FONDATION ROBERT SCHUMAN

POLICY PAPER

Question d'Europe
n°578
30th novembre 2020

La démocratie européenne, un système fondamental à protéger

Eric MAURICE

La démocratie est le fondement politique et moral de l'Union européenne et des Etats qui la composent. Par son bon fonctionnement, elle tend à pacifier les alternances politiques, atténuer les tensions sociales et supprimer l'arbitraire judiciaire, ce qui garantit la paix civile et la prospérité des sociétés européennes. En outre, dans un monde où les marqueurs de la démocratie libérale issue des Lumières européennes sont en recul, la valeur démocratie est un outil de la puissance et de l'influence de l'Union. Sans démocratie fonctionnelle en leur sein, l'Union et ses Etats membres perdraient leur capacité à agir et défendre leurs intérêts, par le maintien d'un multilatéralisme basé sur des règles, ou par la projection de leurs valeurs et de normes suivies par d'autres.

Dans le monde actuel, le politique est devenu « la véritable infrastructure fonctionnelle et symbolique de nos sociétés », note le philosophe Marcel Gauchet. Les campagnes de désinformation et de manipulation visent à saper cette infrastructure en affaiblissant l'autorité, la légitimité et l'efficacité du politique dans les sociétés démocratiques. De ce point de vue, le système démocratique européen peut être considéré comme une infrastructure critique qui doit être protégée, de manière commune, au même titre que les traditionnelles infrastructures matérielles et techniques.

L'élection présidentielle américaine de 2020, après celle de 2016, est un rappel des défis posés aux démocraties les plus établies, de même qu'une démonstration de l'importance du bon fonctionnement et du respect des institutions. La situation aux Etats-Unis résulte en partie de traditions et de conditions spécifiques à ce pays. Mais les mécanismes et les symptômes sont communs à la plupart des démocraties, en particulier en Europe, où les manipulations pour retourner les populations contre l'action de l'Union et des Etats face à la pandémie de Covid-19 s'appuient sur le mécontentement social.

Les menaces qui pèsent sur les systèmes démocratiques sont de nature physique et, de plus en plus, virtuelle, qu'il s'agisse de cyberattaques, de piratages, de désinformation et de manipulation, qui passent principalement par le biais d'internet. Les réponses ne sont cependant pas uniquement techniques. Internet n'est que le moyen de politiques visant à affaiblir les sociétés démocratiques ouvertes, et dont le champ d'action réel touche aux esprits et aux opinions individuelles et collectives.

La multiplication des formes et des moyens de porter atteinte à nos sociétés et nos systèmes démocratiques est reflétée par le concept de menaces hybrides, définies par l'Union comme « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé ».

La réponse engagée depuis plusieurs années repose donc sur une variété de moyens mais aussi, dans le contexte européen, sur une articulation entre le niveau national, qui reste souverain dans de nombreux domaines, et le niveau européen.

Le 2 décembre, la Commission européenne doit présenter son Plan d'action pour la démocratie européenne, issu de plusieurs consultations et de l'expérience des dernières années. Le plan s'articulera autour de trois axes qui couvrent au-delà

du strict champ des menaces hybrides : l'intégrité des élections et la publicité politique ; la lutte contre la désinformation ; le renforcement de la liberté et du pluralisme des médias.

Le double objectif de ce plan, selon la Commission, est de « garantir que les citoyens puissent prendre part au système démocratique par une prise de décision informée et libre de toute interférence ou manipulation illégale », ainsi que d'« améliorer la résilience de nos démocraties ». Il est en cela différent et complémentaire des actions menées par les institutions pour protéger l'Etat de droit lorsqu'il est remis en cause dans certains Etats membres.

Ces actions, menées par le biais de la procédure de l'article 7 du Traité sur l'Union européenne, de l'autorité de la Cour de Justice, du nouveau mécanisme européen de protection de l'Etat de droit et, bientôt, du mécanisme de conditionnalité sur le budget de l'Union constituent le pilier interne de la défense de l'infrastructure démocratique qui sous-tend le modèle européen. Cette étude porte sur les piliers externe – la lutte contre les menaces hybrides et les ingérences électorales – et intermédiaire – la lutte contre la désinformation et le soutien aux médias.

1. AFFRONTER LA MENACE HYBRIDE

Les menaces hybrides résultent du développement constant des nouvelles technologies et de leur utilisation dans la guerre informationnelle théorisée par la Russie et appliquée par d'autres Etats comme la Chine ou l'Iran. Elles sont portées par des moyens non militaires mais au service d'objectifs stratégiques traditionnellement recherchés par des moyens militaires : l'affaiblissement et la vulnérabilité de l'adversaire pour le neutraliser et avancer ses propres intérêts.

Dans le cas de l'Union européenne, la vulnérabilité vient du caractère « imparfait » de la construction communautaire, dans laquelle la cohésion des Etats membres est à la fois un objectif, mais aussi une condition aux prises de décision. Diviser les pays européens pour mieux les empêcher d'agir est une tactique utilisée par les adversaires économiques de l'Union, comme la Chine ou les Etats-Unis. Diviser les citoyens européens pour entamer la cohésion de l'Union est la stratégie poursuivie par ses adversaires politiques comme la Russie et la Chine au travers des menaces hybrides. Ces deux Etats ont tenté de semer la confusion au printemps 2020 sur la nature et l'origine de la Covid-19 et les moyens d'y faire face, tout en intervenant pour faire croire qu'ils venaient en aide aux Européens pour supplanter une Union inactive.

La crise sanitaire, économique et sociale engendrée par la Covid-19 a davantage exposé les sociétés européennes au risque hybride. Comme le souligne la Commission, elle a « montré que les fractures et les incertitudes sociales engendraient une vulnérabilité sur le plan de la sécurité ». Malgré sa prise de conscience, l'Europe reste hautement exposée aux agissements hostiles.

