Cahiers français
Comprendre la société, éclairer le débat public

Grand entretien avec Perrine Simon-Nahum : pourquoi la démocratie est-elle en crise ?

+ La lutte contre le trafic de drogue
+ Remédier aux déserts médicaux
+ Les jeux Olympiques de 1924

Les défis de la démocratie

- Abstention et défiance
- La dérive populiste
- Sécurité et État de droit

Mai-juin 2024 I 439

La Documentation française

Sommaire

5 Politiques publiques

La lutte contre le trafic de drogue à ciel ouvert
Sebastian Roché

15 Dossier

Les défis de la démocratie

16/ **Grand entretien**
avec Perrine Simon-Nahum
Pourquoi la démocratie est-elle en crise ?

24 / Comment rendre notre vie politique plus démocratique ?
Débat entre Marc Lazar et Anne Levade

36 / La sécurité au défi de l'État de droit
Débat entre Dominique Rousseau et Bertrand Mathieu

46 / Les inégalités, un risque pour la démocratie ?
Nicolas Duvoux

54 / Démocratie et transition écologique
Dominique Bourg

62 / Les conséquences démocratiques des mutations de la surveillance numérique
Bernard Benhamou

70 / Former le citoyen
Iannis Roder

80/ Les plus de la rédaction

80/ ***Ce qu'il faut retenir***
81/ ***Les mots du dossier***
82/ ***Les chiffres clés***
83/ ***Les dates clés***
84/ ***Le dossier en dessins***
85/ ***Pour en savoir plus***

87 En débat

Que faire contre les déserts médicaux ?
Magali Dumontet et André Grimaldi

97 Le point sur

Le Parlement européen
Marion Gaillard

103 C'était en... 1924

Le centenaire des jeux Olympiques de Paris
Olivier Gaudefroy

→ Retrouvez l'univers *Cahiers français* sur **www.vie-publique.fr/cahiers-francais**
→ **Les fiches** au format mobile

Dossier

Les défis de la démocratie

16
Grand entretien
avec Perrine Simon-Nahum
Pourquoi la démocratie est-elle en crise ?

24
Comment rendre notre vie politique plus démocratique ?
Débat entre Marc Lazar et Anne Levade

36
La sécurité au défi de l'État de droit
Débat entre Dominique Rousseau et Bertrand Mathieu

46
Les inégalités, un risque pour la démocratie ?
Nicolas Duvoux

54
Démocratie et transition écologique
Dominique Bourg

62
Les conséquences démocratiques des mutations de la surveillance numérique
Bernard Benhamou

70
Former le citoyen
Iannis Roder

80
Les plus de la rédaction

→ Ce qu'il faut retenir
→ Les mots du dossier
→ Les chiffres clés
→ Les dates clés
→ Le dossier en dessins
→ Pour en savoir plus

Les conséquences démocratiques des mutations de la surveillance numérique

Bernard Benhamou
Secrétaire général de l'Institut de la souveraineté numérique

Les démocraties sont confrontées à de nouvelles menaces intérieures et extérieures liées aux évolutions des technologies de surveillance de masse. L'extraction de données sur les individus, qui constitue le « cœur » des modèles économiques publicitaires sur Internet, accentue désormais les risques d'ingérence et de manipulation des opinions publiques. La conception et la régulation des nouvelles générations de technologies comme l'intelligence artificielle ou les technologies d'analyse ADN représentent désormais des enjeux cruciaux pour l'ensemble des sociétés démocratiques.

Avec plus des deux tiers de la population mondiale connectés à l'Internet et 6,5 milliards de smartphones en circulation, les technologies numériques « irriguent » aujourd'hui la totalité des secteurs de l'activité humaine. L'essor des smartphones et des réseaux sociaux a ainsi permis de démultiplier les sources d'information disponibles sur les caractéristiques, les activités, mais aussi les convictions des individus. Les évolutions technologiques de l'Internet ont aussi permis de rendre la surveillance numérique à la fois plus intrusive et plus efficace. En effet, en plus des atteintes aux libertés, ces technologies constituent désormais un risque pour le fonctionnement démocratique de nos sociétés.

