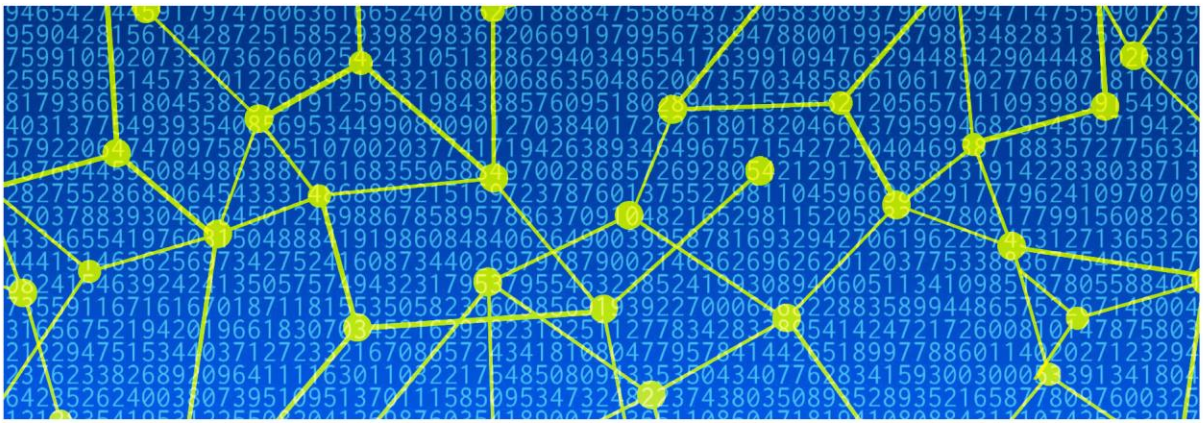

EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 10/2018

sur le paquet de mesures de la Commission concernant des élections européennes libres et équitables

EDPS

17 décembre 2018

Le contrôleur européen de la protection des données («CEPD») est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement nº 2018/1725, «[...] en ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union», et en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

En vertu de l'article 57, paragraphe 1, point g), du règlement 2018/1725, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec pour mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Il formule plusieurs recommandations concernant la proposition de règlement qui visent à améliorer davantage l'articulation entre le cadre juridique de la protection des données, d'une part, et la finalité de cette initiative, d'autre part.

Synthèse

Le fonctionnement de l'Union est fondé sur la démocratie représentative. La communication politique est un élément essentiel à la participation des citoyens, des forces politiques et des candidats à la vie démocratique ainsi qu'au droit fondamental à la liberté d'expression. Ces droits et libertés sont interdépendants avec le droit au respect de la vie privée et familiale, du domicile et des communications ainsi qu'avec le droit à la protection des données à caractère personnel. Plus tôt cette année, dans son avis nº 3/2018 sur la manipulation en ligne, le CEPD a souligné les risques que représente la concentration du marché pour les droits fondamentaux.

Dans le contexte du discours sur l'état de l'Union 2018, la Commission a présenté un paquet «Sécurité» qui met l'accent sur des élections européennes libres et équitables. Ce paquet se compose d'une Communication, d'un Document d'orientation concernant l'application du droit de l'Union en matière de protection des données dans le contexte électoral, d'une Recommandation et d'une Proposition de règlement en ce qui concerne une procédure de vérification relative aux infractions aux règles en matière de protection des données à caractère personnel dans le contexte des élections au Parlement européen. Le CEDP convient de la référence faite au rôle des plateformes de médias sociaux et reconnaît la manière dont cette initiative serait compatible avec le code de bonnes pratiques contre la désinformation en ligne. À la lumière des prochaines élections au Parlement européen qui se dérouleront en mai de l'année prochaine, et des nombreuses autres élections nationales prévues en 2019, le CEPD soutient également les recommandations relatives à l'établissement de réseaux de coopération nationaux en matière d'élections et d'un réseau de coordination au niveau européen. Il profite de cette occasion pour faire part de sa disponibilité à participer à ce réseau européen, lequel compléterait l'action du CEPD dans ce domaine, notamment l'atelier qu'il organise en février de l'année prochaine. Le CEPD est également d'accord avec la recommandation faite aux États membres d'effectuer une analyse approfondie des risques associés aux élections au Parlement européen en vue d'identifier les incidents de cybersécurité potentiels qui pourraient porter atteinte à l'intégrité du processus électoral, et souligne le caractère urgent de cette question.

De manière générale, le CEPD estime que, par souci de clarté, il aurait pu être fait référence au traitement des données à caractère personnel par le Parlement européen, l'Autorité pour les partis politiques européens et les fondations politiques européennes ainsi que le Comité composé de personnalités indépendantes, comme relevant du champ d'application du règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données (auparavant, règlement 45/2001). Par ailleurs, et plus précisément, le CEPD formule plusieurs recommandations quant à la proposition de règlement, notamment celle de préciser la portée des mesures et les objectifs complémentaires de ces sanctions, y compris les décisions du CEPD concluant à une violation du règlement 2018/1725 et une référence au cadre juridique actuel de la protection des données pour une coopération entre les autorités nationales de contrôle chargées de la protection des données et le CEPD, et garantissant la confidentialité de l'échange d'informations dans le cadre de la coopération entre les autorités de contrôle de la protection des données et le Comité composé de personnalités indépendantes.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le 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 (règlement général sur la protection des données)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[2], et plus particulièrement son article 42, paragraphe 1, son article 57, paragraphe 1, point g), et son article 58, paragraphe 3, point c),

vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[3],

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction et contexte

1. Le 12 septembre 2018, dans le contexte du discours sur l'état de l'Union 2018, la Commission a présenté un paquet «Sécurité» qui met l'accent sur des élections européennes libres et équitables. Ce paquet se compose d'une proposition législative et de trois mesures non législatives:
    - une **Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE, Euratom) nº 1141/2014 en ce qui concerne une procédure de vérification relative aux infractions aux règles en matière de protection des données à caractère personnel dans le contexte des élections au Parlement européen** (COM (2018) 636 final/2) (ci-après la «*proposition de règlement*»);
    - une **Communication «Garantir des élections européennes libres et équitables»** (COM (2018) 637 final) (ci-après, la «*Communication*»);
    - une **Recommandation sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen** (C (2018) 5949 final) (ci-après, la «*Recommandation*»); et
    - un **Document d'orientation concernant l'application du droit de l'Union en matière de protection des données dans le contexte électoral** (COM (2018) 638 final) (ci-après, le «*Document d'orientation*»).
2. Ce paquet a été adopté dans le but de garantir des élections au Parlement européen libres et équitables en mai 2019, en tenant compte des nouvelles difficultés que posent la communication en ligne et les récentes révélations apparues, par exemple, dans l'affaire «Facebook/Cambridge Analytica»[4]. Il est présenté conjointement avec une proposition de

règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (COM(2018) 630 final)[5].

3. Il vient compléter la Communication de la Commission du 26 avril 2018 intitulée «Lutter contre la désinformation en ligne: une approche européenne» (COM/2018/236 final), qui entend promouvoir un environnement en ligne plus transparent, plus fiable et plus responsable. L'un de ses principaux objectifs, le code de bonnes pratiques contre la désinformation en ligne, qui est un code d'autorégulation, a été publié le 26 septembre 2018. La Commission a également publié l'avis du groupe de réflexion du forum plurilatéral sur le code de bonnes pratiques[6]. Les actions prévues dans cette Communication, y compris ce code de bonnes pratiques, viennent compléter les actuels travaux menés par le SEAE. Suite aux conclusions du Conseil européen du 28 juin 2018[7], la Commission et le Haut Représentant de l'Union pour les affaires étrangères et la politique de sécurité présenteront, d'ici à la fin de l'année et en collaboration avec les États membres, un projet d'action révisé afin de lutter contre la désinformation[8].
4. La **proposition de règlement** «[vise à ce que] *des sanctions financières puissent être infligées aux fondations ou aux partis politiques européens qui utilisent les infractions aux règles de protection des données comme moyen délibéré d'influencer ou de tenter d'influencer le résultat des élections au Parlement européen*»[9]. Outre les sanctions financières qui pourraient être imposées aux fondations ou aux partis politiques européens, correspondant à 5 % de leur budget annuel[10], un nouveau motif serait «*ajouté à la liste des infractions qui empêchent tout parti politique européen ou toute fondation politique européenne qui en est l'auteur de demander un financement par le budget général de l'Union européenne dans l'année au cours de laquelle la sanction a été infligée*»[11]. Dans sa **Recommandation,** la Commission encourage les autorités nationales de contrôle chargées de la protection des données, instituées en vertu du règlement général sur la protection des données (ci-après, le «*RGPD*») à informer immédiatement et de façon proactive l'Autorité pour les partis politiques européens et les fondations politiques européennes (ci-après, l'«*Autorité*»)[12] de leurs décisions concluant à une infraction aux règlementations relatives à la protection des données, lorsque ladite infraction est liée aux activités politiques d'une fondation politique européenne ou d'un parti politique européen «*en vue d'influencer les élections au Parlement européen*»[13]. En outre, dans le cadre d'affaires impliquant des partis politiques ou des fondations politiques à l'échelle nationale et régionale, la Commission recommande aux États membres d'«appliquer des sanctions appropriées»[14].
5. Par ailleurs, la **Recommandation** encourage la création d'**un réseau national de coopération électorale dans chaque État membre ainsi que d'un réseau européen de coopération concernant les élections au Parlement européen[15]**. Ce dernier fait suite au premier échange organisé par la Commission en avril 2018 entre des pays de l'UE au sujet des meilleures pratiques en matière d'élections. Il se composerait de points de contact nationaux et se réunirait en janvier et avril 2019[16]. Il devrait faire office de processus d'alerte européen en temps réel et de forum pour l'échange d'informations. Les réseaux nationaux auraient notamment pour objectif de partager des informations sur des problématiques susceptibles de nuire aux élections européennes, entre les autorités nationales ayant compétence en matière de questions électorales et de cybersécurité, ainsi qu'entre les autorités nationales chargées de la protection des données et les autorités ou instances nationales de régulation de l'audiovisuel. La recommandation prévoit également que ces réseaux nationaux consultent les autorités nationales chargées de l'application de la loi et coopèrent avec elles, conformément au droit national[17], et que, au besoin, Europol facilite la coopération entre les autorités nationales chargées de l'application de la loi à

l'échelle européenne. De l'avis de la Commission, «*[e]lles pourront ainsi détecter rapidement les menaces potentielles pour les élections au Parlement européen et appliquer les règles existantes sans délai, y compris les sanctions financières prévues, telles que le remboursement de la contribution publique*»[18].

