LA RÉPUBLIQUE
En Marche !

LUTTE CONTRE LES NOUVELLES FORMES D'INGÉRENCE ET DE PROPAGANDE NUMÉRIQUES

PRISE DE POSITION

JUIN 2021

AUTEURS :
Laetitia Avia, Députée,
Sandro Gozi, Député européen,
Mounir Mahjoubi, Député,
Bariza Khiari, membre
du Bureau exécutif
de LaREM et ex-sénatrice.

SYNTHÈSE

À un an de l'élection présidentielle, les menaces par voie numérique sur la démocratie se multiplient et s'accentuent. L'élection américaine de 2016 avait été une mise en garde pour le monde. L'*Internet Research Agency*, une organisation russe de propagande, avait par exemple diffusé des publicités politiques visant à démobiliser l'électorat progressiste afro-américain : 3 000 fausses publicités auraient touché plus de 126 millions d'Américains[1]. En France, en 2017, 8 millions de liens partagés pendant la campagne présidentielle portaient sur des contenus tronqués ou mensongers[2].

L'information est devenue une arme dans une véritable guerre d'influence et de déstabilisation. De la mésinformation à la désinformation, du truquage de vidéo et au partage de données, en passant par la création de faux comptes orchestrant des raids numériques, toutes les stratégies sont mises en œuvre pour fragiliser la démocratie en ciblant deux de ses piliers : le vote et la confiance. L'avantage va nettement aux pourvoyeurs de désinformation puisque les fausses informations se propagent six fois plus vite sur Twitter que les vraies informations[3]. Et près d'un tiers des Français déclare avoir déjà été victime d'une fausse information.

Selon un sondage Viavoice réalisé en mai 2021, 63 % des Français se déclarent préoccupés face à ce risque d'intervention étrangère dans nos démocraties. À raison : certains pays dépenseraient jusqu'à 1 milliard d'euros par an pour manipuler l'information. Ces interventions sur l'espace numérique, orchestrées par des puissances étrangères et relayées par des soutiens français, cherchent à favoriser ou défavoriser des candidats et à déstabiliser notre démocratie. Mais la menace est également interne : les dernières crises sociales comme sanitaires montrent à quel point la diffusion de fausses informations peut être orchestrée par

1. Romain Badouard, Les nouvelles lois du web, Seuil, 2020
2. Bakamo Social, Le rôle et l'impact des éditeurs non traditionnels à la Présidentielle française 2017
3. Romain Badouard, Les nouvelles lois du web, Seuil, 2020

des groupes nationaux, relayés ou non par des puissances étrangères. Ces différents mécanismes de propagation des mesures de déstabilisation nous appellent à considérer qu'il faut davantage s'attacher à la menace numérique en elle-même, et aux moyens de l'éradiquer, qu'à son ou ses émetteur(s).

Agir dès à présent doit permettre de préserver l'élection présidentielle à venir et les scrutins qui suivront. Mais au-delà des seules échéances à venir, il s'agit d'adapter nos fonctionnements aux évolutions du numérique pour mieux armer, de manière pérenne, nos démocraties. Face au risque de voir s'élever une démocratie du soupçon et pour réduire les tentatives de déstabilisation, qu'elles soient étrangères ou « made in France », nous souhaitons, par ces 16 recommandations, réarmer notre démocratie et renforcer la confiance entre citoyens et compositions politiques, à l'aube d'attaques depuis l'étranger que l'on sait inévitables.

Les positions adoptées par notre Mouvement, nourries de la consultation des adhérents d'une série d'auditions d'universitaires, journalistes, enseignants etc., présentent **(1)** des recommandations de politiques publiques, **(2)** un appel transpartisan d'action commune en direction de tous les partis et groupements politiques volontaires français et internationaux, et présentent pour la première fois **(3)** les engagements pris au sein de LaREM pour affronter la menace.

1. ARMER LA FRANCE FACE AUX NOUVELLES FORMES D'INGÉRENCE ET DE PROPAGANDE NUMÉRIQUES

LUTTER CONTRE LES FAUSSES INFORMATIONS

RECOMMANDATION 1 :
Créer un « Pharos des fake news » : une plateforme que chaque Français pourra saisir pour signaler

une fausse information. Cette plateforme pourrait être adossée au CSA.

- **RECOMMANDATION 2 :**
  Rendre obligatoire l'identification des "deepfakes" par un label visible.

- **RECOMMANDATION 3 :**
  Dès avant le vote du *Digital Services Act* européen, demander aux plateformes de mettre en place des mesures d'atténuation et de limitation de la viralité des contenus préjudiciables.

