Déclaration

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Déclaration 03/2021 sur le règlement «vie privée et communications électroniques»

Adoptée le 9 mars 2021

Le comité européen de la protection des données (EDPB) a adopté la déclaration suivante:

L'EDPB salue le mandat de négociation approuvé et adopté par le Conseil sur la protection de la vie privée et de la confidentialité dans l'utilisation des services de communications électroniques (la «position du Conseil»), qui constitue une avancée encourageante vers un nouveau règlement «vie privée et communications électroniques». Il est primordial que le cadre général de l'Union sur la protection des données soit rapidement complété par des règles harmonisées en matière de communications électroniques.

Ainsi qu'il a déjà été indiqué à de nombreuses reprises[1], le règlement «vie privée et communications électroniques» ne doit en aucun cas abaisser le niveau de protection offert par l'actuelle directive «vie privée et communications électroniques», mais devrait compléter le règlement général sur la protection des données (RGPD) en fournissant de solides garanties supplémentaires en matière de confidentialité et de protection en ce qui concerne tous les types de communications électroniques. En aucun cas, le règlement «vie privée et communications électroniques» ne peut être utilisé dans l'objectif de modifier de facto le RGPD. À cet égard, le Conseil soulève, dans le cadre de sa position, une série de préoccupations et l'EDPB souhaite mettre en évidence les questions qui devraient être abordées lors des prochaines négociations.

La présente déclaration est sans préjudice d'une éventuelle déclaration ou d'un éventuel avis plus détaillé rédigé à l'avenir par l'EDPB sur la position des colégislateurs.

[1] Voir, en annexe de la présente déclaration, la liste complète des documents relatifs aux règles en matière de vie privée et communications électroniques produits par l'EDPB et le groupe de travail «article 29».

Préoccupations concernant le traitement et la conservation des données de communications électroniques à des fins répressives et de protection de la sécurité nationale

En ce qui concerne l'article 6, paragraphe 1, point d), et l'article 7, paragraphe 4, l'EDPB rappelle que des mesures législatives imposant aux fournisseurs de services de communications électroniques de conserver des données de communications électroniques doivent être conformes aux dispositions:

- des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (la «charte»);
- de la jurisprudence la plus récente de la Cour de justice de l'Union européenne (la «CJUE»)[2]; et
- de l'article 8 de la convention européenne des droits de l'homme.

L'EDPB estime que le règlement «vie privée et communications électroniques» ne saurait déroger à l'application de la jurisprudence la plus récente de la CJUE, qui prévoit notamment que les articles 7, 8, 11 et l'article 52, paragraphe 1, de la charte doivent être interprétés en ce sens qu'ils s'opposent à des mesures législatives permettant, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. Par conséquent, la charte ne prévoit pas de base juridique pour une action autre que la conservation ciblée à des fins répressives et de protection de la sécurité nationale. Cette base juridique devrait de toute manière être strictement limitée à la fois dans le temps et sur le plan matériel, et devrait être soumise au contrôle d'une juridiction ou d'une autorité indépendante.

En ce qui concerne le fait que les activités de traitement effectuées par les fournisseurs ne soient pas couvertes par le règlement, l'EDPB estime qu'une telle exclusion va à l'encontre du principe d'un cadre cohérent au niveau de l'Union en matière de protection des données. L'EDPB souligne toutefois qu'en cas d'exclusion, le RGPD s'applique.

La confidentialité des communications électroniques nécessite une protection spécifique (articles 6, 6 *bis*, 6 *ter*, 6 *quater*)

La confidentialité des communications est un droit fondamental protégé par l'article 7 de la charte, déjà mis en œuvre par la directive «vie privée et communications électroniques». Ce droit à la confidentialité doit s'appliquer à toutes les communications électroniques, quels que soient les moyens par lesquels elles sont envoyées et indépendamment du fait que les données soient au repos ou en transit, de l'expéditeur au destinataire. Il doit également protéger l'intégrité de l'équipement terminal de chaque utilisateur.

Principe général d'interdictions comprenant des exceptions limitées en ce qui concerne le traitement de données à caractère personnel

L'EDPB soutient pleinement l'approche qui repose sur un principe général d'interdiction, comprenant des exceptions (axées sur la finalité) limitées, spécifiques et clairement définies.

Toutefois, l'EDPB est préoccupé par le fait que certaines exceptions [notamment à l'article 6, paragraphe 1, point c), l'article 6 *ter*, paragraphe 1, point e), l'article 6 *ter*, paragraphe 1, point f), et l'article 6 *quater*] introduites par le Conseil semblent autoriser des types de traitement relativement généraux, et rappelle la nécessité de limiter ces exceptions à des finalités spécifiques et clairement définies. En tout état de cause, ces finalités spécifiques devraient être explicitement énumérées afin de garantir la sécurité juridique et le degré de protection maximal.

[2] Arrêt de la Cour dans les affaires jointes C-511/18, C-512/18 et C-520/18, ainsi que l'affaire C-623/17.

En outre, en vertu des exceptions prévues à l'article 6, paragraphe 1, points b), c) et d), qui autorisent la consultation des données de communications électroniques, y compris leur contenu, pour garantir la sécurité des réseaux et des appareils des utilisateurs finaux, le fournisseur de service de communications électroniques ou ses sous-traitants pourraient avoir libre un accès au contenu de l'ensemble des communications des utilisateurs finaux. Étant donné que cet accès pourrait porter atteinte au droit à la confidentialité de l'utilisateur final et à ses attentes en matière de protection de la vie privée, cette autorisation devrait être proportionnée et, au moins, limitée, afin de rappeler qu'elle ne saurait conduire à la surveillance systématique du contenu des communications électroniques, ni permettre aux fournisseurs ou aux sous-traitants de contourner tout cryptage.

Enfin, le rôle de l'anonymisation en tant que garantie principale devrait être mis en évidence dans le règlement, principe qui devrait être systématiquement privilégié lorsqu'il s'agit de l'utilisation de données de communications électroniques.

L'existence d'un cryptage solide et fiable est nécessaire dans le monde numérique d'aujourd'hui

Un cryptage solide et de pointe devrait constituer la règle générale pour garantir un flux de données sécurisé, libre et fiable entre les citoyens, les entreprises et les gouvernements, et il est essentiel pour garantir le respect de l'obligation de sécurité prévue par le RGPD, par exemple pour les données concernant la santé, ainsi que la protection des systèmes informatiques dans un contexte de menaces croissantes. Le cryptage de bout en bout, de l'émetteur au destinataire, est également le seul moyen de garantir une protection totale des données en transit. Toute tentative éventuelle d'affaiblir le cryptage, même pour la sécurité nationale, par exemple, empêcherait la pleine application de ces mécanismes de protection en raison de leur potentielle utilisation illicite. Le cryptage doit rester uniforme, solide et efficace[3].

Le nouveau règlement doit appliquer l'obligation de consentement pour les cookies et les technologies similaires et offrir aux fournisseurs de services des outils techniques leur permettant d'obtenir facilement ce consentement (article 8[4])

La nécessité d'une approche visant à protéger la vie privée en ce qui concerne les solutions «à prendre ou à laisser»

Il convient de rappeler que les dispositions en matière de consentement prévues par le RGPD s'appliquent dans le cadre des règles en matière de vie privée et communications électroniques. Par conséquent, l'EDPB estime qu'un consentement donné réellement librement est nécessaire pour empêcher les fournisseurs de services d'appliquer des pratiques déloyales, telles que les solutions «à prendre ou à laisser», auquel cas l'accès aux services et aux fonctionnalités est conditionné au consentement d'un utilisateur au stockage d'informations, ou à l'accès aux informations déjà stockées, sur l'équipement terminal d'un utilisateur (les «cookie walls»)[5].

[3] Statement of the Article 29 Working Party on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (Déclaration du groupe de travail «article 29» sur le cryptage et son incidence sur la protection des personnes à l'égard du traitement de leurs données à caractère personnel dans l'UE), 11 avril 2018, disponible en anglais à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

[4] Ainsi que les considérants associés [considérants 20 aaaa) et 21 aa) de la position du Conseil].

[5] Comme indiqué précédemment par l'EDPB dans sa déclaration sur la révision de la directive ePrivacy, adoptée le 25 mai 2018, disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_fr.pdf, et dans ses lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, point 39, disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.

L'EDPB souligne la nécessité d'inclure dans le règlement «vie privée et communications électroniques» une disposition explicite pour consacrer cette interdiction, afin de permettre aux utilisateurs d'accepter ou de refuser le profilage. Ces mêmes fournisseurs de services devraient donc proposer aux utilisateurs d'autres mesures équitables. Ces principes devraient s'appliquer de la même manière à tous les fournisseurs de services, quel que soit leur secteur d'activité ou leur modèle de financement actuel [voir le considérant 21 aa) de la position du Conseil].

La mesure de l'audience doit être limitée à des pratiques non intrusives qui ne sont pas susceptibles de représenter un risque pour la vie privée des utilisateurs

Dans sa position, le Conseil introduit une nouvelle exception liée à la mesure de l'audience, comme le propose le groupe de travail «article 29»[6]. Toutefois, l'exception en matière de mesure de l'audience, telle que proposée par le Conseil, est libellée de manière trop générale et pourrait conduire à une interprétation trop large du champ d'application de ladite exception et, par conséquent, abaisser le niveau de protection des terminaux des utilisateurs finaux.

Par conséquent, l'EDPB souligne que l'exception en matière de mesure de l'audience ne devrait concerner que les analyses de faible niveau nécessaires à l'analyse de la performance du service demandé par l'utilisateur, et devrait se limiter à la présentation de statistiques à l'opérateur du service, et doit être mise en place par l'opérateur ou ses sous-traitants. Par conséquent, cette opération de traitement ne saurait conduire, par elle-même ou avec d'autres solutions de suivi, à un quelconque isolement ou profilage des utilisateurs par le prestataire ou d'autres responsables de traitement. En outre, le service de mesure de l'audience ne devrait pas autoriser la collecte d'informations de navigation relatives aux utilisateurs sur des applications ou des sites web distincts et devrait inclure un mécanisme facile d'utilisation permettant de refuser toute collecte de données.

Moyen efficace d'obtenir le consentement des utilisateurs pour les sites web et les applications mobiles (article 4 *bis*)

L'EDPB considère que le règlement «vie privée et communications électroniques» devrait améliorer la situation actuelle en redonnant le contrôle aux utilisateurs et en répondant à la «lassitude du consentement». L'article 4 *bis* devrait aller plus loin et obliger les navigateurs et les systèmes d'exploitation à disposer d'un mécanisme facile d'utilisation et efficace permettant aux responsables du traitement d'obtenir le consentement, afin de créer des conditions de concurrence équitables pour l'ensemble des acteurs. Le champ d'application du règlement devrait également inclure explicitement les fournisseurs de navigateurs et de systèmes d'exploitation.

Les paramètres de confidentialité devraient, par défaut, protéger le droit à la protection des données à caractère personnel et l'intégrité des terminaux des utilisateurs et permettre à l'utilisateur de donner et de retirer son consentement de manière aisée, contraignante et exécutoire à l'égard de toutes les parties.

Traitements ultérieurs à des fins compatibles [Article 6 *quater* et article 8, paragraphe 1, point g)]

En ce qui concerne les discussions en cours relatives au traitement ultérieur des métadonnées ou données de communications électroniques collectées grâce aux cookies et aux technologies similaires, l'EDPB réaffirme son soutien en faveur de l'approche définie dans le règlement «vie privée et

[6] Voir, également, l'avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies (WP 194), p. 10 et 11, disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.

communications électroniques», telle qu'elle avait été proposée initialement par la Commission européenne et suivie par le Parlement européen, laquelle se fonde sur des interdictions générales, des exceptions précises et le recours au consentement. Un traitement ultérieur à des fins compatibles risquerait d'abaisser le niveau de protection offert par le règlement «vie privée et communications électroniques», notamment en ce qui concerne le traitement des métadonnées de communications électroniques, en autorisant le traitement pour tout usage que le fournisseur de services considère comme répondant à la clause de «compatibilité», alors que le législateur s'est clairement efforcé de limiter, en l'absence de consentement, leur utilisation à des fins spécifiques. L'EDPB tient à souligner que les données susmentionnées peuvent tout de même être traitées sans le consentement de l'utilisateur final et sans risque pour les utilisateurs, une fois qu'elles ont été anonymisées.

Le futur rôle des autorités de contrôle, de l'EDPB et du mécanisme de coopération (articles 18 à 20)

L'EDPB rappelle que, afin de garantir des conditions de concurrence équitables sur le marché unique numérique, il est essentiel d'assurer, dans l'ensemble de l'Union, une interprétation et une application harmonisées des dispositions du règlement «vie privée et communications électroniques» relatives au traitement des données à caractère personnel.

Le contrôle des dispositions relatives à la protection de la vie privée dans le cadre du règlement «vie privée et communications électroniques» devrait être confié aux autorités de contrôle compétentes visées dans le RGPD afin d'assurer une plus grande cohérence

L'EDPB tient à rappeler qu'il existe une interconnexion des compétences claire entre les autorités nationales compétentes au titre de la directive «vie privée et communications électroniques» en vigueur et les autorités de protection des données. Les dispositions relatives à la protection de la vie privée du futur règlement «vie privée et communications électroniques» ne devraient pas être appliquées de manière isolée puisqu'elles sont liées au traitement des données à caractère personnel et aux dispositions du RGPD.

Par conséquent, afin de concilier un niveau élevé de protection des données à caractère personnel et une sécurité juridique et procédurale, le contrôle des dispositions du futur règlement «vie privée et communications électroniques» concernant le traitement des données à caractère personnel devrait être confié aux autorités nationales auxquelles l'application du RGPD incombe, ainsi que cela avait été proposé initialement par la Commission européenne[7].

L'EDPB souligne que, contrairement à la proposition initiale de la Commission européenne, toutes les références aux mécanismes de coopération et de contrôle de la cohérence, prévus par le chapitre VII du RGPD, ont été supprimées de la position du Conseil. Pour les raisons à nouveau exposées ci-dessus, l'EDPB réaffirme que seul un alignement parfait sur le cadre de coopération et de contrôle de la cohérence du RGPD permettrait de réaliser les objectifs du règlement «vie privée et communications électroniques», d'éviter une fragmentation dans la mise en œuvre et l'application du règlement, ainsi que de réduire la charge qui pèse sur les fournisseurs qui, dans le cas contraire, devraient potentiellement s'adresser à plus de 27 autorités de contrôle.

[7] Commission européenne, proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), 10 janvier 2017, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017PC0010, et avis correspondant du groupe de travail «article 29», disponible à l'adresse suivante: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Si des autorités nationales compétentes qui ne sont pas membres de l'EDPB étaient amenées à interagir avec ce dernier, comme le prévoit actuellement la position du Conseil, leur capacité à contribuer, en temps utile, à l'application cohérente du règlement «vie privée et communications électroniques» serait affaiblie au détriment de l'économie numérique et de la protection des droits fondamentaux.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

ANNEXE: liste des documents antérieurs produits par l'EDPB et le groupe de travail «article 29»

- Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_fr.pdf.
- Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies (WP 194), disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.
- Avis 03/2016 sur l'évaluation et la révision de la directive «vie privée et communications électroniques» (WP 240), disponible à l'adresse suivante:https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
- Avis du groupe de travail «article 29» sur la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), disponible à l'adresse suivante: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
- Statement of the Article 29 Working Party on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (Déclaration du groupe de travail «article 29» sur le cryptage et son incidence sur la protection des personnes à l'égard du traitement de leurs données à caractère personnel dans l'UE), 11 avril 2018, disponible en anglais à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
- Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques, adoptée le 25 mai 2018, disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_fr.pdf.
- Déclaration 3/2019 du comité européen de la protection des données sur un règlement «vie privée et communications électroniques», adoptée le 13 mars 2019, disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_fr_0.pdf.
- Déclaration du comité européen de la protection des données sur le règlement «vie privée et communications électroniques» et le futur rôle des autorités de contrôle et du comité européen de la protection des données, adoptée le 19 novembre 2020, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_fr.