisseurs de confiance ») prêtes à intervenir en cas d'incident majeur. Cependant, cela entraînera une concurrence institutionnelle entre le Service Européen d'Action Extérieure (SEAE) et l'Agence Européenne pour la Cybersécurité (ENISA) ;
- **Mécanisme d'examen des incidents de cybersécurité** chargé d'améliorer la posture cybernétique de l'Union en examinant et analysant les incidents majeurs après-coup afin d'éclairer les développements futurs de l'approche de l'Union en matière de cyberdéfense.

8.1 CHRONOLOGIE INSTITUTIONNELLE

- **18 avril 2023** : proposition de la Commission.

8.2 POSITIONNEMENT DU CIGREF

Organisation d'une consultation des membres.

9 ARTIFICIAL INTELLIGENCE ACT

Le « Règlement sur l'intelligence artificielle » est le premier texte, à l'échelle mondiale, ayant pour but de réguler la mise sur le marché, la mise en service ainsi que les utilisations des systèmes d'intelligence artificielle en établissant des règles harmonisées au sein de l'Union : cette réglementation a donc vocation à devenir un standard mondial (effet Bruxelles). Par l'adoption de ce règlement, l'Union souhaite stimuler la recherche et la capacité industrielle, promouvoir les investissements et innovations dans l'IA tout en assurant la sécurité, la protection des droits fondamentaux et la transparence au regard de l'utilisation des systèmes d'IA.

Le règlement établit une classification des systèmes d'IA en trois catégories avec différentes obligations selon une approche fondée sur les risques :

- Les systèmes d'IA présentant des **risques inacceptables** sont interdits ;
    - Exemples : l'identification biométrique à distance en temps réel, la notation sociale.
- Les systèmes à **haut risque** sont soumis à des obligations de transparence, de traçabilité et nécessitent un contrôle humain ;
    - Exemples : gestion des infrastructures critiques, accès aux services essentiels.
- Les systèmes à **risque faible** ou minimal sont quant à eux uniquement soumis à une obligation de transparence.
    - Exemples : filtres anti-spam, *chatbot*.

9.1 CHRONOLOGIE INSTITUTIONNELLE

- **21 avril 2021** : proposition de la Commission ;
- **6 décembre 2022** : orientation générale du Conseil ;
- **14 juin 2023** : position du Parlement.

9.2 POSITIONNEMENT DU CIGREF

- Il faut une régulation plus souple, évolutive, proactive et réactive.
- Il faut créer une entité administrative européenne indépendante dotée d'une mission de régulation réactive pour tenir compte de la dynamique technologique afin d'adapter les obligations et contraintes de l'*AI Act* au contexte du moment.
- Même en présence de « bacs à sable réglementaires » il faut pouvoir tester dans des conditions réelles, notamment en utilisant spontanément des jeux des données de test.

10 RÈGLEMENT E-PRIVACY

Précisant le RGPD, le « Règlement vie privée et communications électroniques » devait entrer en vigueur en même temps que ce dernier mais les négociations ont été bloquées pendant quatre ans au Conseil : c'est ce qui explique le maintien de la directive 2002/58/CE « vie privée et communications électroniques » modifiée en 2009 (directive 2009/136/CE « cookies »). Cependant, cette dernière étant devenue obsolète, il est nécessaire de la remplacer par ce règlement *ePrivacy* afin de tenir compte des nouveaux acteurs du marché et des évolutions technologiques et commerciales apparus depuis les 20 dernières années.

L'article premier du règlement prévoit les deux objectifs du texte :

- Protéger les droits et libertés des personnes physiques et morales pour la fourniture et l'utilisation des services de communication électronique (dont le droit au respect de la vie privée et des communications), ainsi que protéger les personnes physiques à l'égard du traitement des données à caractère personnel ;
- Garantir la libre circulation des données et services de communication électroniques au sein de l'Union.

Le règlement s'appliquera aux personnes physiques et morales se trouvant au sein de l'Union et couvrira notamment le traitement des communications électroniques et des métadonnées, la prospection commerciale ou encore l'utilisation des cookies. Sa mise en œuvre permettra l'utilisation de « *cookie wall* » à condition que l'utilisateur puisse choisir entre cette offre et une autre équivalente n'impliquant pas le consentement aux cookies et fournie par le même fournisseur.

