QUINTA
ASAMBLEA PLENARIA DE LA
RED MUNDIAL
DE JUSTICIA ELECTORAL

Nusa Dua, Bali, Indonesia
HÍBRIDO | HYBRID | HYBRIDE
9-11 • OCT
2022

Deuxième version du « Glossaire : Médias numériques et élections »

Livrable de l'Observatoire des Réseaux Sociaux

Cinquième assemblée plénière du Réseau Mondial de Justice Électorale (RMJE)

Coordination générale : Conseil de l'Observatoire des Réseaux Sociaux

Conception et coordination : Secrétariat technique du RMJE

Coordinateur académique : Rafael Rubio, professeur de droit constitutionnel, Universidad Complutense de Madrid

Global Network on Electoral Justice

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

Table des matières

Introduction

Les réseaux sociaux ont transformé les **campagnes électorales**. Leur irruption dans la société et surtout leur généralisation ont entraîné des changements dans la diffusion de l'information et dans les possibilités d'organisation politique, avec une importance particulière à l'utilisation de la **publicité ciblée**, aux mécanismes de financement, au recrutement et à l'organisation de volontaires.

Ces innovations ne sont pas exclusives à la campagne électorale, mais affectent l'ensemble du processus, de la présentation des candidatures à la proclamation des élus. Les technologies de l'information ont ainsi permis d'étendre l'exercice du droit de vote (Brésil), de faciliter son exercice en améliorant l'information grâce à des mécanismes tels que les **codes QR ou l'utilisation de chatbots**, d'améliorer sa transparence et les possibilités de contrôle (Indonésie), d'augmenter l'efficacité du système et la confiance en celui-ci (en offrant des résultats dans un temps réduit qui raccourcit les moments d'incertitude).

Pendant cette période électorale, les menaces technologiques deviennent plus visibles, car il s'agit d'un moment particulièrement intense qui affecte la légitimité de l'ensemble du système démocratique et dans lequel l'ouverture obligatoire du système à la société peut présenter certaines faiblesses. En période électorale, ces menaces visent les fondements mêmes de la confiance dans le système démocratique : le processus d'élection des représentants, d'où ils tirent leur légitimité.

D'une part, les menaces d'attaques technologiques visant à perturber ou à effondrer, de manière générale ou sélective, le système se sont multipliées. Le système électoral, même lorsqu'il repose sur un groupe important de personnes, dépend de la technologie à des phases clés telles que la compilation et la distribution du recensement ou la transmission des résultats et leur partage. Cette dépendance peut être encore plus grande dans les endroits où l'inscription au recensement est requise ou, évidemment, dans les systèmes qui ont incorporé le vote électronique. Dans ce domaine, il a été fait état d'attaques contre des recensements spécifiques à certains lieux, visant à exclure certains électeurs du processus ou à retarder le vote en provoquant des foules qui découragent le vote de manière sélective, ou encore de menaces contre le système de comptage (Pays-Bas). L'attaque des infrastructures technologiques peut également affecter la campagne électorale, par le vol d'informations privées (comme aux États-Unis lors de la campagne présidentielle de 2016), les attaques DDoS[1] sur des sites web ou l'utilisation illégale de bases de données pour délivrer des messages à un groupe spécifique. La nature globale de

[1] Les attaques par déni de service distribué (DDoS) sont une arme de cybersécurité visant à perturber le service affecté ou à extorquer de l'argent aux entreprises victimes de l'attaque.

ces menaces a conduit à l'élaboration de différents principes et normes pour protéger les processus et les droits concernés[2].

Dans les campagnes électorales également, l'**internet** est devenu un élément de différenciation, et quiconque participe à une élection sait que l'utilisation innovante de la technologie donne une longueur d'avance au premier venu. Il ne s'agit pas seulement de changements quantitatifs qui permettent aux premiers adoptants de prendre l'avantage, mais aussi de changements dans des éléments clés de l'ensemble du processus électoral en termes de canaux, mais aussi en termes d'acteurs et de calendrier. Le **Web 2.0** (caractérisé par le **contenu généré par l'utilisateur**), qui permet aux utilisateurs de publier des messages sous forme audio, vidéo ou textuelle et de les diffuser grâce à d'autres utilisateurs, les rendant ainsi **viraux**, a fait des entreprises qui fournissent la connexion (**FAI**) et de celles qui fournissent le logiciel permettant de réaliser ces publications (**intermédiaires Internet**) les véritables protagonistes des campagnes.

L'importance de la technologie dans ces processus est telle qu'elle a même caractérisé les processus électoraux successifs, du moins dans les campagnes présidentielles américaines, qui tendent à être en avance sur l'introduction de la technologie. Les élections Meetup (2004), les réseaux sociaux (2008), le microciblage (2012) ou encore la publicité sur Twitter et Facebook (2016) ont ainsi été abordés.

Dans les processus électoraux récents, pendant la campagne, il a été possible de voir des pratiques telles que : la capacité de profiler les utilisateurs et d'adapter la communication, payante ou organique, à ces profils (une pratique popularisée par l'entreprise *Cambridge Analytica* lors de la campagne pro-Brexit lors du référendum sur la permanence du Royaume-Uni dans l'Union européenne, qui s'est tenu en 2018) ; l'ingérence d'individus ou de groupes autres que les partis politiques, tant à l'intérieur qu'à l'extérieur du territoire où se déroulent les élections, à l'aide de l'achat de publicité ou par le biais d'actions coordonnées *d'astroturfing*[3] (pratique dénoncée, et démontrée, lors des élections présidentielles américaines de 2016 et 2020) ; la création de faux profils (bots automatisés ou gérés manuellement) pour créer des courants d'opinion favorables (comme lors du référendum irlandais de 2018 sur l'avortement) ; ou l'utilisation de plateformes de communication interpersonnelle pour diffuser massivement des messages de désinformation (notamment l'utilisation de *WhatsApp* par Jair Bolsonaro lors de la campagne présidentielle brésilienne de 2018).[4]

---

[2] Commission de Venise, Principes pour une utilisation des technologies numériques dans les processus électoraux conforme aux droits fondamentaux. Avis 974/2019
[3] Anonyme. Confessions d'un bot russe. Débat, 2022.
[4] Óscar Sánchez Muñoz, Réglementation des campagnes à l'ère numérique. Désinformation et micro-segmentation dans les réseaux sociaux à des fins électorales, CEPC (2020).

La perception de risques accrus pour la démocratie durant cette période conduit à une évolution des réponses juridiques. Celles-ci ont d'abord cherché à apporter une solution à de nouveaux phénomènes en appliquant une interprétation flexible des normes existantes, avec une forte composante de création jurisprudentielle et une dépendance importante à l'égard des opérateurs technologiques (Rubio, 2018). Face au nombre et à l'intensité des menaces, on assiste actuellement à un changement de tendance, à une volonté réglementaire de limiter de manière proactive certaines pratiques et outils dans le domaine de la désinformation, du ciblage et de la publicité politique, qui sont étroitement liés, et dans lesquels la technologie joue un rôle particulier.

Il existe une obligation positive d'assurer les conditions dans lesquelles les électeurs peuvent librement former et exprimer leur opinion et choisir leurs représentants**(droit de voter et d'être élu**). La liberté d'expression (en particulier dans le débat politique) et les élections libres sont des droits qui se complètent mutuellement. Il est donc essentiel d'adapter le cadre juridique, dans ce nouveau contexte, pour garantir les conditions d'un environnement électoral équitable. Dans le scénario numérique, cela implique un certain nombre de difficultés supplémentaires pour protéger la liberté et le secret du vote, de sauvegarder la liberté d'expression et de ne pas porter atteinte au principe d'équité. Pour ce faire, il faut pour l'instant se tourner vers les principes généraux qui affectent les périodes de campagne, comme l'interdiction électorale ou le financement des campagnes électorales et leur contrôle. Ce qui devient beaucoup plus complexe.

Dans cette optique, la familiarisation des opérateurs juridiques avec les concepts les plus courants dans ce domaine, ainsi qu'avec les réglementations et les décisions juridictionnelles en la matière, contribue à améliorer la réponse à cette menace croissante, qui doit nécessairement être hybride et globale. Ce travail fait partie du glossaire : Médias numériques et élections de l'Observatoire des Réseaux Sociaux du Réseau Mondial Justice Électorale, et développé sur cette base, il offre une vue d'ensemble et intégrée des cas et des concepts. Pour des raisons de clarté et de facilité d'identification, nous les avons mis en évidence en caractères gras.

I. La surveillance : la source de tous nos maux ?

Rodrigo Cetina Presuel
Professeur de droit
Universitat Pompeu Fabra Barcelona - École d'administration
Faculté de Droit Harvard
rodrigo.cetina@bsm.upf.edu

Ces dernières années, il est devenu évident que la manipulation politique et les tentatives d'ingérence indue dans les processus électoraux à travers le monde sont devenues monnaie courante et que les réseaux sociaux sont au cœur de ces préoccupations. Il est également évident que les plateformes de réseaux sociaux sont confrontées à un problème de désinformation et d'informations erronées. Si la diffusion de mensonges, d'informations inexactes ou nuisibles et les tentatives de manipulation de l'opinion publique ne sont pas nouvelles, il est devenu évident que les plateformes de réseaux sociaux exacerbent les problèmes liés à ces phénomènes en raison de leurs caractéristiques (qui ne sont en aucun cas uniques, certaines étant partagées avec d'autres TIC et d'autres médias) : la diffusion de l'information n'est pas hiérarchique, elle se propage à grande vitesse et souvent de manière virale parmi les réseaux d'utilisateurs connectés, etc. D'autres caractéristiques plus uniques (bien qu'également présentes dans d'autres médias Internet) sont que les messages peuvent également être délivrés en utilisant des techniques de microciblage (*microtargeting*) et de personnalisation pour diffuser toutes sortes d'informations à des groupes d'utilisateurs spécifiques, et qu'il est très difficile de savoir quels groupes sont exposés à quels messages (chambres d'écho, bulles épistémiques). La diffusion de l'information est un peu plus rapide qu'avec d'autres médias, et l'économie du contenu est également différente.

Glossaire

De tous les concepts à considérer, il faut d'abord parler de la surveillance, puisque, comme nous l'avons mentionné plus haut, ce concept sous-tend toutes les logiques qui opèrent pour donner naissance aux problèmes que ce document explore en relation avec l'ingérence électorale.

La **surveillance** consiste en la collecte et le traitement d'informations à caractère personnel à des fins de soins ou de contrôle. Elle permet l'identification, le suivi et la catégorisation d'individus ou de groupes d'individus. Alors que les pratiques de surveillance existent depuis longtemps et que le suivi systématisé des populations et des individus est une caractéristique de l'État moderne (connue sous le nom de surveillance de l'État), la surveillance contemporaine ajoute deux autres caractéristiques déterminantes : il s'agit d'une surveillance numérique, définie comme la collecte et le traitement de données personnelles informatisées, et de nombreuses

entreprises privées basées sur l'Internet s'engagent dans la surveillance de leurs utilisateurs à des fins privées et pas nécessairement sur mandat du gouvernement, un ensemble d'activités connu sous le nom de surveillance privée.

Outre la définition de la surveillance, il faut nécessairement définir les questions connexes, car le concept de surveillance est présent dans les logiques à l'œuvre dans la plupart des problèmes liés à l'ingérence électorale et à la manipulation politique. Il est donc nécessaire de définir correctement les différentes sous-catégories de la surveillance, ainsi que d'autres termes connexes, afin d'obtenir une image complète des concepts et une meilleure compréhension de ceux-ci, ensemble et séparément.

Ces concepts incluent la **surveillance de l'État** (*state surveillance*) ou les activités de surveillance menées par celui-ci dans le cadre d'objectifs gouvernementaux. La surveillance systématique des populations et des individus est devenue une caractéristique de l'État moderne. La **surveillance privée** (*private surveillance*) est définie comme des activités de surveillance menées par des entités privées qui ne font pas partie du gouvernement. Les entreprises privées basées sur Internet se livrent à la surveillance numérique de leurs utilisateurs à des fins privées et pas nécessairement dans le cadre d'un mandat gouvernemental, bien qu'elles puissent fournir des services ou des technologies de surveillance aux gouvernements et à leurs agences. Elle comprend également la **surveillance numérique** (*digital surveillance)*, ou la collecte et le traitement de données à caractère personnel qui sont informatisées et permettent l'identification, le suivi et la catégorisation d'individus ou de groupes d'individus, ainsi que la surveillance en ligne (surveillance des réseaux sociaux), qui désigne toute activité de surveillance numérique menée sur les plateformes de réseaux sociaux.

Pour les entreprises propriétaires des réseaux sociaux, il s'agit d'une pratique essentielle au cœur de la monétisation de leurs activités lucratives. Pour les gouvernements, Internet, et en particulier les réseaux sociaux, est devenu un espace de surveillance des citoyens à des fins politiques et électorales. Il inclut également les concepts de **surveillance numérique privée-publique** (*private-public digital surveillance)*, c'est-à-dire la combinaison d'activités et d'objectifs de surveillance menés par l'État et par des entités privées. Il s'agit souvent de recourir à des technologies de surveillance privées pour atteindre des objectifs que les gouvernements ne pourraient pas réaliser par eux-mêmes. Un autre concept clé est la **surveillance politique numérique** (*digital political surveillance*), c'est-à-dire l'utilisation des plateformes de réseaux sociaux pour surveiller les citoyens, les empêcher d'agir politiquement et faire taire les dissidents.

D'autres concepts nous aident à brosser un tableau adéquat de l'état actuel de la surveillance en ligne : le **capitalisme de surveillance** (*surveillance capitalism)*, défini comme une forme de capitalisme de l'information dans lequel le système économique

se concentre sur la collecte de données personnelles pour permettre la prédiction et la modification du comportement humain afin de produire des revenus et de contrôler le marché.[5] Un autre concept est l'**instrumentalisation** (*instrumentarianism)*, c'est-à-dire l'instrumentation et l'instrumentalisation du comportement humain à des fins de modification, de prédiction, de monétisation et de contrôle.[6] Selon la définition de Zubboff, il s'agit d'un concept étroitement lié au capitalisme de surveillance.

La surveillance privée active exercée par les plateformes de réseaux sociaux les distingue des autres types de médias. Cette capacité sociotechnique d'enregistrer et de surveiller chaque action d'un utilisateur en ligne permet non seulement aux plateformes de réseaux sociaux d'établir des profils complexes (bien qu'inexacts) de leurs utilisateurs qui, à leur tour, leur permettent de les séparer en groupes et de leur fournir un contenu personnalisé, mais c'est aussi, pour l'essentiel, ce qui sous-tend le modèle d'entreprise des sociétés de réseaux sociaux. Le profit est recherché par la surveillance des utilisateurs, l'extraction et le traitement de leurs données personnelles, la vente de ces données, le profilage des utilisateurs ou la mise en place de systèmes qui leur permettent de vendre de la publicité personnalisée (y compris de la publicité politique ciblée) ou de proposer un contenu personnalisé. Ce type de pratiques est le plus susceptible de maintenir l'engagement d'un utilisateur et son utilisation de la plateforme, d'extraire à son tour davantage d'informations à son sujet pour la monétisation, et ainsi de suite.

L'industrie de la surveillance numérique privée s'est développée de manière de plus en plus sophistiquée, développant une technologie qui dépasse de loin les capacités de surveillance de l'État. Les gouvernements ont commencé à sous-traiter des services de surveillance à des entités privées et à utiliser une technologie à l'origine destinée à la surveillance privée, qui a ensuite été réaffectée à la surveillance de l'État. La surveillance privée et la surveillance publique se combinent pour former un gigantesque appareil de surveillance de l'entreprise et de l'État. Il s'agit d'un partenariat public-privé.

Les intérêts privés et publics ont rendu la technologie de surveillance numérique omniprésente. Les capacités de surveillance numérique se sont développées et sont devenues plus sophistiquées pour couvrir tous les types de personnes dans tous les types de lieux et de situations. Comme mentionné précédemment, la surveillance privée elle-même est devenue une partie très importante de l'industrie numérique, car elle permet de générer des profits grâce à la vente de données et à la publicité. La surveillance numérique privée des utilisateurs est devenue si essentielle à Internet tel

[5] Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. [Les autres grands : Le capitalisme de surveillance et les perspectives d'une civilisation de l'information]. Journal of Information Technology, 30(1), 75-89. https://doi.org/10.1057/jit.2015.5
[6]Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action [Le capitalisme de surveillance et le défi de l'action collective]. New Labor Forum, 28(1), 10-29. https://doi.org/10.1177/1095796018819461, p. 20.

que nous le connaissons que certains décrivent ce modèle économique comme un sous-ensemble du capitalisme, qu'ils appellent le capitalisme de surveillance.
Cependant, la surveillance n'est pas seulement au cœur du modèle économique des plateformes de réseaux sociaux, mais elle peut également être au cœur de nombreux problèmes que nous associons aux réseaux sociaux : les atteintes à la vie privée, la violation du droit à la protection des données personnelles (impliquant le contrôle des données personnelles), la diffusion de discours haineux, la facilitation des abus en ligne, la diffusion de contenus et de publicités ciblés (parfois dans l'intention de manipuler ou de désinformer). Elle peut également être l'une des causes principales du phénomène de la désinformation en ligne lui-même.

En effet, les plateformes de réseaux sociaux ne fondent pas leur modèle économique sur la fourniture de contenu à leurs utilisateurs ni sur le maintien de leur connexion, ni sur le fait d'être le meilleur moyen possible d'obtenir des informations, de rester bien informé ou d'améliorer l'opinion publique et le débat politique. Malgré ce que l'on peut entendre, la promotion de la liberté d'expression ou de la liberté de la presse n'est pas non plus au cœur de leurs activités. Le suivi de leurs utilisateurs y est.

Dans la logique du capitalisme de surveillance, les plateformes de réseaux sociaux cherchent à fournir aux utilisateurs tout contenu susceptible de les inciter à rester sur la plateforme, car une activité accrue des utilisateurs entraîne une surveillance accrue de ceux-ci ou, en d'autres termes, des possibilités accrues de les surveiller et d'extraire des données qui peuvent être transformées en profit d'une manière ou d'une autre.

Les plateformes de réseaux sociaux sont ainsi devenues agnostiques en matière d'information. Cela signifie que leur principale préoccupation est de diffuser n'importe quelle information à n'importe quel utilisateur si cela peut maintenir son engagement et son utilisation de la plateforme, même s'il s'agit d'informations erronées ou de désinformation et indépendamment du fait que le contenu soit abusif ou manipulateur. Cela signifie également que la création de chambres d'écho par la diffusion sélective d'informations, de messages ou de publicités est une préoccupation secondaire, si celle-ci permet de maintenir l'intérêt des utilisateurs. En d'autres termes, un modèle commercial axé sur la surveillance incite les plateformes à être aussi peu sensibles que possible à l'information. Tout est bon pour maintenir l'attention sur les plateformes.

Grâce à l'outil sociotechnique qu'est la surveillance, l'information de qualité (mais aussi de mauvaise qualité) n'est considérée que comme un outil, un moyen de parvenir à une autre fin, et non comme une préoccupation centrale. Les plateformes de réseaux sociaux ne sont qu'un ensemble d'outils, un ensemble de techniques numériques pour diffuser des messages. Entre de mauvaises mains, elles peuvent être utilisées à des fins plus néfastes qui génèrent des troubles électoraux, la stabilité politique et peuvent saper les processus et les institutions démocratiques.

Les plateformes de réseaux sociaux ne sont plus aveugles à ces problèmes et, avec les régulateurs et la société civile, elles prennent des mesures pour atténuer les effets négatifs de la désinformation en ligne. Toutefois, elles ont laissé le problème s'aggraver et devenir systémique jusqu'à ce qu'apparaissent les premières histoires d'ingérence électorale, de tentatives de détruire les institutions démocratiques par la diffusion de fausses informations qui ont conduit à une violence politique bien réelle, y compris la violence sexiste et ethnique.

La résolution de ce problème n'était pas au cœur de leur mode de fonctionnement, du moins pas au début.

S'il est vrai qu'après avoir été impliquées dans des scandales successifs et en avoir subi les conséquences en termes de relations publiques, et sous la pression politique et réglementaire des gouvernements pour qu'ils agissent, les plateformes de réseaux sociaux ont commencé à s'engager dans une surveillance, un filtrage et une modération plus actifs des contenus les plus nuisibles, il n'en reste pas moins que le résultat final a été négatif pour les démocraties et les citoyens du monde entier.

La surveillance numérique privée-publique présente des risques spécifiques pour les citoyens et met en péril leurs droits et leur bien-être. Certains de ces risques compromettent directement la participation politique. La surveillance sous-tend d'autres pratiques qui ont également des effets négatifs sur la démocratie, comme la diffusion de la désinformation, la manipulation politique et l'ingérence électorale.

Selon l'Union européenne, la surveillance politique des réseaux sociaux risque de permettre aux gouvernements de contrôler les citoyens, d'entraver leur action politique et de faire taire les dissidents. La surveillance des réseaux sociaux entraîne une perte de la vie privée et de l'autonomie, car elle sape la capacité de jugement politique des citoyens et peut conduire à un désengagement politique. En effet, la promotion de contenus viraux et de comportements addictifs sur les réseaux sociaux peut détourner les gens de la politique.

À son tour, la personnalisation axée sur la surveillance enferme les citoyens dans des bulles d'information et affecte leur capacité à se forger une opinion, réduisant ainsi leur vision du monde. La personnalisation entraîne également une fragmentation sociale et politique, car la segmentation de l'information et de l'engagement réduit les possibilités de dialogue politique.

La personnalisation par la surveillance peut également contribuer à la désinformation, car elle fausse les opinions et les préférences en diffusant de fausses informations en ligne. De plus, sa diffusion peut fausser les résultats des élections et ainsi porter atteinte à leur intégrité, ce qui affecte alors les résultats. La surveillance est également

essentielle pour permettre la désinformation automatisée, car les comptes automatisés peuvent s'appuyer sur les profils des utilisateurs pour amplifier et exacerber les effets des fausses informations.

Il est particulièrement important que ces concepts soient correctement définis afin d'être mieux compris et de permettre d'identifier correctement les utilisations indésirables des techniques, et d'aider à prendre des mesures pour les combattre. Cette contribution contient une définition de plusieurs des concepts susmentionnés et connexes, s'appuyant sur des travaux antérieurs qui ont abouti à un glossaire de termes liés à l'utilisation de la technologie pour interférer dans les élections et à la manipulation politique en ligne, ainsi qu'à une classification permettant de construire une carte des termes connexes.

Pour compléter ces définitions, nous avons également procédé à une analyse de la jurisprudence et de la législation qui traitent de ces concepts, et, dans le cas de ce chapitre, spécifiquement de celui de la surveillance et de l'activité qui lui est associée. L'objectif est de faire la lumière sur ce que la loi et les tribunaux ont à dire à ce sujet, sur sa définition et ses limites juridiques, notamment sur la manière dont la surveillance en ligne peut porter atteinte aux droits fondamentaux des citoyens et sur la question de savoir si la loi reconnaît de manière adéquate que la surveillance permet la manipulation politique, l'ingérence électorale et peut constituer une menace pour les processus électoraux et les institutions démocratiques, ainsi que sur les réponses à ses effets négatifs qui existent dans la loi.

Cas

Plus précisément, ce document comprend une analyse de plusieurs cas examinés par la Commission électorale centrale (CEC). Tous ces cas sont liés à des campagnes électorales et sont directement ou indirectement liés à l'utilisation de la surveillance pour diffuser des messages politiques et de la propagande électorale, en particulier dans le contexte du règlement général sur les élections (LOREG). Vingt-huit cas et instructions couvrant la période de 2011 à 2021 ont été examinés, ainsi qu'un cas connexe remontant à 2006. Certaines de ces affaires sont des demandes d'approbation, d'autres des consultations et d'autres encore des instructions relatives à l'interprétation des règles électorales et de campagne politique, tandis que d'autres sont des plaintes déposées contre des partis politiques, des hommes politiques ou des agences gouvernementales.

La Cour constitutionnelle d'Espagne a examiné une décision concernant la constitutionnalité de certaines dispositions de la loi électorale générale relatives à la sauvegarde des droits fondamentaux, y compris le droit à la protection des données personnelles liées aux opinions politiques, ainsi qu'une affaire devant le Tribunal

Électoral du Mexique qui analyse la nature des réseaux sociaux et la distribution d'opinions politiques et de propagande électorale par leur biais, ainsi qu'une autre affaire du Conseil national électoral de Colombie qui réfléchit également à la nature des réseaux sociaux et à leur capacité à cibler les utilisateurs et à transmettre des messages politiques et de la propagande électorale aux masses.

Une évaluation globale des cas analysés permet de réfléchir à leurs implications pour la surveillance numérique et à ce que cela signifie pour les processus électoraux ainsi que pour l'utilisation des réseaux sociaux, de manière à renforcer, plutôt qu'à entraver, le débat politique, les choix politiques éclairés et les processus politiques démocratiques sains.

Dans le cas de l'Espagne, sur la base des cas examinés, le Conseil électoral a interprété les lois relatives aux communications électorales de manière à inclure toutes les formes de communication en ligne. Toutefois, il semble que la CEC n'ait pas abordé directement les implications de la surveillance, du microciblage (*microtargeting*) et du profilage en ligne sur la manière dont les messages sont diffusés en ligne. Elle n'a donc pas encore traité plus en profondeur des exigences telles que la transparence ou le contrôle des dépenses de campagne en ligne, afin de garantir des élections libres et équitables. Cela est d'autant plus vrai que les réseaux sociaux restent un outil central dans les communications électorales modernes.

Toutefois, la Cour constitutionnelle espagnole a annulé un article de la loi électorale espagnole (article 58 bis 1) qui aurait permis aux partis politiques de collecter et de traiter des données à caractère personnel relatives aux opinions politiques des citoyens, car il n'offrait pas de garanties suffisantes pour les droits et les données des citoyens et n'était pas en mesure de définir clairement l'intérêt public et constitutionnel qu'il était censé poursuivre. Cela a des implications fortes et directes, en particulier pour la surveillance politique en Espagne. Avec la loi nationale sur la protection des données et le règlement européen sur la protection des données, cela constitue un cadre solide pour les droits des citoyens en matière de protection des données. Dans ce cas, il fournit également un fondement solide pour la protection des données en tant qu'instrument de la liberté d'avoir et d'exprimer des opinions politiques, garantie par la Constitution espagnole et dans le cadre européen pour la protection des droits fondamentaux.

Dans le cas du Mexique, il est clair que le Tribunal Électoral n'a pas fait preuve d'une compréhension suffisante du fonctionnement d'Internet dans l'affaire examinée, et en particulier des réseaux sociaux. Son engagement à placer une limite élevée à la liberté d'expression, ainsi qu'à la liberté d'exprimer une préférence pour un candidat politique ou un autre, est louable, y compris la protection de ces droits pour les membres de la famille des candidats politiques. Toutefois, à l'exception des références à l'Internet comme étant différent des autres médias et de l'inclusion d'une définition du

microciblage (*microtargeting*) et même d'influenceur (*influencer*), ce texte ne reconnaît pas d'autres concepts importants tels que le marketing organique et la viralité des messages. Il attribue également une « présomption de spontanéité » à tous les messages des réseaux sociaux, ce qui est en contradiction avec la façon dont ceux-ci sont utilisés, même à des fins tangentiellement liées à des objectifs commerciaux, politiques ou électoraux. L'autorité électorale mexicaine considère que les réseaux sociaux et Internet sont tellement différents des médias tels que la télévision ou la radio que sa loi électorale ne devrait pas s'appliquer aux communications faites par le biais des médias en ligne, ce qui semble dépassé. Il s'agit peut-être d'un signe que la loi électorale mexicaine devrait être modifiée afin d'inclure les communications électorales en ligne, pour fixer correctement les règles du jeu et maintenir la loi électorale mexicaine en phase avec ce qui se fait dans d'autres pays.

Enfin, le cas de la Colombie est intéressant pour des raisons inverses : il démontre une compréhension plus sophistiquée des réseaux sociaux par le Conseil national électoral de ce pays, statuant sur des communications électorales faites en dehors de la période autorisée par la loi. Si le Conseil a admis que, selon les critères suivis jusqu'alors, l'infraction ne devait pas faire l'objet d'une sanction, il reconnaît toutefois que ces critères doivent évoluer compte tenu de la nature d'Internet et note qu'il en sera de même à l'avenir. Il est intéressant qu'elle tienne compte de la manière dont les communications sont en fait distribuées sur Internet, à la fois en permettant aux messages de cibler directement des groupes spécifiques d'utilisateurs et en comprenant que ces messages peuvent également être mis à la disposition de groupes indéterminés de personnes, et que c'est parfois précisément la stratégie de ceux qui cherchent à distribuer des communications de propagande électorale sur Internet.

II. Désinformation

Vitor de Andrade Monteiro

Les mensonges, les rumeurs et les tromperies n'ont jamais été étrangers à la politique. En effet, la dissimulation et le mensonge sont des figures qui ont toujours été présentes dans les conflits politiques et dans l'environnement démocratique. Certains historiens affirment que le contexte même de ce qui est connu comme le cadre de l'émergence de la démocratie à Athènes est quelque peu fallacieux. Il est suggéré que les motifs du tyrannicide héroïque d'Hipparque par Harmodius et Aristogitus, qui a conduit à l'établissement de la démocratie à Athènes quelques années plus tard, avaient plus à voir avec des raisons passionnées et égoïstes qu'avec un noble esprit démocratique. Malgré cela, la fausse histoire a triomphé et les amants ont été reconnus comme les fondateurs de la démocratie. Ils ont reçu un hommage et leurs descendants ont obtenu des honneurs et des privilèges.

Dans la Rome antique, les dossiers de désinformation étaient utilisés par les empereurs pour rechercher la légitimité et assurer la stabilité de leur règne. Septime Sévère, bien qu'il n'ait aucun lien de parenté avec son prédécesseur Commode (qui était le fils illégitime de Marc Aurèle), tente de créer une fausse relation avec ce célèbre empereur, afin d'être accepté par la population comme le successeur le plus légitime. Comme une grande partie de la population romaine ne savait pas lire et que les informations étaient essentiellement diffusées par le biais d'images, il ordonna de frapper des pièces à son effigie, retouchées de manière à présenter des traits physiques semblables à ceux de Marc-Aurèle et à renforcer son acceptation par la population romaine.

Compte tenu de cette relation de longue date entre le mensonge et la politique, il convient de se demander pourquoi les discussions sur le mensonge en politique sont devenues si importantes aujourd'hui. Pourquoi les ***fausses informations*** (fake news) font-elles l'objet de tant de débats et d'inquiétudes de la part des organes électoraux ? En d'autres termes, si le mensonge a toujours existé en politique, pourquoi est-il encore important de parler de **désinformation**?

La recherche de réponses à ces questions semble passer par deux points. L'une est le phénomène de la **post-vérité**, et son impact sur la compréhension du mensonge (et de la vérité !) aujourd'hui ; l'autre est l'avènement des plateformes numériques et toute la révolution dans le domaine de la communication qui en a découlé. Bien que le champ d'application de ce document ne permette pas une analyse approfondie de chacun des points mentionnés, le développement du thème central de ce document nécessite un passage, même bref, par ces points.

Le terme de **post-vérité** est présenté comme une expression de l'effet qui sert à saisir une image de l'époque actuelle. Il représente le déclin de la rationalité,

l'obscurcissement des faits, le dépassement d'une réalité qui peut être comprise par une logique guidée par l'émotion, la croyance et la subjectivité. En ces temps de post-vérité, les faits objectifs et vérifiables ont moins d'influence sur l'**opinion publique** que les croyances individuelles. Il n'y a pas de faits, mais des interprétations de ces faits. C'est la victoire de la *doxa* sur l'*épistémè*, de l'opinion sur la connaissance. Une étude scientifique méthodologiquement correcte et validée par la communauté académique a le même poids qu'un avis juridique.

La liquidité élevée de notre époque ne permet pas de mener de réflexions exhaustives –et fastidieuses, ce qui explique que les conclusions semblent suivre cette dynamique, en privilégiant l'horizontalité. C'est le triomphe du foie sur le cerveau, de l'apparentement simple sur l'honnêtement complexe. Dans ce scénario, la recherche de la vérité est remplacée par la construction d'une version des faits qui apporte satisfaction et offre une protection contre la dureté de la réalité. Cette réclusion dans la subjectivité oriente la pensée vers un environnement accueillant, qui offre des opinions renforçant des convictions préexistantes, même si celles-ci sont fondées dans le vide. C'est l'environnement idéal pour le développement de **métarécits, de théories du complot et de réalités alternatives** de toutes sortes, qui contribuent toutes à la dévaluation de la vérité en tant qu'élément de la prise de décision politique.

Ce recul de l'idée de vérité est aggravé par l'impact des nouvelles technologies sur l'**écosystème de l'information**. La croissance rapide de la communication par les médias numériques et son insertion de plus en plus profonde dans la société ont entraîné des changements significatifs de différentes natures. Le caractère informel de la communication dans l'environnement numérique, tout en démocratisant le droit d'exprimer une opinion, a fini par renforcer les effets de la post-vérité. En effet, il a rendu possible une concurrence relativement équilibrée entre, d'une part, les faits scientifiquement prouvés et les textes journalistiques professionnels et, d'autre part, les opinions non fondées et la réinterprétation des faits. Ce constat est d'autant plus frappant que le volume de contenu produit chaque minute sur les réseaux sociaux est considérable.

D'autre part, le modèle économique des plateformes numériques encourage l'amplification de la désinformation, car il repose sur la capitalisation de l'attention et de la participation des utilisateurs. Les fausses informations se propagent beaucoup plus vite, plus loin et plus profondément que les vraies informations, et génèrent donc plus de profits. Les effets négatifs de la désinformation sont observés dans divers contextes de la vie sociale, qu'il s'agisse de décisions concernant des questions liées à des problèmes économiques et de santé publique, de l'évaluation des politiques en matière de drogues, de questions religieuses, etc. Toutefois, c'est le contexte politique qui semble le plus sensible à l'influence des **informations manipulées**. Les fausses informations sur ce sujet s'étant révélées se propager significativement plus vite, plus loin, plus profondément et plus largement que d'autres relatives au terrorisme, aux

catastrophes naturelles, à la science et aux légendes urbaines (VOSOUGHI et al., 2018).

La désinformation dégrade le terrain sur lequel se construit le dialogue et encourage le recours à la force comme moyen de résoudre les différends. La démocratie perd de l'espace parce que son existence dépend de la circulation libre et sans entrave des idées (STENGEL, 2020). La **perturbation de l'information** porte atteinte au droit de participer au processus électoral de manière consciente et informée, ce qui entraîne un déficit de légitimité dans le résultat des élections et une atteinte à la normalité du processus électoral.

Au-delà des résultats valides et conformes à la réalité, le processus électoral doit véhiculer un sentiment de validité et de légitimité pour atteindre son objectif principal. À l'image de l'épouse de César, il ne suffit pas que le système de justice électorale fonctionne bien, mais il faut également donner à l'électeur l'impression que le processus électoral s'est déroulé de manière normale et qu'il a permis de révéler la véritable volonté de l'électorat. La mission institutionnelle de la justice électorale consiste donc à produire de la confiance, et c'est précisément sur ce point que les marchands de désinformation se sont concentrés.

Une tendance inquiétante a été identifiée : le **désordre de l'information** dans le contexte électoral vise à attaquer l'intégrité du processus électoral et les autorités liées à l'organe de gestion des élections responsable de sa mise en œuvre. Cette stratégie, constamment associée à une forme de **populisme numérique** (BRUZZONE, 2021), a été identifiée dans plusieurs pays du monde, comme en témoignent les dernières élections présidentielles américaines, le vote du Brexit, les élections brésiliennes de 2018 et 2020, ainsi que les élections présidentielles au Mexique, en Hongrie et au Pérou.

Ces artifices pernicieux tendent à affecter la crédibilité des institutions impliquées dans le processus et à discréditer les résultats obtenus lors des élections. Ce scénario ouvre la porte à des mouvements pro-rupture (comme dans le cas du **Myanmar)** et à des soulèvements populaires suivis de violences et de morts (comme au **Kenya** et en **Côte d'Ivoire**). En outre, l'existence même de l'organe de gestion des élections peut être affectée par les effets de la désinformation, car la perte de réputation ouvre la voie à des réactions législatives (telles que la perte de pouvoirs par l'organe électoral) et à des attaques intensifiées visant à l'asphyxie institutionnelle (telles que la réduction des budgets, des prérogatives fonctionnelles et du personnel). Un exemple frappant est celui de **l'Institut National Électoral du Mexique**, qui, après avoir été victime de plusieurs reportages désinformateurs, a été proposé pour abolition par le président de la République, Andrés Manuel López Obrador.

L'impact de la désinformation peut être renforcé par l'utilisation de **stratégies d'automatisation des profils de** réseaux sociaux, qui permettent la diffusion d'informations manipulées par des ***bots*** ressemblant à des humains pour promouvoir

certains posts, l'amplification des messages provenant de sources peu crédibles et la mention d'utilisateurs influents dans ces posts. Grâce à ce comportement, les *bots* jouent un rôle majeur dans la production de l'effet viral de la désinformation.

Glossaire

Pour bien comprendre le phénomène de la désinformation, il faut se familiariser avec certains concepts qui traduisent des caractéristiques importantes des troubles de l'information. En principe, la définition même de ce que recouvre le concept de désinformation doit faire l'objet d'une attention particulière. Pour certains auteurs, comme Wardle et Derakhshan (2017), la désinformation est l'une des notions incluses dans l'idée de troubles de l'information. Pour eux, il est nécessaire de distinguer les messages vrais de ceux qui sont faux, y compris ceux qui sont créés dans l'intention de nuire, de ceux qui ne le sont pas. Les troubles de l'information constituent ainsi un ensemble qui comprend les figures suivantes : a) **les informations erronées** (***misinformation***), qui est une information produite sans intention de nuire, mais dont le contenu est faux ; b) **la désinformation** (**disinformation**), qui est un contenu délibérément créé pour nuire ; et c) la **malinformation** (***malinformation***), qui est une information fondée sur la réalité, mais utilisée dans l'intention de nuire à quelqu'un, à une organisation ou à un État (Wardle et Derakhshan, 2017).

Malgré l'utilisation fréquente de longue date du terme ***fausses informations*** (fake news) par les médias, son utilisation n'est pas recommandée pour définir le phénomène de la désinformation, car elle ne permet pas de délimiter clairement son objet ni de comprendre correctement le problème. Tout d'abord, je voudrais expliquer que l'expression *fausses informations* (fake news) a été utilisée comme une arme dirigée contre les opposants en raison de leur propre statut d'ennemi, et non contre les informations qu'ils présentent. De plus, comme nous l'avons vu, les troubles de l'information comprennent parfois des informations qui ne sont pas *fausses* (fakes) à l'origine , comme dans le cas de la désinformation. Il est également perçu que l'idée même de nouvelles repose sur quelque chose qui est lié à la vérité, ce qui fait de l'expression *fausses informations* (fake news) un oxymore.

Un autre concept important pour comprendre le phénomène est celui des ***opérations d'information*** (**Information Operations**) ou ***opérations d'influence*** (**Influence Operations**). Il s'agit d'une série de techniques de guerre utilisées pour obtenir des informations, influencer et déstabiliser le processus décisionnel de l'adversaire. Les pratiques humaines de désinformation sont parfois encouragées de manière ordonnée par des entreprises qui créent et gèrent des profils pour produire des ***posts*** et des ***'j'aime'*** afin de stimuler une certaine narration. Ces entreprises sont connues sous le nom de **fermes de contenu ou de fermes à clics (*content* ou *click farms*).** La figure du ***troll*** est aussi particulièrement présente dans la désinformation et se compose d'utilisateurs de plateformes numériques qui cherchent délibérément à

menacer, provoquer, intimider et offenser afin de créer une distraction ou une discorde. Leurs actions peuvent être isolées ou se dérouler de manière ordonnée avec d'autres acteurs. Parfois, leurs actions sont encouragées par des entreprises qui se consacrent à ces objectifs et qui agissent de la même manière que les fermes à clics. Ces dernières sont donc connues sous le nom de ***fermes à trolls*** (troll farms).

Il existe de nombreuses façons de créer des récits dans le domaine de la désinformation, et l'une des plus sophistiquées est la falsification numérique (**deep fakes**), qui consiste à manipuler des images et des vidéos au moyen de l'intelligence artificielle pour combiner des aspects réels avec d'autres aspects fabriqués, dans le but de créer un contenu ultraréaliste dans lequel des personnes disent ou font des choses qui ne se sont pas produites, créant ainsi la confusion chez le destinataire. La désinformation bénéficie souvent de pratiques répréhensibles pour obtenir des résultats. L'***hameçonnage*** (phishing) est l'un d'entre eux et repose sur des attaques ciblées de *pirates informatiques* (hackers) visant à obtenir les données personnelles des utilisateurs.

Cas

Bien que la désinformation ne soit pas un phénomène nouveau dans la société, son impact sur les processus électoraux fait aujourd'hui l'objet d'une plus grande attention de la part des organes électoraux. Ce texte inclut plusieurs cas jugés par le Conseil central électoral (CEC) espagnol, par le Tribunal supérieur électoral brésilien (TSE) et par l'Argentine. Ils démontrent la manière dont les tribunaux électoraux traitent le phénomène de la désinformation par le biais de plateformes numériques dans le processus électoral. La séquence présente certains de ces cas ainsi que des documents traitant des défis posés par la lutte contre la désinformation.

La désinformation affecte la capacité de l'électeur à choisir son candidat en se basant sur des informations exactes et des idées correspondant à la réalité. L'accès à des informations correctes, transparentes et accessibles est donc une condition préalable à une liberté effective. Selon la **Chambre nationale électorale argentine**, dans l'**accord extraordinaire 66/18**, plus il y a d'informations, d'impartialité et de liberté dans le processus électoral, plus la qualité de la démocratie est élevée. La Chambre a enregistré les impacts sur l'amplification de la désinformation par les ***trolls*** (des « commentateurs rémunérés utilisant de faux profils ») et les ***bots*** (« profils simulés avec certains moments d'activité en ligne intense, suivis de longues périodes d'inactivité »). Pour l'institution, « du temps, des ressources et de la créativité » sont nécessaires pour réussir la tâche complexe de contrer la manipulation de l'information, en commençant par mettre l'accent sur l'éducation aux médias. Après avoir analysé le phénomène dans différents contextes électoraux, la Chambre a adopté une série de mesures visant à réglementer la participation des candidats aux élections, telles que la divulgation des résultats de la surveillance des réseaux sociaux et de la

propagande et la création d'un registre des comptes de réseaux sociaux et des *sites web* officiels des candidats, des groupements politiques et des plus hautes autorités électorales.

Dans son **arrêt 3010/02, la Chambre nationale électorale argentine** a réitéré l'importance de l'accès à l'information pour l'exercice du droit de vote, qu'elle a appelé « vote éclairé ». L'importance de **l'accès à l'information pour l'ordre démocratique** a été soulignée dans **l'avis consultatif OC-5/85** de la Cour interaméricaine des droits de l'homme, qui indique que la liberté d'expression est une condition pour que la société puisse prendre des décisions en connaissance de cause. La conclusion de la Cour est qu'une société n'est pas libre si elle n'est pas bien informée, et il est clair que la qualité de l'information est essentielle à une liberté effective.

L'**engagement éthique numérique** est une initiative importante développée par la Chambre électorale nationale argentine pour préserver la qualité du débat démocratique sur les plateformes numériques. Ce document tient compte des préoccupations croissantes concernant la manipulation de l'information sur les réseaux numériques et dans l'environnement numérique, ainsi que son impact sur la démocratie. Cet engagement fait référence à **l'accord 66/18** susmentionnée pour l'enregistrement de l'opportunité de promouvoir l'éducation numérique afin d'améliorer la gestion de l'information politique électorale dans l'environnement numérique. En adhérant à cet engagement, les entités s'engagent à promouvoir « l'honnêteté du débat démocratique lors des prochaines élections nationales, afin de contribuer à atténuer les effets négatifs de la diffusion de faux contenus et d'autres tactiques de désinformation dans les réseaux sociaux et d'autres environnements numériques ». De leur côté, les plateformes numériques adhérentes déclarent « reconnaître la complexité et les tensions qui peuvent exister au cours du processus électoral avec la diffusion ou la prolifération d'informations inexactes ou de fausses nouvelles, et acceptent, dans le cadre de leurs possibilités et de leurs outils, de collaborer avec les autorités compétentes dans ce processus tout en respectant les valeurs démocratiques et la liberté d'expression ». Plusieurs plateformes numériques adhéreront à cet engagement, notamment Google, Twitter, Facebook, WhatsApp, Kwai et TikTok.

Les **plateformes sociales** sont particulièrement importantes dans le cadre des communications contemporaines. En ce sens, le **Conseil central électoral espagnol** a reconnu, dans l'**accord 146/2021 relatif au dossier 293/1215**, la prédominance des réseaux sociaux dans la société d'aujourd'hui, en soulignant qu'ils sont presque essentiels pour les candidats et les groupes électoraux. Dans ces conditions, le comportement des réseaux sociaux à l'égard des partis ne peut être considéré comme un élément politique sans importance. En effet, l'action des plateformes doit respecter le principe d'égalité et ne doit pas servir d'outil pour déséquilibrer le jeu politique. À la lumière de cette constatation, on peut voir que des obligations peuvent naître qui vont au-delà de celles contenues dans leurs contrats d'utilisation. Ainsi, selon la

Commission, la sanction appliquée par Twitter, qui consistait à suspendre les fonctions du profil d'un parti politique en raison du non-respect de ses conditions d'utilisation, était raisonnable par rapport au comportement de l'association.

Au Brésil, malgré l'ampleur effroyable qu'a prise la désinformation dans l'arène politique, rares sont les cas où la question a été débattue devant la plus haute juridiction électorale. Dans deux cas importants, le TSE a débattu de la possibilité d'appliquer la sanction de perte de mandat en raison de la **diffusion de désinformation** par les candidats et de l'**utilisation d'envois massifs** par WhatsApp.

L'**affaire Franceschini** porte sur la **diffusion de désinformation visant à saper le processus électoral par le biais des réseaux sociaux** le jour du scrutin. En bref, un député a diffusé en direct, le jour du scrutin et avant sa clôture, une émission dans laquelle il affirmait qu'il y avait des urnes frauduleuses et qu'il disposait d'informations officielles sur la fraude. Le TSE a estimé qu'il existait des motifs suffisants de licenciement, considérant qu'il y avait eu abus de pouvoir de la part des médias. Selon les données exprimées dans l'arrêt, l'émission a été transmise en direct, avant la fin du vote (le 07/10/2018), à plus de 70 000 personnes (le 12/11/2018, elle comptait plus de 105 000 commentaires, 400 000 partages et six millions de vues). Parmi les discours prononcés à cette occasion, il a été dit que les « urnes étaient falsifiées » et qu'il existait des documents de la justice électorale reconnaissant cette affirmation. La Cour suprême fédérale du Brésil (STF), saisie d'un recours, a confirmé la constitutionnalité de la décision du TSE.

La question de l'utilisation des **envois massifs par** WhatsApp a fait l'objet de l'**affaire Bolsonaro/Mourão**. Devant le tribunal, la candidature présidentielle a été acquittée, faute de preuves solides de l'accusation d'abus de pouvoir économique et d'utilisation abusive des médias. Bien qu'aucune sanction n'ait été imposée dans ce cas précis, l'affaire mérite d'être soulignée car la thèse suivante a été établie dans la thèse jurisprudentielle : « l'utilisation d'applications numériques de messagerie instantanée pour promouvoir des communications de masse contenant de la désinformation et des mensonges au détriment des opposants et au profit d'un candidat peut constituer un abus de pouvoir économique et une utilisation abusive des médias, conformément à l'**article 22 de la loi 64/1990 (loi sur l'inéligibilité),** en fonction de la gravité réelle de la conduite, qui sera examinée au cas par cas ».

Le phénomène de la désinformation redessine la notion de droit à la liberté d'expression. En effet, bien que la **liberté d'expression** occupe une position centrale dans l'environnement démocratique, l'existence même de la démocratie exige la protection d'autres droits constitutionnels qui peuvent être sapés par l'exercice arbitraire de la liberté d'expression, en particulier par le biais de la perturbation de l'information. Dans le **cadre du plan d'action conjoint contre la désinformation**, la **Commission européenne et le haut représentant de l'Union pour les affaires**

étrangères et la politique de sécurité déclarent que le droit à une participation libre, équitable et éclairée aux processus politiques est de plus en plus remis en cause par la diffusion délibérée à grande échelle et la diffusion systématique de la désinformation. Ils appellent également à une détermination politique et à des réponses coordonnées. **L'article 13 de la Convention américaine des droits de l'homme** prévoit le droit à la liberté d'expression et de pensée. La question a été abordée par la Cour internationale des droits de l'homme dans les affaires **Olmedo Bustos et autres (2001), Álvarez Ramos vs. Venezuela (2019), Urrutia Laubraeaux vs. Chili (2020).** Pour la Cour de la CIDH, il existe une double dimension à prendre en compte dans la liberté d'expression : la dimension sociale et la dimension individuelle.

Exprimant leur préoccupation et leur attention face au phénomène de la désinformation et à sa mise en œuvre dans le but de **semer la confusion et d'affecter le droit à une prise de décision** éclairée, qui sont des droits concernés par la liberté d'expression, le rapporteur spécial des Nations unies (ONU) sur la liberté d'opinion et d'expression, le représentant pour la liberté des médias de l'Organisation pour la sécurité et la coopération en Europe (OSCE), le rapporteur spécial de l'OEA sur la liberté d'expression et le rapporteur spécial sur la liberté d'expression et l'accès à l'information de la Commission africaine des droits de l'homme et des peuples (CADHP), ont publié un nouveau rapport intitulé « **Déclaration conjointe sur la liberté d'expression et les « fausses nouvelles » (fake news), la désinformation et la propagande**, qui vise à présenter les caractéristiques et les normes relatives à la désinformation, en soulignant la nécessité de garantir un environnement propice à la liberté d'expression.

Dans le rapport « **L'impact du désordre de l'information (désinformation) sur les élections** », la **Commission de Venise** a noté que l'Internet avait changé la façon dont les électeurs recevaient les messages politiques et que ce changement pouvait rendre possible la diffusion de fausses informations à une échelle sans précédent.

Les cas et les études présentés ci-dessus ne sont que quelques exemples de la manière dont les tribunaux électoraux ont traité les défis de la désinformation dans les campagnes électorales et des difficultés rencontrées pour y faire face.

III. Micro-segmentation et personnalisation : de l'ingérence électorale à la manipulation politique

Leyre Burguera Ameave
Professeur de droit constitutionnel
Faculté de Droit
Universidad Nacional de Educación a Distancia (UNED)
lburguera@der.uned.es

Toute campagne électorale réussie nécessite une connaissance précise des destinataires finaux du message politique. L'analyse des intérêts et des préoccupations des électeurs permet d'élaborer une communication électorale efficace.

Cette finalité a toujours été présente dans l'organisation des campagnes électorales (par le biais de sondages, de focus groups, etc.), mais c'est peut-être aujourd'hui, avec l'émergence du *big data*, que nous sommes plus conscients de son potentiel et des risques qu'il comporte.

Glossaire

Différentes stratégies sont actuellement utilisées pour influencer les messages politiques par le biais de la désinformation ou de la manipulation, dans le but de promouvoir certains objectifs politiques et de saper le déroulement normal des processus électoraux démocratiques. Parmi celles-ci, l'utilisation des techniques de ***microciblage*** (***microtargeting***) et de personnalisation des messages pour concevoir et élaborer la communication électorale mérite une attention particulière.

La manipulation politique et les tentatives d'ingérence indue dans les processus électoraux par le biais de ces deux techniques ont lieu dans le monde entier depuis plus d'une décennie. Des cas paradigmatiques comme la campagne d'Obama en 2012 ou les élections parlementaires indiennes de 2014 ne sont que deux exemples initiaux qui ont ensuite connu un impact plus important au Royaume-Uni (référendum sur le Brexit), en France (élections de 2017) ou aux États-Unis (campagnes de Donald Trump ou d'Hillary Clinton en 2016).

Cette situation est due, en partie, à l'expansion de l'utilisation des réseaux sociaux et au fait que le travail de collecte et d'analyse des données stockées dans ces outils s'est professionnalisé et sophistiqué avec le temps. En conséquence, les réseaux sociaux ont été au centre des préoccupations concernant la publicité électorale ciblée sur des groupes d'utilisateurs spécifiques et le manque de transparence du processus.

La **micro-segmentation** et la personnalisation du message électoral s'expliquent par une inertie communicationnelle qui ne doit toutefois pas être considérée comme négative. Elle pourrait en effet favoriser la motivation et l'engagement politiques, et ainsi augmenter la participation des électeurs aux processus électoraux.

Toutefois, leur conception et leur utilisation par les partis politiques ne sont généralement pas motivées par des intentions aussi sincères ; au contraire, elles cherchent à améliorer la collecte de fonds (dans les pays où le financement des campagnes est essentiellement privé) et à mobiliser l'électorat à un point tel qu'elles peuvent encourager les campagnes négatives, en polarisant et en fragmentant l'électorat lui-même. Ils facilitent également l'ingérence, l'atteinte à la vie privée et au droit à la protection des données personnelles, ainsi que la création de chambres d'écho et de bulles épistémiques.

En discutant des risques potentiels de ces deux outils, le texte fera spécifiquement référence à l'utilisation du *big data* et de l'intelligence artificielle dans ce domaine. La collecte et le traitement de données par des organisations politiques à des fins de communication politique, ainsi que l'utilisation des techniques modernes susmentionnées, ont suscité de nombreux débats et préoccupations quant aux limites à appliquer, y compris le droit à la protection des données à caractère personnel.

Les problèmes et les défis à relever concernent principalement deux questions interconnectées : l'obtention des données nécessaires à la conception des « campagnes axées sur les données » d'aujourd'hui en relation avec le respect des réglementations en matière de protection des données à caractère personnel, et la détermination de l'utilisation de ces données en relation avec les stratégies de désinformation organisée de plus en plus fréquentes. À tout cela s'ajoutent les vulnérabilités des structures technologiques et de leurs modèles économiques, la variété des dispositifs permettant d'obtenir des données, le développement de l'intelligence artificielle, l'assujettissement réglementaire des entreprises technologiques, etc.

Cependant, dans le cas spécifique de la **micro-segmentation**, les risques associés à son utilisation seront abordés. Il s'agit notamment des risques de manipulation politique, car cette technique diminue la capacité critique des citoyens, et de distorsion du processus électoral, car elle peut changer explicitement les règles et les normes.

Dans le cas de la **personnalisation**, les risques associés à son utilisation sont liés à la configuration d'une vision limitée du monde. En effet, elle individualise les informations reçues par les citoyens, réduisant leur vision du monde et la renvoyant à une sorte de bulle d'information. De cette manière, la capacité du citoyen à se forger une opinion et à comprendre ceux qui pensent différemment est clairement limitée.

Cette situation entraîne une fragmentation sociale et politique qui réduit la capacité de dialogue de la société dans laquelle cette technique s'insère.

En bref, des préoccupations qui se sont accrues avec la publication de certains cas de traitement illégal de données personnelles dans le but d'influencer l'opinion politique des électeurs (un cas paradigmatique est celui de *Cambridge Analytica*), et qui ont conduit certains pays à réglementer plus ou moins strictement les questions mentionnées ici. C'est le cas, par exemple, de l'autorité italienne de protection des données (Garant pour la *Protezione dei Dati Personali*) qui, le 6 mars 2014, a publié son document *« Provvedimento in materia de trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale* ». En novembre 2016, l'autorité française *(Commission nationale de l'informatique et des libertés*) l'a fait avec, entre autres, le titre *« Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? »* En avril 2017, l'autorité britannique (*Information Commissioner´s Office*) a approuvé son *« Guidance on political campaigning* ». En outre, le Contrôleur européen de la protection des données a publié le 18 mars 2018 son avis 3/2018 sur la manipulation en ligne et les données à caractère personnel (« avis du CEPD sur la manipulation en ligne et les données à caractère personnel ») et la Commission européenne, à l'approche des élections du Parlement européen de 2019, a adopté le 12 septembre 2018 ses orientations sur l'application des règles européennes en matière de protection des données dans le contexte des élections (« *Orientations de la Commission relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral* »).

Ce texte mentionnera également les deux principaux concepts mentionnés ci-dessus : le microciblage (*microtargeting*) et la personnalisation de la politique, et soulignera l'importance d'examiner d'autres concepts liés, directement ou indirectement, aux deux questions soulevées dans cette contribution. Ainsi, dans ce travail, l'attention est portée sur des notions ou des idées telles que : Web 2.0, réseaux sociaux, profilage, neuromarketing, bulle épistémique, chambre d'écho, données massives *(big data),* falsification numérique *(deep fake),* apprentissage profond *(deep learning),* exploration de données *(datamining), bots*, etc.

Parmi tous les concepts à prendre en compte, il faut d'abord évoquer le **microciblage** (microtargeting), également appelé « ciblage d'audience », « microciblage » ou « micro-segmentation », qui se définit comme la technique de marketing consistant à cibler des messages adaptés aux caractéristiques personnelles des destinataires afin d'influencer leur comportement de consommation. L'objectif est de cibler des messages sur mesure basés sur les données collectées sur chaque individu, combinées à celles collectées à d'autres niveaux, afin d'influencer leur positionnement politique et leur comportement électoral.

La **personnalisation de la communication** consiste à utiliser cette stratégie de collecte de données, ce qui crée un déséquilibre du pouvoir entre les citoyens et les groupes qui contrôlent les données. En effet, elle favorise la manipulation de l'information et la polarisation politique.

Cas

Afin de compléter la signification et l'application des termes abordés, une analyse de la législation actuelle et de la jurisprudence particulièrement pertinente sera effectuée.

Sur le plan législatif, des mesures importantes ont été prises, comme la loi n° 19 884 de 2017 adoptée au Chili, qui réglemente la publicité électorale payante dans son article 2, ou la loi électorale de 1993 adoptée en Nouvelle-Zélande, section 3, qui considère que les opinions politiques personnelles ne sont pas de la publicité électorale. Nous analyserons également deux codes électoraux, tous deux datant de 2014, qui réglementent ces termes (micro-segmentation et personnalisation), mais sous des angles différents. Dans le cas du code électoral géorgien, l'article 51.11 aborde ces questions en affectant les exigences relatives aux sondages d'opinion. L'article 235.5 du code électoral japonais traite de l'utilisation d'un faux nom et punit les infractions éventuelles d'une amende ou d'une peine d'emprisonnement.

Au niveau jurisprudentiel, il convient de souligner, entre autres, l'arrêt 76/2019 du 22 mai 2019 de la Cour constitutionnelle espagnole, qui résout le recours en inconstitutionnalité déposé par le Défenseur du peuple concernant le premier paragraphe de l'article 58 bis de la loi organique 5/1985 du 19 juin sur le système électoral général, incorporé par la loi organique 3/2018 du 5 décembre sur la protection des données à caractère personnel et la garantie des droits numériques. Cet article 58 bis stipule que : « 1. La collecte de données à caractère personnel relatives aux opinions politiques des individus par les partis politiques dans le cadre de leurs activités électorales ne sera couverte par l'intérêt public que si des garanties adéquates sont fournies ». L'indétermination de l'expression « garanties adéquates » a été décisive pour que ce tribunal confirme la nullité de la disposition légale qui autorisait la collecte par les partis politiques de données personnelles relatives aux opinions politiques des citoyens. Auparavant, l'Agence espagnole de protection des données (AEPD) avait publié la circulaire 1/2019 du 7 mars, dans laquelle elle interprétait le nouvel article, établissait certains critères et tentait de mettre en place certaines garanties. Elle n'a pas suffi face à l'ampleur de la controverse soulevée par la possibilité d'un profilage idéologique au service de la personnalisation du message électoral.

De même, il conviendra d'examiner, entre autres, la décision du 3 septembre 2001 du Tribunal Électoral du Pouvoir Judiciaire de la Fédération (TEPJF) du Mexique, qui

étudie un cas de campagne négative en déclarant ce qui suit : « Bien que le débat politique bénéficie d'une protection renforcée, l'électorat ou la citoyenneté ne doit pas être confondu par la propagande politico-électorale, car celle-ci a un impact négatif sur la formation d'une opinion informée et consciente pour l'exercice du droit de vote, ce qui pourrait avoir un effet vicieux sur la configuration du système politique national lui-même ». Par conséquent, l'impact de la désinformation réalisée à l'aide de techniques spécifiques de collecte et de manipulation de l'information sera au cœur de notre réflexion.

En Espagne également, la doctrine de la Commission électorale centrale (CEC) est révisée sur la base de l'instruction publiée en 2007, qui met sur un pied d'égalité les instruments ou mécanismes de communication traditionnels et les nouveaux outils, sans tenir compte de leur potentiel. C'est pourquoi, ancrée dans un règlement à la perspective analogique, elle n'est pas en mesure de traiter efficacement et immédiatement les nombreux défis qui se posent lors de chaque élection. Dans ce sens, nous analyserons, à titre d'exemple, l'Instruction 1/2021, du Conseil central électoral, du 13 mai, sur la diffusion de la propagande électorale au moyen d'envois dans lesquels le destinataire n'est pas identifié par son nom (BOE nº 119, du 19 mai 2021), qui interprète l'article 39.3 de la loi organique sur le système électoral général (LOREG), modifié par la troisième disposition finale de la loi organique 3/2018, du 5 décembre, sur la protection des données à caractère personnel et la garantie des droits numériques, qui introduit le droit des électeurs de s'opposer à leur inscription dans les copies de la liste électorale fournies aux représentants des candidatures pour l'envoi de la propagande électorale par voie postale.

En général, et en ce qui concerne les termes analysés, il existe des cas significatifs dans lesquels les plaintes déposées auprès de la CEC sont rejetées au motif que la participation à des réseaux sociaux n'entraîne aucune interdiction (à condition qu'elle n'implique aucun type de contrat commercial pour sa mise en œuvre). La frontière entre la publicité (cachée ou non) et l'information est floue, surtout lorsqu'il s'agit d'Internet. Les accords couvrant la période 2005-2022 sont passés en revue et examinés.

IV. Intervention de tiers dans la campagne

Rafael Rubio Núñez
Universidad Complutense, Madrid
rafa.rubio@der.ucm.es

La généralisation des technologies de l'information et de la communication **(TIC)** a transformé la nature des **campagnes électorales**, qui sont passées d'une proposition de communication concentrée dans le temps, menée par les candidats et les médias, à une proposition de communication où des tiers ont la capacité d'influencer directement et efficacement le résultat final. Ce type d'influence n'est pas nouveau, il existait déjà à travers les dons et la participation des acteurs publics aux campagnes, mais aujourd'hui, de nouveaux acteurs entrent en jeu, notamment les personnes privées sans affiliation à un parti politique ou à un candidat.

Par conséquent, l'utilisation généralisée de la technologie dans les élections entraîne une augmentation de la participation des tiers à la campagne et de son impact. Bien qu'il ne s'agisse pas à l'origine d'un problème technologique en soi, celle-ci prend une nouvelle dimension avec la technologie. Traditionnellement, la participation d'acteurs extérieurs au processus électoral aux campagnes électorales était presque exclusivement liée au financement des campagnes électorales par des tiers, soit en contribuant à la campagne officielle, soit en organisant des campagnes sur des questions spécifiques, dans le but d'influencer le programme des candidats. À ces formes de participation des individus et des groupes de la société civile, il convient d'ajouter l'implication des fonctionnaires (qui doivent rester neutres dans le processus) ou des médias (dont le rôle est de plus en plus réglementé), qui ont longtemps fait l'objet d'une réglementation, mais dont le rôle a changé en raison des progrès technologiques.

L'émergence de ces nouveaux acteurs, ou la transformation du rôle de certains des acteurs traditionnels sans lien direct avec les candidatures, soulève de nouvelles questions pour la réglementation existante. Il est nécessaire d'apporter une réponse juridique à de nouvelles situations telles que les actions d'individus ou d'organisations sociales qui ont un impact sur les élections, la possibilité d'anonymat, le rôle d'acteurs étrangers dans les processus électoraux ou encore l'utilisation de *bots* qui peuvent menacer l'équité de la compétition électorale.

Si, comme l'affirme Sartori (1993 : 76-77), « [l]'autonomie de l'opinion publique (...) entre en crise, du moins en crise de vulnérabilité, avec l'apparition de la radio, et plus encore avec la télévision », les nouvelles technologies de l'information transforment radicalement le concept d'opinion publique en un puzzle d'opinions de

groupe, sans relation apparente entre elles. Cette fragmentation rend alors impossible le dialogue, qui est l'essence même de l'idée de façonner l'opinion publique.

Glossaire et cas

Traditionnellement, la participation des médias, des candidats, des partis politiques et des autorités aux campagnes est prise en compte. Tous les autres acteurs politiques ont été considérés comme étant en dehors de ce cadre ou comme n'ayant aucune importance. L'émergence des technologies de la communication a modifié les règles du jeu et l'adaptation de ces acteurs leur confère un rôle différent.

Tout d'abord, l'utilisation abondante de ces plateformes par les autorités publiques et les organismes publics dans le cadre de campagnes se distingue par son ampleur. En augmentant la fréquence de leurs communications et les moyens de diffusion de leurs actions, ils peuvent déséquilibrer la compétition électorale avec une plus grande fréquence et un plus grand impact, directement et au moment où l'impact est le plus fort, à la fois par le biais de publications et de contrats de publicité, affectant ainsi l'équité du processus, avec le risque de détournement de fonds publics.

Les organes électoraux tels que la CEC et le TEPJF se sont exprimés sur ce point, qui est peut-être le plus courant, mais aussi le moins nouveau, car il est antérieur à Internet. D'une part, il est intéressant de voir comment, au Mexique, le TEPJF (SUP-RAP-288/2009, SUP-RAP-318/2012) a étendu aux dirigeants, affiliés, militants et sympathisants des partis politiques les obligations constitutionnelles en matière de propagande politique et électorale dans des matières telles que l'obligation de s'abstenir, dans le débat politique et électoral, de dénigrer les institutions et les partis ainsi que de calomnier les personnes. « Toute lecture en ce sens que cette obligation ne contraint que les partis politiques est inacceptable ».

De l'autre côté, il y aurait plus d'interdictions : les réalisations de campagne ne seraient pas autorisées dans les événements publics diffusés sur le web ni les publications électorales dans les comptes et pages officiels des municipalités, des ministères ou de la présidence (CEC entre autres). **196/2011 ; 206/2011 ; 459/2015 ; 601/2015 ; 166/2016 ; 212/2016 ; 293/841 ; 293/842 ; 293/863 ; 293/864 ; 293/869 ; 293/880 ; 293/882 ; 293/891 ; 293/892 ; 293/898 ; 293//901**). Il s'agit également d'un phénomène courant au Mexique, où l'obligation de neutralité des autorités, y compris dans les réseaux sociaux, a été soulevée dès le début**(SUP-RAP-57/2010 ; SUP-RAP 105/2014**) et où les actions du président López-Obrador ont fait l'objet d'une attention particulière de la part du **TEPJF (SUP-REP-139/2019 et ses accumulés ; SUP-REP-142/2019 ; SUP-REP-185/2020 ; SUP-REP-193/2021 ; SUP-REP-312/2021 et ses accumulés ; SUP-REP-382/2021 et ses accumulés**).

Il en va de même pour les médias, dont la définition se brouille au point de perdre le monopole de l'information électorale. Comme le prévoyait Cotino (2008) il y a 15 ans, « [l]es médias de masse traditionnels ne sont plus un pilier fondamental du système démocratique ou, à tout le moins, ils ne sont plus le seul pilier fondamental. L'édifice démocratique est soutenu par de nombreux autres « piliers » du réseau. L'extension de la protection des médias et des obligations qui leur incombent est remise en question par l'émergence de « médias » express ou de « pseudo-médias », qui profitent des facilités offertes par Internet pour créer des sites web *ad hoc* et leur donner l'apparence d'un organe de presse.

Ces plateformes d'information, qui apparaissent et disparaissent en fonction du calendrier électoral, sont soutenues par un site web dans le seul but de donner l'apparence de fiabilité dont jouissent les médias, afin de renforcer la crédibilité de certaines informations. Celles-ci sont généralement diffusées sur les réseaux sociaux avec la participation de réseaux coordonnés d'activistes et de *bots*, ce qui leur permet de diffuser des informations politiques déformées avec la « garantie » d'être considérées comme des médias. Nombre de ces « pseudo-médias », qui ne répondent guère aux normes habituelles de rigueur nécessaires à l'exercice de la profession de journaliste, deviennent les sources d'information les plus largement diffusées pendant la campagne, comme ce fut le cas lors de la campagne présidentielle américaine de 2016, avec des médias créés et gérés depuis une petite ville de Macédoine, Veles (Peirano, 2019) ou les élections présidentielles françaises de 2017, où des médias comme *Sputnik* ou *Russia Today*, après avoir créé une version française pour les élections, ont été parmi les plus consultés tout au long du processus, avec plus de 2 millions d'interactions en un mois. Un phénomène particulier, généralement lié aux médias, est la publication d'informations inadmissibles à certaines périodes, telles que les résultats avant la fermeture des bureaux de vote ou les sondages quelques jours, voire quelques semaines, avant l'élection. C'est le cas au **Costa Rica (ST. Cour suprême, 2018**), où la diffusion des résultats d'une enquête nécessite une autorisation.

Parallèlement à la transformation du rôle des acteurs traditionnels, l'application de la technologie aux campagnes électorales permet, comme nous l'avons vu, l'émergence de nouveaux acteurs susceptibles d'influencer la campagne et d'en accroître l'impact. Comme l'a souligné Clift dès 2007, « certains individus et groupes informels peuvent utiliser Internet pour influencer les résultats électoraux, indépendamment des partis ». Comme nous l'avons vu, il est aujourd'hui à la portée de beaucoup de diffuser des informations en faveur ou contre une option politique, sans lien avec les campagnes officielles, avec un taux d'audience et un impact plus élevés. Tout le monde peut poster un message de soutien ou de critique sur ses réseaux sociaux, rediffuser des messages officiels de campagne ou même demander à ses abonnés de voter... mais aujourd'hui, ces activités peuvent influencer les résultats des élections. Cela renforce

la décentralisation des campagnes électorales, qui ressemblent de plus en plus à un échange où de nombreux expéditeurs communiquent avec de nombreux destinataires sur différentes plateformes sociales.

Ainsi, outre les candidats, les partis politiques et les médias, les « suspects habituels » de la réglementation électorale actuelle, il convient de prêter attention au rôle des organisations et des individus sans lien formel avec les candidatures et au rôle des plateformes sur lesquelles ces individus diffusent des informations relatives à la campagne. Ces nouveaux acteurs peuvent être réels, comme les influenceurs qui, volontairement ou par appât du gain, ont commencé à utiliser leurs réseaux sociaux pour soutenir certaines candidatures politiques, ou créés artificiellement par des organisations étatiques comme l'agence russe *Internet Research Agency* (IRA) qui, lors de la campagne présidentielle américaine de 2016, a créé des dizaines de groupes pour favoriser l'instabilité du processus. Un échantillon de six par Jonathan Albrighth *(Tow Center for Digital Journalism*) indique la génération de plus de 340 millions d'interactions au cours du processus (Peirano, 2019).

Le **droit de vote (voter et être voté)** est directement lié à la campagne électorale, qui, en termes juridiques, fonctionne dans un équilibre permanent entre la **liberté d'expression et d'association**, un droit qui est renforcé dans l'arène politique et en particulier dans la campagne électorale, et l'équité de la campagne. Comme l'a déclaré la Cour CIDH en 2004 (paragraphe 88), « [L]'exercice des droits politiques et la liberté de pensée et d'expression sont intimement liés et se renforcent mutuellement ». Cependant, nous ne pouvons ignorer le fait que la participation de tiers, protégés dans l'exercice de leurs droits fondamentaux, peut affecter **l'équité** du concours, qui vise à garantir l'égalité des chances entre les candidats, et affecter ainsi d'autres droits fondamentaux tels que le droit de vote. L'iniquité est étroitement liée à la **liberté de suffrage**, en supposant qu'une plus grande exposition d'une candidature conditionne la libre participation de l'électeur, et à l'authenticité du vote, en évitant les interférences qui faussent la volonté des citoyens ; dans ce cas, il s'agit de fournir une certitude sur l'origine, la destination et la limite des ressources utilisées dans les campagnes politiques, afin d'empêcher les options politiques d'obtenir des avantages indus.

Le **droit de vote** requiert une participation active pour garantir la possibilité pour les électeurs de former et d'exprimer librement leur opinion ainsi que de choisir leurs représentants. La liberté d'expression (en particulier dans le débat politique) et les élections libres sont des droits qui se complètent mutuellement, mais il ne fait aucun doute que l'équité électorale peut parfois entrer en conflit avec la liberté d'expression d'autrui. Il est donc essentiel d'adapter le cadre juridique et les obligations légales en matière de liberté d'expression à la nouvelle dynamique des campagnes électorales. Dans ce nouveau contexte, garantir les conditions d'un environnement de campagne équitable dans l'arène numérique implique un certain nombre de défis

supplémentaires pour préserver la liberté d'expression sans porter atteinte au principe d'équité.

Ainsi, la règle générale a été de considérer ces activités de particuliers pendant la campagne électorale comme un exercice de la **liberté d'expression**. Ces comportements ont été considérés comme des conduites spontanées, libres et individuelles, basées sur la difficulté qu'ont ces personnes à avoir une influence décisive et, dans le cas où cette capacité existe, sur la légitimité de leur action publique. Le problème se pose dans les cas où l'on peut douter de la spontanéité de ces actions, en raison d'une **interférence** d'acteurs nationaux et **étrangers**. Ces activités peuvent être clairement détectées lorsqu'il y a un paiement pour ces interventions et, de manière plus douteuse, lorsqu'il y a des formes d'action coordonnée qui pourraient impliquer une relation avec la campagne et donc affecter **l'impartialité et l'équité de l'élection.**

La généralisation du **web 2.0**, avec l'extension du **contenu généré par les utilisateurs** (articles de blog, vidéos, photos...) facilite la participation d'individus ayant une capacité d'influence***(influenceurs***). Mais ce n'est pas non plus une nouveauté. Dans l'affaire *Time, Inc. vs. Firestone*, 424 USA. 448 (1976), la Cour suprême a distingué les personnalités publiques de celles qui jouissent d'une importance particulière dans la perception de la société, de la capacité d'exercer une influence et une persuasion dans la discussion de questions d'intérêt public et de développer une participation active dans la discussion de controverses publiques spécifiques dans le but de faire pencher la balance vers la résolution des questions en jeu.

Cette capacité d'influence menace donc la règle générale, surtout lorsque le nombre de personnes supposées avoir une capacité d'influence sur les réseaux sociaux augmente, s'étend, ou effectue ces conduites en dehors de ceux-ci, amplifiant leurs effets par ces canaux (**SUP-REC-1874/2021 et SUP-REC-1876/2021 et ses accumulées**), surtout lorsqu'elles le font de manière rémunérée et coordonnée par le biais de **campagnes d'influence**. Dans ce sens, différents organismes électoraux se sont prononcés, notamment l'INE et le TEPJF, sur l'interdiction de ce type de campagnes de soutien pendant les périodes électorales, à l'occasion des campagnes de soutien au Parti Vert aux élections de 2015 et 2021, pendant l'interdiction électorale, et sur l'obligation de déclarer les dépenses engagées dans ce domaine, à des fins de transparence et de calcul du plafond électoral (**SUP-RAP-542/2015 et ses accumulées et SUP-RAP-172/2021**), étant donné qu'il s'agissait d'actions coordonnées dans lesquelles le paiement à certains des participants a été démontré.

De même, **le ST. Le Tribunal électoral régional de Rio de Janeiro en 2018** a forcé la suppression de messages publiés par des ***blogueurs*** indiquant leur désir de nommer un candidat particulier avant le début de la campagne électorale. Il convient

de souligner trois autres arrêts **du TEPJF (SUP-REC-00887-2018 et SUP-RAP-180/2021 et ses accumulés[7] et SUP-REC 143/2021**) dans lesquels la porte est ouverte pour que ce type de tiers puisse apporter un soutien spécifique à condition qu'ils ne reçoivent aucun type de rémunération en contrepartie, établissant ainsi une sorte de présomption de spontanéité.

Dans ce contexte, le comportement inauthentique apparaît également comme une forme d'influence électorale de la part de nouveaux acteurs. Elles reposent largement sur l'**anonymat**, facilité par la technologie. Dans l'anonymat, les tiers que nous étudions pourraient mener des campagnes qui profiteraient de la liberté de ne pas être soumis à la réglementation électorale pour aller au-delà des règles de la campagne électorale, tant en termes de contenu, avec des campagnes négatives ou la publication d'informations non autorisées lors de la période de silence électoral, en évitant le contrôle déjà signalé lorsque ces actions sont menées par des personnes ayant une capacité d'influence avérée. Cet anonymat rend l'identification difficile, voire impossible, et ouvre la porte à **l'usurpation d'identité** et rend encore plus complexe le contrôle et la responsabilité en cas de violation des interdictions établies.

Il est donc nécessaire d'identifier les personnes qui exercent des activités ayant des répercussions électorales, telles que la création de pages d'information diffusant de fausses informations sur les candidats ou le contrat de publicité politique pendant la campagne. Cela soulève la question de la transparence quant à savoir qui ou quel groupe finance ce projet, et comment. Nous trouvons quelques exemples de ce type de campagne, et de la réponse offerte par les organes électoraux, dans la décision de la **CEC espagnole (688/2019)** sur la campagne promue, prétendument par des personnes se faisant passer pour leurs partisans afin de décourager le vote pour des candidatures rivales, ou la **décision du tribunal de Sao Paulo (2015)** selon laquelle Twitter devait fournir au candidat des données sur les utilisateurs qui l'avaient diffamé sur ce réseau social, dans la même veine que la décision de **la Cour suprême de l'Illinois (2015) et,** de manière documentée et systématique, **le *rapport sur l'enquête relative à l'ingérence de la Russie dans l'élection présidentielle de 2016* du ministère de la justice des États-Unis. Toutefois, dans d'autres cas, comme la plateforme « Voto útil »** [vote utile], qui a fourni des outils permettant d'identifier l'option politique la plus susceptible de battre les candidats de Morena lors des élections fédérales du 6 juin 2021, étant donné qu'elle offrait des informations publiques et qu'il n'y avait aucun lien de quelque nature que ce soit, elle a été considérée comme conforme aux règles électorales **(SUP-REP-319/2021)**.

L'anonymat est étroitement lié à l'utilisation massive de ***bots***, de « faux » comptes anonymes et automatisés, qui apparaissent sur les réseaux comme un utilisateur

[7] https://www.te.gob.mx/sentenciasHTML/convertir/expediente/SUP-REC-00887-2018 et https://www.te.gob.mx/EE/SUP/2021/RAP/180/SUP_2021_RAP_180-1083242.pdf

parmi d'autres. Ces comptes ont pour objectif d'augmenter le volume de distribution de certaines informations en cherchant à faire croire qu'elles sont majoritaires et de créer artificiellement un courant d'opinion, d'acceptation ou de rejet de certaines idées ou de certaines personnes (Sánchez Muñoz, 2020) : 34-40). Bien que les plateformes les aient dans le collimateur et agissent régulièrement pour les retirer de l'espace public, la facilité avec laquelle ils peuvent être créés et gérés grâce à des mécanismes d'intelligence artificielle a donné lieu à une véritable guerre technologique, dont les États sont de simples spectateurs. Les décisions des plateformes, généralement prises sans procédure claire ou garantie, peuvent en outre mettre en péril les droits fondamentaux des personnes concernées, qui voient leurs comptes supprimés sans pouvoir rien faire pour l'empêcher ou les récupérer. Un autre type de menace dans ce domaine est celui des ***trolls***, qui, à partir de leurs comptes personnels, de l'anonymat ou de l'utilisation de faux comptes, contaminent la conversation sur le réseau, parfois jusqu'à la menacer ou la rendre physiquement violente, souvent par le biais de campagnes coordonnées de comportements inauthentiques.

L'achat de **propagande électorale** (***electionering***) sur les réseaux sociaux peut également soulever des questions liées à son acquisition par des tiers. Certains pays, comme l'**Albanie**, interdisent la passation de contrats de publicité électorale avec des personnes qui ne participent pas aux élections (**code électoral de 2012, article 84**) ou le **Canada**, qui distingue la publicité de l'opinion personnelle exprimée sur les réseaux (**loi électorale, article 319**), mais cette interdiction n'est pas universelle et il est toujours possible de passer des contrats de publicité en période électorale avec une intention électorale, même si elle n'est pas identifiée en tant que telle. Si, dans le cas des campagnes de soutien à une candidature, il n'y a aucun doute sur la contribution en nature et la nécessité de la comptabiliser comme telle, le problème se complique lorsqu'il s'agit de campagnes attaquant d'autres candidats, comme celles qui ont eu lieu en Colombie lors de la dernière campagne présidentielle, ou de publicités thématiques, qui ne sont pas directement identifiées à une candidature.

Dans ces cas, de nouveaux conflits apparaissent liés à la coordination, ou à l'absence de coordination, de ces actions avec la campagne officielle, ou à la soumission de ces campagnes publicitaires à des échéances électorales qui limitent la publicité au temps de la campagne officielle et l'interdisent pendant les périodes d'interdiction ou de réflexion. Cet achat affecte des tiers en dehors de la campagne (***rapport sur l'enquête relative à l'ingérence russe dans l'élection présidentielle de 2016*** **par le ministère américain de la justice**, **CEC de l'Espagne (688/2019) ou *l'appel de la représentation* n° 060147858** et ***l'appel interlocutoire de l'appel électoral spécial* n° 060505606**, résolus par le **Tribunal supérieur électoral du Brésil**. Il en va de même pour l'achat de publicité auprès de médias ou de pseudo-médias, qui prétendent faire de la publicité pour leur contenu afin d'essayer d'influencer la campagne (**Costa Rica, XX**), ainsi que pour l'achat de publicité par des entités

gouvernementales, qui interviennent ainsi de manière inappropriée dans la campagne.

Les actions des tiers pendant la campagne affectent également les décisions des plateformes. Celles-ci, en coordination avec les organes électoraux ou de leur propre initiative, adoptent en effet des décisions qui restreignent cette liberté d'expression, telles que la fermeture ou la suspension de comptes, ou la suppression de certains contenus, sans procédure connue au préalable. Cela ouvre la porte aux abus et à l'arbitraire, en particulier lorsque ces décisions sont adoptées de manière automatisée par des algorithmes opaques. Ces actions, auxquelles les États assistent souvent en spectateurs, sont menées sans les garanties nécessaires à la protection des droits affectés, comme si le fait qu'il s'agisse d'entreprises privées les dispensait de respecter les droits fondamentaux. Pour les garantir, ces décisions devraient être prises, au moins pendant les périodes électorales, par les organes électoraux ou au moins dans le cadre d'une procédure claire, transparente et non discriminatoire prévoyant la possibilité de faire appel de la décision, y compris l'obligation de motiver la décision, sous réserve d'un contrôle ultérieur par une autorité judiciaire.

Actuellement, il existe un paradoxe : ces fermetures n'étant pas considérées comme des questions électorales, elles ne bénéficient pas de la protection des organes électoraux dont l'action est limitée aux cas de comptes liés aux partis et aux candidats. On peut citer par exemple la fermeture du compte Twitter officiel du parti politique Vox lors des élections catalanes (2021) ou l'élimination des canaux WhatsApp de tous les partis politiques lors des élections générales d'avril 2019. Dans le cas des contrats de publicité pour des tiers, en l'absence de réglementation claire, les plateformes ont initialement choisi de qualifier cette publicité de politique et de fournir des informations sur les personnes qui ont payé pour celle-ci (afin que les organes électoraux puissent considérer ces paiements comme des contributions de campagne, les inclure dans les rapports et les appliquer au plafond des dépenses). Dans certains pays, les plateformes elles-mêmes ont fini par interdire la passation de contrats de publicité électorale à tout acteur ne faisant pas officiellement partie de la campagne (partis et candidats) et par exiger une identification spéciale.

En outre, il est important de noter que tous les comportements décrits ci-dessus peuvent être adoptés à l'intérieur ou à l'extérieur de l'espace où se déroulent les élections. Il s'agit des actions d'individus, de groupes ou même de médias, situés « virtuellement » en dehors de nos frontières, qui, depuis leur « extraterritorialité », peuvent mener des actions inadmissibles visant à influencer le processus électoral (**campagnes d'ingérence**). Ce phénomène, qui s'est manifesté pour la première fois lors de la campagne présidentielle américaine de 2016 avec l'ingérence avérée de la Russie, s'est amplifié depuis (à partir d'Oxford 16) et pose des défis à la réglementation existante. En effet, l'achat de publicité sur les plateformes numériques pendant le jour de réflexion (interdiction électorale) ou la publication d'informations

électorales, comme les résultats des sondages de sortie des urnes, pendant le jour même de l'élection, ce qui est généralement interdit.

Ces campagnes profitent également de leur anonymat pour promouvoir des actions de faux mouvement de base (***astroturfing***), qui consiste à créer de faux profils sur les réseaux sociaux, et qui est beaucoup plus difficile à contrôler. Bien que les plateformes aient commencé à prendre des mesures pour prévenir ce type d'ingérence externe, ce type d'intervention pose de nouveaux problèmes en matière de contrôle, de preuve et d'adoption de mesures, et l'interdiction de tout type d'action avec des contenus électoraux provenant de l'étranger (identifiés ou anonymes, légaux ou illégaux) est de plus en plus envisagée. Pour cela, la collaboration des plateformes est essentielle.

Conclusions

Tout cela soulève un débat sur le rôle des citoyens et des groupes dans la campagne électorale, ainsi que sur l'établissement d'obligations et de limites à leurs activités, qu'il s'agisse de solliciter des votes (campagnes non officielles), de critiquer des partis ou des candidats (campagnes négatives), d'envoyer des informations non sollicitées à leurs contacts ou de contracter des publicités en faveur ou au détriment d'une option particulière... Car au-delà de l'exercice légitime de la liberté d'expression, ces nouvelles possibilités de participation à la campagne ouvrent en effet la porte à de nouvelles stratégies pour les partis et les candidats, qui peuvent s'appuyer sur des tiers pour mener des actions qui, en raison de leur contenu, du moment où elles sont menées ou de leur coût, ne peuvent l'être en leur nom propre. En outre, cela offre aux groupes indépendants de partis et de candidats, sans aucun lien, une nouvelle possibilité d'influencer les résultats dans l'exercice légitime de leur liberté d'expression pour défendre leurs idées et/ou leurs intérêts. Réalisée à grande échelle, cette pratique peut affecter l'équité de la campagne et créer une zone d'ombre dans la réglementation électorale existante.

Jusqu'à présent, la réponse s'est concentrée sur le contrôle financier, qui est essentiel pour garantir l'équité. En période électorale, afin de garantir l'égalité des chances entre les forces politiques, des plafonds de dépenses sont fixés pour les campagnes électorales et une plus grande transparence du financement est exigée. Cela implique de rendre obligatoire la fourniture d'informations sur les dépenses de campagne pendant les élections, d'améliorer l'efficacité de la supervision et du contrôle des campagnes électorales, et de prévoir des sanctions en cas de non-respect, qui peuvent aller de l'exclusion d'une candidature à l'annulation de l'élection, en passant par la perte totale ou partielle du financement public. En incluant dans cet audit les actions de tiers qui ont fait l'objet d'un paiement ou qui sont considérées comme ayant été effectuées en raison d'une attente future, on tente d'uniformiser les règles du jeu, non sans difficulté, comme nous le verrons plus loin.

Il est donc nécessaire de définir clairement la réponse des autorités électorales aux actions des tiers dans les processus électoraux, à un moment où celles-ci peuvent être décisives, en fournissant un cadre juridique adéquat.

V. Discours de haine et violence politique fondée sur le genre

Ignacio Álvarez Rodríguez
Professeur associé de droit constitutionnel
Faculté de Droit
Universidad Complutense de Madrid
ialvarez1@ucm.es

Il est important de parvenir à un consensus académique minimum sur l'objet de l'étude, car les experts soulignent qu'il est trop large. Nous nous appuyons sur trois institutions qui ont produit des documents de travail éclairants sur le sujet, à savoir le *National Democratic Institute*. Un autre est l'*Observatoire des réformes politiques en Amérique latine (1978-2021)*, rattaché à l'Institut de recherche juridique (IIJ-UNAM) et à l'Organisation des États américains. Le troisième est l'*Institut National Électoral du Mexique.*

Glossaire

Afin d'explorer le cadre juridique de la violence politique basée sur le genre (VPG) pendant la campagne électorale, il est nécessaire d'utiliser un certain nombre de termes techniques, énumérés dans le glossaire.

Il y a tout d'abord la ***cybercriminalité***, également appelée *cybercrime*, une notion qui englobe toute activité criminelle ou illégale exercée sur Internet. Les exemples incluent l'*hameçonnage*, l'utilisation abusive d'informations personnelles, diverses formes de piratage informatique, les discours haineux et l'incitation au terrorisme, ainsi que la diffusion de pornographie enfantine et d'abus sexuels sur des enfants. Ce type de délit concerne tous les appareils numériques, y compris les ordinateurs, les tablettes et les smartphones, qui sont connectés à Internet.

Deuxièmement, nous devons mettre l'accent sur la ***désinformation sexiste***, c'est-à-dire l'utilisation de fausses informations pour semer la confusion ou induire en erreur en manipulant le sexe comme un clivage social clé pour attaquer les femmes et/ou influencer les résultats politiques.

Troisièmement, il met en évidence le concept de ***discours de haine***, qui couvre de nombreuses formes d'expressions ou d'attaques diffusant, incitant, promouvant ou justifiant la haine, la violence ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes pour une grande variété de raisons. Il englobe également les discours polarisants qui encouragent l'intolérance, la haine et l'incitation à la violence par des références explicites ou indirectes à la race, à l'origine nationale ou ethnique,

à la religion, au sexe, à l'orientation sexuelle, à l'âge ou au handicap ou à d'autres groupes immuables, généralement dans le but de créer une différence tangible au sein d'une institution, d'une organisation ou d'une société.

Quatrièmement, nous avons les ***trolls*** d'Internet. Les trolls sont des utilisateurs humains qui harcèlent, provoquent ou intimident intentionnellement les autres, souvent pour détourner l'attention et semer la confusion ou la discorde. Les trolls peuvent agir en tant qu'individus et, en ce sens, ils partagent de nombreuses caractéristiques avec ceux qui se livrent à des discours haineux dans des formats analogues. Ils peuvent également agir en coordonnant leur comportement avec celui d'autres trolls.

Cinquièmement, nous devons mettre en évidence la ***violence en ligne contre les femmes en politique***, définie comme toutes les formes d'agression, de coercition et d'intimidation des femmes dans le cyberespace simplement parce qu'elles sont des femmes. Elle est également connue sous le nom de cyberviolence à l'encontre des femmes. Le phénomène est exacerbé lorsqu'il se produit sur Internet, car les candidates politiquement actives sont confrontées à diverses menaces de la part d'autres candidats, partis et/ou citoyens.

Réglementations internationales et nationales

Le droit international universel (Nations unies) et régional (Union européenne, Conseil de l'Europe, Organisation des États américains) contribue dans une certaine mesure à la poursuite des comportements violents à l'encontre des femmes en politique.

Il en va de même pour un certain nombre de pays, bien que le soutien soit plus rare et, lorsqu'il existe, plutôt vague et imprécis. Certains disposent d'une législation spécifique en la matière ou ont tenté d'adopter des initiatives de ce type (Chili, Argentine, Allemagne, Bolivie, Bosnie, Brésil, Équateur, El Salvador, Mexique, Panama, Paraguay), tandis que d'autres disposent d'une législation non spécifique qui s'applique à ces cas grâce à la criminalisation du discours de haine (Espagne).

Exemples de constitutions:

1. Texte constitutionnel proposé pour le Chili en 2022 (rejeté par référendum en septembre de la même année), article 27 : « 1. Toutes les femmes, les filles, les adolescents et les personnes de la diversité et de la dissidence sexuelle et de genre ont le droit de vivre sans violence fondée sur le genre dans toutes ses manifestations, tant dans la sphère publique que privée, qu'elle soit perpétrée par des particuliers, des institutions ou des agents de l'État. 2. L'État adopte les mesures nécessaires pour éradiquer tous les types de violence fondée sur le genre et les modèles socioculturels qui la rendent possible, en agissant avec la diligence voulue pour la prévenir, enquêter sur elle et la punir, ainsi que pour fournir des soins, une protection

et une réparation complète aux victimes, compte tenu en particulier des situations de vulnérabilité dans lesquelles elles peuvent se trouver ».

2. Constitution de l'Équateur : article 50.7 : « L'État prend des mesures pour assurer [...] la protection contre l'influence de programmes ou de messages préjudiciables diffusés par tout média, qui encouragent la violence, la discrimination raciale ou sexiste, ou l'adoption de fausses valeurs ».
3. Constitution du Kenya, article 33(2) : « Le droit à la liberté d'expression ne s'étend pas aux manifestations suivantes : a. Propagande de guerre, b. Incitation à la violence, c. Discours de haine, ou d. Prosélytisme de haine qui i. Constitue une incitation à l'encontre d'un groupe ethnique, une humiliation d'autrui ou une incitation à causer des dommages, ou ii. Il est fondée sur tout motif de discrimination spécifié ou visé à l'article 27, paragraphe 4 » (y compris le sexe).

Exemples de législation:

1. Allemagne : Cette loi de 2017 oblige les plateformes à supprimer les contenus potentiellement criminels dans un délai de 24 heures. La même loi exige également la suppression des propos « manifestement illicites » dans les 24 heures suivant le dépôt de la plainte.
2. Argentine : Cette loi de 2019 punit spécifiquement les VPG, y compris de sanctions telles que l'avertissement préalable, la dénonciation des faits sur le lieu de travail de « l'agresseur » ou « l'obligation de participer à des programmes de réflexion, d'éducation ou de thérapie visant à modifier les comportements violents ».
3. Bosnie-Herzégovine : Loi de 2006 interdisant l'utilisation de tout langage, image, symbole, contenu audio ou vidéo incitant à la violence ou propageant la haine.
4. Espagne :
    - Loi organique 1/2015 du 30 mars 2015 modifiant le code pénal : criminalise les discours de haine.
    - Loi 15/2022, du 12 juillet, intégrale pour l'égalité de traitement et la non-discrimination : elle demande aux autorités publiques de prévenir et d'encourager la dénonciation de tout type de violence et de discours de haine.

Cas pertinents

Parmi les cas existants, on peut distinguer ceux qui ont donné lieu à des prises de position administratives et judiciaires.

Prise de position administrative

1. En Espagne : le parti politique *Plataforma per Catalunya (PxC)* a déposé une plainte en 2015 contre un collectif autoproclamé « antifasciste » pour avoir publié sur Internet qu'il défendait l'idéologie nationale-socialiste et fasciste. Les faits, selon la formation, constituaient un délit électoral. Par l'accord 196/2015 du 13 mai, le Conseil électoral central a communiqué que, conformément à l'article 151 de la LOREG, il appartient aux tribunaux ordinaires – et non au Conseil électoral central – de déterminer l'existence et la paternité des infractions présumées visées par la formation.
2. Mexique :
    a. TEPJF, Arrêt SUP-REP-70/2021 : les plaintes VPG doivent être traitées par les organes administratifs électoraux (UTCE-INE).
    b. TEPJF, Arrêt SUP-REP-158/2020 : confirme que les UTCE-INE sont compétentes pour traiter les plaintes de VPG et rappelle qu'il doit y avoir un lien de causalité entre l'allégation de VPG et la compétence matérielle de ces organes.

Prise de position judiciaire

Il y a eu des dizaines d'affaires dans lesquelles les hautes cours d'un même pays (le Mexique) se sont prononcées spécifiquement sur le VPG. Les décisions tendent à protéger les femmes, lorsque les faits et les preuves le permettent, d'un point de vue juridique. Cependant, dans d'autres jugements, les tribunaux ont fait pencher la balance en leur défaveur. Cela devrait donner matière à réflexion, car cela montre que la transformation d'une idéologie politique en droit ne fonctionne pas toujours.

Aperçu des cas (tous TEPJF) :

1. Arrêt SUP-REC-91/2020, qui traite de la légalité d'une liste noire de personnes commettant des VPG. La Cour estime qu'une telle liste est constitutionnelle dans la mesure où elle est justifiée par le devoir des administrations publiques d'éradiquer la VPG. La minorité dissidente a émis une opinion dissidente forte dans laquelle elle a reproché à ses collègues une « politique judiciaire inquisitoriale inappropriée ».
2. L'arrêt SUP-REC-61/2020 établit une distinction entre les actes dits de violence politique et les actes de VPG. Il ajoute qu'en cas de plainte pour VPG, [toutes] les personnes impliquées doivent être notifiées personnellement dans les 48 heures.
3. Arrêt SUP-JDC-156/2019, demandant à l'administration électorale de réévaluer une plainte VPG contre un fonctionnaire qui n'a pas obtenu réparation en première instance.
4. Arrêt SUP-REC-594/2019, dans lequel le VPG est comparé à l'inviolabilité parlementaire. La décision de fond statue que les expressions prétendument

violentes sont couvertes alors qu'il appartiendrait au Congrès de les sanctionner. Une opinion dissidente rappelle que l'inviolabilité parlementaire est une question de constitutionnalité et non de légalité.

5. Arrêt SUP-REC-1388/2018, où le VPG exprimé dans plusieurs vidéos Facebook est étudié, la plaignante est confirmée et une série de mesures sont incluses dans l'arrêt pour indemniser la victime (publication dans la presse qu'elle a été soumise au VPG et élaboration d'un protocole par l'administration publique compétente pour prévenir et éradiquer ces comportements).
6. Arrêt SUP-REC-531/2018, confirmant la légalité de l'annulation d'une candidature électorale en raison de la présence d'expressions VPG.

Cas de référence :

1. TEPJF : Arrêt SUP-REP-140/2020. VPG sous forme de violence numérique. Un candidat se plaint des expressions utilisées dans une vidéo Facebook. La Chambre spécialisée a compris que de telles violences ont effectivement eu lieu, même si la législation nationale de l'époque ne les sanctionnait pas, puisqu'elles étaient déjà prévues par diverses normes internationales, de droit comparé et même jurisprudentielles. La minorité de la Haute Chambre est en désaccord avec l'opinion majoritaire en raison de son caractère vague et imprécis.
2. TEPJF : Arrêt SUP-JDC 111/2019, 3 juillet. Elle donne raison à l'homme contre lequel la plainte a été déposée. Il avait posté sur Twitter une vidéo et un article critiquant la gestion du dirigeant, qui ont également été publiés sur différents portails d'information. Les mots exacts étaient les suivants : (la leader) « déstabilise et divise le parti » ; exclut des personnes comme lui de la candidature parce qu'elles « critiquent ce gouvernement de tricheurs » ; cela « divise MORENA - le parti - et il devrait quitter la présidence » ; la compare à Louis XIV et dit qu'elle « a perdu sa boussole ».
3. TEPJF : Arrêt SUP-REP27/2019. La candidate dénonce les membres de la VPG qui ont diffusé sur les réseaux sociaux une interview qui, selon elle, ne la laisse pas en bonne place. Elle fonde sa demande sur le fait que l'attaque est « simplement due au fait qu'elle est une femme ». Un homme est condamné à une amende de plus de huit mille dollars, mais la Haute Cour annule la décision au motif que son droit à un procès équitable a été violé.
4. TEPJF : Arrêt SUP-REP-623/2018. Une candidate diffuse sur les réseaux sociaux une vidéo dans laquelle une autre candidate est traitée de « sorcière de Blanche-Neige » et affirme que, si vous votez pour elle, vous voterez en réalité pour son mari. La Chambre régionale spécialisée a estimé que les stéréotypes étaient discriminatoires et, par conséquent, constituaient des VPG, une conclusion confirmée par la chambre supérieure pour avoir « subordonné et minimisé les capacités de la candidate à la vie politique ».

5. TEPJF : Arrêt SUP-REP-617/2018. Candidate dénoncée par VPG contre un autre candidat parce qu'il lui a dit lors d'une discussion publique sur Facebook : « Je t'ai enseigné comment travailler ; pauvre de toi, tu es risible et pitoyable ; malheureux et frustré ». En premier lieu, la chambre spécialisée considère ces expressions comme des VPG. Toutefois, en deuxième instance, la chambre supérieure a annulé cette décision au motif que les phrases ne constituaient pas une infraction, compte tenu à la fois de ce qui a été dit et du contexte dans lequel cela a été dit, ainsi que de la trajectoire commune des tous les deux à l'époque, qui s'est terminée par une dispute.
6. TEPJF; arrêt SUP-REP-121/2018 et arrêt SUP-REP-142/2018. Le candidat dénonce le citoyen pour des déclarations faites sur Facebook et dans un blog qui pourraient constituer des VPG. L'organe électoral prend des mesures provisoires et ordonne au citoyen de le retirer. Face au refus de cette dernière, il a été condamné à une amende et a fait appel devant la juridiction qui rend les décisions susmentionnées, au motif que son droit à la liberté d'expression avait été violé. La Chambre supérieure confirme les critères de l'INE et rejette la demande du plaignant.
7. TEPJF ; arrêt SUP-JDC-383/2017. La candidate dénonce le fait d'avoir été soumise à des VPG pour les expressions suivantes sur les réseaux sociaux (en particulier Twitter) : « Delfina est-il un nom propre ? Ou l'appelle-t-on ainsi en raison de la façon dont elle est traitée par la personne qui l'a nommée et qui en est le patron ? » Deuxième expression : « Marionnette ». Troisième expression : « Un désastre en matière de gestion en tant que présidente de la municipalité ». Quatrième expression : « Il est regrettable qu'un marionnettiste veuille gouverner l'État du Mexique ». La chambre supérieure du TEPJF a jugé que les déclarations ne constituaient pas des VPG et qu'elles n'étaient pas dirigées contre la plaignante en raison de son sexe, et qu'elles ne l'affectaient pas de manière disproportionnée. Même si les actes sont offensants, poursuit la résolution, cela ne signifie pas pour autant qu'il s'agit d'une violence politique à l'encontre d'une personne. En outre, ajoute le Tribunal, dans les processus électoraux, les candidats doivent faire preuve d'une plus grande tolérance à l'égard des critiques désobligeantes, sévères ou fortes, car la liberté d'expression et, en particulier dans ce cas, la liberté d'information, répondent à un intérêt général plus important.

Conclusions critiques

Il est symptomatique et révélateur que nous ne sachions même pas comment appeler cette « violence » : violence fondée sur le sexe, VPG, violence à l'égard des femmes en politique, violence fondée sur le sexe à l'égard des femmes politiques. Deux autres problèmes sont étroitement liés à ce diagnostic. D'une part, personne ne sait ce qu'est réellement cette violence d'un point de vue juridique. Cependant, nous savons que les

démocraties constitutionnelles sont ou étaient déjà dotées d'un arsenal normatif (y compris pénal) pour lutter contre certaines choses.

Si l'on entend par VPG l'interdiction de tout mauvais traitement, l'éradication de la violence physique ou, en bref, le fait d'éviter ou de tenter de compenser tout type de préjudice juridiquement intolérable pour les femmes (et les hommes), le concept est inopérant parce que de tels comportements - et bien d'autres encore - ont déjà été couverts et sanctionnés de manière adéquate. Par ailleurs, rappelons que la coexistence humaine dans la liberté s'accompagne toujours de perturbations et de bruits qui provoquent des frictions, des désaccords, des manifestations outrancières, et d'autres conditions issues du *zoon politikon*. Si le concept n'est pas seulement destiné à « nommer » une réalité, mais à en construire une *ad hoc*, où les femmes sont maintenues dans des bulles, traitées comme des êtres ayant un besoin permanent de protection et de soins, et où l'on suppose que les mots peuvent blesser autant que les actes, la violence politique fondée sur le genre perpétuera ce qu'elle veut combattre, ainsi que la mise au pilori ininterrompue de ceux qu'elle prétend vouloir protéger à tout prix.

D'autre part, la liberté d'expression, en tant que droit fondamental, doit prévaloir, même avec les limites qui s'imposent. N'oublions jamais que si la liberté d'expression est un droit fondamental qui rayonne sur tous les autres et trouve sa place dans la meilleure tradition constitutionnaliste, l'incitation à la haine est une notion faible et brumeuse créée au détour d'une phrase qui, dans la version que nous avons étudiée ici - la VPG - ne se révèle pas très opérante. Elle l'est encore moins lorsqu'elle est exercée dans des contextes politico-électoraux où le pouvoir se dispute bec et ongles. En épuisant le raisonnement libertaire, il y aura toujours un certain degré d'expression « forte », puisque, avec la liberté d'expression, nous voulons convaincre les autres de la bonté de la nôtre et provoquer un choc des idées. La VPG revient à dire : « Donnez-nous un chèque en blanc et nous, quelques-uns (les quelques *élues*), nous chargerons de gérer le montant ».

Cette question de la VPG dépend beaucoup de la région, du pays, des systèmes constitutionnels (s'il y en a), de la réglementation et du respect des règles électorales, des systèmes juridiques, bref, de tant de variables qu'il est difficile d'extraire des règles générales, en dehors de celle-ci : les accusés sont des hommes et les victimes présumées sont des femmes. Avec de telles mentalités, l'idée est véhiculée, à titre d'exemple, que les hommes engagés dans la lutte contre le trafic de drogue comptent moins que les femmes dans la même situation. Cela pose un vrai problème, car il y a encore des hommes et des femmes courageux qui défient quotidiennement la terreur imposée par ce trafic.

Il faut ajouter que le genre est un concept abscons, confus et bigarré, sur lequel personne ne s'accorde, au contraire, pas même ceux qui en défendent la validité et la légitimité. Certains disent qu'il faut le centraliser, d'autres qu'il faut le détruire. Certains disent que les discriminations de genre seront détruites grâce au genre, et d'autres

parlent même d'*effacer* le sexe, comme si s'attaquer à la nature biologique la plus élémentaire de l'être humain était une chose dont on pouvait sortir indemne (Macbeth l'a déjà dit : « Les actes contre la nature engendrent des perturbations contre la nature »).

VI. Modération dans l'espace numérique en période électorale

María Garrote
Faculté de droit, Universidad Complutense de Madrid
magarrot@ucm.es

La fonction de modération des plateformes numériques pendant la période électorale est, comme nous l'avons vu, l'un des points essentiels de la réponse aux menaces technologiques dans la campagne électorale. Il est donc nécessaire de souligner les risques qui peuvent découler de cette fonction, pourtant absolument nécessaire.

Les procédures de modération interne des contenus constituent une avancée majeure dans la lutte contre la désinformation et la diffusion incontrôlée de publicités politiques ou de messages politiques extrêmes. Toutefois, ces procédures internes suscitent la méfiance et ne sont pas sans risque. Nous pouvons identifier trois menaces majeures dans la fonction de modération : Premièrement, elles peuvent servir de mesures de censure politique. La modération des réseaux sociaux menace la liberté d'expression et facilite le contrôle de l'opinion publique. Il n'est pas facile d'identifier les contenus inappropriés, tant en ce qui concerne leur contenu que leur mode de diffusion. En période électorale, il faut à la fois maximiser le respect de la liberté d'expression et garantir l'égalité des chances à tout moment. Deuxièmement, les plateformes numériques utilisent des algorithmes pour détecter les contenus inappropriés qui peuvent être biaisés. Ce biais algorithmique augmente les erreurs (qui peuvent avoir des répercussions graves et irréversibles sur la compétition électorale), réduit la transparence et automatise les biais humains. Enfin, les décisions des plateformes de réseaux sociaux s'inscrivent dans un cadre qui échappe au contrôle démocratique. Le problème fondamental est que la régulation des contenus publiés sur les réseaux sociaux est laissée aux mains d'entreprises privées, qui appliquent des règles non démocratiques et des mécanismes techniques (basés sur des algorithmes) peu transparents (Sánchez, 2020:119).

Glossaire

La **fonction de modération** pourrait être définie comme l'activité exercée par les entreprises technologiques propriétaires de plateformes numériques ou de réseaux sociaux afin de contrôler le contenu publié par les utilisateurs. Cette activité peut aller jusqu'à la suppression de ce contenu ou la suspension des comptes des utilisateurs. Cette activité de surveillance par les entreprises porte atteinte à deux principes fondamentaux qui devraient régir tout processus électoral : la liberté d'expression et l'égalité des chances pour les candidats.

Afin de comprendre l'étendue de cette fonction et les risques qu'elle peut comporter, il est nécessaire de se référer à un certain nombre de termes techniques liés à cette activité.

Tout d'abord, il convient de mentionner les *algorithmes*, qui sont utilisés de manière intensive par les plateformes numériques et les réseaux sociaux pour, entre autres, compiler et sélectionner le contenu que les utilisateurs voient.

Les **algorithmes** sont un ensemble fini de règles formelles (opérations logiques, instructions) qui permettent à un ordinateur d'obtenir un résultat à partir d'éléments d'entrée. Ces règles peuvent faire l'objet d'un processus d'exécution automatisé et disposer de modèles conçus grâce à l'apprentissage automatique. L*'apprentissage automatique* permet de construire un modèle mathématique pour permettre à un ordinateur de prendre des décisions ou de faire des prédictions sans intervention humaine sur la base de données, qui comprennent un grand nombre de variables inconnues à l'avance. D'autre côté, l'**apprentissage supervisé** est une forme d'apprentissage automatique qui ne fonctionne pas de manière autonome, mais nécessite une intervention humaine. Les données sont présentées à la machine et le processus est guidé par une personne tandis que l'ordinateur travaille en vue d'un résultat spécifique. Grâce, par exemple, à l'étiquetage du contenu, l'apprentissage automatique guidé produira un résultat attendu.

L'utilisation intensive et fréquente d'algorithmes conduit à un autre concept, le **biais algorithmique** : Il s'agit de technologies qui ne prennent pas en compte l'ensemble des idées disponibles et présentent des erreurs répétables dans les résultats d'un système informatique, favorisant un résultat plutôt qu'un autre. Un algorithme peut « programmer » un logiciel de manière à ce qu'il ne prenne pas en charge une gamme complète d'entrées, mais seulement un spectre plus restreint. Ce biais se retrouve dans les résultats des moteurs de recherche et sur les plateformes de réseaux sociaux. Ce concept est lié à l'intelligence artificielle et peut également être décrit comme une manipulation numérique des élections lorsqu'un intermédiaire utilise une présentation sélective des informations pour favoriser son agenda plutôt que celui des utilisateurs, qui dans ce cas sont les électeurs.

La ***technologie des communications numériques*** est l'environnement dans lequel la fonction de modération marchera. Il s'agit de la conception et de la construction de technologies de communication transmettant des informations sous forme numérique. Il s'agit d'outils numériques qui permettent à plusieurs personnes de communiquer entre elles. Dans ce sens, **l'alphabétisation numérique** (ou alphabétisation informatique, médiatique ou informationnelle) fait référence aux compétences complémentaires et interdépendantes, à la fois techniques et sociales, que les individus doivent mobiliser lorsqu'ils utilisent la communication basée sur Internet (y

compris l'hypertexte, les images, l'audio et la vidéo) pour consommer et créer des messages dans divers contextes académiques, civiques et culturels. Il s'agit d'alphabétisation aux pratiques numériques émergentes, où les apprenants compétents doivent être aussi performants dans la communication en face-à-face et imprimée que dans les nouveaux outils en ligne. Les concepts connexes incluent l'alphabétisation informatique, l'alphabétisation aux technologies de l'information et de la communication (TIC), l'alphabétisation informationnelle, l'alphabétisation médiatique, les nouvelles alphabétisations et les multi-alphabétisations.

Dans la communication numérique, nous rencontrons le phénomène des « **chambres d'écho** » (*echo chambers*). En général, ce terme illustre la manière dont les goulets d'étranglement ou les silos de données limitent les options disponibles pour les personnes ou les machines. Sur les réseaux sociaux et autres plateformes interactives, où les technologies sélectionnent souvent des bribes de données à partir d'une source générale en fonction d'algorithmes heuristiques ou d'apprentissage, les utilisateurs ont accès à un flux de réseaux sociaux qui devient une « chambre d'écho » d'idées similaires ou communes. Une chambre d'écho peut également être définie comme une situation dans laquelle les gens n'entendent que des opinions du même type ou similaires aux leurs. Cela signifie que d'autres voix ont été activement exclues et discréditées. Les membres de la chambre d'écho ont été amenés à se méfier systématiquement de toutes les sources extérieures. Dans les bulles épistémiques, les autres voix ne sont pas entendues, tandis que dans les chambres d'écho, elles sont activement sapées.

L'**internet des objets** *(IdO)* consiste à connecter à Internet (et/ou entre eux) tous les appareils dotés d'un interrupteur marche/arrêt. Cela inclut tout ce qui concerne les téléphones mobiles, les écouteurs, les appareils portables et même les machines à laver, etc. Il en va de même pour les composants des machines. L'*IdO* est un gigantesque réseau « d'objets » connectés (ce qui inclut également les personnes). Il s'agit d'une relation entre des personnes, entre des personnes et des choses et entre des choses. Il peut être utilisé ou détourné pour modifier le discours politique en ligne, en accédant et en stockant d'importantes quantités de données personnelles ou relatives aux utilisateurs d'appareils. Cela peut affecter l'engagement civique en ligne ou en politique. Les *botnets de l'IdO* sont des réseaux de dispositifs connectés ou connectés à l'*IdO* qui sont infectés par des logiciels malveillants ou contrôlés par des acteurs malveillants.

Garantir des conditions électorales équitables doit être une priorité dans toute activité de contrôle ou de modération dans le domaine de la communication numérique. Une concurrence loyale qui garantit que chaque parti et chaque candidat sont traités équitablement et bénéficient exactement des mêmes possibilités et ressources financières, indépendamment de leur taille et de leur popularité, afin qu'ils aient une chance égale de présenter leurs arguments aux électeurs. Avec la numérisation de la

politique, ce terme peut être utilisé en relation avec le discours politique en ligne, l'utilisation des réseaux sociaux par les candidats les plus riches, etc. Le concept de **neutralité du réseau**, qui souligne que les fournisseurs de services Internet doivent traiter toutes les données de la même manière, est directement lié à cette notion. Les fournisseurs de services ne peuvent donner la priorité à aucune donnée.

Cas

Initiatives réglementaires

Depuis quelques années, plusieurs initiatives réglementaires ont été proposées qui, entre autres mesures, visent à établir une série de garanties dans l'activité de modération des plateformes numériques. Au niveau des États, l'Allemagne a adopté une loi (2017) sur l'application des lois relatives aux réseaux sociaux qui contient un certain nombre de mesures visant à améliorer l'efficacité de celles-ci et réglemente la procédure de retrait de contenu. Cette loi a toutefois suscité des critiques. En outre, le *Traité interétatique sur les médias* (2020) met l'accent sur la responsabilité des intermédiaires d'Internet et impose des règles pour la fonction de modération.

Au niveau européen, on distingue le *Code de conduite sur la désinformation*, approuvé par la Commission européenne en 2018 sur la base du rapport publié par un groupe d'experts de haut niveau sur les fausses nouvelles (*fake news*) et la désinformation en ligne. Ce code s'engage en faveur de l'autorégulation (il a été signé par Facebook, Google, Twitter, Mozilla et Microsoft) et transfère aux entreprises la responsabilité d'intervenir sur les contenus à travers un contrôle qui peut être plus rapide et plus efficace que celui effectué par les autorités publiques. Toujours en 2018, la Commission et la haute représentante pour les affaires étrangères et la politique de sécurité ont adopté conjointement le *plan d'action contre la désinformation*. Ce plan comprend notamment un volet consacré à la mobilisation du secteur privé, qui passe par l'adhésion et le respect du *Code de conduite*.

Au sein du Conseil de l'Europe, la *recommandation du Comité des ministres sur le rôle et la responsabilité des intermédiaires de l'Internet* de 2018 réaffirme l'obligation selon laquelle toute décision de retrait de contenu doit être étayée par une autorité judiciaire ou une autorité indépendante, soumise en dernier ressort à un contrôle juridictionnel, ainsi que d'autres garanties dans le processus de retrait de contenu. La Commission de Venise a rassemblé de nombreuses initiatives dans deux documents essentiels : un rapport sur les *technologies numériques et les élections* (2019) et les *Principes pour l'utilisation des technologies numériques dans le respect des droits dans les processus électoraux* (2020).

Cas pertinents

Il existe un certain nombre de précédents judiciaires et administratifs qui ont abordé directement ou indirectement la question de la modération des contenus dans la communication numérique.

Il est très intéressant de noter la décision du Conseil électoral central espagnol qui a résolu la plainte contre Twitter pour la suspension du compte du parti politique VOX sur ce réseau social pendant les élections au Parlement de Catalogne le 14 février 2021. La suspension du compte, motivée par la publication d'un message qui contrevenait à la politique sur les discours de haine, a été considérée comme légitime et proportionnée. Cet accord a été ratifié par la Cour suprême dans son arrêt 246/2022 du 28 février.

Le 6 février 2022, le Tribunal supérieur électoral du Costa Rica a statué sur 63 affaires dans lesquelles il a ordonné le retrait de contenus de réseaux sociaux pour violation de la législation électorale du Costa Rica sur l'interdiction de la propagande électorale pendant la période électorale fermée. Tous les contenus étaient des contenus publicitaires et étaient hébergés dans la bibliothèque d'annonces. Il poursuit en « ordonnant à Meta Platforms, Inc. de procéder immédiatement à la suppression de l'espace publicitaire ».

Le Tribunal Électoral du Pouvoir Judiciaire de la Fédération (TEPJF) du Mexique a statué sur plusieurs affaires concernant la publication de messages par des non-candidats sur les réseaux sociaux pendant l'interdiction électorale. Ceux-ci ont été considérés comme de la propagande électorale (plus récemment, SUP-REP-319/2021). SUP-RAP-0172-2021 SRE-JE-0106-2021-Accord 1)

Au Brésil, des décisions pertinentes ont également été prises dans ce domaine. La décision de la Cour supérieure électorale de mai 2019 (appel électoral spécial n° 13351) indique que les messages envoyés via l'application WhatsApp ne sont pas ouverts au public, à l'inverse de ceux hébergés sur les réseaux sociaux tels que Facebook et Instagram. La communication est de nature privée et se limite aux interlocuteurs ou à un groupe limité de personnes, ce qui, en appliquant le canon de proportionnalité au sens strict, justifie la prévalence de la liberté d'expression. Cette ligne d'interprétation est renforcée par la décision d'avril 2020 (l'appel de la représentation nº 060147858) dans laquelle il est dit que la réalisation de propagande électorale sur le profil d'une personne morale sur le réseau social Facebook viole les articles 57-B et 57-C de la loi 9 504/97 et entraîne l'imposition d'une amende.