6. La Commission présente enfin plusieurs recommandations[19] visant à faciliter la **transparence de la publicité à caractère politique** avant les élections au Parlement européen et encourage les États membres à prendre des **mesures appropriées concernant la cybersécurité** du processus des élections au Parlement européen et à participer à des **activités de sensibilisation** avec des tiers, notamment des plateformes en ligne et des prestataires de services informatiques, aux fins d'une meilleure transparence et d'un renforcement de la confiance dans le processus électoral.
7. Le **Document d'orientation** met l'accent sur le cadre de l'Union relatif à la protection des données existant ainsi que sur son application dans le **contexte électoral**. De l'avis de la Commission, puisqu'il s'agit de la première fois que le RGPD sera appliqué dans le contexte électoral européen, il est important pour tous les acteurs impliqués dans les processus électoraux de comprendre clairement comment appliquer ces règles de la meilleure façon possible. La Commission souligne que les autorités nationales chargées de la protection des données «*doivent faire pleinement usage de leurs pouvoirs renforcés pour remédier à d'éventuelles infractions*»[20].
8. Le 18 octobre 2018, le Conseil européen a appelé à adopter des mesures destinées à «*protéger les systèmes démocratiques de l'Union et lutter contre la désinformation, y compris dans le contexte des élections européennes à venir, dans le plein respect des droits fondamentaux. À cet égard, les mesures proposées par la Commission en ce qui concerne les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité, la manipulation illégale des données et la lutte contre les campagnes de désinformation, ainsi que le durcissement des règles relatives au financement des partis politiques européens, méritent de faire l'objet d'un examen à bref délai et d'un suivi opérationnel de la part des autorités compétentes*[21]».
9. Le 25 octobre 2018, le Parlement européen a adopté une résolution qui rappelle que «*les mesures proposées par la Commission pour garantir des élections européennes libres et équitables, en particulier l'amendement législatif visant à rendre plus strictes les règles en matière de financement des partis politiques européens en instaurant la possibilité d'imposer des sanctions financières en cas de violation des règles en matière de protection des données visant à influer délibérément sur le résultat des élections européennes; rappelle que le traitement de données à caractère personnel par les partis politiques dans l'Union européenne est soumis aux dispositions du RGPD et que la violation des principes, droits et obligations prévus par cet acte législatif entraînera des amendes et sanctions supplémentaires*». Dans sa résolution, le PE estime que «*l'existence d'interférences dans les élections constitue un grand risque pour la démocratie, et que l'élimination de ces interférences nécessite un effort commun entre les fournisseurs de services, les législateurs et les acteurs et partis politiques*» et accueille favorablement ce paquet de la Commission[22]. Le 3 décembre 2018, la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a adopté son avis sur la proposition de règlement[23]. Le 6 décembre 2018, la Commission des affaires constitutionnelles a adopté son rapport sur la proposition de règlement[24].
10. Le Contrôleur européen de la protection des données (ci-après, le «*CEPD*») se félicite de la consultation informelle lancée par la Commission au sujet de la proposition de règlement, de la Recommandation et du Document d'orientation avant leur adoption ainsi que du fait qu'une partie de ses observations informelles ont été prises en considération. Il précise néanmoins qu'en raison du court préavis qui lui a été donné, il s'agissait davantage

d'observations préliminaires. En conséquence, il formule les observations formelles qui suivent. En ce sens, il souhaiterait rappeler que, lorsqu'elle adopte une proposition législative ayant trait à la protection des droits et libertés des individus au regard du traitement de leurs données à caractère personnel, comme cela est le cas en l'espèce, la Commission se doit de consulter le CEPD.

2. Observations

2.1. Observations générales

11. Le CEPD **considère la communication politique** comme un élément essentiel à la participation des citoyens, des forces politiques et des candidats à la vie démocratique ainsi qu'au droit fondamental à la liberté d'expression. Il estime en outre que ces droits et libertés sont interdépendants avec le droit au respect de la vie privée et familiale, du domicile et des communications visé à l'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après, la «*Charte*»), ainsi qu'avec le droit à la protection des données à caractère personnel consacré par l'article 8 de la Charte.
12. L'article 2 du traité sur l'Union européenne (ci-après, le «*TUE*») dispose que «*[l]'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes.*» Aux termes de l'article 10, paragraphe 4, du TUE, «*[l]es partis politiques au niveau européen contribuent à la formation de la conscience politique européenne et à l'expression de la volonté des citoyens de l'Union*». L'article 12, paragraphe 2, de la Charte expose ce même principe. L'article 3 du protocole I à la Convention européenne des droits de l'homme garantit à tous un droit à des élections libres. La liberté, la loyauté et la transparence sont reconnues comme des principes clés pour des élections démocratiques[25]. Dans le contexte de l'Union européenne, selon l'article 10, paragraphes 1 et 2, du TUE, «*[l]e fonctionnement de l'Union est fondé sur la démocratie représentative» et «[l]es citoyens sont directement représentés, au niveau de l'Union, au Parlement européen*». L'article 39 de la Charte garantit le droit de vote aux élections au Parlement européen. On estime que le **principe de transparence électorale** est compromis lorsque les électeurs n'ont pas la liberté de chercher, de recevoir et de donner des informations sur le processus et sur les candidats, y compris les sources et les dépenses du soutien financier que reçoit un candidat ou un parti[26]. L'article 11 de la Charte dispose qu'il est obligatoire de respecter **la liberté et le pluralisme des médias**. La Résolution du Parlement européen du 3 mai 2018 sur le pluralisme et la liberté des médias dans l'Union européenne a évoqué la «*concentration du pouvoir aux mains des conglomérats médiatiques, des opérateurs de plateformes et des intermédiaires de l'internet* [qui] *risque toutefois d'avoir des conséquences négatives pour le pluralisme du débat public et l'accès à l'information [...]*»[27]. Le CEPD et, plus récemment, le Comité européen de la protection des données, ont également mis en exergue les risques pour les droits fondamentaux que suppose la concentration du marché[28]. Les autorités de contrôle chargées de la protection des données ont mis en avant l'**importance de l'utilisation des données personnelles pour la communication politique** dans le cadre de la Conférence internationale des commissaires à la protection des données et de la vie privée[29]. Dans ce contexte, le CEPD tient à rappeler qu'aux termes du 56e considérant du RGPD, «*[l]orsque, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique dans un État membre requiert que les partis politiques collectent des*

données à caractère personnel relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé pour des motifs d'intérêt public, à condition que des garanties appropriées soient prévues.»

