Par Benoit Tabaka,
Directeur des affaires publiques, Google France.

ASSURER L'INTÉGRITÉ DES ÉLECTIONS EUROPÉENNES À L'ÈRE DE L'INTELLIGENCE ARTIFICIELLE

Avec plus de 80 élections organisées dans presque autant de pays, le décor est planté pour que 2024 soit l'une des années les plus importantes pour la démocratie mondiale. Et même si les préoccupations intérieures de chaque pays constituent un point central des discussions, cette année électorale historique se déroule dans un contexte de multiples crises régionales et internationales importantes qui vont probablement amplifier les questions de politique intérieure et étrangère mais aussi exposer les scrutins à de nouveaux enjeux.

La France et l'Europe ne demeurent pas en reste. Du 6 au 9 juin 2024, les électrices et électeurs des 27 États membres de l'Union européenne se rendront aux urnes pour élire les membres du Parlement européen.

A l'ère numérique où l'information circule à une vitesse vertigineuse, la sécurité et l'intégrité de celle-ci demeurent cruciales. D'après notre expérience et dans le cadre de ces opérations que certains Etats appellent une "guerre cognitive", les ennemis de la démocratie auront plusieurs objectifs. Tout d'abord, il s'agira de manipuler la foule et les intentions de vote. Ensuite, il s'agira de discréditer les résultats des élections et ainsi faire rejeter le vote exprimé. Enfin, il s'agira de discréditer les personnes publiques ou les partis politiques, comme par exemple au travers du vol de données - comme nous l'avions observé à la veille du scrutin de l'élection présidentielle de 2017.

Depuis plusieurs mois, les équipes de Google sont entièrement mobilisées afin d'aider le bon déroulement de ces élections, qu'il s'agisse de renforcer la visibilité des élections – notamment par la promotion de l'acte de vote auprès des électrices et électeurs, leur permettant de faire un choix éclairé –, de diffuser des informations de qualité, de protéger nos plateformes contre tout type d'abus, ou encore de doter les équipes de campagnes des outils et bonnes pratiques en matière de sécurité.

En particulier, et dans le prolongement de nos actions depuis de nombreuses années, Google renforce la sécurité de ses plateformes pour lutter contre les différentes formes de désinformation. En Europe, un des exemples demeure le Fonds européen pour les médias et l'information (EMIF), auquel nous contribuons financièrement à hauteur de 25 millions d'euros sur 5 ans pour renforcer l'éducation aux médias notamment. 70 projets ont d'ores et déjà été financés dans près de 24 pays, couvrant des sujets allant de la vérification de faits pendant les élections à l'amélioration de l'éducation aux médias. Il est très important que chacun bénéficie des bons outils pour pouvoir faire face à la désinformation et aux ingérences étrangères, quelles que soient les techniques employées. Ainsi, nous soutenons de nombreuses initiatives telles que le TechSoup Europe ou le Global Fact Check Fund.

Plus récemment, **Google et Jigsaw ont lancé une campagne de pré-bunking**, qui vise à intervenir en amont de la production de fausses informations et à sensibiliser les publics cibles. Différentes vidéos courtes sont ainsi en cours de réalisation afin de mettre en évidence les techniques utilisées dans la production de fausses informations – plus d'une dizaine ont été identifiées, à l'instar de la décontextualisation, de l'imitation, ou encore du "cherry picking" c'est-à-dire la mise en avant d'une sélection de preuves à l'appui d'une affirmation, tout en ignorant ou en omettant celles qui la contredisent –, et seront largement diffusées dans les prochaines semaines en France, en Allemagne, en Italie, en Belgique et en Pologne. Enfin, l'intelligence artificielle sera également partie prenante de nos outils afin de renforcer la détection et la suppression de contenus contraires à nos règles ou à la loi (haine, harcèlement en ligne, incitation à la violence, fausses informations…).

Par ailleurs, nous travaillons à sensibiliser nos utilisatrices et utilisateurs aux contenus générés ou altérés par l'intelligence artificielle sur nos différentes plateformes. Comme toute technologie émergente, l'IA présente d'incroyables opportunités mais aussi des risques importants car elle facilite la création de contenus synthétiques trompeurs – les deepfakes. Pour s'en prémunir, Google exige des annonceurs qu'ils divulguent les cas où leurs annonces électorales incluent du contenu représentant de manière non authentique des personnes ou des événements réels ou d'apparence réaliste. Sur YouTube, une mention s'affichera systématiquement sur les contenus "manipulés" ou altérés, mais réalistes pour prévenir les personnes qui les consultent.

Enfin, nous accompagnons responsables de campagnes, candidates et candidats pour leur permettre de disposer des meilleurs outils, notamment en matière de cybersécurité. Dans ce cadre, Google a mis en place divers services comme le Project Shield, permettant de protéger les sites contre les attaques par déni de service (DDoS) - cet outil fournit un "bouclier" contre les attaquants potentiels en filtrant le trafic malveillant, et met également en cache des éléments du site pour alléger la charge sur les propres serveurs des éditeurs de site concernés, ce qui peut améliorer leur performance et dans le même temps réduire les coûts d'utilisation de bande passante - ou le Programme de protection avancée, pour protéger individuellement les personnes. Nous avons également ouvert un centre d'information pour les élections européennes accessible en ligne, regroupant ressources et formations pour aider les équipes de campagne à entrer en contact avec les électeurs et à gérer leur sécurité et leur présence numérique. Lors des élections européennes de 2019, nous avons ainsi dispensé des formations à plus de 2 500 responsables de campagne.

Les équipes de Mandiant Intelligence aident à identifier, surveiller et contrer les menaces émergentes, allant des opérations d'influence coordonnées aux campagnes d'espionnage cyber contre des entités à haut risque. Google rencontre régulièrement dans ce cadre des responsables publics pour partager des informations sur les menaces et les interférences électorales.

Conscients du rôle qui peut être le nôtre - et plus largement de tous les acteurs du numérique - dans le bon déroulement du scrutin, nous sommes persuadés qu'il s'agit d'un travail qui nécessite l'engagement de toutes les parties prenantes : autorités publiques, société civile, etc. afin de créer un environnement numérique plus sûr et plus fiable, pour toutes et tous.