Une prise de conscience progressive

La première cyberattaque organisée dans le but de déstabiliser un Etat européen date de 2007, en Estonie, lorsque la Russie a visé des ministères, le Parlement ainsi que des banques, en représailles au déplacement d'une statue soviétique. Mais c'est avec la crise ukrainienne, en 2014, et le déploiement d'actions paramilitaires, cyber et informationnelles de la part de la Russie, que l'Union a pris la mesure de la menace hybride, dont les conséquences sur les systèmes démocratiques sont devenues manifestes avec l'élection présidentielle américaine de 2016 et, dans une moindre mesure, avec le référendum sur le Brexit en juin 2016.

L'élection présidentielle américaine de 2020 n'a pas été marquée par une ingérence aussi spectaculaire que l'avait été le piratage de l'équipe de campagne démocrate en 2016, avec les révélations destinées à nuire à Hillary Clinton. Mais plusieurs tentatives ont été observées à l'encontre de Joe Biden. Les autorités ont également mis en garde contre des actions de piratage et de désinformation. Facebook et Twitter ont suspendu les comptes de faux médias et journalistes créés par l'Agence russe de recherche sur Internet,

le principal foyer de manipulation en ligne. En outre, le FBI et l'Agence de cybersécurité et de sécurité des infrastructures ont constaté des incursions de pirates identifiés comme russes dans les réseaux d'autorités à différents niveaux, ainsi que des réseaux de l'aviation civile.

Dans l'optique des élections européennes de 2024, et plus encore d'importantes échéances comme les élections fédérales en Allemagne, à l'automne 2021, et l'élection présidentielle en France, au printemps 2022, l'expérience américaine montre que la menace reste présente et multiforme. Elle montre également le rôle des structures fédérales, qui peuvent suivre la situation sur un large territoire à différents niveaux, et l'importance de l'engagement des grandes plateformes numériques en coordination avec les pouvoirs publics.

La réponse de l'Union depuis les agissements russes lors de la guerre en Ukraine a été continue, avec pour objectif de disposer d'une vue d'ensemble et de soutenir les Etats membres dans la prévention et la réponse aux menaces. En 2016, elle s'est dotée d'un Cadre commun en matière de lutte contre les menaces hybrides, comprenant vingt-deux mesures opérationnelles, et complété en 2018 par un plan pour « accroître la résilience et renforcer la capacité à répondre aux menaces hybrides ».

Au niveau européen, le travail d'analyse des risques est effectué par INTCEN, le centre de renseignement et de situation de l'Union, qui dépend du Service européen d'action extérieure (SEAE) et est chargé de l'exploitation des sources « ouvertes » et des analyses fournies par les services de renseignements des Etats membres.

Au sein de l'INTCEN a été créée en 2016 la « cellule de fusion », définie comme le « point central unique pour l'analyse des menaces hybrides », en lien avec les institutions et les Etats membres pour centraliser les signalements et les analyses de risques. La cellule de fusion travaille étroitement avec le Centre européen d'excellence pour la lutte contre les menaces hybrides (Hybrid CoE), un organisme créé en 2017 et basé à Helsinki, qui chapeaute un réseau d'environ 1 200 experts civils et militaires, gouvernementaux et privés, de 28 pays (Union et OTAN). Le Centre conduit des travaux de recherches ainsi que des séminaires et exercices de simulation pour renforcer les capacités des Etats participants, en particulier en matière de coopération entre civils et militaires.

Début 2020, le Centre d'excellence et la Commission ont présenté aux Etats membres un « modèle conceptuel » pour l'analyse des menaces hybrides, qui a été testé pendant la crise de la Covid-19. Les discussions se déroulent dans le cadre d'une autre structure récente, le « groupe de travail horizontal pour améliorer la résilience et lutter contre les menaces hybrides ». Mis en place à l'été 2019 au sein du Conseil, et composé d'experts nationaux, il est chargé, entre autres, de définir des stratégies et modes d'action communs contre tous les types d'action qui restent sous le seuil de l'action militaire et, en particulier, la désinformation. Son travail passe avant tout par un effort pour continuer à identifier les vulnérabilités, au travers de questionnaires soumis aux Etats membres.

Un rapport sur la mise en œuvre de la stratégie adoptée depuis 2016, publié en juillet 2020, note que l'Union s'est adaptée à l'évolution du risque hybride et que « le travail concerté est devenu la norme » au sein des institutions et agences européennes. Il souligne néanmoins qu'en dépit de progrès dans les Etats membres, une « coordination établie » au niveau gouvernemental et « une prise de conscience suffisante » dans les sociétés font encore défaut. Cela est dû en partie au fait que tous les gouvernements ne partagent pas la même appréciation de la menace, ni la même volonté de dévoiler leurs vulnérabilités.

Cette prise de conscience de l'enjeu hybride s'est traduite par la création à l'été 2020 d'une commission spéciale au Parlement européen sur « l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation », qui rendra son rapport à l'automne 2021.

Cyberattaques et piratages

La dépendance de l'ensemble des activités humaines envers les technologies et les systèmes informatiques,

qui s'est encore accentuée avec la crise sanitaire, rend les infrastructures publiques et privées vulnérables aux cyberattaques et piratages. Dans le cadre de la protection de la démocratie, les cybermenaces concernent à la fois le processus électoral (l'intégrité du scrutin) et l'environnement dans lequel il peut se dérouler (la sécurité des infrastructures nécessaires au bon fonctionnement de la société).

Les cyberattaques contre les infrastructures (électricité, communications) ou les services publics (hôpitaux, transports), cherchent à instiller un sentiment de vulnérabilité et peuvent aussi chercher à susciter un chaos empêchant la bonne tenue d'une élection ou, plus généralement, engendrer de la défiance envers l'Etat et le système politique. Opérées par des groupes de hackers travaillant parfois pour le compte de gouvernements, elles prennent souvent la forme d'attaques par déni de service (DDOS), ou de logiciels malveillants envoyés sous une forme anodine - portes dérobées pour bloquer ou contrôler un système de l'extérieur, ou « rançongiciels » bloquant un système et réclamant une somme d'argent.

Outre les entreprises, les hôpitaux sont régulièrement ciblés, par exemple au Royaume-Uni en 2017, en France en 2019 et en République tchèque en 2020. Les attaques sont souvent attribuées à des hackers russes, mais en juin 2020, la Présidente de la Commission a désigné la Chine, en la prévenant que les cyberattaques contre des hôpitaux, en plein crise du coronavirus, « ne peuvent pas être tolérées ».

Ce risque n'est pas exclusivement lié aux processus démocratiques. Il concerne tous les Etats dans le monde, quel que soit leur régime politique. Il fait depuis longtemps l'objet de stratégies à l'échelle nationale et dans le cadre des alliances comme l'OTAN. L'Union a adopté en 2013 une stratégie de cybersécurité, et en 2016 la directive sur la sécurité des réseaux et des systèmes informatiques (SRI), qui vise à accroître les capacités en cybersécurité des Etats membres et à renforcer leur coopération en termes d'information et de réponse aux incidents.

Plus spécifiques sont les cybermenaces liées aux élections, qui par définition concernent avant tous les démocraties. L'intégrité d'un scrutin peut être mise en péril par le piratage des listes électorales ou des systèmes de collecte des résultats, mais aussi par le « hack and leak », le piratage des systèmes internes d'un candidat ou d'un parti, suivis de la publication de documents réels ou truqués afin d'affaiblir ou discréditer le candidat.

Les deux principaux exemples, attribués à la Russie, sont le piratage des courriels du Parti démocrate américain et leur publication par Wikileaks avant l'élection présidentielle de 2016, et les « Macron Leaks » issus du piratage du mouvement En Marche pendant la campagne présidentielle française de 2017. Un piratage du Bundestag en 2015, également attribué à la Russie par la Chancelière allemande Angela Merkel, n'a donné lieu à aucune révélation ou déstabilisation particulière. Les ministères allemands de la Défense et des Affaires étrangères ont également été attaqués en 2018.

Avant les élections européennes de 2019, des attaques par déni de service ont été signalées sur des sites donnant des informations sur les élections européennes dans plusieurs Etats dont la Finlande et la République tchèque. En 2017, avant même les MacronLeaks, la France avait renoncé au vote électronique, autorisé pour les seuls électeurs résidant à l'étranger lors des élections législatives, en raison d'un « niveau de menace élevé de cyberattaques ».

Plus récemment ont été observées des attaques informatiques contre les réseaux de collectivités locales. Cela a été le cas à Marseille et sa Métropole, deux jours avant le premier tour des élections municipales en mars 2020. « Les réseaux impactés sont utilisés par exemple pour éditer les listes d'émargement, pour gérer les procurations, pour gérer tout ce qu'il y a autour de l'élection », a expliqué Guillaume Poupard, directeur général de l'Agence française de la sécurité des systèmes d'information (ANSSI), à la commission spéciale du Parlement sur l'ingérence. Il pointe le risque de piratage d'instituts de sondages les jours de scrutin pour fausser les premières estimations et engendrer la confusion.

L'Union s'appuie sur l'Agence européenne chargée de la sécurité des réseaux et de l'information (Enisa), créée

en 2004, chargée d'aider les Etats membres à établir et coordonner des stratégies nationales de cybersécurité, et les interventions en cas de risque ou d'attaque. Au printemps 2019, l'Enisa a publié une série de recommandations pour les Etats membres et a mené un exercice de simulation avec le Parlement et la Commission afin de tester les capacités déjà en place. L'agence travaille avec les Etats membres, au niveau technique au sein du CSIRT[1] Network, le réseau européen des centres d'alerte et de réponse, et, depuis septembre 2020, au sein du Cyber Crisis Liaison Organisation Network (CyCLONe), dont l'objectif est de favoriser les échanges sur les stratégies nationales et de développer une analyse d'impact coordonnée des incidents.

En vertu de la directive sur la sécurité des réseaux et des systèmes d'information (SRI), l'Union s'est dotée en 2018 d'un groupe de coopération chargé de cartographier les mesures nationales prises pour assurer la sécurité des réseaux et des systèmes informatiques utilisés dans le cadre des élections, et de recenser les insuffisances susceptibles d'affecter les élections européennes. Le groupe a élaboré un « recueil sur la cybersécurité des technologies électorales », dont au moins seize Etats membres ont suivi les recommandations pour sécuriser le scrutin européen.

La stratégie pour une Union de la sécurité, présentée par la Commission en juillet 2020, prévoit de développer la « conscience situationnelle » et la résilience de l'Union, notamment par une meilleure intégration des flux d'information et la révision du protocole opérationnel de l'UE pour la lutte contre les menaces hybrides. En décembre, la Commission présentera une actualisation de la stratégie de cybersécurité, qui inclura une révision de la directive SRI. L'un des éléments pourrait en être le classement en tant qu'infrastructure critique des équipements utilisés pour les élections, afin qu'ils soient couverts par la directive SRI et les obligations qu'elle établit pour les Etats – comme l'a demandé le Parlement européen.

Dans le domaine de la cybersécurité, les menaces sont donc identifiées, et l'enjeu est avant tout de mettre en commun des informations, des méthodologies et des moyens d'action dans un domaine où la souveraineté des Etats reste clairement affirmée et l'analyse du risque inégalement partagée.