13. Dans ce contexte, le CEPD convient de la référence directe faite, notamment dans la Communication et dans le Document d'orientation, **au rôle des plateformes de médias sociaux** et reconnaît la manière dont l'initiative serait compatible avec le code de bonnes pratiques contre la désinformation en ligne[30]. Il constate également que l'évaluation du code de bonnes pratiques «*fera partie intégrante des travaux devant mener à un plan d'action assorti de propositions spécifiques pour une réponse coordonnée de l'UE au défi de la désinformation, que la Commission et la haute représentante présenteront avant la fin de l'année*»[31]. Les publicités à caractère politique sont de plus en plus ciblées, ce qui est le fait d'un traitement à grande échelle des données à caractère personnel, d'un profilage et d'un processus décisionnel algorithmique dont les plateformes de médias sociaux concernées sont responsables en vertu du RGPD et d'autres règlements applicables. Dans ce contexte, le CEPD souhaite réitérer ses encouragements en faveur de l'adoption rapide d'un nouveau règlement «vie privée et communications électroniques»[32] aux fins d'assurer un niveau élevé de protection tant en ce qui concerne le contenu que les métadonnées, et soutient l'objectif consistant à étendre les obligations de confidentialité à un plus grand nombre de services, et notamment aux services de communication dits «par contournement» («OTT»), ce qui reflète l'évolution des technologies[33].
14. Qui plus est, par souci de clarté, l'initiative aurait pu inclure une référence au traitement des données à caractère personnel par l'Autorité, le Parlement européen et le comité de personnalités éminentes indépendantes comme étant un traitement s'inscrivant dans le champ d'application du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, Texte présentant de l'intérêt pour l'EEE (voir l'article 33 du règlement nº 1141/2014[34]).

2.2. Observations concernant la proposition de règlement

15. L'exposé des motifs de la proposition de règlement expose que «*les règles existantes ne permettent pas de décourager et de sanctionner efficacement les violations des règles de protection des données qui sont susceptibles de perturber le débat démocratique et la tenue d'élections libres*». La proposition de règlement vise donc à sanctionner financièrement les «*fondations ou [...] partis politiques européens qui utilisent les infractions aux règles de protection des données comme moyen délibéré d'influencer ou de tenter d'influencer le résultat des élections au Parlement européen*»[35]. La proposition de règlement instaure une procédure de vérification associée aux infractions aux règles de protection des données à caractère personnel, par laquelle:
    1) sans délai injustifié et au plus tard un mois après la décision rendue par l'autorité de contrôle chargée de la protection des données au sens de l'article 4, point 21, du RGPD, «*constatant qu'une personne physique ou morale a enfreint les règles applicables à la protection des données à caractère personnel et s'il découle de cette décision, ou s'il y a d'autres bonnes raisons de croire, que l'infraction est liée aux activités politiques d'un parti politique européen ou d'une fondation politique européenne dans le contexte des élections au Parlement européen*», l'Autorité sollicite l'avis du comité de personnalités éminentes indépendantes (ci-après, le «comité»)[36];

2) «*[l]orsque l'Autorité le demande, le comité rend un avis indiquant si un parti politique européen ou une fondation politique européenne a délibérément influencé ou tenté d'influencer le résultat des élections au Parlement européen en tirant parti d'une infraction aux règles applicables en matière de protection des données à caractère personnel*»[37].
3) lorsque, dans son avis, le comité conclut qu'«*un parti politique européen ou une fondation politique européenne a délibérément influencé ou tenté d'influencer le résultat des élections au Parlement européen en tirant parti d'une infraction aux règles applicables en matière de protection des données à caractère personnel»,* l'Autorité impose des sanctions financières[38].

16. Le CEPD comprend qu'un tel mécanisme est censé être complémentaire avec les sanctions, et plus particulièrement les amendes administratives, que les autorités nationales de contrôle chargées de la protection des données sont habilitées à imposer en vertu du RGPD. Aux termes de l'exposé des motifs de la proposition de règlement, «*un même comportement ne peut faire l'objet d'une double peine*» dans la mesure où le «*comportement sanctionné par la présente proposition est le fait de tirer parti d'infractions aux règles de protection des données pour influencer délibérément ou tenter d'influencer les élections au Parlement européen. L'Autorité ne sanctionnera pas les infractions aux règles de protection des données en tant que telles*»[39].
17. En ce sens, le CEPD considère que la proposition de règlement mériterait **de plus amples précisions quant au champ d'application des mesures** adoptées. En d'autres termes, compte tenu des compétences des autorités de contrôle chargées de la protection des données en vertu du RGPD et du principe de *ne bis in idem* (non-cumul des sanctions) consacré à l'article 50 de la Charte, tel qu'interprété par la Cour de justice de l'Union européenne[40], le dispositif de la proposition de règlement doit être sans équivoque, car il ressort de prime abord de la proposition de règlement que l'**Autorité n'imposerait pas de sanctions en cas d'infractions au RGPD en tant que telles**. À l'évidence, il y a lieu de ne pas attendre du comité et de l'Autorité qu'ils procèdent à une nouvelle évaluation distincte de l'infraction au RGPD qui a déjà été établie par les autorités de contrôle de la protection des données compétentes définies à l'article 4, paragraphe 21, du RGPD. Il doit être clair que le comité et l'Autorité s'appuient sur l'évaluation de l'infraction au RGPD par l'autorité de contrôle chargée de la protection des données et que le champ d'application de la mesure adoptée par l'Autorité doit se limiter à sanctionner un comportement illégal entraînant la violation d'une ou plusieurs dispositions du règlement nº 1141/2014 pour lequel elle a compétence (par ex., une fraude ou une manipulation électorale), ce qui, en vertu de la proposition de règlement, inclurait une infraction commise par le biais d'une violation des règles de protection des données.
18. À cet égard, **la proposition de règlement pourrait préciser les règles juridiques (par ex. règlement nº 1141/2014 et non le RGPD) dont l'infraction serait sanctionnée par l'Autorité ainsi que les objectifs complémentaires d'une telle sanction**.
19. En outre, **le lien entre cette nouvelle disposition et l'article 33, paragraphe 8,** du règlement nº 1141/2014 pourrait être précisé[41].
20. Aux termes de la proposition de règlement, l'Autorité ne soumet cette question au comité que lorsqu'une décision a été rendue par une autorité nationale de contrôle chargée de la protection des données, qui conclut à une infraction à la législation sur la protection des données, et que, soit «*il découle de cette décision (...) que l'infraction est liée aux activités politiques d'un parti politique européen ou d'une fondation politique européenne*», soit «*il y a d'autres bonnes raisons de croire, que l'infraction est liée aux activités politiques*»[42]. **Nous suggérons de préciser si les «bonnes raisons» de croire que l'infraction est liée aux activités politiques doivent être déterminées par l'Autorité uniquement ou**

