Mettez fin à la manipulation et à l'exploitation de nos données !

C'est probablement « la plus massive exploitation de listes nominatives de juifs depuis la rafle du Vel'd'hiv »[1]. Le vendredi 8 avril au soir, de nombreux citoyens français juifs ou supposés l'être ont été les destinataires d'un SMS envoyé par le parti « Reconquête ! » du candidat à la présidentielle Eric Zemmour. Le message les renvoyait vers son site de campagne et vers une lettre leur étant destinée. Il y était question pêle-mêle « d'expansion de l'islam », de « terrorisme islamique », « d'antisémitisme », de « violence quotidienne de la racaille », le but de la propagande étant de s'attirer leurs votes.
L'opération est de grande ampleur : des dizaines de milliers de SMS ont été envoyés par le parti d'Eric Zemmour.

De nombreux destinataires de ces messages intrusifs se sont plaints publiquement, et la Commission nationale de l'informatique et des libertés (CNIL) a ouvert une enquête afin de déterminer si des données personnelles avaient été exploitées illégalement. Les associations françaises J'Accuse et l'UEJF, suivies par la LICRA, SOS Racisme et le MRAP ont décidé de porter plainte contre X.

Illégal ou pas, ce scandale met en lumière les dangers inhérents au profilage et au ciblage publicitaire : le marché opaque des données personnelles permet à tout individu de se procurer des données sensibles afin, par exemple, de créer une liste nationale de Français de confession juive, de cibler une communauté religieuse et chercher à attiser la haine contre une autre.

Cela illustre aussi les dangers liés à l'utilisation des données inférées, soit les données déduites de nos habitudes ou de nos choix en ligne. En tant qu'utilisateurs d'Internet, notre identité est induite, selon des raccourcis permis par les traces numériques que nous laissons en nous connectant quotidiennement.
Ce sont ces moyens détournés que « Reconquête ! » a utilisé.
Pour atteindre les citoyens français juifs ou supposés l'être, l'équipe d'Eric Zemmour a, de son propre aveu, ciblé toutes les personnes ayant manifesté "un intérêt pour le sujet de l'antisémitisme", à partir de données achetées à un courtier en données.

Cela fait longtemps que nous, organisations de la société civile, mettons en garde les décideurs contre les pratiques de profilage et de ciblage. Avec les techniques actuelles, il est devenu aisé de s'adresser à la fois spécifiquement et massivement à des groupes, à des communautés données. Cela participe à l'isolation, la polarisation, la fragmentation et la vulnérabilisation croissante des communautés.

Pourtant, nous pourrions croire que nous sommes protégés par le RGPD (Règlement Général sur la Protection des Données). Selon cette loi européenne, le consentement explicite de l'utilisateur est la condition sine qua non avant toute utilisation d'une donnée sensible partagée par ce dernier. Les données sensibles sont celles qui « révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. »[2]

---

[1] https://www.lemonde.fr/election-presidentielle-2022/article/2022/04/12/envoi-de-sms-au-nom-d-eric-zemmour-a-des-membres-de-la-communaute-juive-une-enquete-ouverte_6121870_6059010.html

[2] https://www.cnil.fr/fr/definition/donnee-sensible

Il est effectivement possible que « Reconquête ! » soit reconnu coupable d'une infraction aux règles du RGPD.

Mais on sait désormais, et cette affaire des SMS vient le confirmer, que cette disposition de la loi ne suffit pas à nous protéger. Dans un grand nombre de cas, il est en effet impossible de savoir d'où venaient les données utilisées et si les personnes concernées ont vraiment donné leur consentement. En effet, c'est souvent de manière détournée, par des pratiques de manipulation que notre "consentement" est obtenu.

Dans le documentaire « Big data, quand les politiques nous ciblent ! »[3] diffusé lundi 11 avril sur France 2, un courtier en données est enregistré en caméra cachée. Il révèle comment une simple case que nous cochons sur un site pour recevoir des infos du site et de « ses partenaires » permet que nos données soient collectées, revendues, exploitées. Sur Internet, ces interfaces truquées, opaques et trompeuses, aussi appelées "dark patterns", sont courantes.
Ce « consentement », arraché au détour d'une navigation sur internet, entraîne notre fichage par des sociétés inconnues et notre ciblage, y compris pour de la propagande politique que nous n'avons jamais demandée.

Cela n'est pas un consentement, c'est un abus de confiance, une quasi-extorsion, celle d'une partie de notre vie privée, d'une partie de notre identité.
Tant qu'on ne mettra pas un terme à ces pratiques, ces scandales et ces violations massives des droits humains ne cesseront d'avoir lieu, avec ou sans consentement des utilisateurs quant à l'utilisation de ces données.

Le Digital Services Act (DSA), texte de loi européen visant à réguler les espaces en ligne, est en cours de discussion en ce moment entre les États membres, le Parlement européen et la Commission. Il faut agir maintenant.

C'est pourquoi les organisations signataires de cette présente lettre demandent instamment à la Présidence française, ainsi qu'aux décideurs européens, de prohiber explicitement et complètement dans le DSA les interfaces truquées (comme dans l'article 13a de la version proposée par le Parlement européen), ainsi que l'exploitation des données sensibles, y compris l'obtention de celles-ci par inférence, à des fins publicitaires.

Signataires:

- AJC Europe
- Alliance4Europe
- Amnesty France
- Corporate Europe Observatory
- Defend Democracy
- Foxglove
- Global Witness
- I Am Here International
- Institute for Strategic Dialogue
- J'Accuse (AIPJ)
- Je Suis Là
- LICRA
- Lie Detectors

[3] https://www.france.tv/france-2/complement-d-enquete/3302491-big-data-quand-les-politiques-nous-ciblent.html

- Panoptykon
- Ranking Digital Rights
- Sum of Us
- The Signals Network
- UEJF
- WeMove Europe

Stop the abuse of our data!

It is probably "the largest scale exploitation of nominative lists of Jews since the Vel'd'hiv round-up". On the evening of Friday April 8th, many members of the Jewish community received a text message sent by “Reconquête!”, the party of presidential candidate Eric Zemmour. The message referred them to his campaign site and to a letter addressed to them. In no particular order, it spoke of "the expansion of Islam", "Islamic terrorism", "anti-Semitism", and "the daily violence of the scum" - the aim of the propaganda being to attract their votes.
The operation is on a large scale: tens of thousands of text messages have been sent by Eric Zemmour's party.

Many recipients of these intrusive messages complained publicly, and the National Commission for Information Technology and Civil Liberties (CNIL) opened an investigation to find out whether personal data had been illegally exploited. The French NGOs J’Accuse and UEJF, followed by LICRA, SOS Racisme and MRAP have decided to file a complaint against an unknown person.

Illegal or not, this scandal highlights the dangers inherent in profiling and advertising targeting: the opaque market of personal data allows any individual to obtain sensitive data in order to, for example, create a national list of French people of Jewish faith, to target a religious community and to seek to stir up hatred against another.

This also illustrates the dangers of using inferred data, i.e. data deduced from our online habits or choices. As internet users, our identities are inferred, based on shortcuts allowed by the digital traces we leave when we connect daily.
These are the backdoor ways that “Reconquête!” has used.

To reach the Jewish community, Eric Zemmour's team has, by his own admission, targeted everyone who has shown "an interest in the subject of anti-Semitism", using data purchased from a data broker.

We, as civil society organizations, have long been warning decision-makers against profiling and targeting practices. With today's techniques, it has become easy to precisely target specific groups, and specific communities at a massive scale. This contributes to the isolation, polarization, fragmentation and increasing vulnerability of communities.

Yet, we might believe that we are protected by GDPR (General Data Protection Regulation). According to this European law, a user's explicit consent is the sine qua non for any usage of sensitive data shared by the user. Sensitive data is that which "reveal[s] the alleged racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person."

It is indeed possible that “Reconquête!” will be found guilty of violating the rules of the GDPR.

But we now know, and this SMS case confirms it, that the provision of this law is not enough to protect us. In a large number of cases, it is indeed impossible to know where the data used came from and whether the persons concerned really gave their consent. Indeed, it is often in a roundabout way, it is through manipulative practices that our consent is obtained.

In the documentary "Big data, quand les politiques nous ciblent!" broadcast on Monday, 11th April on France 2, a data broker is recorded on hidden camera. He reveals how a simple box that we check on a site to receive information from the site and its "partners" allows our data to be collected, resold and exploited. On the internet, these rigged, opaque and deceptive interfaces, also called "dark patterns", are common.
"Consent" is snatched from us while using the internet, leads to us being put on file by unknown companies, and being targeted, including for political propaganda that we never asked for.

This is not consent, it is a breach of trust, a quasi-extortion, of a piece of our privacy, a piece of our identity. As long as these practices are not stopped, this kind of scandal and massive violation of human rights will continue to take place, with or without user consent.

The Digital Services Act (DSA), a European law to regulate online spaces, is currently being discussed by the Member States, the European Parliament and the Commission. We must act now.

This is why the organizations signing this letter ask the French Presidency, as well as the European decision-makers, to explicitly and completely prohibit manipulative interfaces (as in article 13a in the EP’s position), as well as the exploitation of sensitive data, for advertising purposes, including drawing of inferences about special characteristics.

Signatories:

- AJC Europe
- Alliance4Europe
- Amnesty France
- Corporate Europe Observatory
- Defend Democracy
- Foxglove
- Global Witness
- I Am Here International
- Institute for Strategic Dialogue
- J’Accuse (AIPJ)
- Je Suis Là
- LICRA
- Lie Detectors
- Panoptykon
- Ranking Digital Rights
- Sum of Us
- The Signals Network
- UEJF
- WeMove Europe