10.1 CHRONOLOGIE INSTITUTIONNELLE

- **Janvier 2017** : proposition de la Commission ;
- **20 octobre 2017** : position du Parlement ;
- **Février 2021** : orientation générale du Conseil.

11 DÉCISION D'ADÉQUATION UE – ÉTATS-UNIS

11.1 DECISIONS D'ADEQUATIONS ANTERIEURES

11.1.1 SAFE HARBOR

Décision d'adéquation proposée par la Commission européenne permettant le transfert de données entre l'Union européenne et les opérateurs américains adhérents à ses principes de protection des données. Cette décision a été invalidée le 6 octobre 2015 par l'arrêt Schrems de la CJUE.

11.1.2 PRIVACY SHIELD

Mécanisme d'auto-certification des États-Unis reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données personnelles transférées depuis une entité européenne vers des sociétés établies aux États-Unis. Prévoyant la possibilité de recourir à un médiateur, « *ombudsperso* », cette décision d'adéquation est entrée en vigueur le 1er août 2016 mais a été invalidée le 16 juillet 2020 par l'arrêt Schrems II de la CJUE.

11.2 NOUVELLE DECISION D'ADEQUATION : LE *DATA PRIVACY FRAMEWORK* (DPF)

Cette nouvelle décision d'adéquation a pour but de garantir la sécurité et le respect de la vie privée de citoyens européens, tout en favorisant les opportunités économiques pour les entreprises européennes.

Les organisations et entreprises américaines devront mettre à jour leur politique de confidentialité pour se conformer à cette nouvelle décision d'adéquation dans les 3 mois suivant l'entrée en vigueur de cette décision.

Cette nouvelle décision d'adéquation apporte de nouvelles garanties et protections comparée au Safe Harbor et au Privacy Shield :

- Création d'un **mécanisme de recours à double niveau** grâce à une autorité dont les décisions sont contraignantes :
    - Possibilité de porter plainte auprès du « *Civil Liberties Protection Officer* » qui assure la conformité des transferts de données entre les agences de renseignement américaines et le respect des droits fondamentaux, dont la vie privée ;
    - Possibilité d'interjeter un appel de la décision de l'Officer auprès de la « *Data Protection Review Court* » qui pourra notamment supprimer des données collectées en violation du décret présidentiel américain du 7 octobre 2022.

- **Principe de nécessité et de proportionnalité** dans l'accès des autorités de sécurité nationales des États-Unis aux données pour protéger la sécurité nationale.

11.3 CHRONOLOGIE INSTITUTIONNELLE

11.3.1 SAFE HARBOR

- **26 juillet 2000** : décision d'adéquation de la Commission : "Sphère de sécurité" ;
- **Novembre 2010** : résolution du Parlement ;
- **2 décembre 2010** : décision du Conseil ;
- **6 octobre 2015** : arrêt Schrems de la CJUE invalidant le *Safe Harbor.*

11.3.2 PRIVACY SHIELD

- **Juillet 2016** : décision d'adéquation de la Commission : "Bouclier de protection des données entre l'UE et les États-Unis" ;
- **2 décembre 2016** : décision du Conseil ;
- **16 juillet 2020** : arrêt Schrems II de la CJUE invalidant le *Privacy Shield*.

11.3.3 DÉCISION D'ADÉQUATION

- **25 mars 2022** : déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles ;
- **7 octobre 2022** : décret présidentiel du Président américain Joe Biden prévoyant la mise en œuvre de la déclaration conjointe du 25 mars 2022 dans le droit national ;
- **Décembre 2022** : lancement du processus d'adoption de la nouvelle décision d'adéquation par la Commission européenne ;
- **10 juillet 2023** : décision d'adéquation de la Commission européenne.

12 LEXIQUE

12.1 LE TRIANGLE INSTITUTIONNEL : LES INSTITUTIONS DE L'UNION EUROPEENNE

12.1.1 LA COMMISSION EUROPEENNE

« Gardienne des traités », la Commission incarne le pouvoir exécutif et représente l'intérêt général de l'Union. Établie à Bruxelles, elle est composée de 27 commissaires, un par État-membre, chacun doté d'un portefeuille particulier pour un mandat de 5 ans. Elle dispose du monopole de l'initiative législative dans le cadre de la procédure législative ordinaire en proposant des textes législatifs au Conseil de l'Union européenne et au Parlement européen.