- **RECOMMANDATION 4 :**
  Mener une évaluation de la loi Fake news de 2018 en vue des élections à venir.

- **RECOMMANDATION 5 :**
  Établir une liste noire des sites diffuseurs de fausses informations pour assurer la transparence de leur financement publicitaire.

AMÉLIORER LA QUALITÉ DE L'INFORMATION

- **RECOMMANDATION 6 :**
  Rompre l'enfermement algorithmique en période électorale pour assurer aux utilisateurs un pluralisme des contenus dans leurs systèmes de recherche et de recommandation.

- **RECOMMANDATION 7 :**
  Créer et encadrer la propagande numérique électorale sur les réseaux sociaux.

- **RECOMMANDATION 8 :**
  Obliger les plateformes numériques à rendre plus visibles les sources d'informations fiables dans la loi européenne.

MIEUX SENSIBILISER AUX RISQUES NUMÉRIQUES

- **RECOMMANDATION 9 :**
  Généraliser le permis internet.

- **RECOMMANDATION 10 :**
  Assurer une formation aux risques et dérives numériques à toute personne qui le demande, dans les Maisons France Services via les auto-écoles du numérique.

- **RECOMMANDATION 11 :**
  Communiquer des messages de prévention sur les réseaux sociaux et à la TV.

PROTÉGER LA DÉMOCRATIE EUROPÉENNE

- **RECOMMANDATION 12 :**
  Créer un cyber-bouclier européen.

- **RECOMMANDATION 13 :**
  Organiser la réponse collective au niveau de l'Union européenne.

- **RECOMMANDATION 14 :**
  Empêcher dans la loi européenne tout financement de partis politiques par des puissances étrangères.

2. ORGANISER LA RIPOSTE DES PARTIS POLITIQUES EN FRANCE ET À L'INTERNATIONAL

- **RECOMMANDATION 15 :**
  Appeler les partis politiques français à se prémunir et s'engager contre les ingérences et les manipulations de l'information.

- **RECOMMANDATION 16 :**
  Appeler à une conférence internationale des partis progressistes.

3. AU SEIN DE LAREM : METTRE EN PLACE LES OUTILS ET LES PROCESSUS D'ORGANISATION INTERNE CONTRE LES NOUVELLES FORMES D'INGÉRENCE ET DE PROPAGANDE NUMÉRIQUES

- **ENGAGEMENT 1 :**
  Nous systématiserons des tests aléatoires et les protocoles de sécurité.

- **ENGAGEMENT 2 :**
  Nous formerons les salariés et des cadres de campagne.

- **ENGAGEMENT 3 :**
  Nous mettrons en œuvre des protocoles de réactions informatiques et juridiques.

- **ENGAGEMENT 4 :**
  Nous créerons une cellule d'accompagnement des victimes.

LE TEXTE

À un an de l'élection présidentielle, les menaces par voie numérique sur la démocratie se multiplient et s'accentuent. L'élection américaine de 2016 avait été une mise en garde pour le monde. L'*Internet Research Agency*, une organisation russe de propagande, avait par exemple diffusé des publicités politiques visant à démobiliser l'électorat progressiste afro-américain : 3 000 fausses publicités auraient touché plus de 126 millions d'Américains[1]. En France, en 2017, 8 millions de liens partagés pendant la campagne présidentielle portaient sur des contenus tronqués ou mensongers[2].

L'information est devenue une arme dans une véritable guerre d'influence et de déstabilisation. De la mésinformation à la désinformation, du truquage de vidéo et au partage de données, en passant par la création de faux comptes orchestrant des raids numériques, toutes les stratégies sont mises en œuvre pour fragiliser la démocratie en ciblant deux de ses piliers : le vote et la confiance. L'avantage va nettement aux pourvoyeurs de désinformation puisque les fausses informations se propagent six fois plus vite sur Twitter que les vraies informations[3]. Et près d'un tiers des Français déclare avoir déjà été victime d'une fausse information.

1. Romain Badouard, Les nouvelles lois du web, Seuil, 2020
2. Bakamo Social, Le rôle et l'impact des éditeurs non traditionnels à la Présidentielle française 2017
3. Romain Badouard, Les nouvelles lois du web, Seuil, 2020

Selon un sondage Viavoice réalisé en mai 2021, 63 % des Français se déclarent préoccupés face à ce risque d'intervention étrangère dans nos démocraties. À raison : certains pays dépenseraient jusqu'à 1 milliard d'euros par an pour manipuler l'information. Ces interventions sur l'espace numérique, orchestrées par des puissances étrangères et relayées par des soutiens français, cherchent à favoriser ou défavoriser des candidats et à déstabiliser notre démocratie. Mais la menace est également interne : les dernières crises sociales comme sanitaires montrent à quel point la diffusion de fausses informations peut être orchestrée par des groupes nationaux, relayés ou non par des puissances étrangères. Ces différents mécanismes de propagation des mesures de déstabilisation nous appellent à faire évoluer notre approche : il faut maintenant davantage s'attacher à la menace numérique en elle-même, et aux moyens de l'éradiquer, qu'à son ou ses émetteur(s).

