COMMISSION
EUROPÉENNE

Bruxelles, le 12.9.2018
COM(2018) 637 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Garantir des élections européennes libres et équitables

La contribution de la Commission européenne à la réunion des chefs d'Etat et de gouvernement à Salzburg, les 19 et 20 septembre 2018

Garantir des élections européennes libres et équitables

Un moment crucial pour l'avenir de l'Union européenne

L'Union européenne a pour mission essentielle de défendre la démocratie et les valeurs démocratiques. Il s'agit là d'un impératif pour une société caractérisée par le pluralisme et la tolérance, dans laquelle les citoyens européens doivent pouvoir voter en étant sûrs qu'ils ne sont pas induits en erreur. Avec l'état de droit et les droits fondamentaux, la démocratie fait partie de notre identité et définit notre Union.

Les élections au Parlement européen de mai 2019 se tiendront dans un contexte très différent de celui de toutes les élections précédentes. Les défis politiques que doivent relever l'Union et ses États membres sont considérables. Il est absolument nécessaire de bâtir une Union plus robuste, capable d'agir avec crédibilité et force sur un échiquier mondial où les autres puissances internationales, qui ne partagent pas nécessairement tous nos intérêts ou nos valeurs, rivalisent pour exercer le pouvoir. Pour parvenir à une Union solide fondée sur une coopération judiciaire efficace, à un échange d'informations en vue de lutter contre le terrorisme et la criminalité organisée, et à un fonctionnement harmonieux du marché intérieur, il est nécessaire de pouvoir s'appuyer sur une confiance mutuelle entre les États membres et sur une confiance dans nos systèmes démocratiques. Dans ce contexte tout à fait particulier, les élections européennes de mai 2019 façonneront l'avenir de l'Union européenne au cours des prochaines années.

Assurer la résilience des systèmes démocratiques de l'Union fait partie des missions de l'union de la sécurité: les attaques contre les infrastructures électorales et les systèmes d'information sur les campagnes sont des menaces hybrides auxquelles l'Union doit répondre. Il est établi que les campagnes de désinformation massive en ligne menées à des fins politiques, y compris par des pays tiers, qui visent spécifiquement à discréditer et à délégitimer les élections, constituent une menace croissante pour nos démocraties[1]. L'Union européenne devrait prendre toutes les mesures en son pouvoir pour défendre ses processus démocratiques contre les manipulations exercées par des pays tiers ou des intérêts privés. Les périodes électorales se sont révélées particulièrement propices à la désinformation ciblée. Ces attaques nuisent à l'intégrité et à l'équité du processus électoral et à la confiance des citoyens dans leurs représentants: elles remettent véritablement en cause la démocratie elle-même.

Les citoyens européens devraient pouvoir voter en comprenant pleinement les choix politiques qui leur sont proposés, ce qui implique une meilleure prise de conscience des menaces et une plus grande transparence dans notre processus politique. Une sphère publique ouverte, qui protège contre les influences indues, garantit des conditions identiques pour tous,

[1] Voir la communication conjointe au Parlement européen, au Conseil européen et au Conseil – «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides» [JOIN(2018) 16 final] et les conclusions du Conseil européen du 28 juin 2018 (http://www.consilium.europa.eu/media/35943/28-euco-final-conclusions-fr.pdf).

pour des campagnes et des processus électoraux fiables[2]. Il est essentiel que nos démocraties ménagent une place pour des campagnes politiques dynamiques, qui donnent aux électeurs une image claire et non faussée des idées et des programmes des partis qui se disputent leurs voix. Il convient donc de lutter activement, y compris par des sanctions, contre la fraude et les autres tentatives délibérées de manipulation des élections.

Les activités en ligne, y compris pendant les processus électoraux, se développent rapidement, de sorte qu'une sécurité accrue et des conditions identiques pour tous sont essentielles. Les garanties électorales conventionnelles («hors ligne»), telles que les règles applicables aux communications politiques pendant les périodes électorales, la transparence et le plafonnement des dépenses électorales, le respect des périodes de silence et l'égalité de traitement des candidats, doivent également s'appliquer en ligne[3]. La transparence et les restrictions applicables aux publicités à caractère politique à la télévision ou sur les panneaux d'affichage devraient elles aussi s'appliquer de la même manière dans le monde en ligne. Ce n'est pas le cas aujourd'hui et il convient de remédier à ce problème avant les prochaines élections européennes.