En 2013, les révélations de l'informaticien et lanceur d'alerte Edward Snowden sur les programmes de la National Security Agency (NSA), et les dérives liées à la surveillance de masse sont devenues l'un des éléments du débat démocratique sur les technologies. En effet, au-delà des opérateurs de télécommu-

nications, ces programmes de surveillance s'appuyaient sur les données des grandes plateformes de l'Internet et permettaient une surveillance inédite des citoyens. Pour une grande part, ces programmes avaient été développés en dehors d'un cadre légal pourtant favorable aux activités des services de renseignement américains depuis les attentats du 11 septembre 2001. Cette tendance s'est confirmée avec la récente prolongation de la validité de l'article 702 de la loi FISA (Foreign Intelligence Surveillance Act[1]). En effet, cette loi, du fait de son extraterritorialité, impose aux acteurs technologiques américains de transmettre aux services de renseignement les données de leurs utilisateurs non américains, où que ces données puissent être situées dans le monde.

Extraire toujours plus de données sur les utilisateurs…

Comme l'indique Shoshana Zuboff dans son ouvrage *L'Âge du capitalisme de surveillance*[2], les responsables de Google se sont rapidement rendu compte qu'il leur était utile de conserver toutes les requêtes y compris les plus insignifiantes. Cela afin de consolider les profils de leurs utilisateurs et non plus seulement de leur fournir des réponses pertinentes. Ces données sur les utilisateurs que la sociologue américaine nomme le « surplus comportemental » ont ainsi permis la transformation d'un moteur de recherche en acteur publicitaire majeur. Ce que Shoshana Zuboff résumait ainsi : « On croyait chercher sur Google, mais c'était Google qui cherchait en nous. »

GCHQ Bude (Cornouailles) est une station terrestre de surveillance par satellite du gouvernement britannique, exploitée dans le cadre de l'accord UKUSA pour la collecte de données au profit du réseau de renseignement Echelon

NILFANION/CC BY-SA 3.0

La « philosophie » de l'hypertransparence des individus est ainsi devenue le cœur du modèle économique des grandes plateformes publicitaires de l'Internet. Cette évolution correspond aussi à la fin programmée de la vie privée. Ce qu'Eric Schmidt, alors PDG de Google, résumait ainsi : « Si vous faites une chose que vous voulez que personne ne sache, peut-être devriez-vous déjà commencer par ne pas la faire[3]. » Il convient en effet pour ces plateformes de ne jamais tarir ce flux d'informations sur les utilisateurs, qui leur permet de monétiser leurs services. Les acteurs technologiques sont ainsi passés de modèles économiques « productivistes » à des modèles « extractivistes », où l'objectif est d'extraire et de traiter le plus de données possible sur leurs usagers. L'analyse des données des utilisateurs à des fins de « microciblage » est ainsi devenue l'objectif majeur des acteurs publicitaires de l'Internet comme Google ou Facebook. Ainsi, dans un article au titre évocateur, « Ce que 7 brevets effrayants révèlent sur Facebook[4] », le *New York Times* mettait en lumière les méthodes utilisées par le réseau social pour établir des profils psychologiques précis de ses utilisateurs, analyser leurs déplacements et leurs habitudes de vie, de consommation ou encore leur consultation de contenus écrits ou audiovisuels.

Il est ainsi devenu possible de constituer, à des fins de ciblage publicitaire, des profils qui regroupent plusieurs dizaines de milliers de paramètres sur chaque individu, et ce à l'échelle de plusieurs dizaines ou centaines de millions d'individus. Ces profils ultra-détaillés que rassemblent les « courtiers en données » (ou *data brokers*) permettent aussi d'influencer à chaque instant les utilisateurs de ces technologies, en particulier pour faire évoluer leurs habitudes de consommation mais aussi leurs convictions politiques.

En juin 2013, plusieurs journaux dévoilent les pratiques de surveillance mondiale des communications téléphoniques et sur Internet de l'Agence nationale de sécurité américaine (NSA). Des révélations permises par Edward Snowden, informaticien consultant de l'Agence et ancien employé de la Central Intelligence Agency (CIA)

© LAURA POITRAS/ACLU

Des technologies encore plus propices à la surveillance de masse

De nouvelles générations d'objets connectés et de dispositifs comme les automobiles connectées, les capteurs des villes intelligentes ou encore les objets connectés de santé, diversifient encore plus les canaux d'« extraction » d'informations sur les individus. Mais plus que d'accroître les quantités d'informations recueillies sur les usagers, ces évolutions technologiques ont modifié la nature même des activités de surveillance. Ces nouveaux instruments ont ainsi créé des cycles courts entre le recueil des informations et leur utilisation à des fins d'ingérence, de modification des opinions ou des comportements. Au-delà de la lutte contre les activités criminelles liées au terrorisme ou à l'espionnage, il devient possible d'agir sur les individus afin d'influencer à leur insu leurs comportements et même leurs convictions. À l'origine de messages politiques hyperciblés, la société Cambridge Analytica, en lien avec les services de renseignement russes, a ainsi tenté d'influencer les électeurs américains lors de la campagne présidentielle de 2016 ou les citoyens britanniques dans le cadre du référendum sur le Brexit.

La combinaison des données issues des réseaux sociaux et la puissance de traitement des systèmes d'intelligence artificielle peuvent désormais subvertir le fonctionnement démocratique lui-même. Ainsi, pour la

juge à la Cour suprême américaine Elena Kagan, le découpage électoral effectué à des fins partisanes (*gerrymandering*), *a fortiori* assisté par intelligence artificielle, pourrait saper les fondements mêmes de la démocratie. En effet, ces manipulations permettraient de rendre certaines circonscriptions électorales « imperdables », et ce de manière imperceptible pour les citoyens. Pour Elena Kagan : « À mesure que le temps passe, les manipulations liées aux redécoupages électoraux ne feront que s'aggraver. Ce qui était possible avec du papier et un stylo [...] est incomparable à ce qui le deviendra avec le développement de l'intelligence artificielle. À mesure que les données deviendront plus précises et que s'amélioreront les techniques d'analyse, quelque part en chemin, la souveraineté du peuple aura disparu[5]. »

Récemment, les technologies d'intelligence artificielle ont permis de personnaliser à moindre coût les données échangées avec les utilisateurs des services de l'Internet. Plus qu'un accroissement de la capacité d'interception des données, ce sont aussi des capacités inédites d'ingérence et de manipulation « automatisées » des opinions publiques qui ont été « démocratisées ». En plus des entités étatiques, ces technologies de désinformation sont devenues accessibles aux acteurs privés ou encore à des groupes politiques. En effet, pour un coût dérisoire, il devient possible de créer des « robots de désinformation autonomes[6] » qui utilisent des systèmes d'intelligence artificielle générative pour répondre spécifiquement à des millions d'utilisateurs en adaptant leurs réponses à leurs profils, tout en leur faisant croire qu'ils sont confrontés à des personnes ayant des opinions réelles...

L'intelligence artificielle permet désormais une extension des technologies de surveillance au-delà des systèmes traditionnels, qui nécessitaient d'importants moyens humains et logistiques pour recueillir et analyser des données sur l'ensemble des citoyens. Ces technologies représentent un enjeu crucial pour les régimes autoritaires et les dictatures souhaitant assurer leur pérennité. Ce qui conduisait Vladimir Poutine à déclarer : « L'intelligence artificielle représente l'avenir, non seulement de la Russie, mais de l'humanité tout entière. La nation qui sera leader dans le domaine de l'intelligence artificielle dominera le monde[7]. » La Chine a aussi développé un dispositif de surveillance de masse de sa population sans équivalent dans le monde : le crédit social. Ce dispositif orwellien, élaboré par certaines des plus puissantes sociétés chinoises comme Alibaba, permet d'attribuer une note à l'ensemble des citoyens chinois. Le crédit social repose à la fois sur des technologies de reconnaissance faciale et des algorithmes d'intelligence

> *« L'intelligence artificielle permet désormais une extension des technologies de surveillance*

Washington, les 10 et 11 avril 2018. Mark Zuckerberg, directeur général de Facebook, est auditionné par le Sénat des États-Unis sur les défaillances de l'entreprise en matière de protection des données privées