12.1.2 LE CONSEIL DE L'UNION EUROPÉENNE

Également situé à Bruxelles, le « Conseil », également appelé « Conseil des ministres », réunit les ministres des gouvernements de chaque État-membre en fonction des domaines inscrits à l'ordre du jour. Incarnant le pouvoir législatif, il se prononce, en tant que co-législateur avec le Parlement européen, sur les propositions législatives de la Commission dans le cadre de la procédure législative ordinaire.

12.1.3 LE PARLEMENT EUROPÉEN

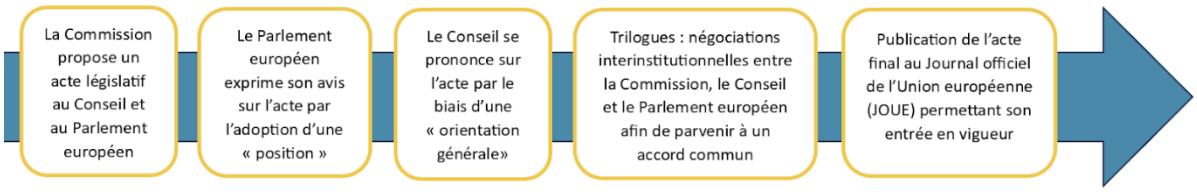
Siégeant à Strasbourg et Bruxelles, les 705 parlementaires européens qui y siègent, élus au suffrage universel direct, représentent les citoyens de l'Union. Co-législateur, il participe conjointement avec le Conseil à l'adoption des actes législatifs proposés par la Commission.

12.1.4 LA COUR DE JUSTICE DE L'UNION EUROPEENNE

Anciennement CJCE (Cour de justice des Communautés européennes), la CJUE est l'institution juridictionnelle de l'Union. En collaboration avec les juridictions nationales, les 27 juges basés à Luxembourg contrôlent la légalité des actes de l'Union et veillent au respect des traités par les États-membres en rendant des décisions obligatoires et exécutoires.

12.2 LA PROCEDURE LEGISLATIVE ORDINAIRE

En vertu de l'article 294 du Traité sur le fonctionnement de l'Union européenne, la procédure de codécision est la procédure législative ordinaire. Cette procédure repose sur le principe de parité entre deux colégislateurs adoptant conjointement les propositions de la Commission européenne : le Parlement européen et le Conseil de l'Union européenne.



12.3 LES ACTES DE L'UNION EUROPÉENNE

12.3.1 RÈGLEMENT

C'est un acte juridique de l'Union européenne de portée générale et obligatoire directement applicable dès son entrée en vigueur afin de garantir une application simultanée et uniforme de la législation européenne au sein de tous les États-membres.

12.3.2 DIRECTIVE

C'est un acte juridique de l'Union européenne nécessitant une transposition par les États-membres destinataires afin qu'elle puisse être contraignante à leur égard quant au résultat à atteindre.

12.3.3 DÉCISION D'ADÉQUATION

En vertu de l'article 45 du RGDP, la Commission européenne peut constater qu'un pays tiers ou une organisation internationale assure un niveau de protection adéquat des données à caractère personnel permettant ainsi le transfert de ces données entre l'Union européenne et l'entité tierce concernée.

Pour cela, elle propose une « décision d'adéquation » au Conseil et au Parlement européen dans laquelle elle évalue le niveau de protection des données en tenant notamment compte du respect des droits de l'Homme et des libertés fondamentales à travers la législation nationale du pays tiers ainsi que de l'existence et du fonctionnement effectif d'autorités de contrôle indépendantes chargées d'assurer le respect des règles en matière de protection des données.

À PROPOS DU CIGREF

Au service de la croissance économique et de la compétitivité de nos membres, grandes entreprises et administrations publiques françaises, utilisatrices de solutions et services numériques, par la réussite du numérique.
Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

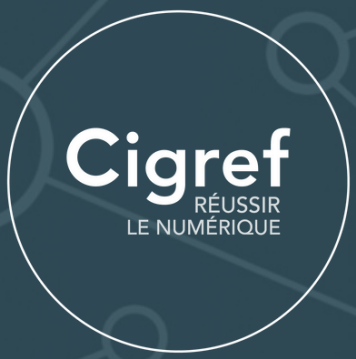
Appartenance
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

NOUS CONTACTER

www.Cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
Cigref@Cigref.fr


Cigref
RÉUSSIR
LE NUMÉRIQUE