Les nouveaux défis et les évolutions récentes

Si la communication en ligne a réduit les barrières et les coûts en matière d'interaction entre les acteurs politiques et les citoyens et offre de grandes possibilités dans ce domaine, elle a également accru les possibilités pour les acteurs malveillants de cibler le débat démocratique et les processus électoraux. L'environnement en ligne permet aux acteurs de présenter plus facilement des informations tout en dissimulant leur origine ou leur objectif, notamment en taisant le fait qu'une communication (une publication sur les médias sociaux, p. ex.) soit une publicité payante plutôt qu'une présentation factuelle, en présentant des opinions comme du travail journalistique ou en opérant une présentation sélective des informations pour susciter des tensions ou des débats polémiques. Il ne faut pas se voiler la face: l'Union européenne et ses systèmes politiques ne sont pas à l'abri de ces menaces.

En outre, l'intégrité des élections peut être sérieusement affectée par des cyberincidents «classiques», y compris par des cyberattaques ciblant les processus électoraux, les campagnes, les infrastructures des partis politiques et les systèmes de candidats ou d'autorités publiques, ou par l'utilisation abusive de données à caractère personnel. Les révélations récentes, notamment dans l'affaire «Facebook/Cambridge Analytica», en sont l'illustration:

[2] La commission de Venise du Conseil de l'Europe fournit des lignes directrices sur les élections (http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-f), y compris pour l'environnement médiatique (http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

[3] Voir la récente publication du Conseil de l'Europe «Internet et campagnes électorales – Étude relative à l'utilisation d'internet dans le cadre des campagnes électorales», préparée par le comité d'experts sur le pluralisme des médias et la transparence de leur propriété (MSI-MED) (https://www.coe.int/fr/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published). Cette étude examine les incidences du déplacement de la publicité électorale vers internet, notamment en ce qui concerne les dépenses électorales et les techniques publicitaires basées sur le microciblage des électeurs, au moyen de messages personnalisés. Voir également la recommandation CM/Rec(2016)5 du Conseil de l'Europe sur la liberté d'internet, qui a trait aux responsabilités des gouvernements, des plateformes et des intermédiaires pour les campagnes politiques menées en ligne par des partis politiques, des candidats et d'autres personnes.

des données à caractère personnel semblent avoir été utilisées abusivement et transmises illégalement à des tiers pour des usages très différents de ceux auxquels elles étaient initialement destinées. Ces affaires ont mis en lumière les risques potentiels de certaines activités en ligne qui sont utilisées pour cibler des citoyens à leur insu au moyen de publicités et de communications politiques, en traitant illégalement et abusivement leurs données à caractère personnel pour manipuler l'opinion, répandre la désinformation ou simplement porter atteinte à la vérité à des fins politiques ou pour attiser les divisions[4].

Soutenir l'organisation d'élections libres et équitables en Europe

Les institutions européennes n'organisent pas d'élections: les actions menées dans ce contexte relèvent avant tout de la compétence des États membres. Ce sont eux qui sont responsables de l'organisation des élections et du suivi de la conduite du processus électoral[5]. Néanmoins, il existe une dimension européenne évidente. En présentant des candidats aux élections au Parlement européen, les partis politiques nationaux et régionaux jouent un rôle de premier plan dans les campagnes électorales européennes. Les partis politiques européens et les fondations qui leur sont associées remplissent une fonction importante en organisant des campagnes complémentaires au niveau européen, notamment pour soutenir les têtes de liste candidates au poste de président de la Commission européenne.

À la suite des élections au Parlement européen de 2014, la Commission s'était engagée, dans son rapport post-électoral de 2015[6], à trouver les moyens de renforcer encore la dimension européenne et la légitimité démocratique du processus décisionnel de l'UE, ainsi qu'à examiner plus en profondeur les raisons de la persistance d'un faible taux de participation dans certains États membres et à y remédier. En février 2018, la Commission a appelé à un dialogue précoce et permanent avec les citoyens sur les questions européennes, à un début plus précoce des campagnes des partis politiques pour les élections au Parlement européen, y compris celles de leurs candidats à la présidence de la Commission européenne, à une plus grande transparence sur les liens entre partis politiques nationaux et européens et à la promotion du droit de vote par les États membres, en particulier auprès des groupes sous-représentés.