© LAWRENCE JACKSON/ THE NEW YORK TIMES-REDUX-REA

artificielle. La note attribuée à chaque citoyen chinois a pour objectif d'évaluer son « comportement » social, financier et politique. Une note de crédit social trop basse leur interdit de se déplacer en train ou en avion, d'accéder à certains services publics ou encore d'obtenir un crédit. Un autre exemple illustre l'importance stratégique pour la Chine de développer les technologies d'intelligence artificielle. En 2021, le piratage de la messagerie Microsoft Exchange attribué à la Chine avait pour but non pas d'espionner les entreprises ou les individus mais bien d'améliorer les algorithmes des systèmes d'intelligence artificielle chinois. La Chine visait ici un renforcement de la surveillance sur deux plans : accroître la connaissance sur les individus et les entreprises et améliorer les algorithmes d'intelligence artificielle qui aideront à leur tour à analyser plus finement les données permettant de mieux contrôler les populations[8].

Surveillance de masse et tests génétiques : de *Minority Report*… à *Gattaca*[9] ?

Au-delà des technologies numériques, de nouvelles formes de surveillance de masse commencent à utiliser les données issues des tests génétiques. Ainsi, en Chine, un programme de collecte en masse des données ADN a été mis en place afin d'établir une cartographie génétique complète de la population[10]. Ces données, une fois collectées, pourraient constituer un instrument de suivi et de contrôle inédit des populations dans l'ensemble du pays.

Depuis plusieurs années, la collecte en masse des informations génétiques, en plus des risques qu'elle représente en termes de surveillance des individus, apparaît comme une menace pour la sécurité nationale des États. Initialement, les analyses génétiques étaient réservées aux seules institutions médicales ou judiciaires ; or depuis, dans de nombreux pays, ces données sont devenues accessibles aux usagers de plateformes privées à des fins de recherche généalogique ou pour détecter les prédispositions d'un individu à des pathologies génétiques. Désormais, les fuites de données génétiques constituent aussi un risque de profilage ethnique ou « racial », comme en témoigne le récent piratage du système du laboratoire de tests génétiques californien 23andMe. En effet, à l'issue de cette cyberattaque, les pirates ont spécifiquement extrait puis mis en vente plusieurs millions de profils génétiques d'utilisateurs d'origine juive ou asiatique[11]. Aux États-Unis, des utilisations « radicales » des tests génétiques ont été envisagées pour systématiser la prévention en santé. Cela a été le cas avec la proposition de loi H. R.1313 (Preserving Employee Wellness Programs Act) introduite en 2017 au Congrès des États-Unis. L'objectif affiché de cette proposition de loi était, grâce à des tests génétiques effectués à grande échelle en entreprise, de développer des mesures de prévention et de détection précoce des maladies. Cette loi prévoyait de déployer ces tests génétiques dans les entreprises américaines et d'imposer des pénalités de plus de 5 000 dollars par an à l'encontre des employés qui refuseraient de se soumettre à ce « screening génétique ».

Les dernières générations de dispositifs et de capteurs médicaux connectés constituent aussi une nouvelle source d'informations à la fois sensibles et à très haute valeur ajoutée. Parallèlement à leurs usages médicaux en matière de suivi et de prévention des pathologies, ces objets médicaux connectés pourraient être exploités pour de tout autres fins, notamment la surveillance de masse. À titre d'illustration, plusieurs millions d'ouvriers chinois sont déjà équipés de casques dotés de capteurs électroencéphalographiques pour suivre en temps réel leur état émotionnel[12]. Par ailleurs, des équipes de recherche travaillent déjà sur des technologies d'intelligence artificielle qui

De jeunes Chinoises montrent leur score de crédit Zhima, un système d'évaluation du crédit social individuel développé par Ant Group, filiale du groupe chinois Alibaba. Hangzhou (province du Zhejiang)

© STRINGER/ IMAGINECHINA/ IMAGINECHINA VIA AFP

permettront la transcription des pensées en texte ou en image. Plus récemment, Apple a montré son intérêt pour le développement d'applications médicales reliées aux capteurs de ses montres connectées ou encore de son casque de réalité mixte Apple Vision Pro[13]. Cependant, en cherchant à identifier les réactions intimes de leurs usagers, les objets connectés peuvent aussi donner naissance à de nouvelles formes de surveillance de masse et de manipulations fondées sur l'analyse des données biométriques. Ce que l'historien Yuval Harari décrit en ces termes :

« Il est crucial de se rappeler que la colère, la joie, l'ennui et l'amour sont des phénomènes biologiques comme la fièvre ou la toux. La technologie qui identifie la toux pourrait également identifier les rires. Si entreprises et gouvernements commencent à collecter nos données biométriques en masse, ils peuvent apprendre à nous connaître mieux que nous ne nous connaissons nous-mêmes, et non seulement prédire nos sentiments mais aussi les manipuler et nous vendre tout ce qu'ils veulent, qu'il s'agisse d'un produit ou d'un politicien. La surveillance biométrique ferait ressembler les stratégies de piratage de données de Cambridge Analytica à des outils de l'âge de pierre[14]. »

Technologies de surveillance… ou surveillance des technologies

Pour les services de renseignement mais aussi pour des acteurs privés voire des entités étrangères, les immenses bases de données collectées par les plateformes de l'Internet représentent une manne inespérée. Ces informations suscitent aussi la tentation de modeler les comportements ou d'agir directement sur la fabrique des opinions publiques sans avoir besoin de disposer de relais « humains » au sein d'un territoire ou d'un pays. C'est la raison pour laquelle des plateformes américaines comme Facebook ou X (ex-Twitter) font l'objet d'investigations multiples en raison des risques de nature politique qu'elles présentent. Le réseau

chinois TikTok a, quant à lui, été interdit en Inde, en 2020, et dans l'État du Montana, en 2023, en raison des menaces sur les données personnelles de ses utilisateurs et de sa capacité à les influencer politiquement.

En matière de surveillance de masse, l'un des premiers objectifs des prochaines générations de régulations devra être de limiter les risques de dérives liées à la diffusion incontrôlée des données personnelles des utilisateurs. À terme, à l'instar du règlement général sur la protection des données (RGPD), les textes européens de régulation des plateformes et des technologies (Digital Markets Act, Digital Services Act, Data Governance Act et Artificial Intelligence Act) devraient inspirer d'autres législations dans le monde. En effet, au-delà du RGPD, il conviendra aussi de rendre plus difficile le développement de modèles économiques fondés sur l'extraction toujours plus importante d'informations sur les individus. De plus, comme le décrit la sociologue Zeynep Tüfekçi, cette logique publicitaire conduit à amplifier les contenus les plus addictifs qui sont aussi les plus politiquement radicaux : « [Les concepteurs des algorithmes de YouTube] se sont rendu compte que si vous pouvez inciter les gens à penser que vous pouvez leur montrer quelque chose de plus *hardcore*, ils sont susceptibles de rester plus longtemps, pendant que Google leur montre des publicités[15]. »

Les démocraties peuvent ainsi se révéler doublement vulnérables aux manipulations numériques. Vulnérabilité aux ingérences étrangères qui prennent appui sur les technologies des plateformes pour développer et amplifier des campagnes de désinformation. Mais aussi vulnérabilités aux pressions internes pour le contrôle et la manipulation des opinions publiques. En effet, ces technologies de surveillance constituent un risque pour l'ensemble des démocraties lorsqu'elles seront utilisées par des responsables politiques qui, comme cela s'est produit aux États-Unis ou dans certains pays européens, souhaitent mettre en cause l'État de droit.

Kit de test génétique par prélèvement salivaire de la société de biotechnologie 23andMe. Le site de la firme a confirmé en octobre 2023 une fuite de données appartenant à 6,9 millions de ses utilisateurs
VEVERVE/CC BY-SA 4.0

Pour les sociétés démocratiques, la détection des ingérences et des atteintes à la démocratie relèvera de plus en plus des technologies liées à la sécurité des données et à l'intelligence artificielle. Les experts de ces technologies pourraient ainsi devenir les seuls à même de vérifier que les opinions publiques n'ont pas été manipulées ou que l'expression des suffrages est restée sincère. À terme, des pressions considérables s'exerceront sur ces experts et leur rôle dans les processus démocratiques ne manquera pas d'éveiller des suspicions de la part des citoyens.

Ainsi, le contrôle par les citoyens des technologies utilisées dans le champ démocratique, et en particulier celles qui interviennent dans les processus électoraux, deviendra encore plus crucial que par le passé. Dans le même temps, il conviendra de redéfinir le périmètre des données sensibles. En effet, les évolutions des technologies d'intelligence artificielle permettent d'analyser des informations en apparence anodines pour déduire des données sensibles sur les individus.

Enfin, les citoyens devront aussi être mieux informés des risques des récentes formes de surveillance et de manipulation qui, comme on a pu le constater lors de la guerre en Ukraine, font désormais partie intégrante des nouvelles formes de ce que l'on nomme désormais les « guerres hybrides ». ●

Notes

[1] Mark Udall et John C. Yang, « How Congress can end the era of warrantless spying on Americans », *The Hill*, 9 janvier 2024 ; https://thehill.com/opinion/technology/4395536-how-congress-can-end-the-era-of-warrantless-spying-on-americans/.

[2] *The Age of Surveillance Capitalism. The fight for a human future at the new frontier of power*, PublicAffairs, New York, 2019 ; traduction française : *L'Âge du capitalisme de surveillance,* Zulma, Paris, 2020.

[3] Richard Esguerra, « Google CEO Eric Schmidt Dismisses the Importance of Privacy », *Electronic Frontier Foundation*, 10 décembre 2009 ; https://www.eff.org/fr/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

[4] Sahil Chinoy, « What 7 Creepy Patents Reveal about Facebook », *The New York Times*, 21 juin 2018 ; https://www.nytimes.com/interactive/2018/06/21/opinion/sunday/facebook-patents-privacy.html.

[5] Zoe Schiffer, « Supreme Court Justice Elena Kagan warns AI-powered gerrymandering could undermine US democracy », *Business Insider*, 28 juin 2019 ; www.businessinsider.com/justice-elena-kagan-warns-ai-powered-gerrymandering-may-hurt-democracy-2019-6. Traduction de l'auteur.

[6] M.J. Banias, « Inside Countercloud: A fully autonomous AI disinformation system », *The Debrief*, 16 août 2023 ; https://thedebrief.org/countercloud-ai-disinformation/.

[7] James Vincent, « Putin says the nation that leads in AI "will be the ruler of the world" », *The Verge*, 4 septembre 2017 ; https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

[8] Dina Temple-Raston, « China's Microsoft Hack May Have Had a Bigger Purpose than just Spying », NPR, 26 août 2021 ; https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

[9] Ces deux films représentent deux visions dystopiques de sociétés où les technologies de surveillance sont mises au service d'un contrôle absolu des individus. Dans *Minority Report*, de Steven Spielberg (2002), il s'agit d'une société dans laquelle l'anticipation des comportements criminels anéantit la notion même de vie privée et de liberté de pensée. Quant à *Bienvenue à Gattaca* (1997), le réalisateur Andrew Niccol y décrit une société tout entière organisée autour de la sélection et de l'« amélioration » génétique des individus, et où les personnes non modifiées sont jugées « inférieures » et sont ostracisées.

[10] Sui-Lee Wee, « China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment », *The New York Times*, 17 juin 2020.

[11] Rebecca Carballo, Emily Schmall et Remy Tumin, « 23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says », *The New York Times*, 26 janvier 2024.

[12] Tara Francis Chan, « China is monitoring employees' brain waves and emotions – and the technology boosted one company's profits by $315 million », *Business Insider*, 1er mai 2018 ; https://www.businessinsider.com/china-emotional-surveillance-technology-2018-4.

[13] Brian Bushard, « Apple Is Considering Treating Mental Health With $3,500 Vision Pro Augmented Reality Headset, Report Says », *Forbes*, 25 octobre 2023 ; https://www.forbes.com/sites/brianbushard/2023/10/25/apple-is-considering-treating-mental-health-with-3500-vision-pro-augmented-reality-headset-report-says.

[14] Yuval Noah Harari, « Yuval Noah Harari : the world after coronavirus », *Financial Times*, 20 mars 2020 ; www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?segmentid=acee4131-99c2-09d3-a635-873e61754ec6. Traduction de l'auteur.

[15] Annabelle Laurent, « On a construit une infrastructure de surveillance pour que les gens cliquent sur des pubs », *Usbek & Rica*, 2 novembre 2017 ; https://usbeketrica.com/fr/article/notre-attention-et-nos-data-ne-sont-pas-a-vendre-au-demagogue-le-plus-offrant.