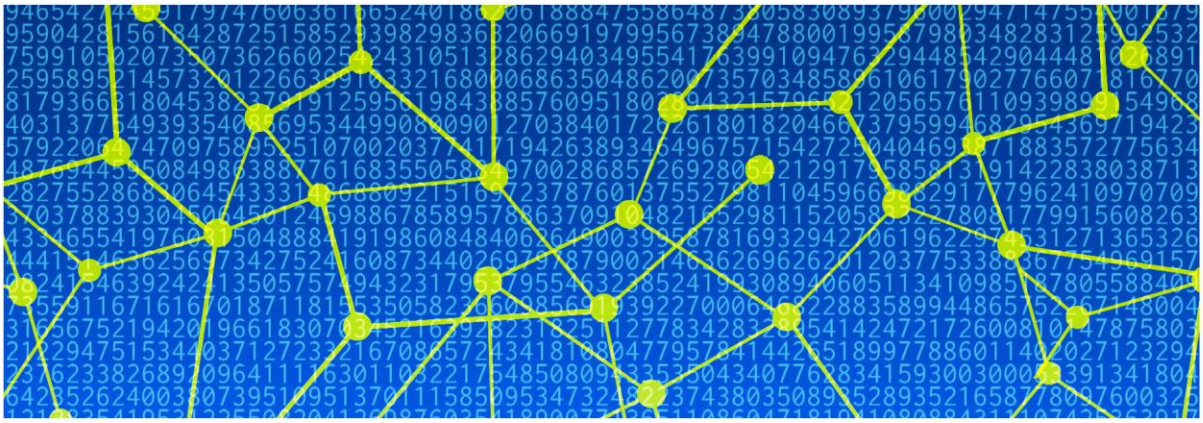

EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 3/2018

Avis du CEPD

sur la manipulation en ligne et les données à caractère personnel

EDPS

19 mars 2018

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel […]», de consulter le CEPD.

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

Synthèse

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.

TABLE DES MATIÈRES

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 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»[2]. 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[3].

- 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[4].

- 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[5].

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 tienne compte des différences dans l'organisation des systèmes politiques nationaux[6].

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[7]. 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[8]. 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[9]. 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»[10].

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[11]. En raison de ce phénomène, les fausses informations et les théories conspirationnistes ont un plus grand pouvoir de persuasion et sont toujours plus répandues[12]. 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[13].

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[14]. Le progrès technologique ne devrait 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[15]. 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[16]. 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.

2. Comment les données à caractère personnel sont utilisées pour déterminer l'expérience en ligne

«*Infonomics*» (économie de l'information) est un terme inventé à la fin des années 90 lorsque les entreprises ont commencé à s'intéresser à la valeur et à la monétisation des données[17]. Aujourd'hui, une visite sur un seul site internet implique généralement de dévoiler son comportement de navigation à plus de 100 tierces parties qui cherchent à limiter leur propre responsabilité juridique en recourant à des «politiques de confidentialité» denses qui peuvent compter jusqu'à plusieurs centaines de pages. L'internet décentralisé qui existait auparavant a fait place à des «communautés» cloisonnées gardées par quelques mastodontes des technologies qui exigent de leurs utilisateurs qu'ils révèlent leur identité et leurs données à caractère personnel. Les membres de ces communautés sont poussés à y demeurer et le contenu proposé par une tierce partie est uniquement accessible au sein de ce cadre[18]. L'analyse de données est utilisée pour interpréter de grands ensembles de données afin de permettre aux entreprises et aux gouvernements de comprendre et d'influencer plus efficacement le comportement des personnes en ce qui concerne leurs achats et leur utilisation des services publics. Même si certaines techniques sont appliquées à des fins d'agrégation et d'anonymisation, l'analyse des données repose sur le traitement des données à caractère personnel[19].

La manipulation en ligne peut être comprise comme le point culminant d'un cycle en trois étapes, de la collecte de données (une forme de traitement de données au titre du droit de l'Union), en passant par le profilage jusqu'au microciblage ou à la personnalisation comme une forme de manipulation dont le degré peut varier d'insignifiant à gravement préjudiciable[20]. Ces étapes font l'objet d'une courte description ci-dessous.

i. Collecte de données

La collecte de données est une forme de traitement de données au titre du droit de l'Union européenne[21]. Les données à caractère personnel sont collectées à partir d'une variété de sources en utilisant différentes techniques de fusion d'ensembles de données. Certaines données sont fournies par les personnes en toute connaissance de cause, par exemple lorsqu'elles remplissent un formulaire en ligne. En revanche, la plupart des données sont automatiquement observées ou enregistrées, décrites comme des «miettes de pain numériques» laissées sans le savoir, conséquence des activités en ligne et hors ligne des personnes[22]. Parmi ces données observées figurent les heures et les lieux de connexion d'un appareil mobile à une antenne de téléphonique mobile ou à un satellite GPS, les adresses IP des terminaux, les points d'accès WiFi, les historiques de recherches, les mention «j'aime» et «partager», les images collectées par les systèmes numériques de vidéosurveillance, les historiques d'achats, la participation aux réseaux sociaux et le comportement de navigation sur tous les appareils[23]. Selon une étude récente, lorsqu'ils cliquent sur «j'aime» et «partager», les gens sont bien plus susceptibles de diffuser des informations jugées «fausses» que des informations vérifiées. Les

ordinateurs zombies (bots) et les trolls, y compris ceux qui agissent au nom d'États tiers hostiles, participent à cette diffusion[24]. Les données collectées auprès des personnes qui remplissent des tests psychologiques en ligne représentent une importante catégorie. Ces tests deviennent souvent très rapidement populaires lorsqu'ils sont consultés et partagés sur les médias sociaux. Lorsque les résultats d'un participant sont combinés aux données personnelles disponibles sur les médias sociaux, ils permettent d'effectuer des prédictions élaborées quant à la personnalité[25].

Les entreprises utilisent des technologies de traçage afin de collecter les données observées, typiquement des cookies ainsi que des «flash cookies», des pixels invisibles, des captures d'empreintes numériques qui permettent de tracer sur plusieurs appareils[26]. Parallèlement, la prolifération des objets connectés et des dispositifs d'écoute installés au domicile comme les enceintes intelligentes (dont le marché est également déjà caractérisé par la concentration) offre de nouvelles possibilités d'observer en temps réel les comportements les plus privés des personnes[27]. Lorsque les messages et le contenu destinés à un individu à partir du profilage suscitent une réaction dudit individu, cette réaction est à son tour surveillée, ce qui génère des données supplémentaires à collecter et à utiliser afin de préciser le profil et les prochains ciblages.

ii. Profilage

Les données à caractère personnel collectées sont étudiées afin de catégoriser des personnes selon des profils précis. Il existe une kyrielle de caractéristiques qui peuvent être mesurées et utilisées afin de déduire les préférences de l'utilisateur à partir d'un profil utilisateur, telles que l'âge, le genre, la localisation, etc.[28]. D'après des estimations, le principal fournisseur de médias sociaux aurait utilisé plus de 52 000 attributs personnels afin de classer les intérêts et les caractéristiques des utilisateurs. Des méthodes statistiques sont ensuite utilisées afin de produire des informations analytiques ou de prédire des comportements ou développements futurs[29]. Le profilage automatisé repère des motifs que l'œil humain ne peut pas déceler par lui-même[30]. Plus les données disponibles sur une personne sont nombreuses et plus le profilage d'un utilisateur s'étend dans le temps, plus les déductions découlant du profil de la personne sont complètes[31]. Des pratiques de profilage plus avancées permettent de noter ou d'évaluer les gens par rapport à des points de référence sur des types de comportements normaux prédéfinis. Un exemple de ces applications est un logiciel de recrutement qui analyse la voix du candidat de manière à évaluer «la maîtrise de la langue, la fluidité, l'esprit critique et l'écoute active»[32]. Autre exemple: la manière de taper sur un clavier d'ordinateur sert de base pour prédire la confiance, la nervosité, la tristesse et la fatigue d'une personne. Une fonction particulière d'une telle déduction est qu'il est possible de prédire l'état émotionnel d'une personne, une donnée extrêmement sensible, à partir d'informations qui ne sont a priori pas sensibles, comme la façon dont elle tape sur un clavier[33].

Combinées aux sciences du comportement, les mégadonnées permettent d'effectuer des déductions sur des traits de personnalité encore plus profonds. Certaines sociétés d'analyse de données se spécialisent dans l'évaluation de personnes sur la base de cinq traits de personnalité, appelés les «Big Five» ou modèle OCEAN, en utilisant les données collectées à partir de tests de personnalité en ligne (voir ci-dessus), une technique qui aurait été exploitée par des militants durant l'élection présidentielle de 2016 aux États-Unis et le référendum sur la sortie du Royaume-Uni de l'Union européenne[34]. Ces évaluations sont ensuite complétées par des caractéristiques supplémentaires, y compris les valeurs et besoins, les mentions «j'aime» et les partages[35]. Le profilage sert également à identifier d'autres personnes qui pourraient

éventuellement être intéressées par un produit et par un service, à savoir le public et les clients analogues détenus par les grandes plateformes de médias sociaux[36].

La qualité des nouvelles connaissances générées à la suite du profilage fait débat. Selon certaines études, grâce aux techniques d'exploration des données, il est possible de prédire la personnalité d'une personne avec une plus grande précision que la plupart de ses amis et famille en sont capables[37]. D'après d'autres études, le profilage est situationnel et, par nature, probabiliste[38]. Dans tous les cas, les conséquences du profilage sur la vie d'une personne ne sont pas négligeables étant donné que les connaissances générées sont ensuite utilisées pour prendre des décisions (automatisées ou non) vis-à-vis d'une personne ou d'un groupe de personnes.

iii. Microciblage et manipulation

Les décisions basées sur le profilage personnalisent l'environnement informatif d'un individu avec un niveau élevé de personnalisation, une pratique appelée microciblage[39]. Elle peut consister en un message plus personnel adressé à un segment de personnes qui partagent certains traits voire potentiellement déterminer les prix de produits ou de services. Le microciblage peut passer par la façon dont les plateformes de médias sociaux choisissent quel contenu apparaît sur le fil d'actualités d'une personne et dans quel ordre.

Les sociétés qui vendent des espaces publicitaires numériques profitent du placement de contenu ciblé en dépit de toute considération éthique: rien ne différencie un bon clic d'un mauvais de la part d'un groupe démographique ciblé[40]. Les conséquences de ces activités de microciblage sont peut-être minimes sur certaines personnes, mais la complexité de la technologie à l'œuvre, les faibles niveaux de confiance et les intentions affichées de plusieurs grands acteurs de la technologie indiquent l'existence d'une culture de la manipulation dans l'environnement en ligne[41]. Cette manipulation peut résulter de stratégies commerciales adoptées par les acteurs du marché eux-mêmes ou d'actions de personnes et d'États qui cherchent à utiliser les plateformes comme intermédiaires pour bouleverser les marchés et la parole publique ou leur nuire.

En outre, la conception de dispositifs et de logiciels est pensée pour susciter un comportement addictif. Des fonctionnalités comme la lecture automatique, des fils d'actualités sans fin, les notifications et les «streak» (échange ininterrompu de messages ou d'images) sont, selon un certain nombre d'anciens employés de l'industrie de la technologie, autant de tentatives délibérées de maximiser l'attention au moyen du microciblage visant les utilisateurs, notamment les enfants, ce qui rappelle les techniques utilisées par l'industrie des jeux d'argent[42]. Les services basés sur l'internet qui ont obtenu des effets de réseau font explicitement appel à la peur de rater quelque chose (*fear of missing out*) ressentie par les gens s'ils ne se rendent pas régulièrement sur l'application[43].

La manipulation se manifeste également par la présentation de contenu microciblé et géré, présenté comme étant le plus «pertinent» pour la personne, mais choisi dans l'objectif de maximiser les revenus de la plateforme. Cela ressemble aux «menus secrets» utilisés pour piloter les utilisateurs des sites de commerce électronique et les «*dark patterns*» utilisés pour les dissuader de prendre des décisions moins souhaitables du point de vue de la plateforme (comme le refus d'ajouter des objets supplémentaires, comme une assurance, à un panier d'achat).

En 2017, les grandes plateformes ont admis qu'aux États-Unis, plus de 125 millions de personnes avaient été en contact avec du contenu «clivant», des publicités et des messages de

la part de faux comptes. D'après d'autres rapports publiés juste avant le présent avis, le nombre de personnes concernées par cette intrusion serait beaucoup plus élevé, même si les effets précis sur le comportement de vote réel demeurent inconnus[44]. Cependant, l'effet dissuasif sur la liberté d'expression qui découle de la surveillance constante qui caractérise l'écosystème numérique peut constituer une forme de manipulation plus importante et chronique[45].

3. L'écosystème numérique de la (dés)information

La manipulation et les fausses informations sont aussi vieilles que l'humanité mais sont devenues des questions de la plus haute importance sur les plans social, juridique et éthique en raison de la numérisation rapide. On espérait et on s'attendait à ce que l'augmentation du nombre de personnes connectées à l'internet fasse naître de nouvelles formes d'engagement civique, grâce à des campagnes en ligne, à la production participative et à des communautés engagées sur les médias sociaux[46]. Toutefois, aujourd'hui, la durabilité du microciblage fait l'objet de débats enflammés[47].

La manipulation par microciblage présuppose l'existence de bases de données comportant divers points d'information sur les personnes et l'accès à ces bases ainsi que des solutions en matière de propriété intellectuelles sous la forme d'algorithmes analytiques qui peuvent effectuer des inférences et des prédictions à propos des personnes qui utilisent ces données. Il s'agit d'un processus qui comprend plusieurs couches dans lequel deux groupes d'acteurs interagissent:

- L'écosystème de la publicité qui repose sur la collecte et sur l'analyse de données à caractère personnel comme modèle d'entreprise le plus répandu.
- Les annonceurs non commerciaux.

Un troisième grand acteur fait son apparition: l'intelligence artificielle, ce qui brouille encore plus les lignes de la responsabilité. En raison de la complexité et de l'étendue de cet écosystème numérique, composé d'entreprises et d'organisations qui, par le passé, étaient peut-être réglementées par différents domaines du droit (droit des consommateurs, droits électoral, droit des médias, droit de la concurrence, etc.), il est plus difficile d'attribuer des responsabilités juridiques à chacune d'entre elles, de faire respecter les règles en vigueur et de garantir que les personnes ont accès à un recours effectif en cas de violations.

i. Les intermédiaires de plateforme au cœur de la publicité numérique

Un nombre très restreint de sociétés gigantesques se sont imposées comme les gardiennes effectives du contenu numérique consommé par la plupart des gens. Elles occupent une position dominante parmi un ensemble d'autres acteurs, y compris les entreprises publicitaires, les courtiers en données et les sociétés d'analyse de données. Lors de la consultation publique sur l'initiative citoyenne européenne de 2015, plus de 7 personnes interrogées sur 10 (72 %) ont déclaré utiliser des plateformes internet comme source d'information. En Europe aujourd'hui, plus d'un tiers des dépenses publicitaires est consacré aux canaux numériques, dépassant les publicités télévisuelles (même si les différences entre les régions sont significatives). Au Royaume-Uni, l'un des marchés numériques les plus avancés, plus de 50 % de chaque livre sterling dépensée dans la publicité sont destinés aux canaux en ligne[48]. Les journaux (63 %) et la télévision (62 %) étaient respectivement les deuxième et troisième sources d'information les plus prisés en ce qui concerne les questions européennes[49]. La plupart du trafic de la recherche a migré vers les téléphones intelligents, où la plus grande entreprise détient 97 % des parts du marché. Les annonceurs qui utilisent l'une des deux principales

plateformes, décrites comme détenant un «duopole», car elles représenteraient entre 80 % et 99 % de l'ensemble de la croissance des recettes provenant de la publicité numérique, ne peuvent pas contrôler l'emplacement de leur publicité. Ces publicités ont été placées sur des sites au contenu raciste, incendiaire ou mensonger par des algorithmes opaques, ce qui a poussé de nombreux grands annonceurs à se retirer des marchés publicitaires programmatiques où l'achat et la vente de publicités se fait par l'intermédiaire de logiciels[50]. Dans de nombreux pays, l'une des deux plus grandes sociétés de technologie est devenue le point d'accès unique à l'internet[51]. Les investissements de capitaux dans les jeunes entreprises sont moins élevés (diminution de 40 % depuis 2015), ce qui indique que les investisseurs estiment que le marché concentré est moins susceptible d'être bouleversé[52].

Les analyses de données pourraient aider les personnes à s'y retrouver dans un environnement informationnel de plus en plus bruyant. Cependant, en réalité, l'équilibre des avantages a été perturbé au détriment des personnes, renforçant ainsi l'asymétrie informationnelle en faveur des détenteurs d'algorithmes propriétaires. En limitant l'exposition à certaines informations, par exemple aux offres d'emploi, en fonction du genre ou de l'état de santé présumé d'une personne, ils peuvent continuer à reproduire des attitudes et des pratiques discriminatoires[53]. En effet, le forum public de discussion et l'espace disponible pour la liberté d'expression sont dorénavant limités par la quête du profit de puissantes sociétés privées qui, en raison d'une complexité technique ou au motif du secret des affaires, refusent d'expliquer comment les décisions sont prises. Les quelques principales plateformes, grâce à leur extraordinaire portée, sont ainsi une cible facile pour les personnes cherchant à utiliser le système à des fins malveillantes.

ii. Les annonceurs non commerciaux

Les annonceurs ne sont pas uniquement des acteurs commerciaux cherchant à obtenir des informations sur les clients[54]. Les gouvernements, les mouvements politiques et idéologiques, les partis politiques, les campagnes, les candidats politiques et autres organisations engagées ont toujours cherché à diffuser leur message, à mobiliser des bénévoles, à recruter des donateurs et, par ailleurs, à influencer l'opinion publique et à constituer des communautés en ligne et hors ligne. Ils sont appelés «annonceurs non commerciaux», étant donné que leur objectif n'est pas de vendre ni de promouvoir un produit ou un service commercial, mais plutôt de faire passer leur message de manière à influencer les opinions politiques, sociales ou autres des personnes et de les inciter à soutenir une cause ou à voter lors d'une élection, ou de les en dissuader[5556].

Il y a peu encore, les annonceurs non commerciaux n'avaient accès qu'à des données limitées sur leur groupe cible. Ils ont à présent commencé à exploiter le même système d'annonces ciblées sur l'internet que celui utilisé par les entités commerciales en explorant en temps réel les réactions et les discussions sur les réseaux sociaux et à agréger des données ainsi qu'à en extraire de la «valeur», comme des déductions sur les traits de personnalité et sur le comportement de vote probable de l'électorat. Bon nombre d'institutions gouvernementales, de groupes politiques et d'autres groupes d'intérêt ont des sites web spécifiques qui, dans une plus ou moins grande mesure, utilisent les technologies de traçage susmentionnées. Ils sont également actifs sur les médias sociaux et ont recours à des outils de ciblage (publicitaires) proposés par les entreprises en ligne[57]. Les annonceurs non commerciaux interagissent avec les plateformes de médias sociaux, comme les «pages fan» ou les «groupes» sur les médias sociaux qui offrent des outils publicitaires et éditoriaux intégrés. Les administrateurs de pages fan peuvent avoir accès aux statistiques d'audience et choisir des publics parmi les personnes abonnées à la page et parmi tous les utilisateurs de la plateforme en fonction de facteurs

démographiques, d'intérêts, du comportement ou d'autres critères afin de mieux personnaliser les messages sur la plateforme. Ils peuvent dès lors personnaliser les messages qui sont ensuite présentés aux publics en fonction du profil et de la localisation[58]. La façon d'utiliser ces outils diffère selon les pays et les types d'organisation[59]. La limite entre «commercial» et «politique» est dans tous les cas floue: tandis que les recherches politiques traditionnelles se penchaient sur l'enregistrement des électeurs et l'affiliation à un parti, aujourd'hui, les analystes de données traitent toute information qui révèle des traits de personnalité.

Les campagnes politiques reposent de plus en plus sur les analyses de mégadonnées pour influencer l'opinion et les votes au moyen de messages ciblés ou d'impressions de publicités en ligne. Dans de nombreux cas, le but présumé est de cibler les gens avec des informations trompeuses[60]. La capacité de l'intelligence artificielle et des mégadonnées d'avoir une influence significative sur les processus démocratiques, évidemment en dehors des États-Unis, est contestée. Certaines preuves empiriques disponibles issues des pratiques observées dans les campagnes politiques aux Pays-Bas et en Allemagne montrent un faible recours aux pratiques de microciblage en raison de limites pratiques, y compris un manque d'expertise, de fonds, les spécificités de la juridiction locale ou le cadre juridique lui-même[61]. En revanche, dans le cadre de l'enquête en cours menée par la commissaire britannique à l'information, ainsi que de l'enquête menée en parallèle par la commission électorale sur les violations présumées de la protection des données lors de la campagne relative au référendum sur le Brexit, les activités de 30 organisations sont surveillées, y compris des partis et des campagnes politiques, des sociétés de données et des plateformes de médias sociaux[62]. Quelle que soit leur efficacité, les annonceurs non commerciaux manifestent un intérêt évident vis-à-vis de l'exploration des techniques de ciblage initialement développées pour le secteur commercial[63].

iii. Intelligence artificielle

Dans cet écosystème numérique, la communication entre les personnes, les entreprises et les États a de plus en plus lieu par l'intermédiaire de systèmes automatisés, lesquels produisent du nouveau contenu généré par des machines. L'intelligence artificielle est utilisée pour exercer une surveillance étroite, pour contrôler, filtrer et censurer les messages que s'envoient les utilisateurs d'applications de messagerie[64]. Les algorithmes d'apprentissage automatique visent à maximiser l'attention et les mentions «j'aime», ce qui expose les médias à la manipulation[65]. Les ordinateurs zombie (*bots*) sur les médias sociaux qui déforment les informations ou exacerbent la colère ou la dissension peuvent être autonomes ou contrôlés par des humains[66]. Il est probable que le nombre d'applications plus sophistiquées de l'intelligence artificielle, comme les «deepfake», les synthétiseurs vocaux et les bulletins d'informations automatisés, augmente en même temps que sa puissance dans cet écosystème alors qu'elles deviennent moins chères à déployer, à moins que l'on ne réussisse à déployer des contremesures. La personnalisation automatique des messages qui prévaut déjà dans l'espace commercial pourrait, si elle est appliquée dans la sphère politique, en théorie inclure l'adaptation du contenu de la page internet d'un candidat ou d'un parti politique selon les préférences politiques connues des visiteurs. Cette personnalisation pourrait également entraver les recherches de qualité et les initiatives de responsabilisation visant à suivre dans quelle mesure les candidats politiques tiennent leurs promesses une fois élus[67].

L'intelligence artificielle est modulable et ces tendances sont dès lors potentiellement sans limite. La relation entre la technologie et la politique est symbiotique: l'accès à la technologie et l'aptitude à l'utiliser déterminent les rapports de force entre les États et entre les régimes et les mouvements de protestation[68].