également en coopération avec l'autorité de contrôle chargée de la protection des données.

21. Par ailleurs, cette nouvelle procédure donnerait lieu à un **nouveau partage d'informations** par les autorités nationales de contrôle chargées de la protection des données au comité[43]. À titre d'illustration, le comité pourrait avoir besoin d'adopter un avis significatif pour accéder aux rapports préliminaires ou d'enquête intermédiaire des autorités chargées de la protection des données. Le CEPD salue le fait que la proposition de règlement prévoit qu'une telle coopération doit s'exercer «*conformément à la législation applicable*». En raison du caractère délicat de la question, il est primordial de garantir la confidentialité d'un tel échange d'informations. Il observe néanmoins qu'une telle coopération entre le **comité et les autorités nationales de protection des données n'est pas couverte par l'article 28 du règlement nº 1141/2014, lequel prévoit explicitement un accord avec les États membres concernant les «*modalités pratiques de [l']échange d'informations, y compris des règles en matière de divulgation d'informations confidentielles ou d'éléments de preuve*»**. Cette disposition ne concerne pas la coopération avec le comité. **Le CEPD recommande donc de modifier également cette disposition de façon à ce que les États membres et le comité puissent également convenir de telles modalités pratiques.**
22. Par ailleurs, la mise en œuvre de la nouvelle procédure nécessiterait, dans certains cas, une coopération entre les **autorités nationales de contrôle chargées de la protection des données et le CEPD** pour faciliter le recueil d'éléments de preuve attestant d'une infraction au RGPD. Le CEPD **recommande de faire brièvement référence au cadre juridique actuel en matière de protection des données qui encadrerait une telle coopération.**
23. Enfin, le CEPD observe qu'en l'état, la proposition de règlement ne couvrirait pas les **cas d'infractions au règlement (UE) 2018/1725**, ces dernières relevant, en vertu du RGPD, du contrôle du CEPD et non des autorités nationales de contrôle chargées de la protection des données. Pour atteindre pleinement les objectifs de la proposition de règlement, le CEPD recommande dès lors d'**inclure les décisions du CEPD concluant à une telle infraction avec les garanties susmentionnées concernant la coopération avec le comité dans le cadre de cette nouvelle procédure**.

2.3. Observations sur la Recommandation

24. Le CEPD **salue la recommandation en ce qu'elle établit des réseaux de coopération nationaux**. Il soutient également la recommandation dans l'instauration du **réseau européen de coopération** concernant les élections au Parlement européen qui doivent se tenir avec le soutien de la Commission. **Le CEPD profite de cette occasion pour faire part de sa disponibilité pour participer à ce réseau, que ce soit en tant que membre ou qu'observateur.**

25. Depuis plusieurs années, le CEPD défend une meilleure collaboration entre les autorités de protection des données et les autres organismes de régulation afin de garantir les droits et les intérêts des personnes au sein de la société numérique. Plus particulièrement, compte tenu de la nature concentrée du marché du numérique et du rôle essentiel tenu par un très faible nombre de grandes plateformes dans la médiation et le ciblage des publicités à caractère politique au cours de ces dernières années, le CEPD a recommandé que les **autorités de concurrence**, qui sont chargées d'identifier les cas de prétendus abus de position dominante et de propositions de fusions, et les **autorités de protection des consommateurs** qui s'intéressent à la transparence et à la loyauté des conditions d'utilisation des services en ligne, soient intégrées à ce dialogue[44]. Une telle initiative

contribuerait à l'application des règles relatives à la protection des données, notamment du RGPD, de façon rigoureuse et parallèlement à d'autres normes concernant les élections et le pluralisme des médias. Elle viendrait en outre compléter l'action du CEPD dans ce domaine, notamment l'**atelier qui se déroulera en début d'année prochaine** entre les organismes nationaux de régulation dans le domaine de la législation relative à la protection des données, du droit électoral et du droit de l'audiovisuel[45].