2. ASSURER L'INTÉGRITÉ DES ÉLECTIONS

Les systèmes démocratiques se caractérisent avant tout par des élections libres, non faussées, dans lesquelles se prononcent les citoyens sur la base d'un débat ouvert et équitable. Contrairement aux dictatures et régimes autoritaires, les pays démocratiques établissent à l'avance des règles claires qui permettent de garantir la sincérité du scrutin et la légitimité des pouvoirs qui en sont issus. Contourner ces règles, fausser les débats et dénaturer les processus électoraux sont les moyens par lesquelles des groupes ou Etats tiers peuvent influer sur le résultat des élections et/ou affaiblir la légitimité des dirigeants élus, et donc leur capacité d'agir.

Dans ce domaine, l'Union ne peut intervenir directement que sur les élections européennes, mais elle peut aussi inciter les acteurs nationaux à suivre des règles ou bonnes pratiques communes. Avant les dernières élections européennes, la Commission a proposé en septembre 2018 une série de mesures et recommandations qui ont servi de base, jusqu'à présent, à l'action commune pour sécuriser les processus électoraux en Europe. La Commission mettait l'accent sur la cybersécurité, la transparence, et la protection des données.

L'une des principales mesures de ce « paquet élections » a été la création du Réseau européen de coopération en matière d'élections au sein duquel les Etats membres échangent sur leurs législations électorales, leur évaluation des risques et leurs campagnes de sensibilisation, ainsi que sur les règles de protection des données ou la cybersécurité. Le Réseau a été un point de contact entre les Etats membres, le Parlement et divers organes comme l'Autorité pour les partis politiques européens et les fondations politiques européennes, Europol ou les régulateurs de médias audiovisuels. La démarche a permis, entre autres, d'identifier les différences d'approche entre les Etats, et de commencer à remédier aux déficiences. A l'avenir, le Réseau de coopération devrait continuer à favoriser un alignement des règles et développer une coopération avec les médias et les plateformes.

[1] Computer Security Incident Response Team, des équipes d'intervention en cas d'incident de sécurité informatique) qui existent dans le public comme dans le privé.

En septembre, la France, la Lettonie et la Lituanie ont proposé d'aller plus loin et de créer un « mécanisme conjoint de protection des élections », disposant d'une réserve d'experts nationaux prêts à aider tout Etat membre à protéger son système électoral contre des attaques. Ce mécanisme s'articulerait autour d'un volet préventif, « sur demande des États membres, afin de déceler les tentatives de déstabilisation des processus électoraux », et un volet retour d'expérience au sein du Réseau de coopération, pour développer les bonnes pratiques communes.

Financement des partis

Au sein du Réseau européen de coopération en matière d'élections, les Etats membres ont établi un tableau des règles en vigueur dans chacun d'entre eux en ce qui concerne le financement et les dépenses des partis, ainsi que des règles applicables aux campagnes et publicités audiovisuelles et sur les réseaux sociaux.

Il est apparu que certains Etats n'avaient pas de règles sur la transparence des donations politiques ou n'interdisaient pas les donations anonymes. Le financement de partis depuis l'étranger n'était pas interdit dans tous les pays, même si certains en limitaient le montant ou exigeaient qu'il soit déclaré. Seulement la moitié des Etats membres, environ, imposaient de la transparence sur la publicité politique. Une minorité d'Etats imposait des règles spécifiques pour les réseaux sociaux.

L'organisation de la vie politique étant une compétence nationale, l'Union ne peut légiférer que sur l'organisation et le financement des partis politiques européens et des fondations qui leur sont liées. Mais les règles mises en place s'appliquent dans le cadre des élections européennes aux partis nationaux fédérés au sein des partis européens et peuvent donc être intégrées dans les règles électorales nationales. Un règlement de 2014, qui octroyait une personnalité juridique aux partis européens, a été amendé en 2018 et 2019, afin notamment de renforcer la responsabilité des partis dans l'utilisation des fonds et permettre de sanctionner les violations des règles sur l'utilisation des données personnelles. La Lettonie a ainsi mis en place une application qui permet de surveiller le financement des partis et de signaler les abus potentiels au bureau de lutte contre la corruption.

Dans le cadre du « paquet élections », la Commission a demandé aux Etats membres d'améliorer la transparence des financements, des dépenses et des publicités politiques. Le travail a été mené en partie par le Réseau européen de coopération en matière d'élections, qui doit en faire un bilan et identifié les vides juridiques restants. La Commission a déjà annoncé que, dans le cadre du plan d'action sur la démocratie européenne, elle présentera d'ici fin 2021 une proposition législative pour accroître les exigences de transparence.

Pour l'instant, les Européens manquent d'informations sur l'ampleur et les mécanismes du financement de partis politiques par des puissances étrangères. Plusieurs enquêtes de presse ont mis en avant les liens qui existent entre la Russie et des partis d'extrême droite comme le FPÖ autrichien, la Lega en Italie et le Rassemblement national en France. Documenter les contournements de la loi est l'un des objectifs de la commission spéciale du Parlement européen sur l'ingérence étrangère, qui se penche, en particulier, sur les allégations de financement politique, légal ou non, par l'intermédiaire de sociétés-relais ou de donateurs utilisant un prête-nom originaire de pays tiers. Son travail pourrait permettre d'élaborer des moyens d'action plus ciblés.

Publicité en ligne

Loin des affiches et des tracts, la communication politique passe par internet et les réseaux sociaux, le plus souvent dans un vide juridique qui permet tous les abus. En ligne, plus encore que sur les murs et dans la rue, les messages viennent de partis établis mais aussi de multiples groupes plus ou moins identifiés, qui viennent influencer et manipuler le débat démocratique.

L'enjeu majeur dans ce domaine est d'empêcher le ciblage des électeurs par le biais des algorithmes et de l'analyse de leurs données personnelles, pour les atteindre par des messages à caractère politique dont l'origine et le bénéficiaire sont souvent opaques.

Comme l'a montré le scandale Cambridge Analytica au Royaume-Uni et aux Etats-Unis, les données personnelles des utilisateurs de plateformes peuvent être utilisées pour des campagnes en ligne. Les contenus, financés par des acteurs tiers, parfois étrangers, peuvent constituer une manipulation des électeurs, en particulier lorsqu'ils privilégient des sujets polarisants ou créent l'illusion qu'un sujet ou une opinion radicale est plus répandu qu'il ne l'est en réalité. La nécessaire transparence concerne deux types d'acteurs : les partis politiques et les mouvements et organisations qui leur sont liés, susceptibles de publier de la publicité politique en ligne ; et les plateformes numériques sur lesquelles les publicités sont diffusées.

En 2018, la Commission a recommandé aux Etats membres, aux partis politiques et organisations de campagne d'encourager la « divulgation active » de l'identité des personnes qui se trouvent derrière des publicités et messages politiques, ainsi que la publication par les partis des dépenses liées à la diffusion des contenus politiques. Avant le scrutin européen de 2019, la commissaire à la Justice a écrit aux dirigeants des partis nationaux de tous les Etats membres pour les inciter à suivre ces recommandations. Selon la Commission, les partis n'ont guère pris de mesures pour lister leurs publicités ou divulguer leurs dépenses en la matière en dehors des informations déjà disponibles sur les plateformes. Certains ont expliqué qu'ils dépendaient en partie des conditions d'utilisation mises en place par les plateformes, comme Facebook en 2019.

Dans le cadre du Code de bonnes pratiques contre la désinformation, les plateformes ont mis en place l'obligation d'indiquer clairement le nom des partis, mouvements ou candidats à l'origine des contenus politiques. Le système a ensuite été appliqué dans les Etats membres. Elles ont également créé des bases de données qui recensent les publicités politiques, dans lesquelles les utilisateurs peuvent consulter les noms des partis ayant eu recours à ces publications, les sommes dépensées et l'audience atteinte, ainsi que les critères en fonction desquels les contenus ont été affichés sur les profils des utilisateurs.

Dans un rapport publié en septembre 2020, la Commission a souligné les carences de ces dispositifs : la recension et la publication des données ne sont pas automatiques et varient selon les plateformes, les bases de données ne permettant que des recherches parcellaires. De plus, les procédures d'autorisation des contenus politiques restent incomplètes, et l'affichage de la mention indiquant qui est à l'origine du message disparaît lorsque ce dernier est partagé – ce qui réduit fortement l'information de l'utilisateur-électeur.

La Commission, le Parlement et les Etats membres demandent aux plateformes de rendre plus transparents les critères d'affichage des publicités politiques et, en particulier, d'ouvrir leurs algorithmes aux chercheurs.

Le plan d'action de la Commission contiendra une initiative législative, prévue en 2021, pour accroître la transparence en matière de publicité politique payante. Les idées évoquées incluent l'interdiction des messages qui ne seraient pas clairement et officiellement payés ou approuvés par les candidats, la pré-validation des messages par les plateformes en coopération avec les autorités électorales et les régulateurs des médias nationaux, l'interdiction du microciblage, le fact-checking obligatoire des publicités politiques, ainsi que la création de portails en ligne, gérés par les autorités électorales, où les informations sur les commanditaires et le financement des publicités.

3. LUTTER CONTRE LA DÉSINFORMATION

En 2018, 45% des personnes interrogées pour une enquête Eurobaromètre citaient Internet comme leur principale source d'information sur les affaires politiques nationales, loin derrière la télévision (77%) mais devant la radio (39%) et les journaux (35%). Les proportions étaient quasiment identiques pour les affaires européennes.

Dans la guerre informationnelle menée contre les démocraties, la désinformation est l'arme la plus répandue, la plus simple à utiliser et la plus complexe à contrer. Son concept même est difficile à définir, car il recouvre plusieurs réalités, qu'il convient de distinguer pour mieux les combattre.

En 2018, à la lumière des agissements des médias russes et de leurs relais dans les Etats membres, la Commission a défini la désinformation comme « les informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public. Par préjudice public, on entend les menaces pesant sur les processus démocratiques ainsi que sur les biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité ».

Mais en 2020, face au développement de l'« infodémie[2] » rendant plus difficile l'adhésion du public aux politiques de santé face à la pandémie de Covid-19, la Commission distingue désormais la désinformation de la mésinformation. La première se caractérise par « une intention d'induire en erreur ou de causer un préjudice public, ou encore de réaliser un gain économique », tandis que la seconde est une information erronée partagée par les citoyens, « à leur insu, de bonne foi avec leurs amis et leur famille ». Cette distinction permet d'essayer de mieux cibler la réponse : « des réfutations bien ciblées, des actions de démystification et des initiatives en matière d'éducation aux médias » pour remédier à la mésinformation ; une action plus directe des pouvoirs publics, y compris par la loi, pour lutter contre la désinformation.

Certains experts, notamment côté français, rejettent cette distinction qu'ils considèrent comme trop simplificatrice, et mettent en avant la notion de « manipulation de l'information », définie comme « la diffusion intentionnelle et massive de nouvelles fausses ou biaisées à des fins politiques hostiles ». Selon eux, la réponse doit avant tout venir de la société civile, à côté de laquelle les pouvoirs publics n'agiraient qu'en appui.

Depuis que la Commission a présenté sa première stratégie contre la désinformation en 2018, le questionnement sur le rôle de chacun des acteurs – pouvoirs publics, partis politiques, médias, citoyens et organisations de la société civile – est au cœur de la réflexion sur les mesures à prendre, au niveau national ou européen. Mais aucune de ces mesures ne sera efficace sans impliquer pleinement un autre acteur : les plateformes internet.

Régulation des plateformes

Par son caractère ouvert, transnational, principalement gratuit et peu réglementé, internet est le champ de toutes les batailles d'influences et d'opinions. Pour se défendre, les démocraties doivent imposer des règles sans attenter aux libertés, contrôler les contenus sans tomber dans la censure, et responsabiliser des entreprises parfois dépassées par leur toute-puissance.

Jusqu'à présent, l'approche européenne a consisté à privilégier l'autorégulation des plateformes, mais sous surveillance. Elle s'est traduite par la mise en place en octobre 2018 d'un Code de bonnes pratiques contre la désinformation, dont les signataires doivent régulièrement rendre des comptes. Le Code compte actuellement seize signataires : neuf associations professionnelles, un groupe de communication et six plateformes (Facebook, Twitter, Google, propriétaire de YouTube, Mozilla, TikTok et Microsoft, propriétaire du réseau professionnel LinkedIn et du moteur de recherche Bing).

Dans un bilan publié en septembre 2020, la Commission estime que le Code a fourni « le cadre d'un dialogue structuré » entre les entreprises et les pouvoirs publics, et permis une plus grande transparence des plateformes, ainsi que des actions concrètes de leur part. Mais elle souligne que, pour être plus efficace, le Code devrait élaborer des définitions communes, des procédures claires et des engagements précis qui soient applicables à tous les signataires et dans tous les Etats membres. Elle note que les chercheurs, les autorités et le grand public restent « très dépendants du bon vouloir des plateformes de partager informations et données » et qu'il est donc « difficile d'évaluer avec précision la rapidité, le caractère exhaustif et l'impact de l'action des plateformes ».

Des centaines de milliers de faux-comptes, gérés par des humains ou par des bots, ont été supprimés par Facebook, YouTube et Twitter, mais sans que les données soient accessibles pour permettre un traçage et une attribution. En outre, le nombre restreint de

[2] La définition de l'Organisation mondiale de la santé, reprise par le Commission est : « une surabondance d'informations sur un problème donné, qui rend la définition d'une solution difficile » [EN : an excessive amount of information about a problem, which makes it difficult to identify a solution], en particulier dans un contexte sanitaire.

signataires limite la portée du Code. Messenger et WhatsApp, propriétés de Facebook et par lesquelles les fausses informations circulent de plus en plus, ne se sont pas engagées, pas plus que Snapchat.

L'approche de la Commission devrait donc être plus offensive et s'engager dans une logique de co-régulation, avec des obligations plus concrètes imposées aux plateformes, lorsqu'elle présentera le 9 décembre son « Digital Services Act », qui complètera, dans ce domaine, le plan d'action pour la démocratie européenne. Il s'agit à la fois de « numériser la démocratie et démocratiser le numérique ».

Modèle économique

Le modèle économique des plateformes et de certains sites favorise la diffusion de contenus sensationnalistes et polémiques qui engendrent du trafic et de l'engagement (« like », commentaires, partages), et donc du profit. L'un des axes de réponse est le contrôle des placements de publicités, pour réduire la mise en avant de contenus qui favorisent la désinformation et la polarisation de la vie démocratique.

Dans le cadre du Code de conduite, les plateformes ont commencé à limiter les « pièges à clics » et les revenus publicitaires qui y sont liés. La publicité sur les sites « imposteurs », qui se font passer pour des sites d'information pour promouvoir un agenda politique, a été bloquée. Mais les plateformes ont continué à permettre la publicité sur des sites pratiquant la désinformation et, surtout, ont continué à accepter des publicités dites « engagées » sur leurs propres services en ligne.

Une étude du centre d'études américain Global Disinformation Index estime que Google génère chaque année environ 60% des revenus publicitaires des sites propageant de la désinformation en Europe, pour un montant de 48 millions $.

Outre un contrôle accru de la manière dont les publicités sont distribuées sur la Toile, la Commission souligne qu'il est nécessaire d'améliorer l'identification des sites de désinformation, y compris par une coopération accrue avec les chercheurs et les vérificateurs de faits. Cette responsabilité devrait être partagée par les plateformes comme par les annonceurs et leurs opérateurs.

Pour l'heure, les plateformes ne mettent pas à la disposition des chercheurs les données qui leur permettraient de retracer et analyser la manière dont les contenus sont publiés, mis en avant et partagés. L'observatoire européen des médias numériques (EDMO) a été mis en place en juin 2020 pour donner aux chercheurs les moyens de développer les outils nécessaires à cette tâche et les réseaux d'échanges. Le plan d'action pour la démocratie européenne devrait inciter plus fortement les plateformes à ouvrir leurs données.

Vérifier les faits

L'Union a mis en place en 2015 sa propre équipe de fact-checkers, le EastStratCom, dédiée à contrer la désinformation russe, à laquelle ont été adjointes en 2017 deux équipes axées sur le voisinage méditerranéen et les Balkans occidentaux. Mais cette « task-force », dont le site EUvsDisinfo est l'un des principaux outils de communication stratégique de l'Union, reste limitée en moyens humains et budgétaires. Et sa méthodologie, sans critères clairs pour qualifier une publication de désinformation, et son action, qui s'assimile davantage à de la contre-propagande anti-russe, sont parfois critiquées et soulignent les limites de l'exercice.

Plus opérationnel est le Système d'alerte rapide, une plateforme sur laquelle les Etats membres et les institutions peuvent signaler des cas de désinformation, échanger leurs analyses et leurs bonnes pratiques et coordonner leur réponse. Mis en place en mars 2019 avant les élections européennes, il a permis, en collaboration avec le Réseau européen de coopération en matière d'élections, de dresser « un tableau complet des activités de désinformation pendant la période électorale ». Il est désormais principalement utilisé pour faire face à la désinformation sur la Covid-19 et a fait preuve de son utilité, même si une étude du Parlement pointe un manque de « standardisation » des informations collectées, et de coordination au niveau des Etats membres.

Alors que la désinformation ne vient plus seulement de Russie, mais aussi de Chine, d'Iran, de Turquie, la lutte doit être menée plus largement, et par tous les acteurs de l'écosystème médiatique.

De plus en plus de médias proposent du fact-checking pour tenter de contrer le flot et l'influence de la désinformation. Cette tâche gigantesque ne peut être assumée par les seuls médias, dont les ressources devraient être, avant tout, consacrées à l'information en fonction de critères professionnels et déontologiques, plutôt qu'à la réaction défensive et incomplète aux fake-news. Elle doit être aussi assumée par la société civile, sur la base de critères fiables et de données complètes. L'action des Etats et de l'Union dans ce domaine ne peut être qu'en soutien, afin de ne pas entrer dans ce que la commissaire Vera Jourova, qui a grandi dans la Tchécoslovaquie communiste, qualifie de « *ministère de la Vérité* ».

L'EDMO, doté d'un budget de 2,5 millions €, met en relation vérificateurs de faits, chercheurs et différents acteurs pour développer des outils afin de mieux comprendre les mécanismes et les effets de la désinformation et de sa propagation, identifier les responsables et organiser la lutte avec des acteurs dans la société civile. Le centre est en activité depuis juin 2020 sous l'égide de l'Institut universitaire européen de Florence. Une seconde phase du projet est prévue, avec un budget de 9 millions €, pour mettre en place un réseau de centres régionaux et nationaux de recherche numérique. Dans ce domaine, les plateformes devraient se voir imposer une plus grande transparence vis-à-vis des chercheurs et de la société civile.

Pluralisme et liberté des médias

L'indépendance des médias, dans le respect des lois et de règles déontologiques, est une des garanties d'un débat libre et non faussé et l'un des remparts contre les abus de pouvoir et l'arbitraire. Economiquement fragilisés par le développement d'internet, les médias traditionnels se retrouvent mis en concurrence avec tous les autres types de contenus, souvent non professionnels, non vérifiés, et non véridiques. « L'information de qualité est en général derrière un *paywall*, et la propagande est toujours gratuite », constate Christopher Wylie, qui a révélé le scandale Cambridge Analytica.

La lutte contre les fausses informations et les manipulations financées par des Etats tiers ou favorisées par le modèle économique d'internet doit donc être équilibrée par un soutien à l'information rigoureuse et aux médias qui la produisent. Y compris face aux intérêts économiques et aux tentatives de contrôle par le pouvoir, comme c'est le cas en Hongrie et en Pologne. La liberté et le pluralisme des médias sont d'ailleurs pris en compte dans le nouveau mécanisme européen de protection de la démocratie.

L'Union finance actuellement dix projets de soutien aux médias et au pluralisme, pour un total de 7 millions €. Plusieurs de ces projets visent à encourager le journalisme d'investigation, et un autre, sous l'égide de Reporters sans Frontières, travaille au développement d'un outil référentiel pour favoriser la transparence et la fiabilité des médias. Deux projets, menés par le Centre pour le pluralisme et la liberté des médias de l'Institut universitaire européen de Florence, sont dédiés à la mise en place d'un mécanisme de réponse rapide aux violations de la liberté de la presse et d'un indicateur du pluralisme basé sur des critères prédéfinis – le Media Pluralism Monitor, qui a rendu son premier rapport en juillet 2020.

62 millions € supplémentaires sont prévus dans le Cadre financier pluriannuel pour 2021-2027, pour lancer d'autres projets d'aide aux médias et au pluralisme, y compris une base de données pour faire la transparence sur la propriété des médias (Media Ownership Monitor).

La Commission prévoit également de soutenir davantage les programmes d'éducation aux médias pour les catégories de population les plus exposées à la manipulation, en particulier les jeunes. L'objectif sera de favoriser « la pensée critique, la capacité à déceler la désinformation et les compétences numériques, ainsi que de soutenir la participation active des citoyens en tant que telle ».

D'autres initiatives existent, hors du cadre de l'Union mais impliquant des Etats membres. C'est le cas en particulier du Partenariat Information et démocratie, initié par RSF et par lequel trente-huit pays, dont vingt Etats membres de l'Union, s'engagent à « promouvoir les cadres juridiques nationaux et internationaux qui respectent et encouragent l'exercice du droit à la liberté d'opinion et d'expression » et demandent aux plateformes de « respecter les principes de transparence, de responsabilité et de neutralité politique, idéologique et religieuse ».

La Commission présentera d'ici fin 2021 une proposition législative contre les recours abusifs visant les journalistes et les défenseurs des droits (souvent désignés sous l'acronyme anglais SLAPPs[3]), utilisés par des individus, des entreprises, voire des gouvernements, mis en cause pour faire pression sur les auteurs d'enquêtes. La journaliste maltaise Daphne Caruana Galizia faisait ainsi l'objet de quarante-sept recours au moment de son assassinat en 2017. Dans une résolution adoptée le 25 novembre 2020, le Parlement demande à la Commission de proposer un texte législatif pour établir des normes minimales dans l'Union. De nombreuses ONG demandent également à la Commission de revoir les règlements dits Bruxelles 1 et Rome 2, qui offrent aux plaignants la possibilité de choisir l'Etat membre dans lequel ils peuvent porter plainte, leur permettant ainsi de choisir les législations les plus sévères en matière de diffamation et de faire porter des coûts de procédure excessifs sur les journalistes visés. La multiplicité des types de recours, directs (diffamation) ou indirects (harcèlement fiscal) et des personnes visées (journalistes mais aussi ONG), rend toutefois la question difficile à traiter d'un point de vue législatif au niveau européen.

***

Le plan d'action pour la démocratie européenne, qui prolonge et développe la stratégie mise en place depuis 2016-2018, intervient dans un contexte évolutif. La tendance de fond de défiance envers les gouvernements et les élites, renforcée par des événements comme le mouvement des Gilets jaunes en France et, plus encore, la pandémie de Covid-19, a modifié l'origine et le parcours des tentatives de désinformation.

La manipulation et le mensonge ne sont plus uniquement diffusés depuis l'étranger, en particulier la Russie. Les Etats membres et l'Union ne font plus seulement face à une ingérence étrangère, mais aussi à un phénomène endogène, même s'il reste encouragé ou financé de l'extérieur. Le complotisme et le refus du pluralisme qui se manifeste aux Etats-Unis se développent aussi en Europe et ne peuvent pas être combattus uniquement pas la réponse hybride ou la régulation des plateformes. La réponse est politique et repose en grande partie sur des facteurs économiques et sociaux, plus encore dans des sociétés européennes fragilisées par la pandémie.

Il existe un lien étroit, même s'il n'est pas systématique, entre l'insatisfaction sociale, la défiance envers les autorités et le vote protestataire, et la réceptivité aux fausses informations et théories du complot. « Plus que l'écart entre régions riches et pauvres, c'est la trajectoire économique et industrielle des lieux qui fait la différence en matière de vote antisystème », relevait une étude de la Commission en 2018. Cette défiance envers le système se traduit souvent par une polarisation des opinions et une recherche d'information alternative remettant en cause l'ordre établi. Une autre étude de la Commission, datant de 2019 et qui s'est vérifié avec la crise de la Covid-19, notait que « l'avis des experts, pertinent et synthétisé, est de plus en plus nécessaire, mais [que] l'autorité de ces experts est remise en question ».

« Le principe selon lequel les politiques sont élaborées sur des éléments prouvés pourrait être reconnu comme un accompagnement essentiel aux principes de la démocratie et de l'Etat de droit. De même, la notion d'institutions scientifiques indépendantes dans le cadre des 'contre-pouvoirs' de la démocratie pourrait être défendue », préconisait le rapport, soulignant ainsi que la lutte contre la désinformation doit fortement s'appuyer sur un sens des responsabilités de la part des autorités dans tous les domaines – politiques ou sanitaires, mais aussi intellectuelles et médiatiques.
De ce point de vue, l'évolution des Etats-Unis depuis 2016, qui s'est traduite par le score plus élevé qu'attendu de Donald Trump le 3 novembre 2020 et l'élection au Congrès de candidats ouvertement complotistes, peut éclairer la réflexion en Europe.

[3] Strategic Lawsuits Against Public Participation (poursuite stratégique contre la mobilisation publique, également, appelée poursuite-bâillon)

D'une part, si les « fake news » se répandent par des sites malveillants et les réseaux sociaux, l'ampleur de la défiance ainsi créée est renforcée par l'attitude de certains médias et forces politiques. La déstabilisation de la démocratie américaine par Donald Trump a été permise par des médias comme Fox News et l'attitude du Parti républicain. La responsabilité déontologique des médias européens, en particulier de certaines chaînes dites d'information, apparaît donc essentielle en complément des initiatives en faveur de l'indépendance et du pluralisme des médias. De même, des règles claires et strictes sur le fonctionnement et la transparence des partis peuvent s'avérer un premier rempart dans la défense de la démocratie.

D'autre part, Donald Trump a brisé un tabou, celui d'un chef d'Etat démocratique contestant le déroulement du scrutin et refusant d'en reconnaître le résultat. Lorsque la démocratie est remise en cause par ceux qui devraient en garantir le bon fonctionnement, il est nécessaire de disposer encore de contre-pouvoirs forts, institutionnels et civiques, pour éviter une déstabilisation majeure de la société. Alors que dans l'Union, deux gouvernements, en Hongrie et en Pologne, rejettent déjà en partie les fondements de l'Etat de droit et disposent de médias à leur service, la défense des contre-pouvoirs par les autres Etats membres et les institutions européennes, notamment la Commission et la Cour de Justice, revêt une importance supplémentaire.

Longtemps théorique, la question de la protection de l'Etat de droit s'est imposée au moment même où l'Union développait une panoplie d'outils, qu'elle s'apprête à renforcer, contre le risque hybride et de l'ingérence étrangère. Confrontés aux limites de l'article 7 TUE, la Commission, le Parlement et les Etats membres - à l'exception de la Hongrie et de la Pologne – cherchent à élargir leurs moyens d'action.

Le mécanisme européen de protection de l'Etat de droit, dont le premier rapport annuel a été débattu pour la première fois par les Etats membres le 17 novembre, est un premier pas vers une action systématique et préventive. Le mécanisme de conditionnalité sur le budget de l'Union, qui doit être mis en œuvre avec le nouveau cadre financier pluriannuel et le plan de relance, est également un outil d'intervention directe dans les Etats qui ne veulent plus suivre les règles. Les stratégies contre les cybermenaces, les ingérences et la désinformation, développées en parallèle, dotent l'Europe d'une panoplie large pour défendre sa démocratie. L'enjeu à venir est une articulation plus affirmée et plus directe de ses multiples dimensions, internes et externes.

Eric Maurice

Responsable du bureau de Bruxelles

de la Fondation Robert Schuman

Ont contribué à cette étude :

Florian Da

Julian Parodi

Assistants de recherche au bureau de Bruxelles

de la Fondation Robert Schuman

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN