

Quand protéger le vote ne suffit plus : la sécurité électorale face aux manipulations de l'information

Fabrice Lollia | 23 septembre 2026 | ARTICLES | 



À l'ère numérique, protéger une élection ne consiste plus seulement à sécuriser les urnes, les bureaux de vote ou le dépouillement. Cela suppose aussi de protéger l'espace informationnel, entendu ici comme l'ensemble des contenus, plateformes, acteurs et mécanismes de circulation qui participent à la formation du jugement des citoyens. Cet espace est désormais exposé à des formes multiples de perturbation : la mésinformation, c'est-à-dire la diffusion d'informations fausses sans intention de nuire ; la désinformation, qui repose sur la diffusion délibérée de contenus faux ou trompeurs ; la malinformation, qui consiste à utiliser de manière nuisible des informations authentiques, souvent sorties de leur contexte ; ainsi que les contenus synthétiques générés par intelligence artificielle, comme les deepfakes. La distinction entre mésinformation, désinformation et malinformation, proposée notamment par [Claire Wardle et Hossein Derakhshan](#), permet de mieux saisir la diversité des mécanismes de manipulation.

Le cas roumain de 2024 en offre une illustration décisive. Lors du premier tour de [l'élection présidentielle](#), Călin Georgescu, candidat nationaliste et souverainiste longtemps marginal dans les enquêtes d'opinion, est arrivé en tête après une progression spectaculaire de sa visibilité sur TikTok. Quelques jours plus tard, la Cour constitutionnelle roumaine a [annulé](#) le processus électoral, dans un contexte marqué par des soupçons de campagne numérique coordonnée, de promotion artificielle et d'ingérence étrangère.

Cet épisode a servi d'électrochoc en Europe. Il a montré qu'une élection pouvait être fragilisée non seulement par une fraude matérielle (bourrage d'urnes, falsification du dépouillement ou pression sur les électeurs) mais aussi par la dégradation des conditions de formation du jugement démocratique. Lorsque des contenus politiques sont amplifiés artificiellement, que l'origine des campagnes demeure opaque ou que des plateformes deviennent des espaces de manipulation asymétrique, c'est la sincérité même du scrutin qui peut être mise en cause. Le cas roumain marque ainsi un changement d'échelle : la manipulation informationnelle n'apparaît plus comme un simple désordre numérique, mais comme une menace institutionnelle pour l'intégrité électorale.

Cet article pose la question de la protection du débat public, dans lequel les citoyens forment leur jugement. Tous les scrutins ne sont pas exposés de la même façon. En démocratie, la présidentielle concentre ces vulnérabilités à un degré particulier, en ce [qu'elle personnalise le pouvoir, polarise davantage les camps et engage plus directement la question de la légitimité politique](#). Les réseaux sociaux ont largement [contribué](#) à transformer des campagnes présidentielles dans la mesure où ils accélèrent la circulation des contenus, favorisent les messages les plus émotionnels, facilitent la diffusion de récits trompeurs et permettent d'amplifier artificiellement certains thèmes. Des organisations telles que [l'Organisation de coopération et de développement](#)

économiques (OCDE) considèrent que la désinformation et le poids des plateformes constituent des enjeux directs pour l'intégrité démocratique.

La problématique peut dès lors être formulée ainsi : comment protéger une élection lorsque la menace ne porte plus seulement sur l'acte de voter, mais aussi sur l'environnement informationnel façonné par les plateformes numériques ?

C'est dans ce cadre que se situe l'argument central de cet article : montrer que, dans les démocraties contemporaines, la protection du vote passe aussi par la protection de l'environnement informationnel. Il est possible d'avoir un scrutin correctement organisé qui laisse pourtant derrière lui un pays divisé, plus méfiant, voire instable face aux irrégularités numériques possibles. Le problème n'est plus uniquement celui des faux contenus isolés, mais plutôt celui d'un climat informationnel **capable d'affaiblir la confiance des citoyens dans les faits, dans le scrutin et, au bout du compte, dans la légitimité du résultat**. Pour saisir cette transformation, l'analyse suivra quatre étapes. Elle montrera d'abord comment les réseaux sociaux reconfigurent la menace électorale. Elle reviendra ensuite sur trois cas révélateurs, puis examinera la manière dont la manipulation contemporaine déborde désormais le simple mensonge. Elle analysera enfin pourquoi la présidentielle constitue un terrain particulièrement vulnérable avant d'en tirer la leçon centrale sur ce que cette mutation impose désormais aux démocraties.

Quand les réseaux sociaux transforment la menace électorale

Pendant longtemps, la sécurité électorale a surtout été pensée autour des questions concrètes et visibles : le bourrage d'urnes, l'intimidation des électeurs, la falsification des résultats, les violences autour du scrutin et les pressions sur les institutions chargées de l'organiser. Ces risques existent toujours et, dans de nombreux pays, ils sont même centraux. Le Mozambique en a donné **une illustration récente** après l'élection d'octobre 2024. La contestation du scrutin a débouché sur des manifestations massives, des affrontements avec la police et de nombreux morts, dans un contexte de critiques sur la régularité du vote et sur les écarts constatés dans le décompte.

Or, une part croissante de la menace électorale se situe désormais dans l'espace informationnel. C'est-à-dire que là où l'on cherchait autrefois à altérer directement le résultat, on cherche aujourd'hui à durcir les camps, à troubler les perceptions, à installer le soupçon, notamment pour rendre la vérité contestable. Les acteurs spécialisés **dans le domaine** de l'intégrité électorale insistent sur le fait que cette évolution affecte directement la crédibilité du processus électoral.

Les réseaux sociaux ne sont pas uniquement de nouveaux supports de communication. Ils ont **changé la mécanique** de la campagne électorale, en en modifiant le rythme, les critères de visibilité et les circuits d'autorité. Une campagne ne se joue donc plus seulement dans les assemblées publiques, les journaux télévisés ou les débats. Elle se joue aussi dans un **flux numérique continu** où l'attention se fait rare, où la visibilité se gagne en temps réel et où les récits les plus efficaces ne sont pas toujours les plus fiables.

Tout d'abord, ils ont changé la vitesse de propagation de l'information, qu'elle soit vraie ou fausse. Une rumeur, une vidéo ou une séquence émotionnelle peut désormais envahir le débat public en quelques heures, comme l'a montré l'élection roumaine de 2024 dont nous avons parlé au début de cet article. La campagne se déroule désormais dans un flux d'information continu qui ne laisse que peu de place au recul réflexif. C'est cette vitesse qui affaiblit la vérification et favorise les réactions impulsives. Une **étude** scientifique, portant sur 126 000 rumeurs diffusées sur Twitter entre 2006 et 2017, montre que les fausses nouvelles y atteignaient plus d'un millier de personnes environ six fois plus vite que les vraies, avec un effet particulièrement marqué dans le domaine politique.

Ensuite, les plateformes numériques ont **reconfiguré** les critères de visibilité en privilégiant les contenus les plus saillants sur le plan émotionnel, conflictuel ou polarisant, au détriment des messages modérés, complexes ou nuancés. Cette logique contribue à déformer la qualité du débat et à **favoriser** la circulation des contenus simplificateurs.

Troisièmement, pendant longtemps, la parole politique passait par des intermédiaires identifiables, à savoir la presse, la télévision, les partis, les institutions et les experts. Aujourd'hui, un influenceur, un compte anonyme ou une communauté numérique coordonnée peut jouer un rôle décisif dans la circulation d'un récit politique. La campagne « **Stop the Steal** », aux États-Unis en 2020, en est un exemple concret. Elle a montré que des groupes Facebook, des influenceurs et des communautés numériques très actives ont contribué à imposer dans l'espace public un faux récit de fraude électorale. Les médias traditionnels, les partis et les institutions ont été dépassés dans leur capacité à imposer les thèmes dominants du débat public. Un autre exemple illustratif du poids des réseaux sociaux est celui de **Madagascar**, où les paroles des institutions ont été fortement concurrencées par celles des réseaux sociaux lors du renversement du régime en octobre 2025.

Enfin, les réseaux sociaux ont changé la texture émotionnelle de la campagne : peur, moquerie, indignation, sentiment d'humiliation ou d'injustice sont mis de l'avant. Or, une campagne présidentielle est déjà, par nature, une période de tension que les réseaux rendent désormais plus permanente et plus intense. L'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) **rappelle** d'ailleurs le rôle croissant des réseaux sociaux dans l'accès à l'information politique. Le cas des États-Unis est, à cet égard, éclairant. Le **récit de la fraude** de 2020 a prospéré non seulement parce qu'il circulait vite, mais aussi parce qu'il activait un ressort émotionnel puissant, celui de la dépossession et de la colère. Dans cet environnement, le débat

électoral devient plus réactif, plus conflictuel, tout en restant vulnérable aux séquences de déstabilisation.

Autrement dit, les réseaux sociaux n'ont pas simplement ajouté un canal aux campagnes présidentielles ; ils en ont transformé les conditions mêmes, en modifiant la vitesse à laquelle un récit s'impose, les critères qui lui donnent de la visibilité, les acteurs capables de le porter et les émotions qui en assurent la diffusion. C'est cette transformation qui rend aujourd'hui les campagnes plus exposées aux manipulations de l'information.

Trois cas révélateurs : la Roumanie, les États-Unis et Madagascar

La Roumanie a rendu visible ce que beaucoup considéraient comme un risque secondaire. En décembre 2024, la Cour constitutionnelle roumaine a annulé l'ensemble du processus électoral présidentiel après la déclassification d'éléments faisant état d'interférences et de manipulations informationnelles ayant affecté la campagne. À la suite de cet événement, la Commission européenne a ouvert une procédure formelle contre TikTok, estimant qu'il existait des risques pour l'intégrité électorale. Ce précédent est décisif parce qu'il marque un changement d'échelle. Une campagne numérique n'est plus traitée comme un simple désordre informationnel mais comme une menace institutionnelle susceptible d'affecter la « sincérité du scrutin », c'est-à-dire la capacité des électeurs à former librement leur jugement dans un environnement informationnel loyal, non faussé par des manipulations artificielles, coordonnées ou étrangères.

Le cas roumain montre ainsi que la question ne se limite pas au faux contenu. C'est celle d'un environnement de plateforme capable d'altérer la visibilité des acteurs, la hiérarchie des récits et, finalement, les conditions mêmes de la compétition électorale. Le cas roumain marque alors une rupture en ce sens : le risque électoral ne se limite plus à la fraude visible ou à la propagande classique et inclut désormais la possibilité qu'une architecture de circulation algorithmique devienne un facteur de distorsion du scrutin.

Le cas américain prolonge ce constat sur un registre différent. Lors des présidentielles de 2016 puis de 2020, Twitter (aujourd'hui X) a joué un rôle important dans la circulation de récits trompeurs et de messages polarisants et, plus largement, dans l'instauration d'un climat de défiance autour du scrutin. Cet exemple n'a pas seulement montré que Twitter pouvait devenir un lieu de polarisation politique, mais a également confirmé que, sur cette plateforme, les fausses nouvelles circulent mieux que les vraies. Dans le même temps, environ 53 % des adultes américains déclaraient, en 2020, s'informer au moins en partie via les réseaux sociaux. Le problème n'est pas la présence de faux contenus, mais plutôt la capacité des plateformes à en accélérer la circulation dans un environnement déjà polarisé. Le problème ne se résume pas à TikTok ou à Twitter : dans d'autres contextes, comme celui de Madagascar, on s'aperçoit que Facebook reste la plateforme centrale de structuration de l'opinion politique en temps de crise.

La conjugaison de ces trois cas montre que, en écho aux travaux de Soroush Vosoughi sur Twitter, la menace n'épouse plus le même format et que, lorsqu'un réseau social devient un passage obligé de l'information politique, il devient aussi un levier d'influence, de polarisation et donc de déstabilisation.

Quand la manipulation ne passe plus par le mensonge

La manipulation de l'information ne peut être réduite à la seule diffusion de fausses nouvelles. Dans les campagnes présidentielles contemporaines, la manipulation ne porte pas uniquement sur le vrai ou le faux. Il s'agit, comme le montre le cas roumain, d'une action plus large sur la visibilité des récits, leur cadre d'interprétation et, finalement, sur les conditions propres au jugement politique. Cette technique demeure classique mais elle n'a rien perdu de son efficacité.

Aux États-Unis, l'élection de Donald Trump en 2024 offre un autre contexte d'analyse. La forme la plus visible reste l'altération du contenu. Il s'agit alors de diffuser un récit faux, trompeur ou falsifié pour nuire à un adversaire ou renforcer un camp. Durant la campagne, plusieurs intox ont ainsi visé à discréditer Kamala Harris, qu'il s'agisse de faux récits personnels ou de fausses contestations de son éligibilité. Le but n'était pas uniquement de désinformer ponctuellement ; il s'agissait aussi d'éroder la crédibilité attachée à une candidature dans la durée.

Mais la manipulation ne consiste pas toujours à inventer du faux ; soit de désinformer. Elle peut aussi consister à donner à un contenu une visibilité qu'il n'aurait jamais acquise spontanément (mésinformation). Ce qui est manipulé, c'est la visibilité du fait falsifié : on fait apparaître, de façon centrale, massive et évidente, quelque chose qui ne l'était pas spontanément. Quelques comptes très actifs, des relais militants, des communautés coordonnées ou des réseaux automatisés suffisent à imposer un thème dans la conversation générale. Le but n'est pas toujours de convaincre, mais d'occuper l'espace, de saturer l'attention et de créer un effet de présence.

En Allemagne, lors de la campagne des élections fédérales du 23 février 2025, des chercheurs ont identifié un réseau de plus de sept cents faux comptes diffusant des messages pro-russes et hostiles à Friedrich Merz, alors chef de la CDU/CSU (Union chrétienne-démocrate d'Allemagne / Union chrétienne-sociale) et principal candidat à la chancellerie. Principalement actifs sur les réseaux sociaux, ces comptes visaient à amplifier un discours politique défavorable à Merz, dont la position pro-ukrainienne l'exposait à des opérations d'influence pro-russes. Merz est devenu chancelier fédéral en mai 2025.

La manipulation peut aussi agir de manière plus subtile, par ce qu'on pourrait appeler un cadrage orienté. Cela signifie qu'on ne

ment pas directement ; on va sélectionner, isoler, répéter et retirer du contexte, en mettant en avant un détail pour lui donner une portée générale forte et significative. On transforme ainsi une séquence secondaire en vérité dominante. Ce qui change, ce n'est pas seulement le contenu du message, mais aussi la manière dont il est présenté, hiérarchisé et, surtout, rendu signifiant. Par **exemple**, lors de la campagne européenne de 2024, le parti d'extrême droite portugais Chega (« C'est assez » en portugais) a été accusé d'avoir diffusé une vidéo tronquée d'un échange entre son dirigeant, André Ventura, et un travailleur migrant, de façon à imposer une lecture politique plus favorable au parti. Ce qui était en jeu n'était pas l'invention d'une scène mais le **cadre interprétatif** retenu pour lui donner un sens immédiatement exploitable dans la situation.

À ce stade, l'analyse doit se déplacer vers un niveau plus profond, tenant à la réception de l'information. Les **travaux** de Paul Charon sont ici particulièrement utiles. Par la notion « d'architexte », il désigne une trame mentale qui construit des schémas prêts à l'emploi et rend certains contenus trompeurs immédiatement plausibles. Un récit trompeur fonctionne d'autant mieux quand il vient se loger dans une histoire que le public connaît déjà : le complot, la trahison des élites, la fraude cachée, la nation menacée, etc. Cette approche montre ainsi que dans ce cas, il ne s'agit plus seulement de se focaliser sur les faits, mais sur les cadres d'interprétation qui leur donnent du sens.

Elle devient encore plus puissante lorsqu'elle s'arrime à l'émotion, vecteur de viralité important de la circulation de l'information sur les réseaux sociaux. Les contenus sont créés non pas pour informer mais pour provoquer une réaction. Le but est de faire réagir le citoyen en le poussant à partager le contenu par l'émotivité. La manipulation devient alors d'autant plus efficace qu'elle active une peur, une colère ou un sentiment d'humiliation déjà présents dans le corps social.

L'émergence des contenus génératifs, en particulier les deepfakes audio, constitue un signal supplémentaire. Un exemple notable s'est produit en Slovaquie en 2023, où, deux jours avant les élections législatives, un enregistrement attribué à Michal Šimečka, dirigeant du parti Progressive Slovakia, et à la journaliste Monika Tódová, a circulé en ligne, les présentant comme discutant prétendument d'une manipulation électorale. Cet épisode ne permet pas d'affirmer que l'intelligence artificielle a déterminé le résultat du scrutin ; il illustre cependant la manière dont un contenu synthétique, diffusé à un moment critique d'une campagne, peut acquérir une viralité importante, compliquer les efforts de vérification et affaiblir la confiance dans le processus électoral.

Au Pakistan, lors des élections générales de février 2024, le parti d'Imran Khan, à l'inverse, a utilisé l'IA pour **diffuser des discours recréant la voix de son leader emprisonné**, montrant que ces outils peuvent servir aussi bien à manipuler qu'à contourner une contrainte politique. Dans ces deux cas, on voit comment l'intelligence artificielle accroît encore la puissance des plateformes. Elle ne se limite plus à la circulation des récits ; elle en produit la matière même et complique encore le travail de vérification.

Enfin, la manipulation peut prendre une forme plus diffuse via le **brouillage**. Dans ce cas, le but est de rendre toute lecture incertaine en multipliant les versions concurrentes et de faire naître l'idée que rien n'est véritablement vérifiable. C'est d'ailleurs la raison pour laquelle on distingue explicitement la mésinformation, la désinformation et la malinformation. Comme expliqué précédemment, la première renvoie à une information fausse partagée sans intention de nuire, la deuxième à un contenu faux délibérément fabriqué pour tromper ou causer un dommage, et la troisième à une information authentique utilisée de manière malveillante, souvent hors contexte. Un exemple intéressant est celui du modèle « **firehose of falsehood** ». Cette stratégie repose sur la diffusion rapide, répétée et massive de récits multiples, parfois contradictoires, afin de saturer l'espace informationnel et de rendre plus difficile l'établissement d'une version stabilisée des faits.

Pris ensemble, ces procédés montrent que la manipulation numérique agit à plusieurs niveaux. Elle fabrique des contenus, organise leur circulation, active des cadres de lecture déjà présents dans l'esprit du public et, finalement, brouille la capacité collective à distinguer ce qui est vrai, plausible ou faux. Nous ne sommes donc plus dans un simple problème de mensonges ou de fausses nouvelles, mais dans une action plus large qui interroge les conditions de réception, d'interprétation et de jugement de l'information. En ce sens, la manipulation de l'information est moins une simple pathologie du débat public qu'une technique de déstabilisation du jugement démocratique lui-même. Ces mécanismes n'affectent pas tous les scrutins de la même façon. C'est dans la présidentielle qu'ils trouvent aujourd'hui l'un de leurs terrains les plus sensibles.

Pourquoi les élections présidentielles sont-elles particulièrement exposées ?

De la même manière que les élections présidentielles, des élections législatives peuvent, dans un régime parlementaire, devenir des cibles majeures lorsqu'elles déterminent la formation du gouvernement, l'orientation diplomatique ou les choix stratégiques d'un pays. Il est donc plus juste de parler de scrutins nationaux décisifs. Les présidentielles constituent toutefois un cas d'intensification, car elles concentrent plus fortement l'attention médiatique, la personnalisation du pouvoir, les affects politiques et les enjeux de légitimité autour d'une figure centrale.

Cette vulnérabilité est particulièrement forte dans le cadre des élections présidentielles, car ces scrutins concentrent pouvoir, attention médiatique, émotions politiques et enjeux de légitimité, rendant toute tentative d'influence sur les perceptions collectives particulièrement rentable.

Les présidentielles concentrent plusieurs fragilités que d'autres scrutins portent moins fortement. Elles personnalisent au maximum l'affrontement en simplifiant les camps en présence, ce qui transforme plus facilement le débat en duel symbolique.

Dans un tel cadre, les attaques circulent plus facilement et les tentatives de délégitimation politique deviennent plus rentables. C'est aussi le scrutin où la question de la légitimité est la plus sensible. Quand un président est élu au nom d'un pays, ce n'est pas seulement un résultat qui est produit ; c'est une autorité qui est installée. Lorsqu'une campagne nourrit durablement le soupçon ou le sentiment de manipulation, l'autorité issue du scrutin peut être fragilisée dès l'origine, même en l'absence d'irrégularité prouvée. Madagascar en a donné une [illustration lors de la présidentielle de 2023](#). Celle-ci s'est déroulée dans un climat de boycott de l'opposition, de faible participation et de contestation persistante. Ce qui montre qu'un scrutin peut être formellement tenu tout en restant politiquement fragilisé dans sa réception.

Enfin, les élections présidentielles, ou plus largement les élections nationales qui déterminent l'orientation de l'exécutif, constituent des cibles [privilégiées](#) pour les stratégies d'ingérence extérieure. Parce qu'elles concentrent l'attention médiatique, peuvent modifier l'orientation stratégique d'un pays et offrent une forte visibilité internationale, elles représentent un moment particulièrement attractif pour des acteurs cherchant à influencer le débat public, tester des capacités de nuisance ou fragiliser la confiance démocratique.

Ce que cette transformation impose aux démocraties

Nous sommes face à un problème systémique qui tient à la vitesse de circulation, à la surcharge informationnelle, à la fragmentation des publics, ainsi qu'aux fragilités des médiations et aux lenteurs des réponses institutionnelles. Ce n'est pas uniquement la lutte contre la désinformation qu'il faut améliorer, mais l'ensemble de la sécurité électorale qu'il serait utile de repenser.

La première évolution à assumer est doctrinale. En pensant à la sécurité électorale principalement comme une affaire de procédure (sécurisation des bureaux, fiabilité du dépouillement, intégrité des listes), une partie croissante de la menace continuera d'échapper aux institutions. L'idée défendue ici est celle de l'acceptation de l'environnement informationnel comme faisant partie intégrante de la crédibilité du scrutin. Une présidentielle ne se fragilise pas seulement quand l'urne est compromise ; elle se fragilise aussi lorsque les conditions de formation du jugement démocratique se dégradent. Les acteurs spécialisés dans la protection de l'intégrité électorale, tels que [Viginum](#) en France, insistent d'ailleurs de plus en plus sur ce point afin d'assurer la crédibilité du scrutin.

Cela implique, ensuite, une adaptation des institutions. Les autorités électorales, les pouvoirs publics et les acteurs chargés de garantir la régularité du scrutin doivent apprendre à répondre plus vite, plus clairement et plus simplement aux récits trompeurs qui menacent la crédibilité du processus. C'est déjà ce qui se passe dans de nombreux pays dotés d'une cellule info-communicationnelle de riposte, mais ce n'est pas le cas dans l'ensemble des pays dotés d'un vote démocratique. Le silence, le retard ou le langage trop technique laisse un vide, et ce vide est toujours occupé par des récits concurrents, parfois trompeurs, souvent plus simples, plus rapides et plus émotionnels. Dans ce domaine, il ne s'agit pas uniquement de corriger le faux, mais d'éviter qu'il ne s'impose comme cadre de compréhension avant même que la réponse institutionnelle n'arrive, comme le montrent certains [cas](#). Cette logique rejoint les [constats de l'OCDE](#) qui insiste précisément sur la nécessité de renforcer la transparence, la coordination et la résilience collective face à la désinformation.

Mais la réponse ne saurait se réduire à une solution technologique unique. Dans de nombreux pays, la biométrie est avancée comme un moyen de sécuriser les élections, en améliorant la vérification de l'identité des électeurs et la traçabilité des opérations d'enregistrement. Sur ce point, l'argument n'est pas sans fondement. [Les travaux de Marielle Debos](#) sur la biométrie en contexte électoral au Tchad en 2016 montrent que cette technologie est souvent présentée comme un moyen de fiabiliser les listes et de limiter les inscriptions multiples. Mais en pratique, dans ce cas précis, elle n'a pas permis d'organiser des élections plus transparentes et crédibles. Elle en souligne au contraire les limites : coûts élevés, dépendance technique, risques de pannes, vulnérabilité cyber et exclusion possible de certains électeurs.

La biométrie peut ainsi renforcer certains maillons du processus électoral, mais elle demeure un outil de [complémentarité et non de substitution](#). Elle ne règle pas à elle seule les crises de confiance ou les manipulations de l'information qui caractérisent les fragilités institutionnelles entourant une présidentielle.

[Le cas malgache](#) est, de ce point de vue, intéressant. Le lancement en janvier 2026 d'un programme national d'enrôlement biométrique pour bâtir une identité numérique a été présenté par les autorités comme un levier de modernisation administrative permettant d'éviter des erreurs susceptibles d'affecter la régularité du scrutin, comme les doublons, les erreurs et certaines irrégularités susceptibles d'affecter la liste électorale. Cet exemple montre bien ce que la biométrie peut apporter : une meilleure fiabilité du registre, donc une partie de la réponse. Mais il met également en garde contre une approche [technosolutionniste](#) qui ne peut pas, à elle seule, résoudre la défiance, la circulation des récits trompeurs, la polarisation et, plus largement, la crise du jugement collectif qui peut entourer une présidentielle.

La question des intermédiaires de confiance devient alors centrale. Quand le débat se durcit, leur rôle devient encore plus puissant. Médias, journalistes, autorités indépendantes, chercheurs, acteurs de vérification et institutions de régulation doivent être en mesure d'établir les faits mais aussi de les rendre visibles dans un espace qui valorise davantage le choc que l'explication. Le défi n'est pas celui de la vérité mais celui de la circulation. Une information exacte mais inaudible ne suffit pas à stabiliser le débat public.

Cette transformation appelle enfin à un effort civique à plus long terme. Aucune démocratie ne peut espérer supprimer totalement la manipulation informationnelle. En revanche, elle peut réduire son efficacité si les citoyens sont mieux préparés à reconnaître certaines techniques simples : émotions instrumentalisées, image sortie de son contexte, récit trop parfait pour être vrai, répétition organisée, environnement trop propice à la réception de l'information (architexte), etc. Cette préparation n'est pas un luxe, elle relève de l'hygiène démocratique.

*

* *

Le risque électoral connaît une transformation. Il ne se limite plus à la fraude visible, à la pression physique ni même à l'irrégularité du dépouillement. Il passe aussi par la dégradation du climat informationnel dans lequel se déroule l'élection choisie ici : la présidentielle. C'est pourquoi protéger le vote physiquement ne suffit plus. Une démocratie peut sécuriser ses bureaux, ses listes et ses opérations de dépouillement, tout en laissant se détériorer ce qui donne sens au scrutin, à savoir les conditions dans lesquelles les citoyens s'informent, interprètent, débattent et acceptent le verdict des urnes. Le risque n'est plus seulement de fausser le résultat, mais aussi de miner la confiance nécessaire pour qu'un résultat, même régulier, soit reconnu comme légitime. La priorité est donc lisible. Les démocraties doivent cesser de penser la sécurité électorale comme une affaire uniquement de procédure. Elles doivent protéger à la fois le vote, le registre, le débat public et les conditions de la confiance collective. Cela suppose d'articuler sécurité technique, vigilance informationnelle, capacité de réponse institutionnelle, solidité des intermédiaires de confiance et préparation des citoyens aux nouvelles formes de manipulation.

Crédits photo : [Alicja Nowakowska/iStock](#)

● — ●● — ● ●● — ● — ● ●●

Fabrice Lollia

Fabrice Lollia est directeur de l'Observatoire des Dynamiques Stratégiques Afrique-Océan Indien (ODS-AOI) et chercheur associé au DICEN-IDF. Ancien membre des services spécialisés de la Police nationale française, docteur en sciences de l'information et de la communication et titulaire d'un Executive MBA, ses travaux portent sur la stratégie, la sécurité/sûreté, la gouvernance numérique et l'intelligence artificielle, avec un intérêt particulier pour les environnements complexes d'Afrique et de l'océan Indien.

Comment citer cette publication

Fabrice Lollia, « Quand protéger le vote ne suffit plus : la sécurité électorale face aux manipulations de l'information », *Le Rubicon*, vol. 6, 23 septembre 2026 [<https://lerubicon.org/quand-protoger-le-vote-ne-suffit-plus-la-securite-electorale-face-aux-manipulations-de-linformation/>].