---

[4] Voir le rapport intermédiaire publié par l'autorité britannique chargée de la protection des données (ICO) après le lancement d'une enquête formelle sur le recours à l'analyse de données à des fins politiques, à la suite d'allégations de traitement illicite de données et de microciblage de publicités à caractère politique au cours du référendum britannique sur l'UE (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). Ce rapport souligne que «*l'évolution rapide, sur le plan social et technologique, de l'utilisation des mégadonnées implique une méconnaissance des techniques de traitement des données en coulisse, ou une transparence limitée sur ces techniques (algorithmes, analyse, appariement des données et profilage), qui sont utilisées par les organisations et les entreprises pour microcibler les individus. Ce qui est clair, c'est que ces outils peuvent avoir un impact significatif sur la vie privée des personnes. Il importe de parvenir à une plus grande et réelle transparence quant à l'utilisation de ces techniques, afin de garantir que les personnes exercent un contrôle sur leurs propres données et que la loi soit respectée. Lorsque l'objectif de l'utilisation de ces techniques est lié au processus démocratique, il est indispensable de mettre en place des normes de transparence élevées*». Le rapport souligne également l'importance de mieux intégrer les préoccupations relatives à la protection des données dans le cadre réglementaire plus large qui régit les élections.

[5] Dans le cadre du droit de l'Union et de leurs obligations internationales.

[6] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Rapport sur les élections au Parlement européen de 2014 [COM(2015) 206 final].

L'Union européenne a déjà pris certaines mesures importantes pour renforcer la résilience démocratique en Europe, notamment grâce au nouveau cadre européen en matière de protection des données, en vigueur depuis mai dernier. Ce règlement général sur la protection des données, qui est devenu directement applicable dans toute l'Union européenne, fournit les instruments nécessaires pour remédier aux cas d'utilisation illicite de données à caractère personnel dans le contexte électoral. Des travaux sont également en cours pour promouvoir un environnement en ligne plus sûr en renforçant notre résilience globale face aux cybermenaces, y compris la désinformation en ligne et la manipulation des comportements.

Il est important de faire la plus grande clarté sur la manière de mettre en œuvre les règles européennes en matière de protection des données dans ce nouveau contexte, et nous devons également intensifier nos efforts pour accroître la sensibilisation, la transparence et la sécurité. Les citoyens doivent pouvoir déterminer qui leur parle en ligne à travers les messages publicitaires et politiques, et qui finance les publicités à caractère politique ou les messages politiques. Des orientations sur la manière de mettre en œuvre les nouvelles règles en matière de protection des données dans le contexte des élections européennes devraient contribuer à une plus grande clarté et à une meilleure compréhension, car le renforcement de la coopération et de l'échange d'informations entre les autorités compétentes et avec d'autres parties prenantes contribuera à accroître la sécurité.

Le train de mesures visant à renforcer la résilience démocratique présenté en même temps que la présente communication comprend des actions équilibrées, complètes et ciblées visant à favoriser l'intégrité et le bon déroulement des élections de 2019 au Parlement européen. Il s'agit d'une responsabilité commune de tous les acteurs intervenant dans le processus électoral, qui requiert une vigilance constante et une adaptation souple à un environnement dynamique et à de nouvelles avancées technologiques. En fournissant des orientations, des recommandations et les outils nécessaires, les partis politiques européens et nationaux, les gouvernements nationaux, les autorités, les entités privées et les parties prenantes peuvent tous collaborer avec plus de clarté à la création d'un environnement démocratique plus sûr et plus équitable.

Les États membres sont en outre encouragés à appliquer ces principes aux autres élections et aux référendums qu'ils organisent au niveau national.