4. Valeurs et droits fondamentaux en jeu

La microciblage et la manipulation en ligne semblent mettre considérablement en péril un certain nombre de droits et de libertés inscrits dans la charte des droits fondamentaux de l'Union européenne (ci-après, la «charte»).

i. Protection des données et autres libertés

La vie privée et la protection des données à caractère personnel sont des droits fondamentaux au titre des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. L'article 7 protège le droit au respect de la vie privée et familiale, du domicile et des communications, tandis que l'article 8 établit un droit distinct de protection des données à caractère personnel. Ces deux droits sont soumis à une pression évidente car les informations personnelles sont indispensables à l'écosystème de l'information numérique.

La vie privée et la protection des données à caractère personnel font partie des «libertés» de l'Union européenne, qui comprennent la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information et la liberté de réunion et d'association (articles 10, 11 et 12). Elles sont également clairement en jeu en raison de la capacité des grands intermédiaires de plateforme soit de faciliter, soit d'entraver la diffusion de l'information. Par exemple, un contenu qui est mal indexé ou classé par un moteur de recherche en ligne est moins susceptible de toucher un grand public, voire d'être vu. Autrement, un algorithme de recherche peut également présenter un biais vis-à-vis de certains types de contenu ou de fournisseurs de contenu, risquant ainsi d'affecter les valeurs afférentes telles que le pluralisme et la diversité des médias. C'est particulièrement vrai en ce qui concerne les moteurs de recherche en ligne prétendument dominants[69].

ii. Pluralisme des médias

L'article 11 de la charte dispose qu'il est obligatoire de respecter la liberté et le pluralisme des médias. Dans une résolution de décembre 2017, le Parlement européen fait référence à 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». Le comité d'experts du Conseil de l'Europe prépare également une recommandation sur le pluralisme des médias et sur la transparence de leur propriété.

Certaines preuves montrent que cette concentration et élimination du journalisme local facilite la propagation de la désinformation[70]. Les médias sociaux ont été utilisés pour encourager les gens à voter, à voter pour un candidat particulier et pour les décourager de se rendre aux urnes («cuisine électorale — *gerrymandering* numérique»). Le plus grand fournisseur de média social a lui-même encouragé les électeurs à exercer leur droit de vote et rien ne l'empêche de faire l'inverse. Par rapport à la couverture d'un reportage par les médias traditionnels, il n'existe aucune trace de décision éditoriale, seuls les résultats d'un filtrage opéré par un algorithme subsistent. En théorie, les intermédiaires en ligne pourraient permettre à un parti politique dont les intérêts commerciaux ou idéologiques se rejoignent de toucher plus facilement leurs sympathisants ou vice-versa. D'anciens employés de médias sociaux ont récemment affirmé avoir dû empêcher des questions conservatrices d'être en tête des tendances sur le site[71]. La question est moins de savoir si les plateformes en ligne prétendument dominantes font (délibérément ou non) usage de leur pouvoir pour influencer les votes que le

fait qu'elles ont, en principe, la capacité d'influer sur les processus de prise de décision politiques[72].

Les règles de concurrence de l'Union européenne permettent aux États membres d'intervenir au titre de l'article 21, paragraphe 4, du règlement sur les concentrations, afin de protéger la pluralité des médias. Certains ont appelé de leurs vœux une redéfinition de ces règles à la lumière des bouleversements causés par les intermédiaires de plateforme et par la concentration du marché.

iii. Élections libres

En outre, 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[73]. Dans le contexte de l'Union européenne, l'article 39 de la charte garantit le droit de voter aux élections parlementaires européennes. De manière générale, des élections sont libres lorsque les candidats peuvent se présenter sans que les autorités ne leur mettent des bâtons dans les roues et que l'électorat dispose de vraies options et a librement accès aux informations sur ces options. Une intervention de l'État dont découle une inégalité des chances entre les candidats lors de la campagne électorale peut nuire à l'impartialité des élections. Le principe de transparence électorale n'est pas respecté si 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[74]. Dès lors, ces droits sont également remis en cause par la manipulation en ligne.

5. Cadres juridiques applicables

La complexité de l'écosystème de l'information numérique invoque une variété de secteurs réglementaires qui ont jusqu'à présent eu peu de raisons d'interagir. Cette section met en relief la pertinence des droits fondamentaux avant de présenter les secteurs de réglementation pertinents au titre du droit de l'Union européenne, à savoir la protection des données, le principe du pluralisme des médias, l'audiovisuel.

i. Règles et principes de protection des données

Dans l'Union européenne, les règles de protection des données ont été élaborées en ce qu'elles participent au respect de tous les droits et libertés fondamentaux, et pas uniquement de la protection des données[75]. Des règles spécifiques qui régissent le traitement des données à caractère personnel sont énoncées dans le règlement (UE) 2016/679 (le «RGPD») qui remplace la directive 95/46/CE à partir du 25 mai 2018[76]. Le RGPD exige que tout traitement de données à caractère personnel, de toute information liée à une personne physique identifiée ou identifiable, respecte les principes de traitement des données, y compris la licéité, la loyauté et la transparence, la limitation de la finalité, la minimisation des données et autres. Les données à caractère personnel qui révèlent des opinions politiques sont considérées comme une «catégorie particulière de données à caractère personnel» qui méritent un niveau de protection plus élevé. Le traitement desdites données est généralement interdit à moins qu'une ou plusieurs des dérogations énumérées ne s'applique[77]. Une personne morale, y compris des partis politiques et des organisations de la société civile, ou une personne physique, comme un candidat politique indépendant, qui traite des données à caractère personnel dans le cadre de son activité professionnelle est contrainte de respecter le RGPD.

Le RGPD est précisé et complété par la directive 2002/58/CE (directive «vie privée et communications électroniques»), qui fait actuellement l'objet d'une révision. Ladite directive établit des règles spécifiques afin de protéger la confidentialité et la sécurité des communications électroniques, y compris des garanties contre les violations de la vie privée par des communications non sollicitées effectuées à des fins de prospection directe. La notion de «prospection directe» n'est pas définie dans la directive, même si d'aucuns avancent qu'elle s'appliquerait à la demande de financement ou de soutien en faveur d'une cause politique, au fait d'encourager les personnes à voter ou à ne pas voter pour un parti politique ou pour un candidat, de demander des donations par courrier électronique, sur les réseaux sociaux ou par d'autres moyens de communication électronique[78]. Depuis 2009, la directive «vie privée et communications électroniques» exige que toute partie qui stocke ou obtient des informations, comme les témoins permanents (*tracking cookies*), sur l'appareil d'une personne, obtienne le consentement de cette dernière, sauf en cas d'exception[79].

Champ d'application

Le RGPD s'applique tout d'abord aux responsables du traitement et aux sous-traitants établis dans l'Union européenne[80] et aux responsables du traitement et aux sous-traitants établis à l'extérieur de l'Union s'ils offrent des biens et des services à des personnes dans l'Union ou surveillent leur comportement au sein de l'Union[81]. Tandis que les institutions gouvernementales, les mouvements politiques ou engagés qui sont actifs dans les États membres de l'Union sont couramment établis sur leur territoire, les entreprises numériques qu'ils emploient peuvent être enregistrées soit sur le territoire des États membres de l'Union, soit dans les pays tiers. Certaines sociétés peuvent avoir des succursales et des filiales dans l'Union, d'autres peuvent ne pas avoir d'accords stables dans l'Union. Par exemple, selon certaines études, certaines campagnes basées dans l'Union s'appuient sur les informations fournies par des sociétés d'analyse de données qui ne sont pas basées dans l'Union, lesquelles se spécialisent dans le profilage des personnes afin de prédire leurs préférences personnelles et leur comportement politique[82]. De telles activités seraient considérées comme étant un suivi du comportement de ces personnes aux fins du RGPD. Cela signifie que les sociétés d'analyse de données établies en dehors de l'Union et effectuant le profilage de personnes au sein de l'Union seraient soumises au RGPD et obligées de se conformer aux règles en matière de loyauté (y compris une base juridique adéquate pour le traitement), de transparence du traitement, de profilage et autres obligations. Le RGPD serait également souvent appliqué aux sociétés effectuant le profilage de personnes physiques qui résident en dehors de l'Union, si elles ont des succursales, des filiales ou autres établissements sur le territoire de l'Union. À cette fin, la citoyenneté ou la résidence des personnes profilées n'est pas pertinente. Le RGPD peut dès lors potentiellement étendre la protection juridique, comme le droit à l'information, l'accès aux données à caractère personnel et le droit de rectification aux personnes dans les pays tiers[83].

Responsables du traitement et responsabilité

Au vu de la multiplicité d'acteurs et d'activités associés à l'écosystème de l'information numérique, il peut être difficile d'identifier tous les responsables du traitement et tous les sous-traitants et de garantir que la responsabilité soit correctement attribuée au titre du RGPD[84]. Ainsi, lorsqu'un annonceur non commercial sous-traite l'analyse de mégadonnées à d'autres sociétés, il convient d'envisager soigneusement la question du contrôle du traitement de données à caractère personnel, ce qui aura des répercussions en matière de conformité et de responsabilité en vertu du RGPD. Si l'externalisation des mégadonnées a lieu au sein d'une relation responsable-sous-traitant dans laquelle l'annonceur non commercial fixe les finalités et les moyens du traitement, et que l'entreprise d'analyse de données traite exclusivement les

données en son nom, alors le RGPD exige qu'un contrat ou un autre acte juridique réglemente leur relation[85]. Cependant, l'existence d'un tel contrat ne signifierait pas automatiquement que l'entreprise qui analyse les données soit réellement un sous-traitant. Il est probable qu'une entreprise soit un sous-traitant, par exemple, dans la mesure où elle effectue des analyses de données au nom d'un parti politique aux fins d'une élection spécifique, tandis que le parti politique est susceptible d'être le responsable en ce qu'il détermine la finalité du traitement. Plus la société est libre de décider quelles données collecter et comment appliquer ses techniques d'analyse, plus il est possible qu'une société soit considérée comme un responsable conjoint du traitement[86].

La relation entre la plateforme et les organisations qui emploient ses services fait l'objet d'un recours juridictionnel qui est actuellement pendant devant la Cour de justice de l'Union européenne (CJUE)[87]. Dans ses conclusions, l'avocat général estime que la plateforme et le créateur d'une page fan devraient tous deux être considérés comme responsables du traitement[88]. D'après ces conclusions, tout parti politique, candidat ou mouvement idéologique qui est présent sur le réseau social du fait d'une page fan «a la possibilité d'influer sur la mise en œuvre concrète d'un outil [publicitaire]» en utilisant des filtres afin de définir une audience personnalisée et de désigner les catégories de personnes qui vont faire l'objet d'une collecte de leurs données à caractère personnel par la société de média social. Une telle société aurait ainsi toutes les responsabilités du responsable du traitement au titre du RGPD, y compris l'obligation de déterminer un fondement juridique pour le traitement, d'informer les personnes que leurs données sont traitées et de prouver sa conformité au RGPD[89].

Limitation de la finalité

Le principe de limitation de la finalité requiert que la finalité de la collecte d'informations personnelles soit spécifiée au moment de ladite collecte. Les informations ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Chaque changement de finalité doit être spécifié[90].

Les analyses de données comprennent des méthodes et des schémas d'utilisation que ni l'entité qui collecte les données ni la personne concernée ont envisagé ou auraient pu imaginer au moment de la collecte. Le traitement algorithmique des données à caractère personnel permet de générer de nouvelles données. Lorsque la personne concernée partage quelques données discrètes, il est souvent possible que ces données soient fusionnées, ce qui génère une deuxième, voire une troisième, génération de données sur cette personne[91].

Par exemple, des informations limitées sur les sympathisants d'un parti politique contenues dans ses bases de données ou des informations de base sur les membres d'une organisation, fournies par ces derniers pourraient être fusionnées avec des données sur le comportement d'achat d'une personne obtenues auprès de courtiers en données[92]. En utilisant des outils fournis par les plateformes de médias sociaux, ces données peuvent être combinées en fonction des informations démographiques (par ex. données sur la situation familiale) et des informations sur le comportement et les intérêts individuels. En appliquant les méthodes d'analyse de données susmentionnées, la campagne politique ou l'organisation basée sur l'adhésion intéressée peut déduire des profils psychologiques ou des préférences politiques détaillées à propos de personnes à partir d'ensembles de données qui, à première vue, ne sont pas liés et ne sont pas sensibles.

L'inquiétude que suscite l'utilisation, au moyen d'algorithmes, de données issues de profils pour d'autres finalités est de voir ces données perdre leur contexte original. Le fait de donner

une nouvelle finalité aux données affectera probablement l'autonomie informationnelle de chacun, continuera de diminuer le contrôle exercé par les personnes concernées sur leurs données, mettant ainsi à mal la confiance envers les environnements et les services numériques[9394]. D'où l'importance cruciale de la limitation de la finalité comme principe de la législation relative à la protection des données.

Ainsi, le traitement légitime effectué par des annonceurs non commerciaux ainsi que par des parties à l'écosystème publicitaire exigerait tout d'abord d'établir un fondement juridique pour le traitement, comme le consentement de la personne concernée. L'obtention du consentement explicite serait essentiel au traitement de toutes informations sensibles qui révèlent des opinions politiques ou religieuses, et le consentement ne serait pas valide s'il devenait une condition pour utiliser le service.

Ils devraient informer les personnes concernées des futures formes de traitement dans lesquelles qu'ils appliqueraient et surveiller leurs pratiques de près afin de garantir qu'ils n'ont pas dépassé les limites autorisées du traitement dans le cadre des finalités énoncées[95].

ii. Règles relatives aux médias audiovisuels

La directive de l'Union européenne «Services de médias audiovisuels» est en cours de révision. Elle couvre la coordination à l'échelle de l'Union des législations nationales relatives à tous les médias audiovisuels, c'est-à-dire à la fois les émissions de télévision traditionnelles et les services à la demande. Un des objectifs de la révision est notamment de traiter les «discours de haine» et de garantir le pluralisme des médias. Dans le même temps, dans l'Union, la publicité politique à la télévision est habituellement réglementée et les radiodiffuseurs publics sont soumis à des exigences en matière d'impartialité. Il n'existe toutefois pas de réglementation équivalente pour l'utilisation des prédictions algorithmiques des préférences et du comportement de vote dont l'incidence peut être toute aussi grande, si ce n'est supérieure[96]. Par conséquent, d'aucuns ont plusieurs fois demandé l'application des normes traditionnelles relatives à la responsabilité des médias aux plateformes de médias sociaux. Étant donné que les plateformes choisissent quelles informations présenter à qui, elles jouent le rôle de journalistes responsables des sujets tendance. La question se pose donc de savoir si les plateformes de médias sociaux, au travers de leurs algorithmes qui classent et présentent des propositions de tierces parties, exercent une forme de contrôle éditorial traditionnellement opéré par les professionnels des médias et endossent dès lors des responsabilités particulières des médias[97].

Pendant longtemps, les radiodiffuseurs étaient obligés de faire preuve de retenue en publiant les résultats des sondages d'opinion et de faire respecter des périodes de calme avant le jour des élections (silence électoral). Dans certains cas, la réglementation de la publicité politique s'étendait au rationnement du temps dont disposaient les partis sur les radiodiffuseurs publics afin que les grands et les petits partis politiques et candidats bénéficient de conditions politiques équitables[98]. Cependant, le passage à la «télévision fragmentée numérique», où les campagnes politiques ont de plus en plus lieu en ligne, avec l'utilisation des outils d'analyse et de microciblage susmentionnés, soulève des interrogations sur l'application des règles de radiodiffusion aux grandes plateformes et pousse les autorités audiovisuelles et médiatiques à comprendre comment elles fonctionnent.

iii. Réglementations électorales

Dans les États membres de l'Union, les réglementations nationales en matière de campagne imposent des obligations de divulgation des donations et/ou des dépenses des candidats lors des campagnes électorales[99]. Même si ces règles s'appliquent autant aux campagnes en ligne que hors ligne (traditionnelles), lesdites règles deviennent plus difficiles à appliquer car les partis dépendent des services de publicité numérique tiers et des outils de médias sociaux. Par exemple, les dépenses en matériaux de campagne déclarées ne donnent peut-être pas suffisamment de détails sur les dépenses en publicité numérique et services associés, par exemple des publicités ciblées sur les médias sociaux, des services d'analyse, la création de bases de données d'électeurs, la collaboration avec des courtiers en données. Ces messages diffusés en ligne, y compris sur les réseaux sociaux, incluent rarement une adresse bibliographique mentionnant qui les a publiés, ôtant ainsi aux électeurs la possibilité d'identifier qui dépense de l'argent afin d'essayer de les influencer lors des élections[100]. Un manque de transparence de ces pratiques peut avoir des conséquences négatives sur la loyauté et sur la liberté du processus décisionnel.

iv. Protection des consommateurs

Au titre de la charte des droits fondamentaux de l'Union européenne, les consommateurs ont le droit de bénéficier d'un haut niveau de protection des consommateurs. Jusqu'à présent, deux principes distincts sous-tendent le droit de la consommation européen: mettre les consommateurs en situation d'être des acteurs souverains du marché, leur donner les droits et les informations nécessaires pour agir en tant que tels, et protéger les consommateurs dans les situations où ils sont la partie la plus faible dans des négociations commerciales et où ils ne sont pas en mesure de protéger eux-mêmes leurs droits, leurs intérêts (économiques) et leur sécurité[101].

L'Union européenne a dûment adopté diverses mesures de protection des utilisateurs de produits et de services, quel que soit l'endroit où ils sont fournis ou consommés dans le marché intérieur[102]. L'un de ces instruments, la directive sur les pratiques commerciales déloyales, interdit les pratiques commerciales trompeuses, agressives ou autrement déloyales[103][104][105]. De telles pratique sont illégales dans le cadre des pratiques commerciales des entreprises vis-à-vis des consommateurs. Le ciblage et la publicité politiques et idéologiques ne relèvent pas du champ d'application du droit de la consommation. Cependant, les activités qui reviennent à manipuler des personnes au moyen d'informations trompeuses, à personnaliser des arguments politiques en fonction de profils personnels intrusifs présentent des similarités évidentes avec les abus traités dans le droit de la consommation[106]. Le droit international sur les droits de l'homme tend à établir une distinction entre les destinataires du ciblage politique et les destinataires du ciblage commercial[107]. Toutefois, comme indiqué dans la résolution susmentionnée sur l'utilisation de données personnelles pour la communication politique, «bien que la communication politique présente parfois un caractère promotionnel - certaines particularités le distinguent du marketing commercial»[108].

v. Droit de la concurrence

Dans notre avis préliminaire sur «Vie privée et compétitivité à l'ère de la collecte de données massives» de 2014, puis dans notre avis 8/2016 sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*), nous avons affirmé que le droit de la concurrence jouait un rôle crucial en ce qu'il garantit la responsabilité des acteurs dominants du marché et protège la démocratie contre un pouvoir excessif du marché. Certains éléments

prouvent que la concentration a fourni une cible facile aux opérateurs malintentionnés au sein de l'«écosystème» qui maintient le microciblage. Les intérêts des personnes devraient être mieux reflétés lors de l'évaluation d'éventuels abus de position dominante ou de fusions de sociétés qui ont peut-être concentré un pouvoir considérable en matière d'informations[109]. Par exemple, en décembre 2017, l'autorité allemande de concurrence (Bundeskartellamt) a publié une évaluation juridique préliminaire dans le cadre des poursuites pour abus de position dominante contre Facebook. Elle a estimé que Facebook abusait de sa position dominante car l'utilisation de son réseau social était subordonnée au fait que Facebook soit autorisé à amasser sans limite toutes sortes de données générées en utilisant des sites web tiers et en les fusionnant avec le compte Facebook de l'utilisateur[110]. Étant donné que le microciblage peut dépendre des données à caractère personnel collectées par ce réseau de média social, les conclusions de l'office fédéral de lutte contre les cartels (autorité allemande de concurrence) sont donc aussi pertinentes dans le contexte du présent avis.

Les motifs d'intervention au titre de la protection des données, de la protection des consommateurs et du droit de la concurrence afin de gérer d'éventuelles conséquences négatives du microciblage pour les droits fondamentaux des personnes ont fait l'objet d'un débat entre les organismes de régulation respectifs lors de la deuxième réunion de la Digital Clearinghouse[111]. Il a été décidé de continuer de l'envisager comme un domaine de collaboration éventuel entre les organismes de régulation, y compris les autorités électorales et des médias. Le CEPD continuera de coordonner cet effort en tenant également compte des travaux en cours effectués par la Commission européenne[112], et par les autorités nationales de régulation[113].

6. Recommandations

La manipulation en ligne est un problème complexe et il n'existe aucune solution simple. Aucun domaine de réglementation n'est à même de s'y attaquer seul. Dans le présent avis, nous avons toutefois avancé que la protection des données devait constituer un aspect non négligeable de la solution. Nous émettons ci-après cinq recommandations d'action issues de la législation relative à la protection des données auxquelles les autorités indépendantes compétentes en matière de protection de données peuvent apporter une précieuse contribution, en commençant par achever la réforme du cadre de protection des données et par le faire strictement respecter, faire en sorte que les organismes de régulation parviennent à une compréhension collective de la question, s'appuyer sur les mesures existantes aux niveaux national et européen pour coopérer avec d'autres organismes de régulation, l'autorégulation et une plus grande autonomisation individuelle.

I. Achever et exécuter les règles de protection des données

Il est crucial de consolider la protection de catégories particulières de données, les principes de transparence, de limitation de la finalité et de minimisation des données, et les garanties contre le profilage illicite et les prises de décision automatisées.

Le cadre européen relatif à la vie privée et à la protection des données serait incomplet sans un instrument juridique destiné à protéger le droit à la vie privée garanti par l'article 7 de la charte des droits fondamentaux. La proposition de règlement «vie privée et communications électroniques» a le potentiel pour cesser d'inciter la manipulation et le traçage permanents des personnes.

À cette fin, nous avons déjà conseillé au législateur d'inclure les ajouts suivants à la proposition de règlement[114]:

- une interdiction totale et explicite de l'accès subordonné à l'acceptation du traçage («*tracking walls*»);
- une interdiction explicite de la pratique consistant à exclure les utilisateurs qui disposent d'applications permettant de bloquer les publicités ou autres et de modules d'extension installés pour protéger leurs informations et leurs équipements terminaux;
- une confirmation que le traitement des données aux fins de la fourniture de publicités ciblées ne peut être considéré comme nécessaire à l'exécution d'un service; et
- une obligation que les navigateurs et autres logiciels ou systèmes d'exploitation proposent des contrôles par défaut qui facilitent l'accord ou le refus du suivi.

Le CEPD continuera d'apporter son soutien au Parlement européen et au Conseil afin de garantir une finalisation rapide de la nouvelle législation et d'encourager la création d'une ligne de référence durable en ce qui concerne le respect de la vie privée et la protection des données[115]. Nous estimons qu'ainsi, l'Union européenne favorisera l'apparition de nouveaux modèles d'entreprise et de technologies et d'entreprises plus respectueuses de la vie privée, ce qui participerait à lutter contre les risques que représente l'écosystème sous-jacent du microciblage.

II. Les organismes de régulation devraient chercher un diagnostic collectif du problème

Les analyses de données offrent des possibilités sans précédent: profiler des personnes afin de noter, classer, évaluer leur comportement et prendre des décisions en toute connaissance de cause à leur propos. Elles personnalisent les expériences et l'exposition aux informations des personnes afin d'influencer leur comportement et leurs choix, que ce soit leurs décisions d'achat en tant que consommateurs ou en tant que citoyens engagés dans la vie civique[116]. L'enjeu est d'exploiter la technologie de manière à aider les personnes à s'associer plus librement et plus efficacement aux prises de décisions civiques, de gérer les risques d'une manipulation indue et de remettre en cause l'idée d'une personne comme un soi quantifié[117].

Les autorités de protection de données et tous les organismes de régulation concernés doivent comprendre les pratiques locales en matière de microciblage, y compris dans quelle mesure les mouvements politiques et idéologiques pratiquent le profilage et le ciblage de personnes, sur quelles sources de données à caractère personnel ils s'appuient et quels outils ils utilisent pour les profiler et les cibler. Même s'il est possible de repérer certaines tendances mondiales et régionales, il est nécessaire que les autorités procèdent à des enquêtes par pays en raison de la diversité des cadres institutionnels et des conditions sociales et juridiques[118]. De nombreux efforts ont déjà été déployés au niveau national et la Commission est à la tête de travaux visant à trouver des solutions[119]. Les organismes de régulation peuvent étudier les lignes directrices existantes émises par les autorités de protection des données sur les campagnes électorales et leur champ d'application afin de les étendre à d'autres mouvements sociaux et idéologiques qui pratiquent le profilage et le ciblage des personnes au moyen de messages non commerciaux. Il est en particulier crucial de comprendre la différence entre la notion d'intérêt public au titre de la législation relative à la protection des données et celle des intérêts privés des entreprises ou des mouvements politiques afin de lutter contre les violations et contre la manipulation dans

l'espace politique en ligne. Les organismes de régulation devraient travailler ensemble pour aller plus loin sur cette question.

III. Les organismes de régulation devraient coopérer entre secteurs

Les réponses actuelles aux fausses nouvelles («*fake news*») doivent être encouragées par une plus grande coopération interagence[120].

Premièrement, l'antitrust (règles en matière d'entente) et la vie privée convergent alors que les autorités se rendent compte qu'une grande partie des abus structurels découle de distorsions sur un marché numérique victime de superconcentration. Lesdites règles ont un rôle primordial à jouer en ce qu'elles surveillent le comportement des sociétés dominantes et utilisent le contrôle des opérations de concentration pour éviter les effets néfastes à plus long terme des concentrations.

Deuxièmement, la coopération entre les organismes de régulation de la protection des données et les organismes de régulation de la protection des consommateurs pourrait permettre d'enquêter sur l'écosystème sous-jacent qui facilite le microciblage politique, à savoir les services en ligne fournis par l'industrie de la publicité, les courtiers en données, les sociétés d'analyse de données et les plateformes de médias sociaux[121]. Au titre du droit de la protection des consommateurs, ils peuvent être à la fois «commerçants» à part entière[122] et fournisseurs de services de profilage et de ciblage à des tierces parties. Les autorités de protection des données et celles de protection des consommateurs peuvent dès lors réfléchir à des normes en matière de transparence et d'inéligibilité des termes contractuels, et notamment des services en ligne, qui exigent une plus grande transparence de la part des sociétés quant à leur prise de décision dans les opérations de traitement des données[123].

Les synergies pourraient également se pencher sur le potentiel aspect persuasif du ciblage comportemental en étudiant la «loyauté» de certaines fonctions desdits services en ligne[124], qui visent avant tout à persuader les clients de fournir davantage d'informations personnelles afin d'obtenir des données de profilage plus précises, et présentent des capacités de ciblage plus nuancé, faisant ainsi augmenter la valeur du service auprès des annonceurs (commerciaux et politiques).

Troisièmement, la coopération avec les réglementations électorales est devenue cardinale. Les règles relatives à la protection des données et à la vie privée et aux communications électroniques qui couvrent les activités politiques et l'intérêt public comportent des exemptions. Les organismes de régulation doivent travailler main dans la main afin de garantir que la manipulation ne puisse pas passer entre les mailles du filet réglementaire. Comme indiqué dans la résolution sur l'utilisation de données personnelles pour la communication politique, «les Commissaires à la protection des données et à la vie privée pourraient jouer un rôle croissant dans la planification des actions coordonnées, notamment en coopération avec d'autres autorités de surveillance compétentes dans les domaines des télécommunications, de l'information, des sondages d'opinion et des activités électorales»[125]. En effet, la législation relative à la protection des données, le droit électoral et le droit de l'audiovisuel ont des principes communs, tels que la transparence et la loyauté, et la coopération entre les organismes de régulation respectifs, notamment en période électorale, pourrait rendre leur application plus cohérente et renforcer la protection des personnes contre d'éventuelles pratiques de microciblage déloyales.

Selon un projet de recherche de l'Union européenne conduit en 2013, il existe un manque de coordination entre les organismes de régulation de la protection des données sur la question du traitement de données aux fins des efforts de campagne électorale[126]. Mis à part une exception notable[127] concernant l'application de la législation relative à la protection des données et à l'audiovisuel au cours des campagnes électorales, il semble qu'il n'existe pas de coopération active entre différents domaines de réglementation, c'est-à-dire entre les autorités compétentes en matière de protection des données, les autorités électorales et celles des médias à l'échelle nationale ou européenne. Cependant, dans le contexte des campagnes électorales, les organismes de régulation dans les trois domaines juridiques (protection des données, élections et médias) semblent rencontrer des difficultés lorsqu'il s'agit d'appliquer les principes communs de «transparence» et de «loyauté» aux nouvelles réalités des campagnes électorales qui englobent le traçage, le profilage et le ciblage des personnes en ligne. Les rapports présentés par les partis politiques dans lesquels ils détaillent leurs dépenses de campagne et les enquêtes des autorités électorales peuvent fournir de précieuses informations aux autorités de protection des données quant aux pratiques en matière de collecte et de traitement de données utilisées par les campagnes électorales (avec ou sans l'aide de tiers). Cela peut continuer d'alimenter l'évaluation de leur respect des exigences du RGPD, y compris la responsabilité, la licéité, la transparence et la loyauté du traitement des données. Les autorités de protection des données ont une connaissance approfondie du fonctionnement de l'écosystème publicitaire numérique qu'elles pourraient partager avec les autorités de l'audiovisuel de manière à les aider à appliquer les règles relatives à la publicité politique à l'environnement en ligne. Ce ne sont là que quelques exemple des éventuels avantages qui pourraient naître d'une coopération plus active entre les organismes de régulation.

Comme nous l'avons affirmé dans notre avis précédent, les autorités de régulation dans chaque domaine du droit sont dotées de compétences limitées et disposent dès lors d'un nombre limité d'outils. Par exemple, les autorités de protection des données peuvent uniquement aborder la licéité, la transparence et la loyauté du profilage et du ciblage dans la mesure où un traitement de données à caractère personnel entre en ligne de compte[128], il ne revient pas au droit relatif à la protection des données de réguler la loyauté et la véracité des messages personnalisés. Par conséquent et au vu des risques potentiels de voir le microciblage dépasser le cadre du droit à la protection des données pour s'étendre aux domaines des libertés d'expression et d'information, de l'égalité et des élections libres, il est nécessaire d'explorer les perspectives de coopération entre les organismes de régulation de la protection des données et les autres organismes de régulation.

IV. L'autorégulation et les codes de conduite devraient être encouragés

La manipulation en ligne est trop systémique, représente une trop grande menace pour les valeurs et les droits fondamentaux pour laisser le secteur industriel y remédier. Cependant, l'autorégulation a un rôle important à jouer.

Au titre du RGPD, les autorités nationales de contrôle, le comité européen de la protection des données, les États membres de l'Union européenne et la Commission doivent encourager l'élaboration de codes de conduite «destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises»[129]. Comme l'indique le groupe de travail «Article 29», l'adhésion à un code de conduite peut participer à démontrer une volonté de transparence. Les codes «peuvent être rédigés afin de spécifier l'application du RGPD en ce qui concerne le traitement loyal et transparent, les informations fournies au public et aux personnes concernées et la protection des enfants, entre autres questions»[130]. En outre, la

rédaction d'un code de conduite peut inciter les partis politiques, les campagnes électorales et autres associations engagées sur les plans social et politique à engager une discussion sur la dimension éthique du traitement des données, comme les décisions de certains responsables du traitement de ne pas recourir à certaines opérations de traitement des données[131].

V. Habiliter les personnes à exercer leurs droits, y compris l'action collective

Le cryptage, les applications et les extensions de navigateurs qui visent à mettre au jour le ciblage, ainsi que d'autres mesures de sécurité destinées à protéger les informations personnelles, sont des obstacles à la manipulation.

Les courtiers en données, les réseaux publicitaires, les fournisseurs de réseaux sociaux et d'autres acteurs économiques numériques détiennent des fichiers de plus en plus complets sur les personnes participant à la société numérique actuelle, et les citoyens perdent le contrôle des empreintes numériques qu'ils laissent derrière eux. Ciblées, profilées et évaluées par des acteurs souvent hors de leur portée ou dont elles ne soupçonnent même pas l'existence, les personnes peuvent se sentir démunies. Elles doivent être habilitées à prendre le contrôle de leur identité. Même lorsqu'elles ont officiellement reçu une forme ou l'autre de «notification» et qu'elles ont eu l'occasion de «consentir» aux conditions générales, les personnes se retrouvent souvent dans un système conçu pour maximiser la monétisation des données à caractère personnel, sans leur laisser vraiment ni le choix ni une possibilité de contrôle[132].

La transparence n'est qu'un élément de la solution, le raisonnement derrière le Honest Ads Act (loi sur les publicités honnêtes) bipartite, qui obligerait tout au plus les acheteurs de publicités politiques en ligne à révéler leur identité.

D'après diverses enquêtes, environ 75 % des consommateurs n'ont pas confiance dans la manière dont les marques de médias sociaux et les sociétés de prospection commerciale gèrent leurs données[133]. Moins de deux Européens sur 10 ont l'impression de totalement contrôler les informations qu'ils fournissent en ligne tandis qu'un tiers estime qu'il ne les contrôle absolument pas[134].

Nous avons déjà demandé aux entreprises numériques qui déploient d'importants efforts dans la recherche de solutions innovantes pour l'utilisation des données à caractère personnel de faire preuve du même esprit innovant dans la mise en œuvre de la législation relative à la protection des données[135]. Notre *avis de 2016 sur les systèmes de gestion des informations personnelles* étudiait le concept de technologies et d'écosystèmes visant à habiliter les personnes à contrôler le partage de leurs données à caractère personnel («systèmes de gestion des informations personnelles», ou «PIMS» en abrégé). Nous avons analysé le potentiel des PIMS pour permettre aux utilisateurs de contrôler leurs informations personnelles et suggéré à la Commission et aux États membres de prendre des mesures afin d'encourager la recherche et le développement et le déploiement sur le marché dans le domaine des PIMS.

Pour que les droits fondamentaux soient «pratiques et effectifs»[136], toutes garanties juridiques, technologiques et en matière de politique *ex ante* mises en place par les responsables du traitement et par les sous-traitants doivent être associées au droit *ex post* à un recours effectif dont bénéficient ceux dont les droits et les libertés ont été violés[137]. Étant donné que, dans l'ensemble, le microciblage repose sur des processus de prise de décision automatisés, il comporte des défis particuliers en ce qui concerne la capacité des personnes à obtenir un recours effectif. Ces défis englobent l'opacité de la décision elle-même, son fondement, la question de savoir si les personnes ont consenti à l'utilisation de leurs données dans la prise de décision, ou sont même conscientes de la décision qui les affecte[138]. Les personnes auront peut-

être des difficultés à accéder à leurs données à caractère personnel à cause d'obstacles d'ordre procédural[139] ou, en raison d'une asymétrie de l'information entre les responsable du traitement et les sous-traitants, à évaluer l'exhaustivité des informations qu'elles reçoivent à la suite de demandes d'accès. Étant donné qu'il est difficile de déterminer qui est responsable de la décision, les personnes éprouvent dès lors plus de difficultés à comprendre à qui adresser leur plainte[140]. En outre, il existe un certain nombre d'obstacles auxquels les personnes qui forment un recours en justice sont généralement confrontées[141].

À la lumière de ces obstacles et d'autres à l'exercice effectif des droits au titre du RGPD, le règlement, par rapport à la directive relative à la protection des données, envisage des manières supplémentaires d'exercer ce droit. En particulier, l'article 80 du RGPD prévoit le droit de la personne concernée de «mandater un organisme, une organisation ou une association à but non lucratif», dans certaines conditions, pour qu'il exerce certains droits en son nom, ainsi que la possibilité pour les États membres de prévoir que ces organisations puissent exercer des fonctions similaires, de leur propre initiative, indépendamment de tout mandat confié par une personne concernée. Même si l'introduction de ce droit devrait être reconnue comme une grande avancée[142], le CEPD recommande ce qui suit afin de garantir intégralement le droit à un recours effectif:

- aux législateurs de l'Union: ajouter une disposition explicite concernant les voies de recours collectives et les recours effectifs ou clarifier la formulation du règlement «vie privée et communications électroniques» (par exemple en confirmant explicitement l'applicabilité de l'article 80 du RGPD), afin de garantir le plein accès aux mécanismes de recours collectifs tels qu'ils sont prévus par le RGPD[143];

- aux États membres lorsqu'ils font usage de leur pouvoir d'appréciation en ce qui concerne l'application de l'article 80, paragraphe 2, du RGPD: prévoir dans leur législation nationale un droit d'ester en justice pour les entités, les organisations ou associations à but non lucratif d'intérêt public qui sont actives dans le domaine de la protection des droits et des libertés des personnes concernées afin d'introduire des réclamations devant l'autorité de contrôle et d'exercer les autres droits des personnes concernées mentionnés dans ledit article, indépendamment de tout mandat confiée par une personne concernée.

Le CEPD estime qu'une telle approche participerait à ce qu'en pratique, les droits des personnes concernées soient appliqués de manière plus cohérente et égale dans les différentes juridictions de l'Union. Cette question est particulièrement importante dans le contexte des pratiques de traitement de données sensibles telles que le profilage des personnes et les prises de décision automatisées qui peuvent avoir une incidence négative sur l'exercice des droits civiques de millions de personnes lorsqu'elles sont illicites, opaques ou déloyales. Par exemple, une violation de données dans une base de données d'électeurs qui conduit à la révélation de profils d'électeurs accompagnés d'informations sur leur personnalité et sur leur mode de vie et de leur profil psychologique peut être perçue comme une atteinte particulièrement grave au droit du respect de la vie privée. L'accès à un mécanisme «opt out» de recours collectif[144] pourrait permettre aux organisations d'intérêt public de traiter cette atteinte, même si les personnes, en raison des motifs susmentionnés, ne sont peut-être pas en position d'engager des procédures contre le responsable du traitement et/ou contre le sous-traitant[145].

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

NOTES

[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].

[2] 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].

[3] 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].

[4] https://www.cnil.fr/fr/communication-politique-quelles-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.

[5] 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].

[6] 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».

[7] 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 nº 4/2015 du CEPD, «Vers une nouvelle éthique numérique: données, dignité et technologie», 11.9.2015, p. 6.

[8] Les profils utilisés pour prédire le comportement des personnes font peser un risque de stigmatisation, de renforcement des stéréotypes existants, de ségrégation sociale et culturelle 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 nº 4/2015 du CEPD, p. 13 (références omises).

[9] Avis nº 7/2015 du CEPD, «Relever les défis des données massives», p. 9.

[10] Rapport du groupe consultatif sur l'éthique du CEPD, janvier 2018, p. 28.

[11] Voir, par exemple, The Economist, «How the World Was Trolled», 4-10.11.2017, vol. 425, nº 9065, p. 21-24.

[12] Allcott, H. et Gentzkow, M., «Social Media and Fake News in the 2016 Election», *Journal of Economic Perspectives*, vol. 31, nº 2, Stanford University, 2017, p. 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf, p. 219.

[13] 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, nº 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, nº 1, DOI: 10.14763/2016.1.401, p. 9.

[14] 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».

[15] 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.

[16] Avis préliminaire «Compétitivité à l'ère de la collecte de données massives», 2014; avis nº 4/2015 «Vers une nouvelle éthique numérique: données, dignité et technologie», 2015; avis nº 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.

[17] http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf, audition de la commission de l'énergie et du commerce de la Chambre des représentants des États-Unis intitulée «Algorithms: How Companies' Decisions About Data and Content Impact Consumers», 27.11.2017, p. 2.

[18] https://www.wsj.com/articles/its-time-to-bust-the-online-trusts-1509487518 (Cf. article NYC, article Yelp WSJ), Lowe, L., «It's Time to Bust the Online Trusts», *The Wall Street Journal*, 31.10.2017.

[19] Certaines données ainsi créées ne sont pas liées à des personnes. Il s'agit de données qui découlent d'activités telles que l'analyse des régimes météorologiques, l'exploration spatiale, les tests scientifiques de matériaux ou de conceptions ou les risques associés au négoce de titres sur les marchés financiers. Mais il s'agit en grande partie des données que nous générons nous-mêmes ou qui sont créées sur nous (Abrams, M., «Origins of Personal Data and its Implications for Governance», The Information Accountability Foundation, voir http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf).

[20] Sur la base du cadre proposé par https://biblio.ugent.be/publication/8541057. Pour en savoir plus, voir: https://www.maastrichtuniversity.nl/sites/default/files/mcel_master_working_paper_20172_mondschein_2.pdf.

[21] Article 4, paragraphe 2, du RGPD.

[22] Schwartz, E., «Finding our way with digital bread crumbs», *MIT Technology Review*, 18 août 2010; groupe de travail «article 29» sur la protection des données, «Lignes directrices relatives au droit à la portabilité des données», WP 242.

[23] Rapport du rapporteur spécial des Nations unies sur le droit à la vie privée du 19 octobre 2017, points 31-32; avis 2/2010 du groupe de travail «article 29» sur la publicité comportementale en ligne, p. 7, 10-11.

[24] Facebook a récemment révélé que pendant la campagne présidentielle de 2016, plus de 62 000 utilisateurs s'étaient engagés à assister à 129 événements organisés par des trolls russes, comme des rassemblements des groupes antagonistes Heart of Texas et United Muslims of America qui attiraient leurs publics respectifs au même endroit et au même moment; source. «Lorsque la nouvelle mensongère selon laquelle les résultats des élections auraient été falsifiés en Sicile a commencé à se répandre en ligne le jour de l'élection, des utilisateurs de Twitter ont retwitté des informations erronées environ 1 000 fois selon une analyse de EU DinsinfoLab. Mais sur Facebook, la même histoire a été partagée plus de 18 000 fois, et ce uniquement sur les pages Facebook publiques. Nous ne savons pas comment cette fausse information s'est propagée sur les pages privées des utilisateurs Facebook (et notamment qui a participé à sa diffusion)», **source.**

[25] Bisclegio, P., «The Dark Side of That Personality Quiz You Just Took», *The Atlantic*, 13.7.2017. https://www.theatlantic.com/technology/archive/2017/07/the-internet-is-one-big-personality-test/531861/.

[26] Avis du groupe de travail «article 29» sur la capture d'empreintes numériques. Pour un aperçu des différentes méthodes de traçage, voir Mondschein, C., «The Regulation of Targeted Behavioural Advertising in the European Union», mémoire de master, Maastricht Center for European Law, 2017/2. En 2017, une méthode permettant de suivre une personne sur plusieurs navigateurs sur le même appareil a été publiée; Nordrum, A., «Browser Fingerprinting Tech Works Across Different Browsers for the First Time», *IEEE Spectrum*, 24.2.2017 https://spectrum.ieee.org/tech-talk/telecom/internet/new-online-fingerprinting-technique-works-across-browsers [consulté le 18.3.2018].

[27] Helberger, N., «Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law», 2016, p. 3.

[28] Monschein, p. 9.

[29] Vermeulen, G., Lievens, E., éds., *Data protection and privacy under pressure: transatlantic tensions, EU surveillance, and big data*, Maklu, Antwerp, Apeldoorn, Portland, 2017, p. 316.

[30] Kaltheuner, F. et Bietti, E., «Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR», *IRP&P*, vol. 2, nº 2, 2017, p. 3. 3.

[31] Mondschein, p. 11.

[32] Kaltheuner et Bietti, p. 5.

[33] Kaltheuner et Bietti, p. 4.

[34] OCEAN est l'acronyme de Ouverture, Conscienciosité, Extraversion, Agréabilité, Neuroticisme. Voir par exemple Grassegger, H. et Krogerus, M., «The Data That Turned the World Upside Down», Stanford Public Policy Program, 28.1.2017; Polonski, P., «How artificial intelligence conquered democracy», 8.8.2017, http://theconversation.com/how-artificial-intelligence-conquered-democracy-77675 [consulté le 18.3.2018].

[35] Par ex. Mahmud, J., «Leveraging cognitive computing and social media data to generate deep constituent insights», IBM Watson Innovations, https://www-01.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/Jalal%20Mahmud%27s%20Presentation/$file/Jalal%20Mahmud%27s%20Presentation.pdf.

[36] Voir le rapport de la commission de l'énergie et du commerce de la Chambre des représentants des États-Unis, sous-commission sur la communication et les technologies et sous-commission sur le commerce numérique et la protection des consommateurs, audition intitulée «Algorithms: How Companies' Decisions About Data and Content Impact Consumers», 27.11.2017. Au moins une autorité de protection des données a émis des doutes sur la légalité de l'utilisation d'«audiences personnalisées» à partir de fichiers clients afin de créer des «audiences similaires» sans le consentement des personnes concernées; communiqué de presse de l'autorité bavaroise de protection des données (Bayerisches Landesamt für Datenschutzaufsicht), «Facebook Custom Audience bei bayerischen Unternehmen», 4.10.2017.

[37] L'efficacité de ces prédictions a été évaluée dans l'une des expériences effectuées par des chercheurs de Stanford. Ils ont découvert qu'en «exploitant les mention "j'aime" d'une personne sur Facebook, un ordinateur était en mesure de prédire la personnalité de quelqu'un avec davantage de précision que la plupart de ses amis et de sa famille. Seul(e) l'époux ou l'épouse d'une personne a presque réussi à obtenir le même résultat que l'ordinateur». Les prédictions de l'ordinateur étaient basées sur les articles, vidéos, artistes et autres éléments que la personne avait aimés sur Facebook. https://news.stanford.edu/2015/01/12/personality-computer-knows-011215/.

[38] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, «Data is power: «Towards additional guidance on profiling and automated decision-making in the GDPR», *Journal of Information Rights, Policy, and Practice*, vol. 2, nº 2, 2017, p. 9.

[39] Ce terme récent est de plus en plus utilisé pour faire référence à toutes les fois qu'un procédé d'échantillonnage est basé sur une segmentation détaillée de l'audience cible, la plupart du temps dans les publicités en ligne afin de créer des messages ou des offres personnalisés et d'évaluer correctement leur incidence. Dans un contexte politique, le terme a pour la première fois été utilisé dans le cadre d'activités de lobbying lors la campagne présidentielle aux États-Unis; Barbu, O., «Microtargeting in social media: definitions and ethical issues», Studia Universitatis Babes Bolyai Ephemerides, 2013, p. 83-90, 58. Le terme «microciblage politique» a été défini comme suit afin d'établir une différence avec le microciblage commercial: l'utilisation de différents moyens de communication (courriel, téléphone, porte-à-porte, courrier et publicité sur les médias sociaux, etc.) afin de communiquer et d'établir une relation avec les électeurs potentiels; Bodó, B. et Helberger, N. et de Vreese, C., «Political microtargeting: a Manchurian candidate or just a dark horse?», *Internet Policy Review*, vol. 6, nº 4, 2017. DOI: 10.14763/2017.4.776. Voir également Colin J. Bennett, «Voter databases, microtargeting, and data protection law: can political parties campaign in Europe as they do in North America?», *International Data Privacy Law*, vol. 6, nº 4, 2016, p. 261-275.

[40] Damian Tambini, cité dans Pennycook et Rand, *The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings*, 2017.

[41] Dans un article de 2012 intitulé «The art of manipulation», un brillant entrepreneur et conférencier dans le domaine de la technologie déclarait: «Nous construisons des produits destinés à persuader les gens de faire ce que nous voulons qu'ils fassent. Nous appelons ces personnes "utilisateurs" et même si on ne le dit pas tout haut, nous espérons secrètement que chacun d'entre eux devienne férocement accro»; https://techcrunch.com/2012/07/01/the-art-of-manipulation/ [consulté le 18.3.2017].

[42] Voir par exemple, Wu, T., *The Attention Merchants* (Les marchands d'attention), 2017; McNamee, R., «Why not regulate social media like tobacco or alcohol?», https://www.theguardian.com/media/2018/jan/29/social-media-tobacco-facebook-google [consulté le 18.3.2017]; https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/ [consulté le 18.3.2017].

[43] Voir par exemple https://www.psychologytoday.com/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo [consulté le 18.3.2017].

[44] Certains articles parus le 17.3.2018 révèlent que les données de 50 millions de profils Facebook auraient été obtenues et utilisées de manière abusive; Rosenberg, M., Confessore, N., Cadwalladr, C., «How Trump Consultants Exploited the Facebook Data of Millions», *New York Times*; Cadwalladr, C. et Graham-Harrison, E., «Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach», *The Guardian*.

[45] Voir par exemple le rapport de l'administration nationale des télécommunications et de l'information du Ministère américain du commerce, «Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities», 13.5.2016.

[46] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52016DC0288 Communication de la Commission du 25 mai 2016 intitulée «Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe» [SWD8(2016) 172 final].

[47] Parmi les exemples d'engagement figurent l'organisation et la participation à des campagnes ou à des pétitions sociales en ligne, la constitution de communautés engagées sur les médias sociaux, la participation en ligne des citoyens à l'attribution des budgets locaux, l'élaboration et l'évaluation de la législation, la production participative d'idées de politiques. Pour plus d'exemples, voir:

https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE253/RAND_PE253.pdf, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF373/RAND_CF373.pdf.

[48] Comité d'experts sur le pluralisme des médias et la transparence de leur propriété (MSI-MED), étude de faisabilité sur l'utilisation de l'internet dans le cadre des élections, MSI-MED (2016)10rev, 9 mars 2017, p. 8, https://rm.coe.int/16806fd666.

[49] http://ec.europa.eu/justice/citizen/document/files/2015_public_consultation_booklet_fr.pdf, p. 11.

[50] Voir par exemple, entretien de Digiday UK avec le PDG de Guardian Media le 19.12.2017; Financial Times, «Advertisers' challenge to Facebook and Google», 12.2.2018, https://www.ft.com/content/d43fd706-0fec-11e8-8cb6-b9ccc4c4dbbb.

[51] Global Voices AdVox a effectué une étude critique de cette initiative: «Free Basics in Real Life: Six case studies on Facebook's internet "On Ramp" initiative from Africa, Asia and Latin America», 27.7.2017.

[52] CNBC, «Seed funding slows in Silicon Valley», 1.8.2017; https://www.cnbc.com/2017/08/01/seed-funding-slows-in-silicon-valley.html [consulté le 18.3.2018].

.[53] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, p. 9. Certains universitaires font preuve de moins d'optimisme quant au potentiel de la communication personnalisée. Ils suggèrent que la publicité en ligne ciblée n'est pas parvenue à atteindre un taux de clics sur les publicités supérieur à 0,5 %. Il semble dès lors que «la technologie demeure insuffisante» pour avoir une influence substantielle sur le comportement d'une personne. https://policyreview.info/articles/analysis/should-we-worry-about-filter-bubbles, p. 10.

[54] Les informations obtenues grâce à l'analyse des mégadonnées peuvent être utilisées à diverses fins, y compris pour décider qui recruter, évaluer le risque de crédit (*credit scoring*), évaluer des demandes d'asile, détecter et suspendre des faux comptes sur les médias sociaux. Pour un aperçu, voir *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, p. 4-6.

[55] https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00035/544506-00035.pdf, The Progress & Freedom Foundation, «Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech»,7.12.2009; p. 18.

[56] Ibid., voir également https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, p. 3 et 5. Voir également des idées en matière d'application pratique des analyses de données et d'intelligence artificielle dans le domaine public: https://medium.com/@drpolonski/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first-7b1257cb4285.

[57] Voir par ex. p. 29, http://webbut.unitbv.ro/Bulletin/Series%20V/BULETIN%20I/03_Biea.pdf; p. 12, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.

[58] https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f Albright, J., «Cambridge Analytica: the Geotargeting and Emotional Data Mining Scripts», *Medium*, 13.10.2017.

[59] https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting Dobber, T., Trilling, D., Helberger, N., de Vreese, C. H., «Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques», *Internet Policy Review*, 31.12.2017.

[60] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, p. 3.

[61] https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, Woodley, S. C., et Howard, P. N., «Computational Propaganda Worldwide: Résumé, Université d'Oxford, p. 8.

[62] https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/, Denham, E., commissaire à l'information, «The Information Commissioner opens a formal investigation into the use of data analytics for political purposes», 17.5.2017 et «Update on ICO investigation into data analytics for political purposes», 13.12.2017, bureau de la commissaire à l'information.

[63] Les chercheurs dans le domaine du microciblage d'électeurs estiment que les campagnes fondées sur les données et que les techniques de microciblage qui y sont associées seront de plus en plus présentes dans le paysage politique européen. Voir par ex. https://academic.oup.com/idpl/article-abstract/6/4/261/2567747?redirectedFrom=fulltext, p. 262.

[64] Ng, J. Q., 2015, https://citizenlab.ca/2015/07/tracking-censorship-on-wechat-public-accounts-platform/

[65] Marwick et Lewis, 2017.

[66] Brundage, M. et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018, p. 45.

[67] Voir O'Neil, C., «Weapons of Math Destruction», 2016, p. 195.
[68] Brundage et al., p. 44.
[69] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 36, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea.
[70] Voir par ex., Moore, M., *Tech Giants and Civic Power*, Centre for the Study of Media, Communication and Power, Policy Institute, King's College London, 2016.
[71] Comité d'experts sur le pluralisme des médias et la transparence de leur propriété (MSI-MED), étude de faisabilité sur l'utilisation de l'internet dans le cadre des élections, MSI-MED (2016)10rev, 9 mars 2017, p. 13, https://rm.coe.int/16806fd666.
[72] Ibid.
[73] http://www.venice.coe.int/webforms/documents/?pdf=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» du 21.10.2010, étude nº 558/2009, p. 4.
[74]http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-%20The%20new%20political%20campaigning_final.pdf, Goodman, E., Labo, S., Moore, M., et Tambini, D., *The New Political Campaigning*, Media Policy Brief 19, Media Policy Project, London School of Economics and Political Science mars, 2017, p. 6.
[75] Considérant 2 du RGPD.
[76] L'analyse présentée dans le présent avis se fonde sur le RGPD.
[77] Article 9 du RGPD.
[78] La proposition de règlement «vie privée et communications électroniques» de la Commission énonce que les «messages que les partis politiques envoient à des personnes physiques, en recourant aux services de communications électroniques, afin d'assurer leur promotion» ainsi que «les messages envoyés par d'autres organisations à but non lucratif pour servir les objectifs de l'organisation» relèvent du champ d'application de la «prospection directe». Considérant 32 de la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), 10.1.2017, COM(2017) 10 final. Selon les orientations sur les campagnes politiques du bureau du commissaire britannique à l'information, la définition de prospection directe couvre également les activités de campagne politique.
[79] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:fr:PDF. Journal officiel de l'Union européenne L337/11, directive 2009/136/CE du 25 novembre 2009. Pour de plus amples informations sur les différentes implications de cette disposition, voir https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.
[80] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, considérant 22 de la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE, 2017/0003 (COD).
[81] Article 3, paragraphe 2.
[82] Voir par exemple http://www.telegraph.co.uk/news/2017/02/24/exclusive-tiny-canadian-company-helped-swing-brexit-vote-leave/; https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns.
[83] Pour un exemple d'une telle application, voir https://medium.com/personaldata-io/quick-guide-to-asking-cambridge-analytica-for-your-data-52f9e74bd059;
https://www.theguardian.com/technology/2017/oct/01/cambridge-analytica-big-data-facebook-trump-voters.
Lorsqu'on lui a demandé si Cambridge Analytica fournirait aux électeurs américains qui demanderaient l'ensemble des 5 000 points de données de leurs profil au titre du droit britannique relatif à la protection des données, le PDG Alexander Nix a répondu, à tort, que la loi ne s'appliquait pas aux Américains.
[84] Voir un problème similaire dans le cadre de la santé mobile: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_fr_0.pdf.
[85] Article 28, paragraphe 3, du RGPD.
[86] Orientations sur les mégadonnées de l'ICO, p. 5.
[87] Demande de décision préjudicielle présentée à la CJUE dans l'affaire C-210/16, http://curia.europa.eu/juris/document/document.jsf?text=&docid=181773&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1.
[88] Voir conclusions de l'avocat général dans l'affaire C-210/16, http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=FR.
[89] Voir conclusions de l'avocat général dans l'affaire C-210/16, point 57, http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=FR.

[90] Article 5, paragraphe 1, point b).
[91] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 32-33, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea.
[92] Par exemple, pour comprendre quelles informations les partis politiques détiennent sur les électeurs en Allemagne, consulter l'adresse: https://policyreview.info/articles/analysis/restrictions-data-driven-political-microtargeting-germany.
[93] «Incompatible: The GDPR in the Age of Big Data», (Incompatible: le RGPD à l'ère des mégadonnées), Setton Hall Law Review, vol. 47, nº 995, 2017, p. 1006-1007, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr
[94] Ibid., p. 34.
[95] Zarsky, T. Z., «Incompatible: The GDPR in the Age of Big Data», *Setton Hall Law Review*, vol. 47, nº 995, 2017, p. 1008-1009, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.
[96] Ibid., p. 47-48.
[97] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 40, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea.
[98] Comité d'experts sur le pluralisme des médias et la transparence de leur propriété (MSI-MED), étude de faisabilité sur l'utilisation de l'internet dans le cadre des élections, MSI-MED (2016)10rev, 9 mars 2017, p. 6, https://rm.coe.int/16806fd666.
[99] Goodman, E., Labo, S., Moore, M., et Tambini, D., *The New Political Campaigning*, Media Policy Brief 19, Media Policy Project, London School of Economics and Political Science, 2017, p. 9, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.
[100] Commission électorale britannique, «Political finance regulation at the June 2017 UK general election. Report on the UK Parliamentary General Election held on 8 June 2017», novembre 2017, p. 12-15, https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/237550/Political-finance-regulation-at-the-June-2017-UK-general-election-PDF.pdf.
[101] Helberger, N., Zuiderveen Borgesius, F. et Reyna, A., «The perfect match? A closer look at the relationship between EU consumer law and data protection law», *Common Market Law Review*, vol. 54, nº 5, 2017, p. 7, https://www.ivir.nl/publicaties/download/CMLR_2017.pdf.
[102] Avis préliminaire du CEPD, p. 23.
[103] Article 6, paragraphe 1.
[104] Cela pourrait violer l'article 6, paragraphe 1, point a) et l'annexe I nº 7 UCPD, p. 149 des politiques, stratégies et statistiques en matière de protection des consommateurs, https://ec.europa.eu/info/policies/consumers/consumer-protection_fr.
[105] En montrant de fausses mention «j'aime» aux consommateurs, un commerçant peut induire les consommateurs en erreur quant à sa propre réputation ou à la réputation de ses produits ou services, ce qui peut mener les consommateurs à prendre des décisions commerciales qu'ils n'auraient pas prises autrement. Article 6 de la directive, http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_fr.pdf, p. 144.
[106] Par exemple, «[s]elon des recherches récentes, la réussite sur les médias sociaux peut avoir un effet auto-renforçant. Chaque profil et post Facebook contient de nombreuses "informations sociales": chaque utilisateur peut immédiatement constater la réussite ou l'absence de réussite apparentes de certains posts et profils en regardant le nombre de partages, de mentions "j'aime" et d'abonnés que Facebook ne manque pas d'afficher. Un fort niveau d'interaction peut donc indiquer la grande importance et validité de certains messages. [...] De nombreuses personnalités publiques, en particulier les hommes et femmes politiques, comptent des centaines de milliers de faux abonnés sur Twitter. En revanche, Facebook compte moins de profils automatisés, mêmes si leur nombre s'élèverait tout de même à environ 65 millions (en mars 2017, Facebook avait fermé jusqu'à deux milliards de profils au total)», http://www.delorsinstitut.de/2015/wp-content/uploads/2017/04/20170419_SocialNetworksandPopulism-Dittrich.pdf.
[107] La Cour européenne des droits de l'homme a reconnu que les autorités nationales ont une plus large marge d'appréciation lorsqu'elles déterminent la nécessité et la proportionnalité d'une interférence avec la liberté d'expression commerciale [voir par ex. Markt intern Verlag GmbH et Klaus Beermann c. Allemagne, 20 novembre 1989; Krone Verlag GmbH & Co. KG c. Autriche (nº 3), 11 décembre 2003, point 31], alors que la liberté de débat politique mérite un niveau de protection plus élevé, et que seuls des motifs graves peuvent justifier l'interférence dans ce type de débat (voir par ex. Lingens c. Autriche, 8 juillet 1986).

[108] https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_fr.pdf, Garante per la Protezione dei Dati Personali, résolution sur l'utilisation de données personnelles pour la communication politique, voir préambule [doc. web n.1170616].

[109] Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*), p. 14.
[110] Communiqué de presse de l'autorité de concurrence: «Nous sommes principalement préoccupés par la collecte de données en dehors du réseau social de Facebook et par la fusion de ces données avec un compte d'utilisateur Facebook. Au moyen des interfaces de programmation (API), les données sont transmises à Facebook et collectées et traitées par Facebook, même lorsqu'un utilisateur de Facebook se rend sur d'autres sites web. Ce phénomène se produit également lorsque, par exemple, un utilisateur ne clique pas sur le bouton "j'aime" mais a consulté une page dans laquelle ce bouton est intégré. Les utilisateurs n'en ont pas conscience. Et au vu de l'état actuel des choses, nous ne sommes pas convaincus que les utilisateurs ont donné leur consentement effectif pour le traçage de données effectué par Facebook et pour la fusion de ces données avec leur compte Facebook. L'étendue et la forme de la collecte de données enfreint les principes européens obligatoires de protection des données.», https://webgate.ec.europa.eu/multisite/ecn-brief/en/content/germany-bundeskartellamt.
[111] https://edps.europa.eu/sites/edp/files/publication/17-11-30_statement_2nd_meeting_dch_en.pdf, deuxième réunion de la Digital Clearinghouse, Bruxelles, 27.11.2017.

[112] https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_fr, Commission européenne, «Consultation publique sur les fausses nouvelles et la désinformation en ligne», du 13.11.2017 au 23.02.2018.

[113] Par exemple https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.
[114] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_fr.pdf, Avis 6/2017, avis du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement «vie privée et communications électroniques»), p. 16-17.
[115] https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en, Contrôleur européen de la protection des données, «A crucial moment for communications privacy», 27.9.2017.

[116] Davantage d'informations sur les différentes pratiques de profilage: proposition de *Privacy International*, p. 4-6.
[117] https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_fr_0.pdf, CEPD, Avis 1/2015, «La santé mobile. *Concilier innovation technologique et protection des données*», point 32.
[118] https://policyreview.info/articles/analysis/restrictions-data-driven-political-micro-targeting-germany, Kruschinski, S., Haller, A., «Restrictions on data-driven political micro-targeting in Germany», *Internet Policy Review*, vol. 6, nº 4, 31.12.2017.

[119] Référence au rapport du groupe d'experts.
[120] Voir par exemple le rapport du groupe d'experts; pour un aperçu des stratégies, Caplan, R., Hanson, L., Donovan, J., «Dead Reckoning: Navigating Content Moderation after "fake news"», Data&Society, 2018; projet de loi d'Emmanuel Macron exigeant que les plateformes en ligne révèlent la présence d'informations sponsorisées; Royaume-Uni **; Allemagne **.
[121] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf, Common Market Law Review, Vol.54 (2017), Issue 5. «The perfect match? A closer look at the relationship between EU consumer law and data protection law», *Common Market Law Review*, vol. 54, nº 5, 2017, p. 28,
[122] http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf, p. 143. De même, conformément au droit de la protection des données, en fonction de l'activité de traitement des données en jeu, ils peuvent être responsables du traitement et sous-traitants.
[123] Avis préliminaire du CEPD, p. 35.
[124] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf Common Market Law Review, Vol.54 (2017), Issue 5. «The perfect match? A closer look at the relationship between EU consumer law and data protection law», *Common Market Law Review*, vol. 54, nº 5, 2017, p. 20-22,

[125] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/1170616 Garante per la Protezione dei Dati Personali, résolution sur l'utilisation de données personnelles pour la communication politique. [doc. web n. 1170546].

[126] http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II-Repository_CNIL_UJI_October-2016.pdf, Phaedra II «Guidance on political campaigning», octobre 2016, p. 2.
[127] https://www.cnil.fr/sites/default/files/atoms/files/guide_cnil_et_csa.pdf. CNIL, «Pluralisme dans les médias audiovisuels. Règles "Informatique et Libertés"». Plus récemment, l'ICO a également déclaré qu'il coopérait avec la commission électorale dans le cadre de l'enquête sur l'analyse de données à des fins politiques, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.

[128] Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*), p. 11.
[129] Ce pouvoir n'est pas limité au contrôleur mais s'étend aussi aux États membres, aux autorités de contrôle, au comité et à la Commission.
[130] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, groupe de travail «article 29», Guidelines on transparency under Regulation 2016/679 (Lignes directrices sur la transparence au titre du règlement 2016/679), p. 19.
[131] Issu de la recherche empirique sur le recours aux techniques de microciblage politique par les partis politiques néerlandais: Avis nº 7/2015 «Relever les défis des données massives». «D66 et le parti des seniors 50PLUS en particulier adoptent une position de principe contre la collecte de données et le recours au ciblage comportemental politique (PBT). Là où D66 se présente comme un champion de la vie privée et dès lors ne collectera ni n'utilisera jamais d'informations sur les électeurs (ou groupes d'électeurs), le chef de la campagne de 50PLUS met en garde contre le risque d'utilisation irresponsable des données collectées au moyen "de pratiques qui frisent le harcèlement", ce qu'il qualifie d'"irresponsables sur le plan moral"». (https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting).
[132] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf, avis 9/2016, avis du CEPD sur les systèmes de gestion des informations personnelles. Vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel, paragraphe 1.

[133] Communiqué de presse: European and Middle Eastern consumers deeply conflicted over piracy and security priorities, 17.5.2017.https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968.
[134] Commission européenne, Protection des données. Règles relatives à la protection des données à caractère personnel au sein et à l'extérieur de l'UE. https://ec.europa.eu/info/law/law-topic/data-protection_fr.
[135] Avis nº 7/2015 «Relever les défis des données massives», p. 29; ainsi que https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf, p. 14.
[136] Sur la doctrine «pratique et effectif», voir https://academic.oup.com/hrlr/article-abstract/5/1/57/606751, Mowbray, A., «The Creativity of the European Court of Human Rights», *Human Rights Law Review*, vol. 5, nº 1, 1.1.2015.

[137] Article 47, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne. La Cour de justice a inscrit le droit à un recours effectif dans son arrêt du 15 mai 1986 comme un principe général de la jurisprudence de l'Union (arrêt Johnston, C 222/84, Rec. 1986, p. 1651 ; voir également arrêt du 15 octobre 1987, Heylens, C 222/86, Rec. 1987, p. 4097, et arrêt du 3 décembre 1992, Borelli, C-97/91, Rec. 1992, p. I-6313).
[138] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 41-42, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea. Voir également l'avis du groupe de travail «article 29» sur le profilage et la prise de décision automatique, p. 5.
[139] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 41,42, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea.
[140] Comité d'experts sur les intermédiaires d'internet (MSI-NET), rapport de réunion du 6 octobre 2017, MSI-NET (2017)06, Annexe 4 «Projet final de l'étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires», p. 41-42, https://rm.coe.int/msi-net-4e-reunion-18-19-septembre-2017/168075f8ea.
[141] Direction générale des politiques internes, «Présentation générale des systèmes de recours collectif existant dans les États membres de l'Union européenne», voir par ex. p. 9, http://www.europarl.europa.eu/RegData/etudes/note/join/2011/464433/IPOL-IMCO_NT(2011)464433(SUM01)_FR.pdf.

[142] Lors de l'élaboration du RGPD, le CEPD a conseillé au législateur, à la lumière des obstacles incontestables que posent l'obtention d'une réparation dans la pratique, de donner la possibilité aux personnes d'être représentées par des entités, des organisations et des associations lors des procédures juridictionnelles. Voir avis du CEPD 3/2015 «Une grande opportunité pour l'Europe – Recommandations du CEPD relatives aux options de l'UE en matière de réforme de la protection des données», p. 6. https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_fr.pdf.

[143] Avis du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques.

[144] La possibilité qu'une entité représentative engage une action collective au nom de victimes non identifiables (*opt-out*).

[145] En ce qui concerne le recours collectif «opt-out», le Bureau européen des unions de consommateurs (BEUC) a indiqué qu'«il a été prouvé dans plusieurs cas que le "opt-out" est bien plus efficace que le "opt-in" (en moyenne, environ 1 % seulement de l'ensemble des consommateurs lésés "opt-in"). Il est difficile de faire en sorte que les consommateurs signent une action "opt-in" étant donné qu'ils doivent le faire au début des procédures, avant de savoir si elles aboutiront. Le recours collectif "opt-out" fonctionne avec succès au Portugal, aux Pays-Bas et en partie en Espagne. Il est autorisé en Belgique et au Royaume-Uni (dans ce dernier pays, pour les demandes d'indemnisation privées, et il a été introduit très récemment, il est donc encore trop tôt pour procéder à une évaluation)», http://www.beuc.eu/publications/beuc-x-2017-086_ama_european_collective_redress.pdf. Pour un aperçu des mécanismes de recours collectif disponibles en Europe, voir https://www.opensocietyfoundations.org/sites/default/files/litigation-kosa-hungary-thirdparty-20170201.pdf.
Dans sa recommandation du 11 juin 2013 relative à des principes communs applicables aux mécanismes de recours collectif en cessation et en réparation dans les États membres en cas de violation de droits conférés par le droit de l'Union (2013/396/UE), la Commission a notamment jugé que le recours aux mécanismes de recours collectifs «opt-out» peut être justifié «par des motifs tenant à la bonne administration de la justice» (article 21), http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:JOL_2013_201_R_NS0013.