

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Résumé de l'avis du Contrôleur européen de la protection des données sur le paquet de mesures de la Commission concernant des élections européennes libres et équitables

[Le texte complet de l'avis en allemand, anglais et français est disponible sur le site internet du CEPD www.edps.europa.eu]

(2019/C 47/05)

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 n° 3/2018 sur la manipulation en ligne, le Contrôleur européen de la protection des données (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 CEPD 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 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) n° 45/2001 et la décision n° 1247/2002/CE⁽¹⁾ [auparavant, règlement (CE) n° 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 (UE) 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.

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) n° 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»),

⁽¹⁾ JO L 295 du 21.11.2018, p. 39.

- 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»⁽⁷⁾. 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]⁽⁸⁾.
 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⁽⁹⁾. 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⁽¹⁰⁾, 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⁽¹¹⁾.
 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»⁽¹²⁾. Outre les sanctions financières qui pourraient être imposées aux fondations ou aux partis politiques européens, correspondant à 5 % de leur budget annuel⁽⁸⁾, 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»⁽⁹⁾. 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»)⁽¹⁰⁾ de leurs décisions concluant à une infraction aux réglementations 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»⁽¹¹⁾. 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⁽¹²⁾.
 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⁽¹³⁾.

⁽⁷⁾ Communication, p. 2.

⁽⁸⁾ http://europa.eu/rapid/press-release_IP-18-5681_fr.htm

⁽⁹⁾ 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>

⁽¹⁰⁾ Disponible à l'adresse suivante: <https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf>

⁽¹¹⁾ Communication, p. 10.

⁽¹²⁾ Exposé des motifs de la proposition de règlement, p. 2.

⁽¹³⁾ Voir article 27, paragraphe 4, point a), du règlement (UE) n° 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

⁽¹⁴⁾ Exposé des motifs de la proposition de règlement, p. 6.

⁽¹⁵⁾ Cette Autorité a été instituée en vertu du règlement (UE) n° 1141/2014 (article 6).

⁽¹⁶⁾ Recommandation n° 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 nationales dans le cadre des élections au Parlement européen». Soulignement ajouté.

⁽¹⁷⁾ Recommandation n° 11.

⁽¹⁸⁾ Recommandations n°s 1 à 5, incluse.

Ce dernier fait à la suite du premier échange organisé par la Commission en avril 2018 entre des pays de l'Union européenne 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 ⁽¹⁴⁾. 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 ⁽¹⁵⁾, 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» ⁽¹⁶⁾.

6. La Commission présente enfin plusieurs recommandations ⁽¹⁷⁾ 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» ⁽¹⁸⁾.
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» ⁽¹⁹⁾.
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 influencer 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 Parlement 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 ⁽²⁰⁾. 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 ⁽²¹⁾. Le 6 décembre 2018, la Commission des affaires constitutionnelles a adopté son rapport sur la proposition de règlement ⁽²²⁾.

⁽¹⁴⁾ 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

⁽¹⁵⁾ Communication, note de bas de page n° 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».

⁽¹⁶⁾ Communication, p. 7.

⁽¹⁷⁾ Recommandations nos 7 à 10 incluse et nos 12 à 19 incluse.

⁽¹⁸⁾ Communication, p. 8, point 3 «L'application des règles de protection des données au cours du processus électoral».

⁽¹⁹⁾ Conclusions disponibles à l'adresse suivante: <https://www.consilium.europa.eu/media/36777/18-euco-final-conclusions-fr.pdf>

⁽²⁰⁾ 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.

⁽²¹⁾ 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>

⁽²²⁾ 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>

10. 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.

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 (CE) n° 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 (UE) 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

Contrôleur européen de la protection des données