Les mesures proposées dans ce paquet visent à:

1. fournir des orientations spécifiques concernant le traitement des données à caractère personnel dans le cadre d'élections;
2. recommander des meilleures pratiques pour lutter contre les risques de désinformation et de cyberattaques et pour promouvoir la transparence et la responsabilité en ligne dans le processus électoral de l'UE; et améliorer la coopération entre les autorités compétentes et mettre en place des outils leur permettant d'intervenir et, si nécessaire, d'instaurer des sanctions afin de préserver l'intégrité du processus électoral;

3. faire face aux situations dans lesquelles les partis politiques ou les fondations qui leur sont associées bénéficient de pratiques qui enfreignent les règles de protection des données et visent à influencer délibérément ou de tenter d'influencer les résultats des élections européennes.

En proposant ce train de mesures, la Commission a veillé à éviter les charges administratives inutiles et à ne pas limiter de manière inappropriée la marge de manœuvre des partis et fondations politiques européens, régionaux et nationaux.

1. Les moyens de défense actuels de l'UE pour la tenue d'élections libres et équitables

L'Union a déjà pris des mesures importantes pour protéger l'intégrité des élections et pour renforcer le processus démocratique.

Le règlement général sur la protection des données (RGPD)[7] étant directement applicable dans toute l'Union depuis le 25 mai 2018, l'Union européenne est désormais dotée de tous les moyens nécessaires pour prévenir et traiter les cas d'utilisation illicite de données à caractère personnel. De la sorte, elle est devenue une référence en la matière.

Qui plus est, l'acte concernant l'élection des membres du Parlement européen a été modifié récemment, notamment pour accroître la transparence du processus électoral européen[8]. Le règlement révisé sur le statut et le financement des partis politiques européens[9], adopté le 3 mai 2018, renforce la reconnaissance, l'efficacité, la transparence et la responsabilité des partis et fondations politiques européens. La recommandation (UE) 2018/234 de la Commission[10] souligne les étapes essentielles visant à rendre plus efficace la conduite des élections au Parlement européen de 2019.

La directive 2002/58/CE du Parlement européen et du Conseil (directive vie privée et communications électroniques)[11] couvrait les communications non sollicitées effectuées à des fins de prospection directe, et notamment les messages à caractère politique diffusés par des partis politiques ou d'autres acteurs participant au processus politique. Elle garantissait également la confidentialité et la protection des informations stockées dans l'équipement

[7] 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) (JO L 119 du 4.5.2016, p. 1).

[8] Décision (UE, Euratom) 2018/994 du Conseil du 13 juillet 2018 modifiant l'acte portant élection des membres du Parlement européen au suffrage universel direct, annexé à la décision 76/787/CECA, CEE, Euratom du Conseil du 20 septembre 1976 (https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1531826494620&uri=CELEX%3A32018D0994).

[9] Règlement (UE, Euratom) n° 1141/2014 du Parlement européen et du Conseil du 22 octobre 2014 relatif au statut et au financement des partis et fondations politiques européens (JO L 317 du 4.11.2014, p. 1).

[10] Recommandation (UE) 2018/234 de la Commission du 14 février 2018 visant à renforcer le caractère européen des élections au Parlement européen de 2019 et à rendre leur conduite plus efficace (JO L 45 du 17.2.2018, p. 40).

[11] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

terminal d'un utilisateur, tel qu'un téléphone intelligent ou un ordinateur[12]. La proposition de règlement sur la vie privée et les communications électroniques[13], en cours de négociation, renforcera encore le contrôle exercé par les citoyens en renforçant la transparence et élargira la portée de la protection au-delà des opérateurs de télécommunications traditionnels pour y inclure les services de communications électroniques basés sur l'internet.

En outre, la Commission a récemment présenté une approche européenne pour lutter contre la désinformation en ligne dans sa communication du 26 avril 2018[14]. Par la présente communication, la Commission cherche à promouvoir un environnement en ligne plus transparent, plus fiable et plus responsable. L'un de ses principaux résultats attendus est l'élaboration d'un ambitieux **code de bonnes pratiques contre la désinformation**, qui devrait notamment engager les plateformes en ligne et l'industrie de la publicité à assurer la transparence et à restreindre les possibilités de ciblage des publicités à caractère politique[15]. Ce code devrait être publié en septembre 2018[16] et produire des résultats mesurables à partir d'octobre.

