Chercheurs sous surveillance : les enjeux de la protection des données de recherche

7 mai 2019

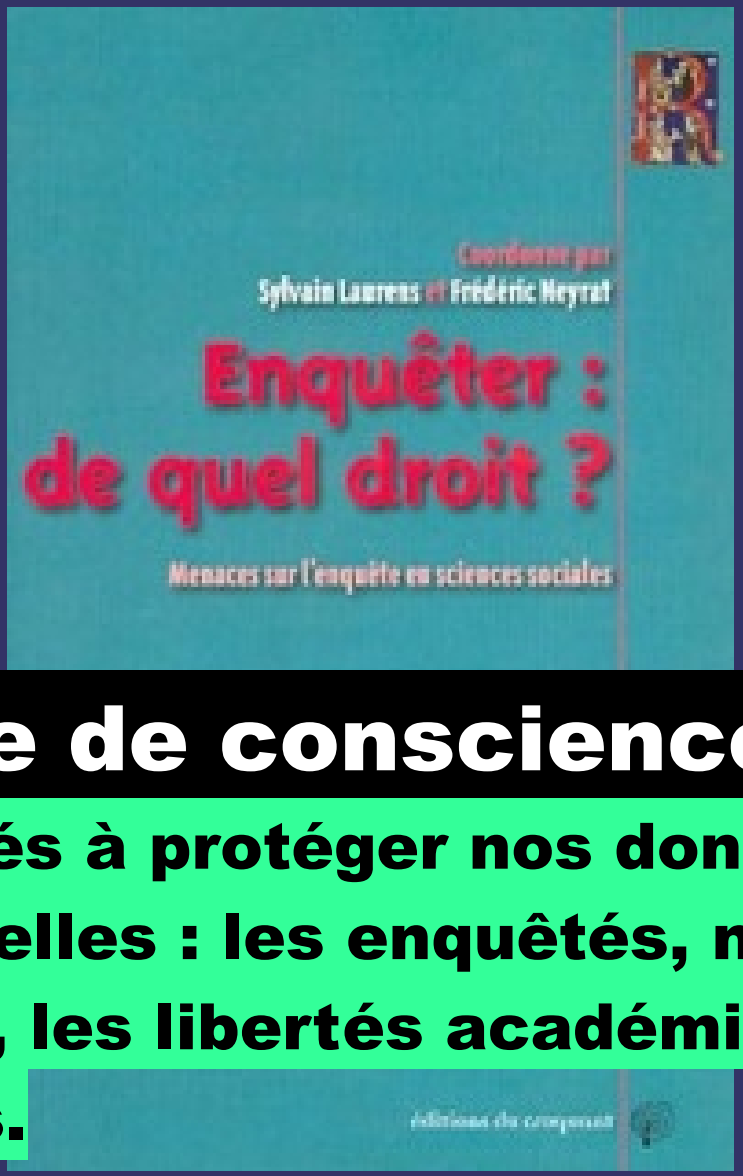
Félix Tréguer
CERI Sciences Po

- Prise de conscience

- Techniques de surveillance

- Moyens de protection et leurs limites

- Les GAFAM dans l’ESR



Une prise de conscience croissante

des difficultés à protéger nos données et à travers elles : les enquêtés, nos sources, nos terrains, les libertés académiques, nous-mêmes.

Des problématiques aggravées par le contexte (anti)terroriste et de répression des mouvements sociaux

Libération

Qui protège les chercheurs de la surveillance de ...

Qui protège les chercheurs de la surveillance de l'Etat ?

Par Marwan Mohammed, Sociologue au CNRS, Centre Maurice-Halbwachs. — 8 novembre 2015 à 18:56

En facilitant les écoutes, la loi renseignement promulguée en juillet menace le travail des chercheurs en sciences sociales et la confidentialité de leurs sources. La possibilité de mieux connaître des sujets sensibles comme la radicalisation ou la criminalité organisée est en jeu.

Des revendications collectives émergentes qui restent toutefois isolées

MEDIAPART
VEN. 8 FÉVR. 2019 - ÉDITION DU MATIN

Pour un droit à la recherche

11 DÉC. 2017 | PAR LES INVITÉS DE MEDIAPART | BLOG : LE BLOG DE LES INVITÉS DE MEDIAPART

Des chercheur-e-s en sciences sociales qui se définissent comme «pas uniquement des fonctionnaires d'État», mais «des sentinelles du présent», protestent en estimant que «la judiciarisation de la recherche commence à être un vrai problème à l'échelle internationale, témoignage d'un front large pour la déstabilisation de nos professions».

DEPUIS LES ATTENTATS DE NOVEMBRE 2015 qui ont frappé la ville de Paris, les chercheurs et les chercheuses en Sciences sociales éprouvent de plus en plus de difficultés à

Quelles techniques de surveillance ? (communes au renseignement et à la police judiciaire)

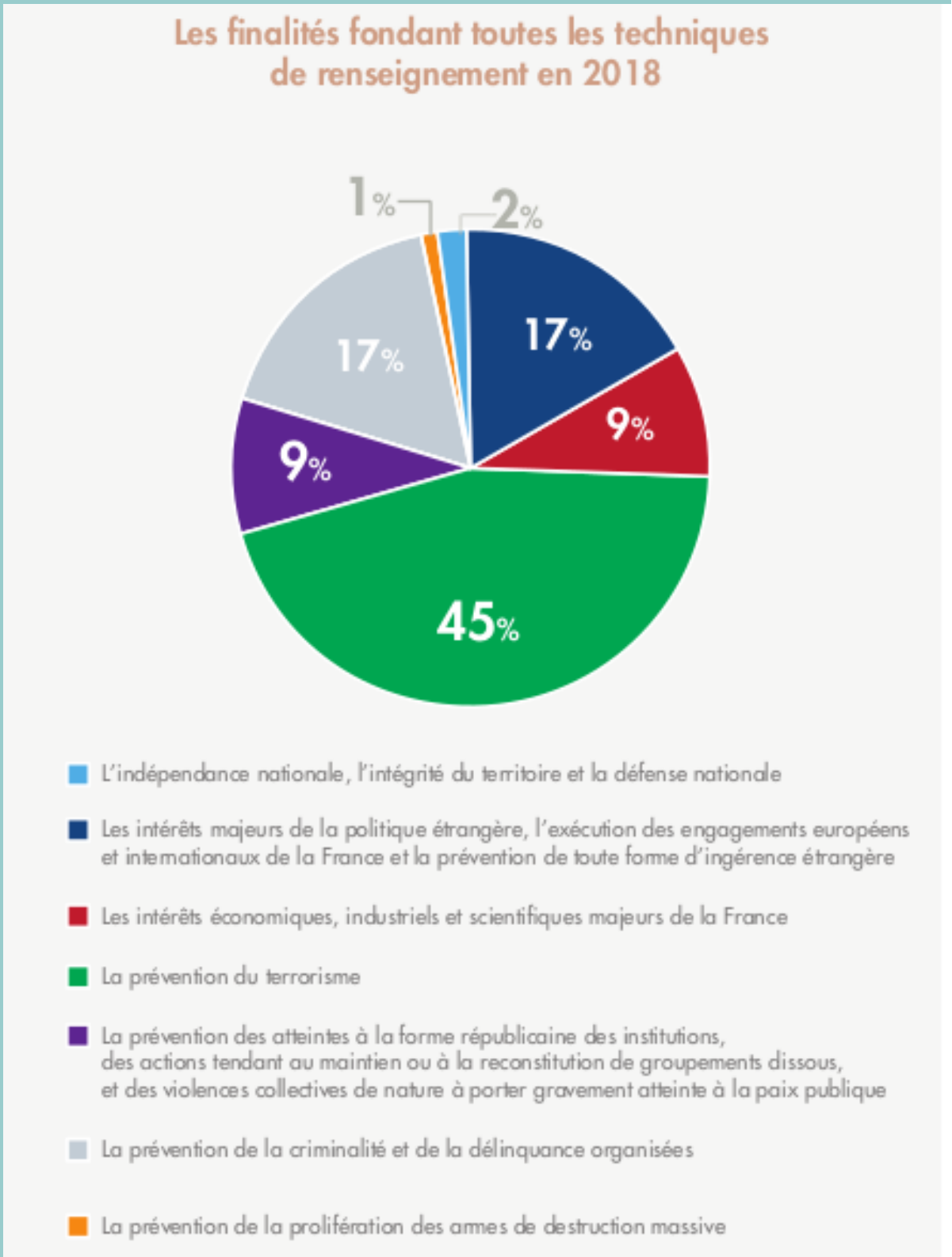
Techniques classiques :

- Réquisitions de données (dont géolocalisation)
- Interceptions des correspondances
- Sonorisation de lieux ou véhicules

Techniques plus récentes :

- Saisies numériques (captations à distance ou perquisitions informatiques)
- IMSI-catcher

Les finalités très larges du renseignement donnent une idée du type de terrains à risque.



Source : rapport 2018 de la CNCTR

Quelles techniques de surveillance ? (renseigement intérieur)

En matière (anti)terroriste seulement :

- **« Boîtes noires » (scan en masse des données traitées par une infrastructure numérique) pour tenter de repérer « des connexions à certaines heures, depuis certains lieux, sur certains sites » et « de repérer ainsi un trafic caractéristique »**
  (J.Y. Le Drian, 15 avril 2015)

- **Surveillance en temps réel des métadonnées (étendue aux n+2 en juillet 2016)**

Quelles techniques de surveillance ? (renseignement extérieur)

Techniques exploratoires (non-ciblées) relatives aux communications internationales (DGSE) :

- **Collecte de donneés en masse des communications transfrontières, autorisées pour de vastes catégories de trafic Internet**

- **Depuis 2018, les résidents français situés sur le territoire national peuvent être légalement surveillés dans ce cadre juridique censé être dérogatoire**


« Nous voulons d'abord permettre l'exploitation des données d'un identifiant technique rattachable au territoire national interceptées dans le cadre de la surveillance des communications internationales, alors même que son utilisateur est en France ».
Nicole Belloubet, ministre de la justice, mai 2018

« La levée de doute prendra la forme d'une vérification ponctuelle sur les données de connexion légalement interceptées dans le cadre de la surveillance des communications internationales.

Il s'agit d'opérations très rapides, non répétées et susceptibles de mettre en évidence un graphe relationnel ou la présence à l'étranger d'une personne, qui pourra alors être surveillée si elle présente une menace ».

Nicole Belloubet, ministre de la justice, mai 2018

Face à la surveillance d’État, quelles protections pour les chercheurs ?

En droit ? Aucune protection particulière du secret professionnel

Lors de l'examen de la loi renseignement par le Conseil constitutionnel en 2015, ce dernier refuse que les chercheurs fassent l'objet d'une protection spéciale:

« Considérant, en troisième lieu, que le principe d'indépendance des enseignants-chercheurs n'implique pas que les professeurs d'université et maîtres de conférences doivent bénéficier d'une protection particulière en cas de mise en œuvre à leur égard de techniques de recueil de renseignement dans le cadre de la police administrative » (Décision n° 2015-713 DC du 23 juillet 2015).

Sécurité informatique et cryptographie

Comment réduire les risques d'accès non-autorisés ou de fuites des données et communications ?
(surveillance administrative, investigations judiciaires, vols de matériel ou de données, etc.)

Quelques bonnes pratiques à connaître

Aldridge, Medina, and Ralphs (2010). The Problem of Proliferation: Guidelines for Improving the Security of Qualitative Data in a Digital Age. *Research Ethics* 6(1): 3–9.

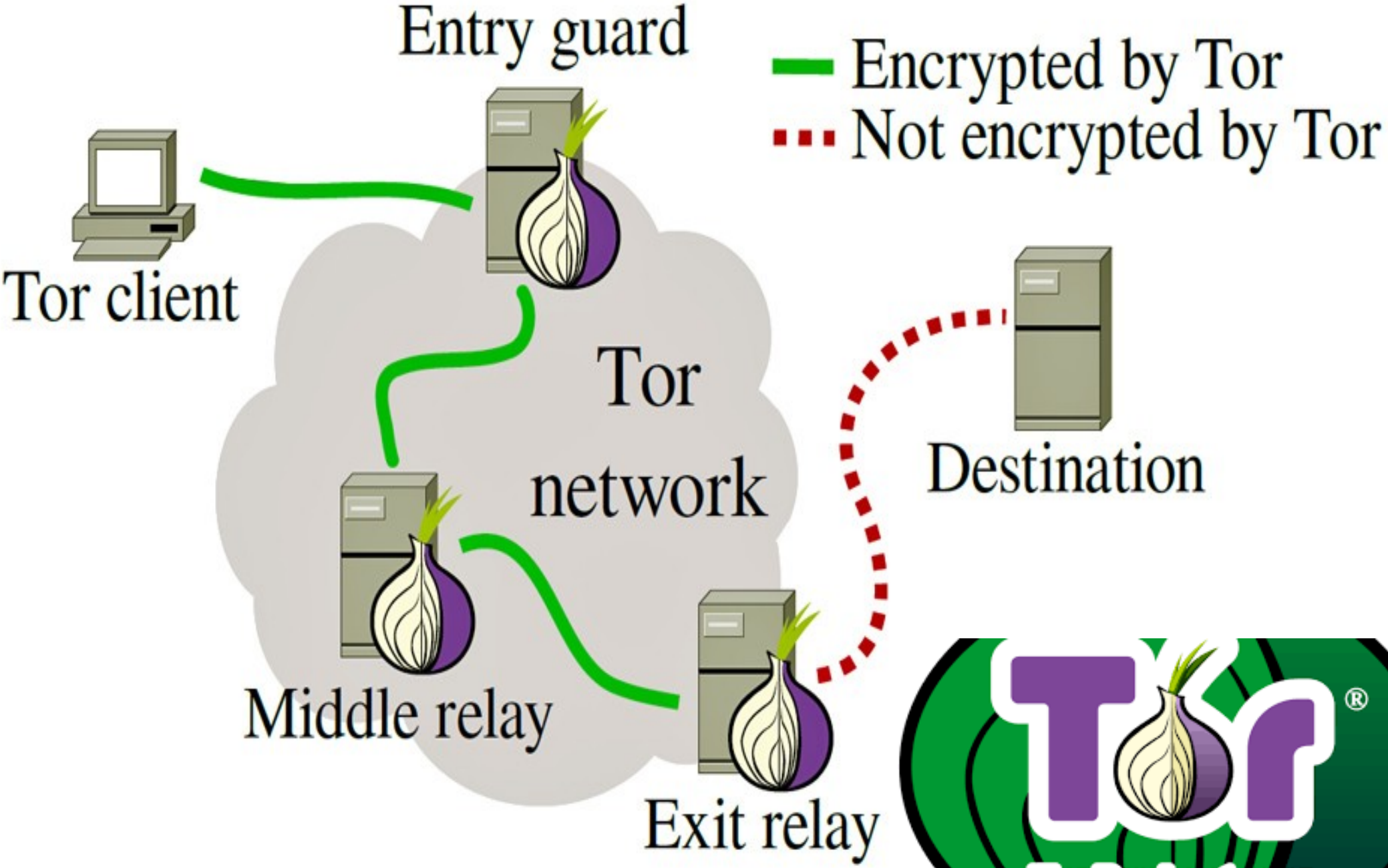
- **« Faites des sauvegardes de vos travaux en cours sur des disques durs chiffrés sur des supports amovibles chiffrés (ex : clé USB), et conservez dans un endroit séparé de votre ordinateur de travail.**
- **Assurez vous que tous les membres d'une équipe de recherche utilisent les mêmes procédures de sécurité.**
- **Les notes de terrain sur papier doivent être détruites aussitôt que possible après le chiffrement numérique.**
- **La simple suppression de fichiers du disque dur d'un ordinateur ne permet pas de les faire disparaître complètement.**
- **Anonymisez vos notes d'entretien et de terrain aussitôt que possible au cours du processus de collecte de données ».**

Voir aussi : Cardorel & Groshens (2018). Anonymat et confidentialité des données qualitatives : Le retour d'expérience de beQuali. In La diffusion numérique des données en SHS - Guide de bonnes pratiques éthiques et juridiques.

Chiffrer et dissimuler des données sur un support de stockage

VeraCrypt

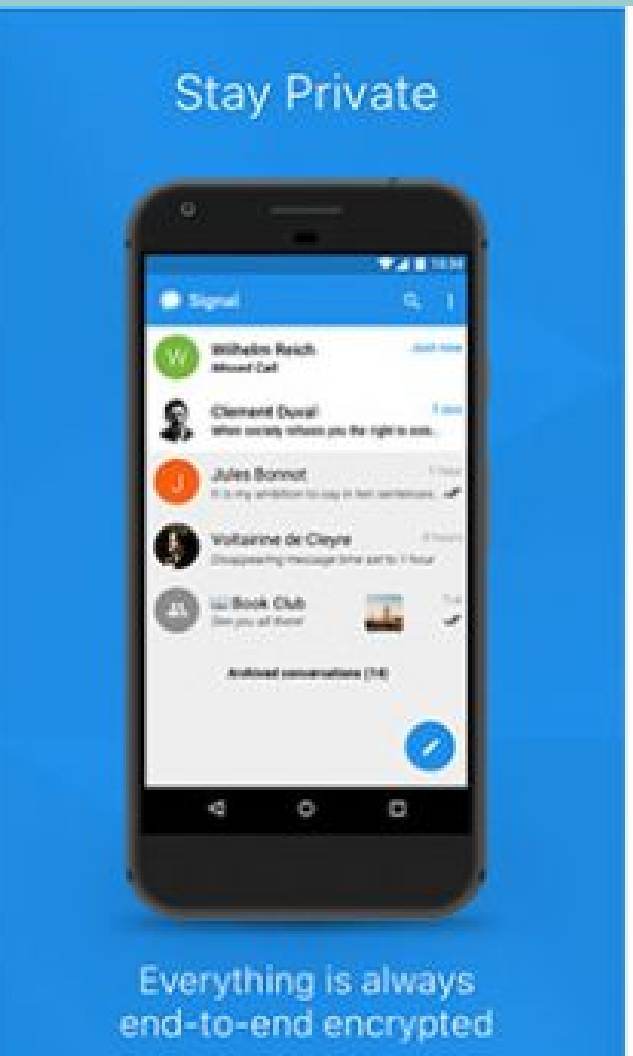
Anonymiser votre navigation, contourner la censure d'Internet



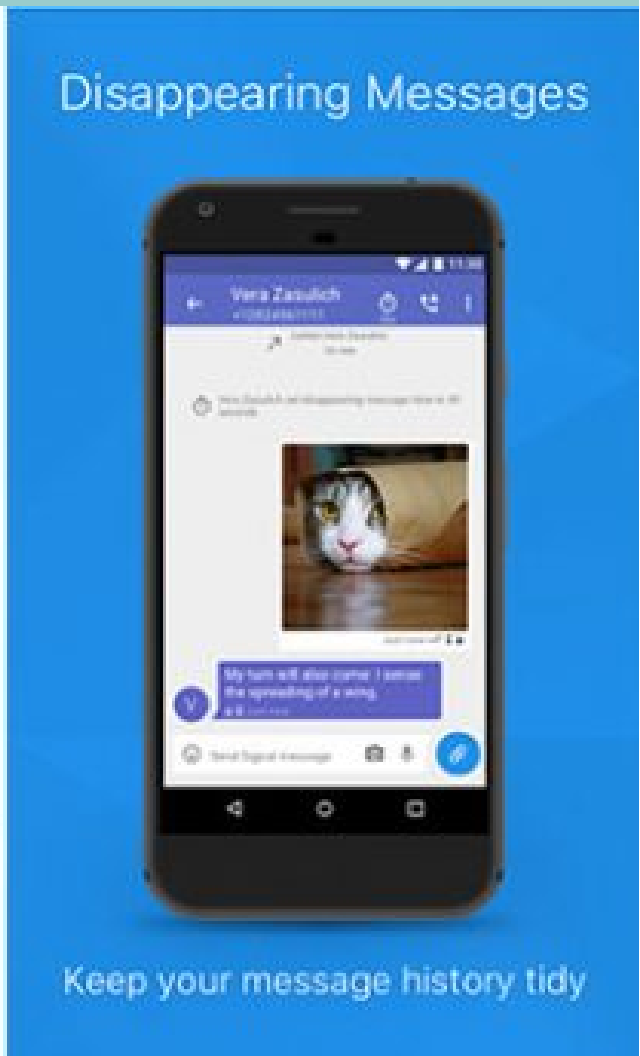
Chiffrer ses correpondances

PGP

matrix



Secure Your Messages
With
Signal Private Messenger



Embarquer votre système d'exploitation sécurisé (intégrant divers outils crytographiques) sur une clé USB. Cela permet de ne pas laisser de traces sur l'ordinateur utilisé

Le chiffrement : une protection relative !!

Il peut être contourné techniquement de diverses manières ; les outils peuvent présenter des failles (volontaires ou non).

La justice peut également vous forcer à livrer vos mots de passe (voir la décision du Conseil constitutionnel sur l'article 434-15-2 du code pénal, qui bafoue le droit à ne pas s'accuser soi-même).

Engager une démarche collective, en parlant de ces enjeux avec nos collègues, dans nos labos et établissements…

Quelques acteurs associatifs dédiés à la protection des données organisent des formations, tels nothing2hide.org (mais aucun soutien institutionnel).

Accueil | Actualités | Formations | Qui sommes-nous | Faire un don

PROTÉGER L'INFORMATION

Journalistes, avocats, blogueurs, militants, *simples* citoyens…. Nous avons tous quelque chose à cacher. Nothing2hide est une **structure associative** dont


Dans nos pratiques, résister à l’emprise des GAFAM et à leurs modèles d’affaire toxiques, fondés sur la collecte massive et constante de données personnelles et la publicité ciblée.

Des universités et des labos dépourvus, qui se désinvestissent trop souvent des enjeux liés aux outils numériques et s'appuient sur les GAFAM (c'est gratuit, mais nous sommes le produit).

UNIVERSITÉ PARIS 13

FORMATIONS

Inscrivez-vous à la formation Google Digital Active de Google à l'université Paris 13 du 26 au 29 mars 2018 !

Des alternatives existent pourtant, telles que celles proposées par framasoft.

Elles se construisent hors de l'université, là encore sans soutien public significatif.

- Google Doc : https://framapad.org/

- Google Drive : https://framadrive.org/

- Doodle : https://framadate.org/

- Dropbox : https://framadrop.org/

- Slack ou Facebook Groups/Messenger : https://framateam.org/

- Google Form : https://framaforms.org/

- Skype : https://framatalk.org/

- services blog des GAFAM : https://frama.wiki/

- Pour le reste, voir : https://framasoft.fr/#topPgCloud

Face au risque de surveillance, conjurer l’auto-censure

La conscience du risque d’être surveillé peut suffir à produire ses effets politiques (dissuasifs, normalisant).

Il faut avoir conscience des risques, sans pour autant sombrer dans la paranoïa.

Chercheurs sous surveillance : les enjeux de la protection des données de recherche

Félix Tréguer
CERI Sciences Po