Agir dès à présent doit permettre de préserver l'élection présidentielle à venir et les scrutins qui suivront. Mais au-delà des seules échéances à venir, il s'agit d'adapter nos fonctionnements aux évolutions du numérique pour mieux armer, de manière pérenne, nos démocraties. Face au risque de voir s'élever une démocratie du soupçon et pour réduire les tentatives de déstabilisation, qu'elles soient étrangères ou « made in France », nous souhaitons, par ces 16 recommandations, réarmer notre démocratie et renforcer la confiance entre citoyens et compositions politiques, à l'aube d'attaques depuis l'étranger que l'on sait inévitables.

Les positions adoptées par notre Mouvement, nourries de la consultation des adhérents d'une série d'auditions d'universitaires, journalistes, enseignants etc., présentent **(1)** des recommandations de politiques publiques, **(2)** un appel transpartisan d'action commune en direction de tous les partis et groupements politiques volontaires français et internationaux, et présentent pour la première fois **(3)** les engagements pris au sein de LaREM pour affronter la menace.

1 ARMER LA FRANCE FACE AUX NOUVELLES FORMES D'INGÉRENCE ET DE PROPAGANDE NUMÉRIQUES

1. LUTTER CONTRE LES FAUSSES INFORMATIONS

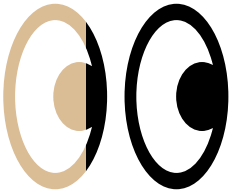
RECOMMANDATION 1 :
Créer un « Pharos des fake news » : une plateforme que chaque Français pourra saisir pour signaler une fausse information.

Pour lutter efficacement contre la diffusion et la viralité d'une fausse information, il faut pouvoir traiter le contenu rapidement et compter sur le soutien de la communauté des internautes.

Sur le modèle du « Portail d'harmonisation, d'analyse, de recoupement et d'orientation des signalements » (Pharos), qui permet à chaque internaute de signaler des contenus et comportements illicites repérés en ligne, nous proposons de créer une plateforme dédiée au signalement des fausses informations sur les réseaux sociaux. Un organisme indépendant, tel que le CSA, pourrait se voir confier la gestion d'une telle plateforme active en période électorale.

RECOMMANDATION 2 :
Rendre obligatoire l'identification des *deepfakes* par un label visible.

Le « deepfake », ou « hypertrucage », est un procédé de manipulation audiovisuelle qui recourt aux algorithmes de l'apprentissage profond (« deeplearning ») pour créer des truquages photographiques, audio ou vidéo particulièrement réalistes. Selon un sondage Viavoice de mai 2021, 39 % des Français déclarent ne pas être en mesure d'identifier un "deepfake", 19 % se sont déjà faits avoir et 13 % ne savent pas ce qu'est un "deepfake". Souvent parodique, il peut concourir à de la mésinformation s'il n'est pas visionné et écouté en connaissance de cause. Il peut aussi être une source de désinformation volontaire, dans le but de faire dire ou faire faire à quelqu'un quelque chose de compromettant.



39 %

des Français déclarent ne pas être en mesure d'identifier un "deepfake", selon un sondage Viavoice de mai 2021.

Face à ce nouveau procédé au potentiel considérable, nous proposons une obligation de transparence sur les contenus altérés, avec une obligation, pour la personne qui publie un tel contenu, de le signaler comme étant un « deepfake » ou « vidéo truquée », de préférence avec un bandeau ou une signalétique incrustée à l'image, de la même manière que les CGU[1] des plateformes prévoient aujourd'hui l'obligation de signaler les comptes parodiques et placements de produits. En cas de non-respect de cette règle, les plateformes seraient fondées à agir

1. CGU : conditions générales d'utilisation

sur le contenu (suppression, démonétisation etc.), et la personne à qui cette vidéo truquée porte préjudice pourra faire valoir devant le juge une volonté manifeste de tromper les internautes.

RECOMMANDATION 3 :

Dès avant le vote du *Digital Services Act* (DSA) européen, **demander aux plateformes de mettre en place des mesures d'atténuation et de limitation de la viralité des contenus préjudiciables.**

Les régulations actuellement discutées en France comme en Europe portent principalement sur les contenus illicites, plus simples à réguler. Il convient d'accentuer l'action des plateformes dans la réduction de la viralité des fausses informations, et par conséquent dans l'atténuation de ses effets néfastes sur la démocratie.

Le DSA demandera aux plateformes de mettre en place des mesures d'atténuation et de limitation de la viralité des contenus préjudiciables telles que les fausses informations, sans pour autant procéder à leur suppression, dans la mesure où ces contenus ne sont pas illégaux. Alors que le DSA ne sera effectif que dans plusieurs mois au mieux, nous appelons les plateformes à s'engager dès aujourd'hui

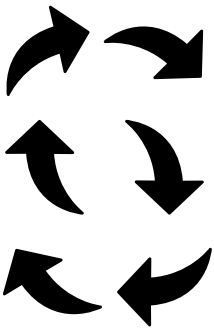
RECOMMANDATION 4 :

Mener une évaluation de la loi « Fake news » de 2018 en vue des élections à venir.

La loi prévoit une obligation de transparence pour les plateformes, qui devront signaler les contenus sponsorisés, en publiant le nom de leur auteur et la somme payée. Celles qui dépassent un certain volume de connexions par jour devront avoir un représentant légal en France et rendre publics leurs algorithmes.

Cette loi crée une action judiciaire en référé pour pouvoir faire cesser rapidement la circulation de fausses nouvelles. C'est le juge des référés qui qualifiera la « fausse nouvelle », selon la définition de la loi de 1881, avec 3 critères : la fausse nouvelle doit être manifeste, être diffusée massivement et de manière artificielle, et conduire à troubler la paix publique ou la sincérité d'un scrutin.

Après deux ans d'une application encore trop faible, et au regard de l'importance primordiale de cette loi dans la préservation de notre système



6X PLUS VITE

que les vraies informations : c'est la vitesse à laquelle les fausses informations se propagent sur Twitter.

démocratique, nous en proposons une évaluation expresse afin d'identifier les moyens de renforcer sa mise en œuvre en vue des prochaines échéances électorales.

RECOMMANDATION 5 :
Établir une liste noire des sites diffuseurs de fausses informations pour assurer la transparence de leur financement publicitaire.

Les contenus publicitaires permettent de rémunérer les sites qui les hébergent. Or, de grandes entreprises françaises financent, malgré elles, des sites complotistes ou diffusant largement des fausses informations. Afin d'éviter que les annonceurs abondent financièrement ce type de site, nous proposons d'établir une liste noire des sites diffusant des fausses informations, gérée par le « Pharos des *fake news* » et mise à disposition des annonceurs. Cette liste donnera d'autres critères qualitatifs de sélection aux annonceurs. Ceux-ci devront rendre publique la liste des sites internet diffuseurs de fausses informations avec lesquels ils entretiennent une relation commerciale, avec pour objectif que cette transparence, et le « *name and shame* » qui en résultera, réduise ces sources de financement.

2. AMÉLIORER LA QUALITÉ DE L'INFORMATION

RECOMMANDATION 6 :
Rompre l'enfermement algorithmique en période électorale pour assurer aux utilisateurs un pluralisme des contenus dans leurs systèmes de recherche et de recommandation.

Les algorithmes des plateformes considèrent l'information comme un produit marketing et présentent des contenus ciblés qui plairont à l'utilisateur sur la base de ses précédentes recherches. Cela crée des mécanismes d'enfermement algorithmique qui limitent le champ informationnel des utilisateurs, en leur présentant continuellement le même genre de contenus et d'idées. Cela est particulièrement délétère en période électorale où le pluralisme politique doit être garanti par les médias.

En période de campagne en particulier, il peut être demandé aux plateformes de mettre en œuvre une politique exigeante de correction des biais afin d'offrir aux utilisateurs un pluralisme des opinions politiques dans leurs systèmes de recherche et de recommandation de contenus. Il s'agit de s'assurer que les contenus, articles, postes, groupes, ou vidéos recommandées ne viennent pas enfermer l'utilisateur dans une opinion politique donnée, mais lui proposent au contraire des avis différents, assurant le pluralisme de l'information, et donnant ainsi la possibilité à l'utilisateur de se forger une opinion sans être influencé par les algorithmes.

RECOMMANDATION 7 :
Créer et encadrer la propagande numérique électorale sur les réseaux sociaux.

Si le numérique, et en particulier l'usage des réseaux sociaux, constitue

une telle menace sur notre démocratie, c'est aussi parce que la démocratie n'a pas suffisamment investi ces espaces. Pire : elle les délaisse en période électorale, laissant le champ libre aux fausses informations et aux « deep fakes ».

Il convient d'adapter les outils de communication et d'information électorales aux outils numériques. Afin d'assurer la diffusion d'éléments fiables, mais aussi de toucher un public plus jeune qui regarde peu la télévision, nous proposons d'amener la campagne officielle jusqu'aux réseaux sociaux et de l'encadrer. Cela pourrait en particulier passer par la création d'éléments de propagande numérique, normés selon les mêmes conditions que la propagande audiovisuelle, et diffusés sur les réseaux sociaux à large échelle, via des contenus sponsorisés émis par le CSA et poussés par les plateformes auprès des utilisateurs français, de manière à assurer la stricte égalité entre les candidats.

SI LE NUMÉRIQUE, ET EN PARTICULIER L'USAGE DES RÉSEAUX SOCIAUX, CONSTITUE UNE TELLE MENACE SUR NOTRE DÉMOCRATIE, C'EST AUSSI PARCE QUE LA DÉMOCRATIE N'A PAS SUFFISAMMENT INVESTI CES ESPACES.

● **RECOMMANDATION 8 :**
Encourager les plateformes numériques à mettre en avant les sources d'informations fiables.

Dans le cadre des débats européens à venir autour du *Digital Services Act*, il pourrait être prévu une obligation pour les plateformes de privilégier et rendre plus visibles les sources d'informations fiables, professionnelles et respectueuses des principes déontologiques, comme l'a proposé RSF[1] dans sa contribution au DSA.

1. RSF : Reporters sans Frontières

Dans l'attente de ces travaux, et dans la perspective des prochaines échéances électorales, une discussion peut être engagée avec les plateformes afin de les encourager à mettre en œuvre des partenariat de collaboration avec des entités, journalistiques ou non, concourant à la fiabilité des informations, notamment à travers des activités de « *fact checking* » - de la même manière que ces plateformes ont aujourd'hui des partenariats avec des acteurs de la sociétés civile qualifiés de « signaleurs de confiance ».

3. MIEUX SENSIBILISER AUX RISQUES NUMÉRIQUES

RECOMMANDATION 9 :
Généraliser le permis internet à tous les jeunes.

Au-delà des dispositifs actuels d'éducation aux médias et de formation aux outils numériques, la sensibilisation aux usages, risques et dérives du numérique est essentielle dès le plus jeune âge. C'est en apprenant aux jeunes le fonctionnement des réseaux sociaux, de l'économie de l'attention et de l'enfermement algorithmique, que nous pourrons davantage les armer et développer leur esprit critique face aux dérives et tentatives de manipulation.

Pour ce faire, une meilleure formation des enseignants aux outils et usages du numérique est essentielle. Mais il convient également de renforcer des dispositifs aujourd'hui facultatifs tel que le permis internet, programme de prévention dispensé par des intervenants extérieurs et gendarmes aux fins de sensibiliser les enfants au civisme en ligne. Aujourd'hui, seul un quart des enfants de CM2 a pu passer et obtenir ce permis. Au collège et au lycée, les formations « PIX » traitent davantage de l'utilisation des outils informatiques que de leur fonctionnement et des dérives dans leurs usages.

Au regard du succès et de l'efficacité de ce dispositif dit « permis internet », nous soutenons sa généralisation, à la fin de l'école primaire et à la fin du collège, comme cela a été proposé par le Groupe LaREM dans le PJL[1] Principes républicains.

RECOMMANDATION 10 :
Assurer une formation aux risques et dérives numériques à toute personne qui le demande, dans les Maisons France Services via les auto-écoles du numérique.

Dès 2022, chaque canton disposera de sa Maison France Services. Elle est

1/4

seulement des élèves de CM2 a été formé aux risques numériques via le Permis internet.

1. PJL : Projet de loi

UN TIERS DES FRANÇAIS DÉCLARE AVOIR DÉJÀ ÉTÉ VICTIME D'UNE FAUSSE INFORMATION.

le lieu privilégié pour rendre accessibles les services essentiels dont chaque Français a besoin dans sa vie quotidienne. À ce titre, les Maisons France Services peuvent également accueillir des formateurs intervenant auprès des adultes, non seulement pour leur apprendre à utiliser des outils numériques, mais aussi pour les former à la compréhension de ces outils, de leur fonctionnement et de leurs dérives.

C'est pourquoi nous proposons de créer au sein des Maisons France Service une formation aux usages, risques et dérives du numérique, offerte dans toute la France et dispensée à toute personne qui en ferait la demande. Au-delà des éléments essentiels sur la maitrise des outils, ces formations mettraient l'accent sur le risque d'enfermement algorithmique, la qualité des sources, les dangers de manipulation de l'information (chiffres utilisés à mauvais escient, image truquée, rognée ou anachronique), la mésinformation (titres chocs trompeurs, articles écrits trop vite sans recul sur les faits).

RECOMMANDATION 11 :
Communiquer des messages de prévention sur les réseaux sociaux et à la télévision.

Si le regard est souvent orienté autour de la question des réseaux sociaux et de la responsabilité des plateformes, les chaînes de télévision ont également une double responsabilité. D'abord, elles peuvent être des vecteurs, volontaires ou non,

de fausses informations et de discours de haine : l'exemple de la chaîne américaine Fox News est probant. Ensuite, les seniors qui propageraient les fausses informations sept fois plus que le reste de la population sont les premiers consommateurs de programmes TV.

Il serait pertinent de rendre obligatoire la diffusion de spots d'information sur les dangers que représentent les fausses informations dans les mois précédant les élections, au même titre que les campagnes d'information officielles en période électorale. Ces messages de sensibilisation porteraient sur la vigilance à apporter aux fausses informations sur les réseaux sociaux. Ces campagnes de sensibilisation pourraient également être reprises dans le cadre de la propagande numérique visée à la recommandation 5, diffusées à large échelle, sous le contrôle du CSA.

4. PROTÉGER LA DÉMOCRATIE EUROPÉENNE

RECOMMANDATION 12 :
Créer un cyber-bouclier européen.

Le coût de des cyberattaques est colossal : quelques 400 milliards par an à l'échelle mondiale. Les menaces cyber touchent l'ensemble des citoyens européens dans leur quotidien, elles ne connaissent aucune frontière. Ces menaces directes au bon fonctionnement de l'ensemble des États membres de l'Union européenne appelle une réponse défensive coordonnée.

Comme le proposait le programme Renaissance, nous recommandons la mise en place un soutien mutuel entre États en cas d'attaque informatique, avec (1) un fonds européen pour le cyber pour réduire notre dépendance, (2) une cyber-police européenne, en charge de répondre à la criminalité en ligne et combattre l'usage d'internet par les terroristes, (3) une capacité européenne contre les cyber-attaques de puissances étrangères, avec notamment une assistance mutuelle entre États membres.

RECOMMANDATION 13 :
Organiser la réponse collective au niveau de l'Union européenne.

L'Union européenne et ses membres sont particulièrement visés par les attaques étrangères. Il est temps de mieux coordonner nos réponses et de donner à l'Union les moyens de faire face aux projets de déstabilisation d'autres grandes puissances.

Cela passe d'abord par une prise de conscience politique : les luttes contre la désinformation et contre l'ingérence étrangère devraient être inscrites dans de la politique de sécurité et de défense commune (PSDC) et de la politique étrangère (PESC) de l'UE, et discutée au niveau des chefs d'État.

En cas d'ingérence flagrante, les États membres devraient disposer de plans d'alerte et d'urgence collectifs et disposer de sanctions telles que le boycott économique, les restrictions financières ou l'interdiction de voyager.

RECOMMANDATION 14 :

Empêcher dans la loi européenne les financements des partis politiques par des puissances étrangères.

Nous soutenons la révision du règlement n°1141/2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes prévue en 2021. Elle permettra de rendre illégal en Europe l'engagement dans toute sorte d'activité secrète pour le compte d'un gouvernement étranger visant à influencer la politique européenne, à introduire une interdiction de dons provenant de l'extérieur de l'Union, à l'exception de ceux émanant d'électeurs vivant en dehors de l'UE et de l'EEE, ou l'obligation pour les partis de signaler lorsqu'ils sont approchés par une puissance étrangère qui propose de leur fournir une assistance électorale.

Déjà en partie régulés mais avec encore de forts potentiels de déstabilisation, les dons et les publicités achetés par des crypto-monnaies, qui permettent l'anonymat, devraient être également interdits.

2 ORGANISER LA RIPOSTE DES PARTIS POLITIQUES EN FRANCE ET À L'INTERNATIONAL

Les exemples étrangers le confirment : tous les partis démocratiques sont concernés par des tentatives d'ingérence et des attaques étrangères.Les mouvements français n'y échappent pas davantage. Nous devons, dès aujourd'hui, à la fois relever le niveau de vigilance et de protection de chaque parti, et s'engager à ne pas alimenter ces pratiques.

RECOMMANDATION 15 :
Appeler les partis politiques français à se prémunir et s'engager contre les ingérences et les manipulations de l'information.

Aucune élection française ne doit être perturbée par des puissances étrangères et leurs relais. Nous appelons tous les partis et groupements politiques français à rédiger et cosigner une charte commune qui les engagent à se protéger et à combattre les pratiques d'ingérence.

L'authenticité du débat politique, et du scrutin qui en résulte, sont des tenants précieux de notre vie démocratique. C'est pourquoi nous appelons l'ensemble des partis, forces et mouvements politiques de France, à conjuguer leurs efforts de manière transpartisane pour lutter contre ces tentatives de déstabilisation numérique. Nous proposons de rédiger et cosigner une charte commune marquant notre volonté de combattre ces menaces numériques et de mettre en œuvre des mécanismes de protection vis-à-vis de ces dérives et pratiques d'ingérences.

Cette charte porterait notamment des engagements en matière de :

- lutte contre la désinformation ;
- lutte contre la haine et la violence en ligne ;
- transparence des campagnes numériques ;
- outils et processus d'organisation interne contre ces menaces.

RECOMMANDATION 16 :
Appeler à une conférence internationale de mobilisation des partis progressistes.

Les formations politiques dans le monde sont toutes concernées par ces menaces nouvelles. Elles ont également toute la responsabilité d'y répondre et de s'organiser. Nous appelons à l'organisation d'une conférence internationale ouverte aux formations politiques françaises, européennes et étrangères, soucieuses de préserver nos systèmes démocratiques. Cette réunion favorisera des actions communes, l'échange de bonnes pratiques, et pourra aboutir sur des engagements mutuels.

AUCUNE ÉLECTION FRANÇAISE NE DOIT ÊTRE PERTURBÉE PAR DES PUISSANCES ÉTRANGÈRES ET LEURS RELAIS.

3

AU SEIN DE LAREM : METTRE EN PLACE LES OUTILS ET LES PROCESSUS D'ORGANISATION INTERNE CONTRE LES NOUVELLES FORMES D'INGÉRENCE ET DE PROPAGANDE NUMÉRIQUES

La menace d'ingérence dans le cadre de campagnes électorales est protéiforme. La virulence et le niveau de sophistication technique des puissances étrangères et de leurs relais intérieurs promettent des attaques constantes, d'une violence inédite.

Déjà, la puissance volumétrique des raids de militants et de bots mine une prise de parole libre et sans risque dans le cadre du débat démocratique. Et demain ? Les tentatives de déstabilisation du débat et de fragilisation des parties prenantes des campagnes électorales viennent menacer nos démocraties dans leur principe même.

C'est pour cela que LaREM renforce d'ores et déjà ses protocoles d'action afin de faire face aux différentes menaces : nous le devons à nos adhérents. Parce que le mouvement majoritaire est aussi une cible privilégiée des agents étrangers, il nous appartient d'être exemplaires.

Notre première démarche a été d'analyser les risques : probabilité de réalisation, évaluation des conséquences pour les personnes et pour la campagne, priorisation. Les tentatives de vol de données par hameçonnage constituent le risque le plus évident auquel LaREM fait face. L'expérience des MacronLeaks a donné à voir des attaques particulièrement élaborées, d'autant plus difficiles à détecter.

Si ce risque est connu, les tentatives de manipulation directe de l'opinion publique pourraient, elles, atteindre un nouveau stade. L'usage de « deep fakes », de « bots », les raids visant à faire émerger des sujets toxiques ou les faux comptes affiliés se faisant passer pour un groupe politique sont autant de menaces de mieux en mieux structurées, à prendre résolument en compte.

À partir de ce diagnostic, nous avons adopté une série d'engagements. De telles mesures pourraient par ailleurs être abordées lors des discussions concernant la charte transpartisane proposée par la recommandation 15.

ENGAGEMENT 1 :
Nous systématiserons des tests aléatoires et les protocoles de sécurité.

Des tests fréquents et aléatoires viseront régulièrement les salariés et les parlementaires LaREM afin d'analyser le taux potentiel de réussite d'une attaque. En cas d'hameçonnage ou de prise de contrôle et afin de limiter l'impact d'un vol de données :

— Les accès sont systématiquement limités : aucun administrateur ne dispose de l'ensemble des accès.

— Bonne pratique de la campagne de 2017, nous poursuivons les actions de *blurring* qui visent à réduire l'opportunité d'attaques extérieures en intégrant des contenus non authentiques dans les informations qui pourraient être piratées.

— Enfin, depuis mai 2021, la double authentification et l'expiration des mots de passe est généralisée à l'ensemble des salariés afin de

renforcer la sécurité de l'accès aux informations professionnelles et confidentielles.

ENGAGEMENT 2 :

Nous formerons les salariés et des cadres de campagne.

Engagement fort que notre mouvement prend pour ses équipes et ses adhérents, LaREM formera l'ensemble des salariés et des cadres de campagne aux risques d'ingérence numérique, avant chaque campagne électorale. Ces formations auront pour but de sensibiliser aux risques autant que donner des ressources clés en main pour faire face à tout type d'attaque numérique : parcours d'alerte interne, règles basiques d'hygiène numérique, usage des outils de riposte, recours juridique, etc.

ENGAGEMENT 3 :

Nous mettrons en œuvre des protocoles de réactions informatiques, juridiques et d'expertise.

Parce que les attaques seront nombreuses et intenses, il sera nécessaire d'apporter des réponses rapides, claires et efficaces. Pour cela, des protocoles ont été mis en place afin de prédéterminer des réponses aux menaces envisagées qui pourraient concerner des salariés et les équipes de campagne. Les protocoles prennent en compte aussi bien des éléments de réponse techniques que juridiques, et reposent sur les équipes internes et le soutien d'universitaires, journalistes ainsi que des plateformes numériques.

ENGAGEMENT 4 :

Nous créerons une cellule d'accompagnement des victimes.

La nécessité de la prise en charge des victimes est primordiale. Des « kompromats » aux raids numériques sur les réseaux sociaux, jour et nuit, par milliers, c'est aussi bien la santé mentale, la sécurité physique, que la dignité des victimes et de leurs proches qui peuvent être pris pour cibles par des acteurs malveillants. En cas d'attaque, une cellule d'accompagnement et de soutien prendra directement en charge les victimes pour leur apporter un soutien psychologique.

GLOSSAIRE ET TYPES DE MENACES

- « **Deep learning** » : ou apprentissage profond, est un ensemble de méthodes d'apprentissage automatique permettant de modéliser avec un haut niveau d'abstraction des données. Algorithme : une suite finie et non ambiguë d'opérations mathématiques ou d'instructions permettant de résoudre une classe de problèmes.

- « **Fact checking** » : est une technique consistant à vérifier en temps instantané la véracité des faits et l'exactitude des chiffres présentés dans les médias par des personnalités politiques et des experts.

- « **Feed** » : qualifie le *flux web* alimenté sur les réseaux sociaux.

1. VOL D'INFORMATION

- **Hameçonnage** : (« *phishing* » en anglais) est une technique frauduleuse destinée à leurrer un internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de pass etc.) et/ou bancaires, en se faisant passer pour un tiers de confiance.

- « **Kompromat** » : désigne l'utilisation de documents compromettants, authentiques ou fabriqués pour nuire à une personnalité politique, un journaliste, un homme d'affaires ou tout autre figure publique.

- **Vol de données personnelles** : des pirates accèdent à une base de données et la diffusent. Cela met

en cause l'image de l'organisation et impacte ceux qui y travaillent (adresse révélée, appels répétés, spams).

- **Piratage discret** : des assaillants gagnent l'accès à l'ensemble d'un système informatique et volent des informations stratégiques.

2. MANIPULATION DE L'OPINION PUBLIQUE

- **« Trap »** : Des déstabilisations simples menées, sans expertise technique, en jouant sur des détails. Par exemple, en achetant un nom de domaine proche de celui utilisé par un candidat ('jlm2017' qui dirigeait vers le site de Benoit Hamon) ou en changeant un caractère d'un compte sur les réseaux sociaux.

- **« Deepfakes »** : grâce à des algorithmes très puissants qui se basent sur des extraits réels, des assaillants imitent la voix ou l'image de candidats pour y adjoindre des propos inventés.

- **« Fake news »** : des informations inventées et diffusées dans un but malveillant.

- **« Astroturfing »** : avec l'utilisation de faux comptes et d'outils permettant de générer des phrases complexes, les assaillants donnent la fausse impression qu'un sujet ou une opinion émerge.

- **« Bot » ou « robot »** : un agent logiciel automatique ou semi-automatique qui interagit avec des serveurs informatiques. Il agit comme un programme utilisé par un humain.

3. PRISE DE CONTRÔLE

- **Déstabilisation d'une infrastructure digitale** : des pirates envoient un grand nombre de requête à un service, provoquant le blocage de l'accès pour les utilisateurs et permettant de réaliser un chantage.

- **Infrastructure physique** : des assaillants prennent contrôle d'équipements pour espionner (télévision, micros etc.) ou pour détruire (par une sollicitation trop importante).

- **« Leak »** : des pirates volent des documents officiels et y joignent des faux (cas des MacronLeaks).

- **« Ransomware »** : des assaillants s'introduisent dans un système puis rendent inutilisable les données (par cryptage) avant de demander une rançon.

EM!