Plus précisément, les signataires du code de bonnes pratiques devront accepter de priver les sites web «imposteurs» et les sites web qui hébergent de fausses informations de recettes publicitaires, garantir la transparence sur les contenus sponsorisés, en particulier les publicités à caractère politique et les publicités engagées, mettre en place des systèmes et des règles de marquage clairs pour les robots[17], afin de veiller à ce que leurs activités ne puissent pas être confondues avec des interactions humaines, et intensifier les efforts de suppression des faux comptes. Les signataires devront également convenir de faciliter l'évaluation des contenus par les utilisateurs en encourageant l'élaboration d'indicateurs de fiabilité des sources de contenu, diluer la visibilité de la désinformation en rendant les contenus fiables plus faciles à trouver, et fournir aux utilisateurs des informations sur la hiérarchisation des contenus par les algorithmes. Enfin, les signataires devront fournir un accès aux données des plateformes aux organismes reconnus de vérification des faits et aux universités. 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.

[12] Les utilisateurs doivent donner leur consentement avant que les sites web ne puissent accéder à ces informations ou suivre leur comportement en ligne, par exemple en stockant des témoins de connexion (*cookies*) sur leur appareil.
[13] 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»), COM(2017) 10 final.
[14] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: «Lutter contre la désinformation en ligne: une approche européenne», COM(2018) 236 final.
[15] Pour préparer ce code de bonnes pratiques, la Commission a organisé, en mai 2018, un forum composé d'un «groupe de travail» (constitué des principales plateformes en ligne et de représentants du secteur de la publicité et des principaux annonceurs) et d'un «groupe de réflexion» (constitué de représentants des médias et de la société civile).
[16] Après que le groupe de réflexion aura rendu son avis.
[17] Les robots incluent les publications automatisées sur les plateformes de médias sociaux et les applications plus interactives comme les robots conversationnels, qui interagissent directement avec les utilisateurs.

Pour ce qui est des cyberincidents plus «traditionnels», tels que le piratage de systèmes informatiques ou la défiguration de sites web, les définitions des infractions et le niveau minimal des sanctions en matière d'attaques contre les systèmes d'information ont été harmonisés au niveau de l'Union européenne par la directive 2013/40/UE relative aux attaques contre les systèmes d'information.

Le groupe de coopération institué en vertu de la directive (UE) 2016/1148 du Parlement européen et du Conseil[18] a conclu que la cybersécurité des élections constitue un défi commun. Ce groupe de coopération, composé des autorités nationales compétentes en matière de cybersécurité, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), a cartographié les initiatives nationales existantes en matière de cybersécurité des réseaux et des systèmes d'information utilisés pour les élections. Il a recensé les risques associés à un niveau insuffisant de cybersécurité susceptible d'affecter les prochaines élections au Parlement européen, et a élaboré un recueil sur la cybersécurité des technologies électorales, qui comprend des mesures techniques et organisationnelles fondées sur les expériences et les meilleures pratiques. Ce recueil fournit des orientations pratiques aux autorités chargées de la cybersécurité et aux organismes de gestion électorale.

2. L'amélioration de la résilience démocratique: des réseaux de coopération plus nombreux, une plus grande transparence en ligne, une protection accrue contre les incidents de cybersécurité et une intensification de la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen

Vu l'ampleur du défi et compte tenu du partage des responsabilités formelles dans ce domaine entre de multiples autorités, des résultats significatifs ne seront obtenus que si tous les acteurs concernés collaborent.

La présente communication est accompagnée d'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. Afin de garantir la tenue d'élections libres et équitables, cette recommandation doit être mise en œuvre par tous les acteurs en temps utile pour les élections de 2019 au Parlement européen.

Dans la recommandation, nous encourageons chaque État membre à mettre en place et à soutenir un réseau électoral national. Les autorités des États membres compétentes en matière électorale devraient coopérer avec les autorités compétentes dans des domaines connexes (comme les autorités chargées de la protection des données, les autorités de régulation des

[18] 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).

médias, les autorités chargées de la cybersécurité, etc.) en temps utile et de manière efficace. Le cas échéant, elles devraient également collaborer avec les services répressifs. Elles 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. Les législations européenne et nationales doivent être respectées et appliquées. Dans cette perspective, 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.

