

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Résumé de l'avis du contrôleur européen de la protection des données sur la manipulation en ligne et les données à caractère personnel

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

(2018/C 233/06)

La numérisation de la société et de l'économie a des répercussions mitigées sur l'engagement civique dans les prises de décision et sur les obstacles à la participation du public aux processus démocratiques.

Grâce à l'analyse des mégadonnées et aux systèmes d'intelligence artificielle, il est dorénavant possible de collecter, de combiner, d'analyser et de stocker pour une durée indéterminée d'énormes volumes de données. Un modèle d'entreprise dominant dans la plupart des services fondés sur le web est apparu au cours des vingt dernières années. Il repose sur le traçage en ligne des personnes, sur la collecte de données sur leur personnalité, sur leur état de santé, sur leurs relations, sur leurs réflexions et avis de manière à générer des revenus publicitaires numériques. Ces marchés numériques se concentrent aujourd'hui autour de quelques sociétés qui jouent dans les faits le rôle de gardiens de l'internet et disposent de valeurs de capitalisation boursière corrigées de l'inflation plus élevées qu'aucune autre société dans l'histoire.

Cet écosystème numérique connecte des personnes dans le monde entier, plus de 50 % de la population mondiale ayant accès à l'internet, même si cet accès est très déséquilibré selon la situation géographique, la richesse et le genre. L'optimisme initial suscité par le potentiel de l'internet et des médias sociaux en matière d'engagement civique a fait place à des inquiétudes selon lesquelles les gens sont manipulés, premièrement au travers de l'exploitation permanente d'informations qui relèvent souvent de l'intime, deuxièmement du contrôle des informations qu'ils voient en ligne selon la catégorie dans laquelle ils sont placés. L'aspect «viral» d'un scandale est un élément de valeur clé pour de nombreux services axés sur des algorithmes et dont les produits et les applications sont conçus pour maximiser l'attention et l'addiction. La connectivité, tout du moins dans le modèle actuel, a mené à la division.

Le débat qui en résulte tourne depuis autour des informations («contenu») trompeuses, erronées ou calomnieuses présentées aux gens dans l'intention d'influencer le discours politique et les élections, phénomène appelé «fake news» ou «désinformation en ligne». Les solutions portent particulièrement sur les mesures de transparence, sur le fait de révéler la source de l'information, tout en négligeant la redevabilité des acteurs de l'écosystème qui profitent de ces comportements néfastes. Parallèlement, la concentration du marché et l'essor de la domination des plateformes font peser une nouvelle menace sur le pluralisme des médias. Pour le CEPD, la crise de confiance dans l'écosystème numérique illustre l'interdépendance du respect de la vie privée et de la liberté d'expression. La réduction de l'espace privé dont disposent les gens, qui découle de la surveillance inévitable exercée par les entreprises et par les gouvernements, a une incidence négative sur la capacité et la volonté des gens de s'exprimer et de tisser librement des liens, y compris dans la sphère civique qui est essentielle à la bonne santé de la démocratie. Le présent avis s'intéresse dès lors à la manière dont les informations personnelles sont utilisées à des fins de microciblage des personnes et des groupes pour leur offrir un contenu spécifique, aux valeurs et aux droits fondamentaux en jeu, et aux lois adoptées pour atténuer les menaces.

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, raison pour laquelle nous avons lancé la «Digital Clearing House» (chambre de compensation numérique) en 2017. Au vu des inquiétudes selon lesquelles les campagnes politiques exploitent peut-être l'espace numérique de manière à contourner les lois en vigueur⁽¹⁾, nous estimons qu'il est à présent temps que cette collaboration s'étende aux organismes de régulation électoraux et de l'audiovisuel.

1. POURQUOI PUBLIONS-NOUS LE PRÉSENT AVIS

i. Un intense débat public en cours

Aujourd'hui, l'incidence des vastes écosystèmes complexes d'informations numériques, non seulement sur l'économie de marché, mais également sur l'économie politique, et la manière dont l'environnement politique interagit avec l'économie font l'objet d'un débat public intense. Les principales plateformes sont au cœur de cet écosystème et tirent un avantage disproportionné de la croissance de la publicité numérique, élargissant leur pouvoir relatif à mesure qu'elle se développe. Les données à caractère personnel sont nécessaire pour segmenter, cibler et personnaliser les messages présentés aux personnes, mais la plupart des annonceurs ne sont pas conscients de la manière dont de telles décisions sont prises et la plupart des personnes ne sont pas conscientes de la manière dont elles sont utilisées. Le système récompense le contenu sensationnel et qui fait le buzz et ne fait, en général, pas de distinctions entre les annonceurs, qu'ils soient commerciaux

⁽¹⁾ Voir, par exemple, <http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html> [consulté le 18.3.2018].

ou politiques. Certaines révélations mettant en lumière la façon dont les «fake news» (désinformation) sont propagées de façon délibérée grâce à ce système ont suscité des craintes quant à la menace qui pourrait peser sur l'intégrité des démocraties. Les systèmes d'intelligence artificielle, dont le marché est également caractérisé par la concentration, sont eux-mêmes alimentés par les données et, s'ils ne sont pas contrôlés, ils accroissent l'éloignement et l'irresponsabilité des prises de décision dans cet environnement.

ii. Pertinence de la législation sur la protection des données et des campagnes politiques

Les droits fondamentaux au respect de la vie privée et à la protection des données constituant clairement un facteur clé pour remédier à cette situation, cette question devient dès lors une priorité stratégique pour toutes les autorités indépendantes compétentes en matière de protection des données. Dans leur *résolution sur l'utilisation de données personnelles pour la communication politique* de 2005, les organismes de régulation de la protection des données ont exprimé des inquiétudes essentielles en matière de protection des données au niveau mondial, liées au traitement croissant des données à caractère personnel par des acteurs non commerciaux. Il y était particulièrement fait référence au traitement de «données sensibles touchant aux activités ou convictions morales et politiques réelles ou supposées ou aux choix électoraux» et à l'établissement «de manière intrusive [du] profil de diverses personnes qui sont couramment classées — parfois de façon inexacte ou sur la base d'un contact superficiel — dans la catégorie des sympathisants, des partisans, des adhérents ou des membres d'un parti»⁽¹⁾. Cette résolution internationale demandait une application plus stricte des règles de protection des données relatives à la minimisation des données, au traitement licite, au consentement, à la transparence, aux droits des personnes concernées, à la limitation de la finalité et à la sécurité des données. Il est peut-être temps de renouveler cette demande.

La législation de l'Union européenne en matière de protection des données et de confidentialité des communications électroniques s'applique à la collecte de données, au profilage et au microciblage, et si elle est correctement mise en œuvre, elle devrait contribuer à minimiser les préjudices issus des tentatives de manipuler des personnes et des groupes. Le traitement des données sur les électeurs effectué par des partis politiques relève du règlement général sur la protection des données. Selon ce règlement, les données à caractère personnel qui révèlent des opinions politiques constituent une catégorie de données particulière. Le traitement desdites données est généralement interdit à moins qu'une des dérogations énumérées ne s'applique. Dans le cadre d'une campagne politique, les deux dérogations suivantes sont particulièrement pertinentes et méritent une citation complète:

- «(d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;
- (e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée; [...]
- (g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.»

Le considérant 56 précise l'article 9, paragraphe 2, point g): «[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».

Plusieurs autorités de protection des données ont élaboré des règles ou des lignes directrices sur le traitement des données à des fins politiques:

- En mars 2014, l'autorité italienne de protection des données a adopté des règles relatives au traitement des données à caractère personnel effectué par les partis politiques. Ces règles insistaient sur l'interdiction générale d'utiliser des données à caractère personnel publiées sur l'internet, comme sur les réseaux sociaux ou sur les forums, à des fins de communication politique, si ces données avaient été collectées à d'autres fins⁽²⁾.
- En novembre 2016, la Commission nationale de l'informatique et des libertés française (CNIL) a ajouté des lignes directrices à ses recommandations de 2012 sur la communication politique, en y spécifiant les règles relatives au traitement des données personnelles issues des réseaux sociaux. La CNIL a particulièrement souligné que l'agrégation de données personnelles d'électeurs destinée à établir leurs profils et à les cibler sur les réseaux sociaux est licite uniquement si elle se fonde sur le consentement comme motif de traitement des données⁽³⁾.

⁽¹⁾ La résolution est disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_fr.pdf [consulté le 18.3.2018].

⁽²⁾ <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267> «Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale» publié dans le Journal officiel de l'autorité italienne de protection des données, numéro 71 du 26.3.2014 [doc. web n. 3013267].

⁽³⁾ <https://www.cnil.fr/fr/communication-politique-queles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux> «Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?» publié par la Commission nationale de l'informatique et des libertés le 8.11.2016.

- En avril 2017, le bureau du commissaire à l'information (ICO) du Royaume-Uni a publié une version actualisée de ses *orientations sur les campagnes politiques* (Guidance on political campaigning), qui comprenait également des lignes directrices sur l'utilisation des analyses de données dans les campagnes politiques. L'ICO y expliquait que lorsqu'une organisation politique charge une entreprise tierce d'effectuer des analyses, cette entreprise est alors susceptible d'être un sous-traitant tandis que l'organisation est responsable du traitement. Il convient de tenir compte de certaines dispositions spécifiques prévues dans la loi de protection des données qui gouvernent la relation entre sous-traitant et responsable afin que le traitement soit légal ⁽¹⁾.

Les lignes directrices des autorités nationales de protection des données peuvent offrir une interprétation supplémentaire qui fait autorité sur les dispositions juridiques relatives à la protection des données et au respect de la vie privée, qui tiennent compte des différences dans l'organisation des systèmes politiques nationaux ⁽²⁾.

iii. L'objet du présent avis du CEPD

La vision du CEPD est d'aider l'Union européenne à ouvrir la voie en montrant l'exemple dans le dialogue mondial sur la protection des données et sur le respect de la vie privée à l'ère numérique en apportant des solutions politiques interdisciplinaires aux défis que posent les mégadonnées et en développant une dimension éthique dans le traitement des informations personnelles ⁽³⁾. Nous avons demandé que la personne concernée soit traitée «en tant qu'individu et non uniquement en tant que consommateur ou qu'utilisateur» et mis en lumière des questions éthiques quant aux effets du profilage prédictif et de la personnalisation déterminée par un algorithme ⁽⁴⁾. Nous avons appelé de nos vœux une évolution responsable et durable de la société numérique basée sur le contrôle de chacun sur ses données à caractère personnel, sur une ingénierie et une responsabilité conscientes du respect de la vie privée et sur une mise en œuvre cohérente ⁽⁵⁾. Dans son rapport de janvier 2018, le groupe consultatif sur l'éthique du CEPD fait observer que «le microciblage du démarchage électoral modifie les règles de la parole publique en ce qu'il réduit l'espace disponible pour débattre et échanger des idées», ce qui «requiert de toute urgence un débat démocratique sur l'utilisation et l'exploitation des données dans les campagnes politiques et les prises de décisions» ⁽⁶⁾.

La question de l'utilisation d'informations et de données à caractère personnel afin de manipuler les gens et la politique est évidemment beaucoup plus vaste que le droit à la protection des données. Un environnement en ligne personnalisé et microciblé crée des «bulles de filtrage» au sein desquelles les gens sont toujours exposés au même type d'informations et confrontés à moins d'opinions, d'où une polarisation politique et idéologique accrue ⁽⁷⁾. En raison de ce phénomène, les fausses informations et les théories conspirationnistes ont un plus grand pouvoir de persuasion et sont toujours plus répandues ⁽⁸⁾. D'après des recherches, la manipulation des fils d'actualité ou des résultats de recherche pourrait influencer le comportement des gens en matière de vote ⁽⁹⁾.

Le CEPD souhaite aider à garantir que le traitement des données à caractère personnel, selon la formulation du règlement général sur la protection des données, serve l'humanité et non l'inverse ⁽¹⁰⁾. Le progrès technologique ne devrait

⁽¹⁾ https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf, Bureau du commissaire à l'information, «Guidance on political campaigning» [20170426].

⁽²⁾ En vertu de l'article 57, paragraphe 1, point d), «chaque autorité de contrôle, sur son territoire: [...] encourage la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du présent règlement».

⁽³⁾ Voir «Montrer l'exemple: La stratégie 2015-2019 du CEPD», p. 17. «Les mégadonnées renvoient» selon nous «à la pratique consistant à combiner d'énormes volumes d'informations émanant de sources diverses et à les analyser, en utilisant le plus souvent des algorithmes d'autoapprentissage pour éclairer la prise de décisions. L'une des valeurs les plus importantes des mégadonnées pour les entreprises et les gouvernements découle de la surveillance des comportements humains, aux niveaux collectif et individuel, et réside dans leur potentiel prédictif», avis n° 4/2015 du CEPD, «Vers une nouvelle éthique numérique: données, dignité et technologie», 11.9.2015, p. 6.

⁽⁴⁾ Les profils utilisés pour prédire le comportement des personnes font peser un risque de stigmatisation, de renforcement des stéréotypes existants, de ségrégation sociale et d'exclusion, et cette «intelligence collective» nuit au choix individuel et à l'égalité des chances. Ces «bulles de filtrage» ou «chambres d'écho personnelles» pourraient finir par étouffer la créativité, l'innovation et les libertés d'expression et d'association qui ont précisément permis aux technologies numériques de prospérer, avis n° 4/2015 du CEPD, p. 13 (références omises).

⁽⁵⁾ Avis n° 7/2015 du CEPD, «Relever les défis des données massives», p. 9.

⁽⁶⁾ Rapport du groupe consultatif sur l'éthique du CEPD, janvier 2018, p. 28.

⁽⁷⁾ Voir, par exemple, The Economist, «How the World Was Trolled», 4-10.11.2017, vol. 425, n° 9065, p. 21-24.

⁽⁸⁾ Allcott, H. et Gentzkow, M., «Social Media and Fake News in the 2016 Election», *Journal of Economic Perspectives*, vol. 31, n° 2, Stanford University, 2017, p. 211-236. <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>, p. 219.

⁽⁹⁾ Dans l'une des expériences, il a été dit à des utilisateurs de plateformes sociales comment leurs amis disaient avoir voté, ce qui a entraîné une augmentation significative d'un point de vue statistique du nombre de personnes qui ont voté au sein d'un segment de la population (0,14 % de la population en âge de voter, c'est-à-dire environ 340 000 électeurs) lors des élections du Congrès à mi-mandat en 2010; Allcott, H. et Gentzkow, M., «Social Media and Fake News in the 2016 Election», *Journal of Economic Perspectives*, vol. 31, n° 2, Stanford University, 2017, p. 211-236. Dans une autre étude, les chercheurs ont affirmé que des différences dans les résultats de recherche Google étaient en mesure de modifier de 20 % les préférences électorales des électeurs qui n'avaient pas fait leur choix; Zuiderveen Borgesius, F., Trilling, D., Möller, J., Bodó, B., de Vreese, C., Helberger, N., «Should we worry about filter bubbles?», *Internet Policy Review*, vol. 5, n° 1, DOI: 10.14763/2016.1.401, p. 9.

⁽¹⁰⁾ Considérant 4 du 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, ci-après le «RGPD».

pas être ralenti mais plutôt dirigé selon nos valeurs. Il est crucial de respecter les droits fondamentaux, y compris le droit à la protection des données, afin de garantir l'impartialité des élections, notamment en vue des élections au Parlement européen de 2019 ⁽¹⁾. Cet avis est le dernier en date d'une série de larges engagements du CEPD sur la question de savoir comment appliquer la protection des données afin de répondre aux inquiétudes les plus urgentes en matière de politique publique. Il s'appuie sur les précédents travaux du CEPD sur les mégadonnées et sur l'éthique numérique et sur la nécessité de coordonner la réglementation de marchés compétitifs et équitables ⁽²⁾. L'avis résumera tout d'abord le processus selon lequel les données à caractère personnel alimentent et déterminent le cycle prédominant de surveillance, de microciblage et de manipulation numériques. Les rôles des divers acteurs de l'écosystème de l'information numérique y seront ensuite abordés. Les droits fondamentaux en jeu, les principes de protection des données pertinents ainsi que d'autres obligations juridiques pertinentes seront évoqués. Pour conclure, il sera suggéré que le problème de la manipulation en ligne ne fera probablement que s'aggraver, qu'aucune approche réglementaire ne suffira à elle seule, et que les organismes de régulation doivent dès lors collaborer de toute urgence afin de lutter non seulement contre les abus localisés, mais également contre les distorsions structurelles créées par une concentration excessive du marché.

7. CONCLUSION

La manipulation en ligne représente une menace pour la société car les bulles de filtrage et les communautés en vase clos compliquent la compréhension et le partage d'expériences entre les personnes. L'affaiblissement de ce « ciment social » peut saper la démocratie ainsi que plusieurs autres droits et libertés fondamentaux. La manipulation en ligne est également un symptôme de l'opacité et du manque de responsabilité au sein de l'écosystème numérique. Il s'agit d'un problème réel et urgent, et la situation est susceptible d'empirer en raison de l'augmentation du nombre de personnes et d'objets connectés à l'internet et de l'importance croissante des systèmes d'intelligence artificielle. L'utilisation irresponsable, illicite ou contraire à l'éthique d'informations personnelles est en partie à l'origine du problème. La transparence est nécessaire mais n'est pas suffisante. La gestion de contenu est peut-être nécessaire mais ne saurait compromettre les droits fondamentaux. Un des aspects de la solution est ainsi de faire rigoureusement respecter les règles en vigueur, en particulier le RGPD, en les associant à d'autres normes relatives aux élections et au pluralisme des médias.

Afin de faire avancer le débat, au printemps 2019, le CEPD organisera un atelier lors duquel les organismes de régulation nationaux dans les domaines de la protection des données, du droit électoral et du droit audiovisuel pourront explorer ces interactions plus avant, discuter des défis auxquels ils sont confrontés et envisager des perspectives d'actions conjointes, en tenant également compte des prochaines élections parlementaires européennes.

Il a été affirmé dans le présent avis que la technologie et le comportement sur le marché sont néfastes en raison de déséquilibres et de distorsions structurels. Nous avons demandé l'ajustement des incitations à innover. Les géants et les pionniers de la technologie ont jusqu'à présent profité de l'absence relative de réglementation dans l'environnement dans lequel ils sont actifs. Les industries traditionnelles et les concepts de base de juridiction territoriale, de souveraineté, mais également les normes sociales, y compris la démocratie, sont affectés. Ces valeurs dépendent d'une pluralité de voix et d'un équilibre entre les parties. Aucun acteur ou secteur n'est à même de s'y attaquer seul. La protection des données est un élément de la solution et joue peut-être un plus grand rôle que nous ne l'avions imaginé. Dépendre de la bonne volonté d'acteurs commerciaux qui ne rendent finalement pas de comptes ne suffit pas. Nous devons à présent intervenir afin que les bénéfices de la numérisation soient plus équitablement répartis.

Bruxelles, le 19 mars 2018.

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

⁽¹⁾ Comme affirmé par la Cour européenne des droits de l'homme dans l'affaire *Orlovskaya Iskra c. Russie*, «des élections libres et la liberté d'expression, notamment la liberté du débat politique, constituent l'assise de tout régime démocratique. [...] Les deux droits sont interdépendants et se renforcent l'un l'autre: par exemple, la liberté d'expression est l'une des "conditions" nécessaires pour assurer "la libre expression de l'opinion du peuple sur le choix du corps législatif". C'est pourquoi il est particulièrement important, en période préélectorale, de permettre aux opinions et aux informations de tous ordres de circuler librement. Dans le contexte des débats électoraux, l'exercice sans entrave de la liberté d'expression des candidats revêt une importance particulière» (références omises dans le texte), point 110. <http://hudoc.echr.coe.int/eng?i=001-171525>

⁽²⁾ Avis préliminaire «Compétitivité à l'ère de la collecte de données massives», 2014; avis n° 4/2015 «Vers une nouvelle éthique numérique: données, dignité et technologie», 2015; avis n° 7/2015 «Relever les défis des données massives. Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes», 2016; avis 8/2016, «Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*)», 2016.