26. Le CEPD prend note de la **recommandation nº 6 qui vise à encourager les autorités nationales de contrôle au titre du RGPD à coopérer avec l'Autorité**. Si elle n'est pas contraignante, cette Recommandation suppose néanmoins une nouvelle mission pour les autorités nationales de contrôle en vertu du RGPD: celle d'évaluer systématiquement s'il découle de leur décision, ou s'il existe d'autres «bonnes raisons» de croire, que l'infraction à la législation sur la protection des données établie dans leur décision est liée aux activités politiques d'un parti politique européen ou d'une fondation politique européenne en vue d'influencer les élections au Parlement européen et d'informer l'Autorité immédiatement et de façon proactive. Ainsi que nous l'avons mentionné plus haut au sujet de la proposition de règlement, le CEPD met en avant le fait qu'une telle coopération ne peut avoir lieu que dans le respect des obligations des autorités nationales de contrôle chargées de la protection des données en vertu du cadre légal applicable et, partant, il salue le fait que la Recommandation précise que les autorités nationales de contrôle en vertu du RGPD doivent coopérer «***dans le respect des obligations qui leur incombent en vertu du droit de l'Union et de la législation nationale*».**
27. **S'agissant de la cybersécurité**, la Recommandation met l'accent sur les principes existants consacrés dans la directive (UE) 2016/1148 («directive NIS»)[46] et le règlement (UE) 910/2014 («règlement eID»)[47]. Les exigences de sécurité relatives à ces instruments sont complétées par les dispositions pertinentes portant sur la sécurité des données à caractère personnel exposées dans le RGPD. En conséquence, le CEDP admet que les autorités nationales compétentes désignées en vertu de la directive NIS doivent faire partie des réseaux de coopération nationaux visés par la Recommandation.
28. Le CEDP **note l'attention accordée à la sécurité du réseau et des informations en tenant compte de tous les systèmes d'information utilisés pour l'organisation des élections** (recommandation nº 12). Il souligne que lesdits systèmes jouent un rôle fondamental, même lorsqu'aucun outil de vote électronique n'est proposé aux votants. La gestion des listes électorales, la préparation des bureaux de vote, l'enregistrement des candidats, des listes et des partis désignés, le décompte des voix et la communication des résultats du scrutin ainsi que les procédures ultérieures reposent généralement sur des systèmes d'information et des réseaux complexes de ces systèmes. Des attaques, réelles ou présumées, visant l'intégrité, la confidentialité ou la disponibilité de tels systèmes ou réseaux peuvent être utilisées pour saper la crédibilité et remettre en cause la légitimité du vote, même si aucun préjudice véritable n'est effectivement constaté.
29. Les enjeux et les risques sont bien plus élevés lorsque le processus électoral réel se fait par voie électronique, dans des bureaux de vote ou, mieux encore, lorsqu'une quelconque forme de vote en ligne est employée. Il a été observé que les systèmes de vote électronique fréquemment utilisés dans les pays tiers et dans l'Union présentaient des défaillances importantes. La complexité de tels systèmes, qui s'explique notamment par les objectifs apparemment contradictoires de préservation du secret des votes et de garantie de la possibilité de contrôler l'exactitude des résultats du scrutin, rend difficile, voire impossible, d'expliquer l'intégrité de tels systèmes à de nombreux citoyens et leur permettre ainsi d'accorder le même degré de confiance et de transparence que celui atteint au moyen de bulletins exprimés sur papier. **Le risque que de véritables attaques ou des déclarations**

mensongères concernant ces attaques ne mette à mal la confiance dans les élections semble plus élevé qu'avec les systèmes de bulletins de vote papier traditionnels. Même des problèmes de disponibilité, notamment des interruptions temporaires du processus de vote en raison de légères défaillances techniques, peuvent faire que certains votants perdent la possibilité d'exercer leur droit fondamental ou augmenter les craintes de manipulations.

30. Dans ce contexte, le CEPD **soutient la recommandation faite aux États membres de procéder à une «*analyse approfondie des risques associés aux élections au Parlement européen en vue d'identifier les incidents de cybersécurité potentiels qui pourraient porter atteinte à l'intégrité du processus électoral*»** (recommandation nº 16). Compte tenu de la complexité de cette tâche et de l'application ultérieure des mesures techniques et organisationnelles appropriées, ainsi que du peu de temps restant avant les élections, **le CEPD insiste sur le caractère urgent de cette question et du lancement de ce processus sans plus attendre**.

2.4. Observations sur le Document d'orientation

31. Le CEPD **prend note du Document d'orientation** qui vise à fournir des orientations spécifiques concernant le traitement des données à caractère personnel lors des élections aux partis politiques européens et nationaux, aux gouvernements nationaux, aux autorités, aux entités privées et aux parties prenantes[48].
32. De manière générale, s'il regrette que le Document d'orientation ne fournisse pas d'exemples concrets de bonnes pratiques, le CEPD salue la référence à certaines règles ou orientations en matière de traitement des données à des fins politiques élaborées par des autorités nationales de protection des données et qui incluent des exemples concrets de bonnes pratiques[49].
33. Le CEPD se félicite également de la référence faite, **au point 1 consacré au cadre de l'Union relatif à la protection des données**, aux **pouvoirs de contrôle**, ce qui inclut les éventuelles sanctions en cas d'infraction, car il est essentiel que les acteurs concernés aient connaissance du processus de contrôle qui est en place ainsi que des éventuelles sanctions pouvant être appliquées en cas d'infraction à la législation sur la protection des données.
34. Qui plus est, le CEPD se réjouit du fait que, au **point 2.1. consacré aux responsables du traitement et sous-traitants de données**, la nécessité d'entreprendre une évaluation au cas par cas de chaque situation soit mise en avant ainsi que de la référence faite au cas où des candidats se présentent à une élection indépendamment de tout parti politique. Lesdits candidats représentent alors les responsables du traitement des données traitées aux fins de la campagne électorale à laquelle ils participent. Néanmoins, les divers scénarios de responsables du traitement et de sous-traitants de données envisageables auraient pu être davantage détaillés: plus particulièrement, les partis et fondations politiques sont susceptibles d'être considérés comme des responsables du traitement, ou comme des responsables conjoints du traitement avec les plateformes, notamment avec les fournisseurs de médias sociaux utilisés pour cibler les messages politiques[50]. Les courtiers en données et les sociétés d'analyse de données font plus souvent office de sous-traitants de données. Dans le cadre d'un processus électoral, ces entités doivent uniquement traiter les données au nom des responsables du traitement, et non agir en tant que tels. D'autres orientations peuvent être consultées dans l'avis 1/2010 du groupe de travail «Article 29» sur la protection des données, concernant les notions de «responsable du traitement» et de «sous-traitant»[51].
35. Pour finir, le CEPD salue la référence faite, aux **points 2.3 sur les exigences en matière de transparence et 2.4. sur le profilage, la prise de décision automatisée et le microciblage**, et au regard des plateformes de médias sociaux, aux **droits de la personne**

concernée, en vertu du RGPD, à obtenir des informations sur le traitement de ses données et à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé et produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

3. Conclusion

36. Le CEPD considère la communication politique comme un élément essentiel à la participation des citoyens, des forces politiques et des candidats à la vie démocratique ainsi qu'au droit fondamental à la liberté d'expression. Il estime en outre que ces droits et libertés sont interdépendants avec le droit au respect de la vie privée et familiale, du domicile et des communications visé à l'article 7 de la Charte, ainsi qu'avec le droit à la protection des données à caractère personnel consacré par l'article 8 de la Charte.
37. Il convient de la référence faite, notamment dans la Communication et dans le Document d'orientation, au rôle des plateformes de médias sociaux et reconnaît la manière dont cette initiative serait compatible avec le code de bonnes pratiques contre la désinformation en ligne.
38. À la lumière des prochaines élections au Parlement européen qui se dérouleront en mai de l'année prochaine, et des nombreuses autres élections nationales prévues en 2019, le CEPD soutient également les recommandations relatives à l'établissement de réseaux de coopération nationaux en matière d'élections et d'un réseau de coordination au niveau européen. Il profite de cette occasion pour faire part de sa disponibilité à participer à ce réseau européen, lequel compléterait l'action du CEPD dans ce domaine, notamment l'atelier qu'il organise en février de l'année prochaine.
39. Le CEPD est également d'accord avec la recommandation faite aux États membres d'effectuer une analyse approfondie des risques associés aux élections au Parlement européen en vue d'identifier les incidents de cybersécurité potentiels qui pourraient porter atteinte à l'intégrité du processus électoral, et souligne le caractère urgent de cette question.
40. De manière générale, le CEPD estime que, par souci de clarté, il aurait pu être fait référence au traitement des données à caractère personnel par le Parlement européen, l'Autorité et le comité, comme à un traitement relevant du champ d'application du règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données (auparavant, règlement 45/2001).
41. Par ailleurs, et plus spécifiquement, le CEPD formule plusieurs recommandations concernant la proposition de règlement, parmi lesquelles:
    - préciser le champ d'application des mesures ainsi que les objectifs complémentaires de telles sanctions;
    - inclure les décisions du CEPD concluant à une infraction au règlement 2018/1725;
    - inclure une référence au cadre juridique de protection des données actuel encadrant la coopération entre les autorités nationales de contrôle chargées de la protection des données et le CEPD; et
    - garantir la confidentialité de l'échange d'informations dans le cadre de la coopération entre les autorités de contrôle de la protection des données et le Comité composé de personnalités indépendantes.

Bruxelles, le 18 décembre 2018

Giovanni BUTTARELLI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] Communication, p. 2.
[5] http://europa.eu/rapid/press-release_IP-18-5681_fr.htm
[6] Le code et son annexe ainsi que l'avis de l'organe de réflexion sont disponibles à l'adresse suivante: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.
[7] Disponible à l'adresse suivante: https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.
[8] Communication, p. 10.
[9] Exposé des motifs de la proposition de règlement, p. 2.
[10] Voir article 27, paragraphe 4, point a), du règlement nº 1141/2014 ainsi que la fiche d'information de la Commission sur des élections européennes libres et équitables, disponibles à l'adresse suivante: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_fr.pdf.
[11] Exposé des motifs de la proposition de règlement, p. 6.
[12] Cette Autorité a été instituée en vertu du règlement nº 1141/2014 (Article 6).
[13] Recommandation nº 6. Qui plus est, dans sa Communication, p. 7, la Commission «*invite les États membres à promouvoir, dans le respect du droit national et du droit de l'Union applicables, le partage d'informations entre les autorités chargées de la protection des données et les autorités chargées de la surveillance des élections et du suivi des activités et du financement des partis politiques, lorsqu'il ressort de leurs décisions ou lorsqu'il existe des motifs raisonnables de croire qu'une infraction est liée aux activités politiques de partis ou fondations politiques nationaux dans le cadre des élections au Parlement européen*». Soulignement ajouté.
[14] Recommandation nº 11.
[15] Recommandations nº 1 à 5, incluse.
[16] Communication, p. 7, et fiche d'information de la Commission sur des élections européennes libres et équitables, disponibles à l'adresse suivante: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_fr.pdf.
[17] Communication, note de bas de page nº 20: «[c]*ela concernerait en particulier les cas où un processus électoral est ciblé dans une intention malveillante, y compris les incidents fondés sur des attaques contre les systèmes d'information. Selon les circonstances, des enquêtes pénales, pouvant aboutir à des sanctions pénales, pourraient se révéler opportunes. Comme indiqué ci-dessus, les définitions des infractions et le niveau minimal des sanctions en matière d'attaques contre les systèmes d'information ont été harmonisés par la directive 2013/40/UE».*
[18] Communication, p. 7.
[19] Recommandations nº 7 à 10 incluse et nº 12 à 19, incluse.
[20] Communication, p. 8, point 3 «L'application des règles de protection des données au cours du processus électoral».
[21] Conclusions disponibles à l'adresse suivante: https://www.consilium.europa.eu/media/36777/18-euco-final-conclusions-fr.pdf.
[22] Voir points 10 à 12 de la Résolution P8_TA-PROV(2018)0433 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données (2018/2855(RSP)), disponible à l'adresse suivante: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0433+0+DOC+PDF+V0//FR, soulignement ajouté.
[23] Disponible à l'adresse suivante: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-630.530&format=PDF&language=FR&secondRef=02
[24] Disponible à l'adresse suivante: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2018-0435+0+DOC+PDF+V0//FR
[25] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2010)037-f
Commission européenne pour la démocratie par le droit (Commission de Venise), «Rapport sur le calendrier et l'inventaire des critères politiques d'évaluation d'une élection», p 4 et 5, étude nº 558/2009, Strasbourg, le 21.10.2010.

[26] http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-%20The%20new%20political%20campaigning_final.pdf
London School of Economic, Media Policy Brief 19, «The New Political Campaigning», p. 6. Mars 2017.
[27] Voir la Résolution P8_TA(2018)0204 du Parlement européen du 3 mai 2018 sur le pluralisme et la liberté des médias dans l'Union européenne (2017/2209(INI)), point S, disponible à l'adresse: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0204+0+DOC+PDF+V0//FR .
[28] Avis du CEPD nº 3/2018 sur la manipulation en ligne et les données à caractère personnel, et Compte rendu du Comité européen de la protection des données relatif aux conséquences de la concentration économique sur la protection des données adopté le 27 août 2018.
[29] Résolution sur l'utilisation des données personnelles pour la communication politique, Montreux (Suisse), du 14 au 16 septembre 2005.
[30] Communication, p. 2 et 5 et Document d'orientation, point 2.4.
[31] Communication, p. 6.
[32] 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 (le règlement «vie privée et communications électroniques»), COM(2017) 10 final, 2017/0003 (COD).
[33] Voir l'avis nº 6/2017 du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement «vie privée et communications électroniques»), et son blog disponible à l'adresse https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en .
[34] Règlement (UE, Euratom) nº 1141/2014 du Parlement européen et du Conseil du 22 octobre 2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes (JO L 317 du 4.11.2014, p. 1).
[35] Exposé des motifs, p. 2.
[36] Article premier, paragraphe 3, de la proposition de règlement introduisant un nouvel article 10 bis. Ce comité a été institué en vertu du règlement nº 1141/2014 (article 11). Voir également le 4e considérant de la proposition de règlement.
[37] Article premier, paragraphe 4, de la proposition de règlement introduisant une deuxième phrase à l'article 11, paragraphe 3, alinéa 1, du règlement nº 1141/2014.
[38] Article 6, point a), de la proposition de règlement introduisant un nouveau point vii) à l'article 27, paragraphe 2, point a), du règlement nº 1141/2014.
[39] Exposé des motifs, p. 4.
[40] Voir en particulier les points 40 et suivants de l'arrêt de la Cour (grande chambre) du 20 mars 2018, Garlsson Real Estate SA contre Commissione Nazionale per le Società e la Borsa (Consob), C-537/16, ECLI:EU:C:2018:193, dans lequel la Cour affirme que «*la circonstance selon laquelle l'infliction de ladite sanction pénale dépend d'un élément constitutif supplémentaire par rapport à la sanction administrative pécuniaire de nature pénale n'est pas, à elle seule, de nature à remettre en cause l'identité des faits matériels concernés. Sous réserve de vérification par la juridiction de renvoi, la sanction administrative pécuniaire de nature pénale et la procédure pénale en cause au principal semblent ainsi avoir pour objet une même infraction*» et qu'«*une limitation du principe ne bis in idem garanti à l'article 50 de la Charte peut être justifiée sur le fondement de l'article 52, paragraphe 1, de celle-ci*».
[41] L'article 33, paragraphe 8, du règlement nº 1141/2014 stipule que «*[l]es partis politiques européens et les fondations politiques européennes, les États membres et les organismes ou experts indépendants habilités à procéder à des missions de contrôle des comptes en vertu du présent règlement sont responsables, conformément au droit national applicable, des dommages qu'ils causent lors du traitement des données à caractère personnel conformément au présent règlement. Les États membres veillent à ce que des sanctions effectives, proportionnées et dissuasives soient appliquées en cas de violation du présent règlement, de la directive 95/46/CE et des dispositions nationales adoptées en vertu de celle-ci, notamment en cas d'utilisation frauduleuse des données à caractère personnel*».
[42] Article premier, paragraphe 3, de la proposition de règlement.
[43] Article premier, paragraphe 4, de la proposition de règlement modifiant l'article 11 du règlement nº 1141/2014.
[44] Avis du CEPD sur la manipulation en ligne et les données à caractère personnel, p. 19. Voir également la «Résolution sur la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans

l'économie numérique» adoptée le 23 octobre 2018 par la Conférence internationale des commissaires à la protection des données et de la vie privée, disponible à l'adresse suivante: https://icdppc.org/wp-content/uploads/2018/10/DCCW_adopted-resolution_FR.pdf

[45] Avis nº 3/2018 du CEPD sur la manipulation en ligne et les données à caractère personnel, p. 22.

[46] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1.

[47] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73.

[48] Communication, p. 4.

[49] Voir la note de bas de page 1 renvoyant au rapport émis en juillet 2018 par les autorités britanniques de protection des données (Information Commissioner's Office, ICO) qui résume les conclusions politiques découlant de l'enquête qu'elles ont conduite au sujet de l'utilisation de l'analyse des données à des fins politiques, et mettant un accent particulier sur la campagne pour le référendum de l'UE et le recours aux médias sociaux, ainsi que la note de pied de page 3 faisant référence aux règles adoptées par l'autorité italienne de protection des données en mars 2014, aux orientations additionnelles communiquées par la Commission nationale française pour la protection des données (CNIL) en novembre 2016 pour compléter ses recommandations de 2012 sur la communication politique, et précisant les règles de traitement des données à caractère personnel sur les réseaux sociaux, ainsi que les orientations sur les campagnes politiques («Guidance on political campaigning») publiées par l'ICO.

[50] Voir l'arrêt de la Cour (grande chambre) du 5 juin 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH, affaire C-210/16, ECLI:EU:C:2018:388.

[51] Avis 00264/10/EN, WP 169, disponible à l'adresse: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_fr.pdf, qui devra être actualisé à la lumière du RGPD dans un avenir proche.