La Commission recommande également aux États membres de désigner des points de contact pour participer à un réseau européen de coopération concernant les élections au Parlement européen. Elle soutiendra ce réseau de coopération en organisant, d'ici janvier 2019, une première réunion des points de contact désignés. Tout en respectant les compétences nationales et les exigences procédurales applicables aux autorités concernées, ce forum constituera le noyau d'un processus d'alerte européen en temps réel et une plateforme d'échange d'informations et de pratiques entre les autorités des États membres.

Les partis et fondations politiques et les organisations chargées des campagnes doivent garantir des pratiques transparentes dans les communications politiques qu'ils adressent aux citoyens et veiller à ce que le processus électoral européen ne soit pas faussé par des pratiques déloyales. La Commission présente des mesures concrètes pour renforcer la transparence afin que les citoyens puissent voir qui est à l'origine des communications politiques qu'ils reçoivent et qui les finance[19]. Les États membres devraient favoriser et faciliter cette transparence, ainsi que les efforts déployés par les autorités compétentes pour surveiller les infractions et faire respecter les règles, y compris en appliquant des sanctions si nécessaire. Le cas échéant, les autorités répressives devraient également être associées pour garantir une réaction appropriée aux incidents et l'application de sanctions appropriées[20].

La résilience, la dissuasion et la défense sont essentielles pour construire une cybersécurité solide pour l'Union européenne[21]. Les autorités européennes et nationales compétentes, les partis et fondations politiques et les organisations chargées des campagnes devraient être

[19] Ces propositions s'inscrivent dans une complémentarité avec le code de bonnes pratiques élaboré par le forum plurilatéral organisé par la Commission à la suite de sa communication du 26 avril 2018 sur la désinformation en ligne.

[20] Cela 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.

[21] Dans leur communication conjointe de septembre 2017, la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et la Commission européenne reconnaissent la nécessité d'une réponse globale pour doter l'Union d'une cybersécurité solide fondée sur la résilience, la dissuasion et la défense, JOIN(2017) 450 final.

pleinement conscients des risques pour les élections de l'année prochaine et déployer des efforts appropriés pour protéger leurs réseaux et leurs systèmes d'information[22].

3. L'application des règles de protection des données au cours du processus électoral

Le règlement (UE) 2016/679 du Parlement européen et du Conseil (règlement général sur la protection des données)[23], qui est devenu directement applicable dans l'Union le 25 mai 2018, fournit à l'Union les outils nécessaires pour faire face aux cas d'utilisation illicite de données à caractère personnel dans le contexte électoral.

Étant donné que c'est la toute première fois que ces règles seront appliquées dans le contexte électoral européen à l'occasion des prochaines élections au Parlement européen, il est important que tous les acteurs participant aux processus électoraux (c'est-à-dire les autorités électorales nationales, les partis politiques, les courtiers en données et les analystes de données, les plateformes de médias sociaux et les réseaux d'annonces publicitaires en ligne) comprennent clairement comment appliquer au mieux ces règles, ce qu'elles autorisent et ce qu'elles interdisent.

La Commission a donc élaboré des orientations spécifiques pour mettre en évidence les obligations en matière de protection des données qui sont pertinentes dans le contexte électoral. Afin de lutter contre les tentatives malveillantes d'utilisation abusive des données à caractère personnel des individus, en particulier à des fins de microciblage, les autorités nationales chargées de la protection des données, en tant qu'autorités chargées de veiller au respect du règlement général sur la protection des données, doivent faire pleinement usage de leurs pouvoirs renforcés pour prendre des mesures à l'égard d'éventuelles infractions.

4. Le renforcement des règles de financement des partis politiques européens

[22] Le recueil élaboré par le groupe de coopération créé au titre de la directive (UE) 2016/1148 fournit des orientations utiles à cet égard. La directive (UE) 2016/1148 vise à atteindre un niveau commun élevé de résilience en matière de cybersécurité dans toute l'Union. Afin d'atteindre cet objectif, la directive soutient le développement des capacités nationales en matière de cybersécurité et protège la fourniture de services essentiels dans des secteurs clés. En vue de renforcer les efforts menés en vue d'une mise en œuvre adéquate de la directive, la Commission injectera jusqu'en 2020 plus de 50 millions d'euros au titre du programme relatif au mécanisme pour l'interconnexion en Europe (MIE). Les mesures de gestion des risques prévues par la directive (UE) 2016/1148 sont des valeurs de référence pertinentes pour le processus électoral. Le RGPD prévoit également des obligations de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité pour les données à caractère personnel en cours de traitement. Il s'applique à tous les acteurs intervenant dans le processus électoral et prévoit aussi l'obligation de communiquer les violations de données à caractère personnel aux autorités compétentes en matière de protection des données, ainsi qu'aux personnes concernées (voir les orientations émises par la Commission).

[23] 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) (JO L 119 du 4.5.2016, p. 1).

Les partis et fondations politiques sont évidemment les principaux acteurs des élections. Ils rivalisent pour obtenir les voix des électeurs grâce à leurs campagnes. Afin de garantir des conditions équitables et de protéger tous les partis et fondations politiques contre les actes de malveillance, il est essentiel d'empêcher que se produisent des situations dans lesquelles un parti peut tirer profit de pratiques illégales contraires aux règles de protection des données. Quant aux actes qui ne se limitent pas à porter atteinte à la vie privée des individus mais peuvent également influencer le résultat des élections au Parlement européen, ils doivent être sanctionnés. Parallèlement à l'invitation faite aux États membres d'appliquer si nécessaire de telles sanctions aux partis et fondations au niveau national, la Commission propose d'introduire une modification ciblée du règlement (UE, Euratom) n° 1141/2014 afin de prévoir des sanctions proportionnées dans les cas impliquant des partis et fondations politiques au niveau européen. Cette modification, qui renforce les règles existantes, vise à garantir que les élections au Parlement européen puissent se dérouler conformément à des règles démocratiques strictes et dans le plein respect des valeurs fondatrices de l'Union, en particulier la démocratie, les droits fondamentaux et l'état de droit.

La Commission invite instamment le Parlement européen et le Conseil à veiller à ce que ces modifications ciblées soient en vigueur avant les élections au Parlement européen de 2019.

5. Conclusions

Les événements récents ont montré que les risques de manipulation du processus électoral, que ce soit par des attaques contre des systèmes d'information, par l'utilisation abusive de données à caractère personnel ou par des pratiques opaques, sont réels et aigus. L'UE n'est pas à l'abri. Les activités en ligne dans le contexte électoral présentent une nouvelle menace et nécessitent une protection spécifique. C'est en nous préparant aujourd'hui que nous servirons aux mieux les citoyens et la démocratie. Nous ne pouvons pas attendre de constater après des élections ou des référendums que de telles activités ont eu lieu et y répondre après coup.

La protection de la démocratie dans l'Union est une responsabilité partagée et solennelle de l'Union européenne et de ses États membres. Et le temps presse. Tous les acteurs concernés doivent intensifier leurs efforts et coopérer afin de dissuader, de prévenir et de sanctionner les interférences malveillantes dans le système électoral. Les mesures proposées par la Commission dans le cadre de ce paquet soutiennent ces efforts.

La Commission fera rapport après les élections au Parlement européen de 2019 sur la mise en œuvre de cet ensemble de mesures.

Les prochaines étapes avant les élections au Parlement européen de 2019

- *La Commission invite instamment le Parlement européen et le Conseil à veiller à ce que les modifications ciblées du règlement (UE, Euratom) n° 1141/2014 soient en vigueur avant les élections au Parlement européen de 2019.*

- *En collaboration avec la haute représentante, la Commission soutiendra la préparation de réponses européennes communes pour réagir à toute ingérence étrangère dans les élections au sein de l'Union européenne*[24]*. Dans le droit fil des conclusions du Conseil européen de juin 2018, elles présenteront en coopération avec les États membres, d'ici décembre 2018, un plan d'action assorti de propositions spécifiques pour une réponse coordonnée de l'UE au défi de la désinformation.*

- *La Commission intensifiera la sensibilisation et maintiendra son dialogue avec les autorités des États membres dans le cadre de la conférence de haut niveau sur les menaces liées au cyberespace pour les élections. Les résultats de cette conférence, qui se tiendra les 15 et 16 octobre 2018, alimenteront le prochain colloque sur les droits fondamentaux (des 26 et 27 novembre 2018), axé sur «la démocratie dans l'Union européenne».*

[24] À cet effet, il pourrait également être recouru aux mesures élaborées au titre du cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance.