

# Formation à l'auto-défense numérique dans le militantisme

Bernardettes

**Diapos transmises après la formation**

**Formation en constante évolution  
donc merci pour vos retours**

## D'où viennent les infos

Sites internet militants/gouvernementaux/autres

Retours d'expériences en ligne et dans la vie réelle

Historique procédures judiciaires

Discussions plus ou moins techniques durant les formations ou durant d'autres moment plus informels avec des personnes plus ou moins techniques

Participation à des formations organisées par d'autres personnes

Ma formation d'ingénieur en informatique

Congrès de cyber-sécurité

Mon expérience de militante

Tests

Infos européennes (principalement françaises)

Sources précises disponibles si demandées

**INTRODUCTION :**

**les objectifs de la formation**

**Conseil : N'utilisez jamais d'outils numériques  
!**

**CECI EST UNE FORMATION QUI NE VOUS  
SERVIRA PAS**

# Introduction – les compromis

Outils numériques = risques (et toujours des risques)

Plus on veut de **sécurité**, plus cela demande de **l'énergie souvent**  
→ **faire des compromis !**

Savoir ce que vous voulez cacher et pourquoi avant de vouloir le cacher (même si le cacher « au cas où » c'est bien aussi)

# Introduction – travail de groupe

Votre connaissance en culture de la sécurité numérique influe sur votre sécurité en tant que militant·e mais aussi sur la sécurité du groupe



# Introduction - brèves

Plus tôt vous commencerez mieux c'est :

- si vous souhaitez faire des actions plus engageantes un jour ou si vous avez de gros soucis judiciaire un jour, c'est important d'être le moins fiché possible
- c'est difficile de devoir recommencer une identité (numérique ou pas) à zéro

Ne pas se faire repérer avec des pratiques sécuritaires au dessus de la masse : si on est tout.e seul.e cagoulé.e au milieu de la masse, forcément la police va plus d'intéressé à vous

Se sécuriser même si on n'en à pas besoin est utile pour les autres qui en ont besoin

Si on a besoin d'un maximum de sécurité le mieux c'est ne pas dévoiler comment on se protège même si un avis extérieur est intéressant : métaphore open-source / propriétaire

# Introduction – flirte avec la légalité

Les procédures mises en place par la police rentrent **normalement** dans le cadre de la loi

Possibilités d'utiliser des procédures illégales → pas dans un dossier d'instruction

**franceinfo:**

Publié le 16/11/2023 18:00

**La reconnaissance faciale utilisée illégalement depuis 2015 par la police et la gendarmerie selon un média d'investigation, la CNIL se saisit du dossier**

La Cnil a annoncé mercredi lancer "une procédure de contrôle" vis-à-vis du ministère de l'Intérieur, après la publication d'informations par le site d'investigation Disclose concernant l'utilisation non déclarée par la police d'un logiciel de vidéosurveillance.

# Le Monde

SOCIÉTÉ

## Tarnac : la justice enquête sur des écoutes illégales menées avant l'affaire du sabotage

La juge instruit sur le chef "d'atteinte au secret des correspondances" et "à l'intimité de la vie privée".

Par Laurent Borredon

Publié le 09 janvier 2012 à 11h36, modifié le 24 février 2012 à 13h04 ·  Lecture 4 min.

# Introduction - De qui se protéger ?

# Introduction - De qui se protéger ?

## > Police

- D'une préparation d'action
- D'une **action**
- D'une **perquisition** (au poste ou chez vous)
- De la communication post action
- De la communication en dehors d'un cadre d'action (fichage)

## > Justice

- Les pièces à convictions lors d'un procès

## > Potentiel.les « hackeuse.r.s »

- d'un groupe politique opposé
- d'une entreprise adverse
- ou hasardeu.ses.x

# Introduction - Pourquoi se protéger ?

- Ne pas être fiché.e
- Protéger les autres
- Réduire les risques de se faire interpellé
- Réduire les pièces à conviction une fois interpellé
- Réduire les risques que l'action soit connue à l'avance

# Les impacts d'être fiché.e

- Emploi
- Reconnaissance faciale
- Problème aux douanes
- La police est moins aimable avec vous
- Méprise médiatique (Serge Ste Soline)
- FPR (fichier des personnes recherchées) = 600k personnes dont 20k fichées S dont 2k pour écologie radicale
- De nombreux fichiers existe : FPR, TAJ, FSPRT, EUROPOL, FNAEG

Comment ont été identifiés les militants qui ont reçu cette lettre de "reconnaissance d'infraction" à leur domicile, alors que, sur place, les contrôles n'étaient pas systématiques ?

**Olivier Caracotch :** C'est bien simple, toutes ces personnes étaient connues de nos services de police. Quand je parle de "connues", cela ne veut pas dire qu'elles avaient toutes des antécédents judiciaires. Je veux juste dire que les officiers du ministère public qui ont dressé les procès-verbaux connaissaient déjà leur identité. En aucun cas, il n'a été question de caméras ou de reconnaissance faciale.

# Les impacts d'être fiché.e

**BFM** 06.08  
**TV.**

## **SERGE D.**

Manifestant blessé samedi à Sainte-Soline

- Fiché S pour son appartenance à l'ultra-gauche
- G7 de Biarritz, Notre-Dame-des-Landes
- Deux mois de détention provisoire
- Fils d'un anarchiste en lien avec les autonomistes basques

Première  
Edition

**BASSINES: TOUJOURS DANS LE COMA, QUI SONT-ILS ?**

## Fichier des personnes recherchées

Service : CIAT DE CALAIS

Dossier FPR : GLANZ, GASPARD

Utilisateur : 227202

Les informations contenues dans cette fiche ont un caractère confidentiel et ne peuvent être communiquées qu'aux seules personnes autorisées à en prendre connaissance : Les autorités judiciaires, les services de police et de gendarmerie, les autorités administratives dans le cadre de leurs compétences.

### Identité principale

Identité **GLANZ, GASPARD**  
Né le 22/04/1987 à STRASBOURG (67)  
Nationalité **FRANCAISE**

### Informations générales

Mesure immédiate **Ne pas attirer l'attention**  
Motif **Sûreté de l'état**  
Sommaire **1 identité, 1 fiche**  
Fiche active **S 13 08110 ST**

### Fiche active

Fiche **S 13 08110 ST** **Sûreté de l'état**  
Mesure immédiate **Ne pas attirer l'attention**  
Motif **INDIVIDU MEMBRE DE LA MOUVANCE ANARCHO AUTONOME (OU PROCHE DE LA MOUVANCE D EXTREME GAUCHE RADICALE) SUSCEPTIBLE DE SE LIVRER A DES ACTIONS VIOLENTES**  
Service demandeur **DIRECTION GENERALE DE LA SECURITE INTERIEURE LEVALLOIS PERRET (92)**  
**TEL (H.OUVRABLES) 01.77 [REDACTED]**  
**TEL (PERMANENCE) 01.77 [REDACTED]**  
Conduite à tenir **S03 S04 S05**

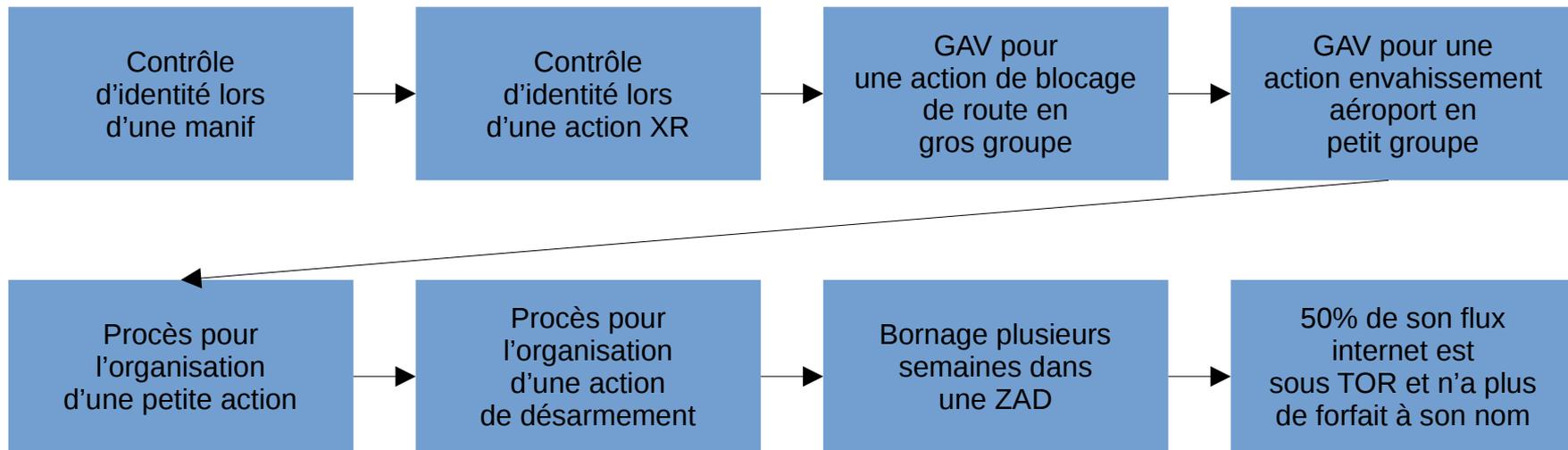
**SCANDALE**

**Une fiche S révélée  
pour la première fois !**



# Le parcours de la radicalisation

Exemple :



## Qu'est ce que la culture de sécurité ?

La culture de la sécurité est un ensemble de pratiques et d'attitudes, que n'importe qui peut suivre, qui sont élaborées pour améliorer la sécurité des communautés politiques

Le mieux c'est de faire une formation exclusivement la dessus

L'auto-défense numérique s'inscrit dans la culture de la sécurité

# PROGRAMME DE LA JOURNÉE

# Les deux niveaux de formation

## MATIN

Signal ou Télégram ou autre chose ?

Bonnes pratiques contre les écoutes/perquiz

## APREM

Ne pas se faire pirater ses comptes

Laisser le minimum de traces

Avoir deux cartes SIM

Bonnes pratiques contre les perquizz

# I – LES OUTILS NUMÉRIQUES DE CHAT

SOMMAIRE - Matin

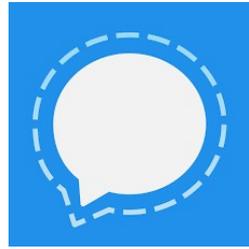
▶ **I – LES OUTILS  
NUMÉRIQUES DU CHAT**

A . Le monde du libre  
B . Différences entre Signal et  
Telegram

**II – BONNES PRATIQUES**

A . Écoute  
B . Bornage

# Les différents outils numériques de chat



# Les différents outils numériques de chat



Telegram



Signal



WhatsApp



Messenger



Protonmail



Mattermost



Jitsi



Olvid

# A . Le monde du libre

## SOMMAIRE - Matin

### I – LES OUTILS NUMÉRIQUES DU CHAT

- A . Le monde du libre
- B . Différences entre Signal et Telegram

### II – BONNES PRATIQUES

- A . Écoute
- B . Bornage

## Le monde du libre



**Différence ?**

## Le monde du libre



**Différence ?**

**Libre et non-libre**

**Chiffrement de  
l'information**

# Différence entre **open-source**, **libre** et **propriétaire**

Le mouvement du libre est social, il soutient des valeurs philosophiques et politiques, alors que le mouvement de l'open source met en avant la méthodologie de développement et de diffusion du logiciel.

La définition du libre défendue par Richard STALLMAN dès 1980 est constituée de 4 libertés :

- Liberté d'exécuter le programme, pour tous les usages
- **Liberté d'étudier le fonctionnement du programme** et de l'adapter à ses besoins
- Liberté de redistribuer des copies. Principe ou philosophie sous-jacente : aider autrui
- Liberté d'améliorer le programme et de publier les améliorations. Philosophie sous-jacente : en faire profiter toute la communauté

# Exemple ligne de code

Il y a un champ de texte

Il y a un bouton nommer « Envoyer »

Le champ de texte est à gauche du bouton

Attendre que l'utilisateur.ice fasse quelque chose

Si l'utilisateur.ice clique sur « Envoyer »

Chiffrer le message avec l'algorithme « Signal Protocol »

Envoyer un message composé du contenu du champ de texte

Puis rafraichir la page

Si l'utilisateur.ice clique sur « fermer l'application »

Fermer l'application



# Différence entre **open-source**, **libre** et **propriétaire**



# Différence entre **open-source**, **libre** et **propriétaire**



TOR



BigBlue  
Button



Linux



LibreOffice



Firefox



Framasoft



Cryptpad



Mattermost  
t



Jitsi



NextCloud  
(rdv)

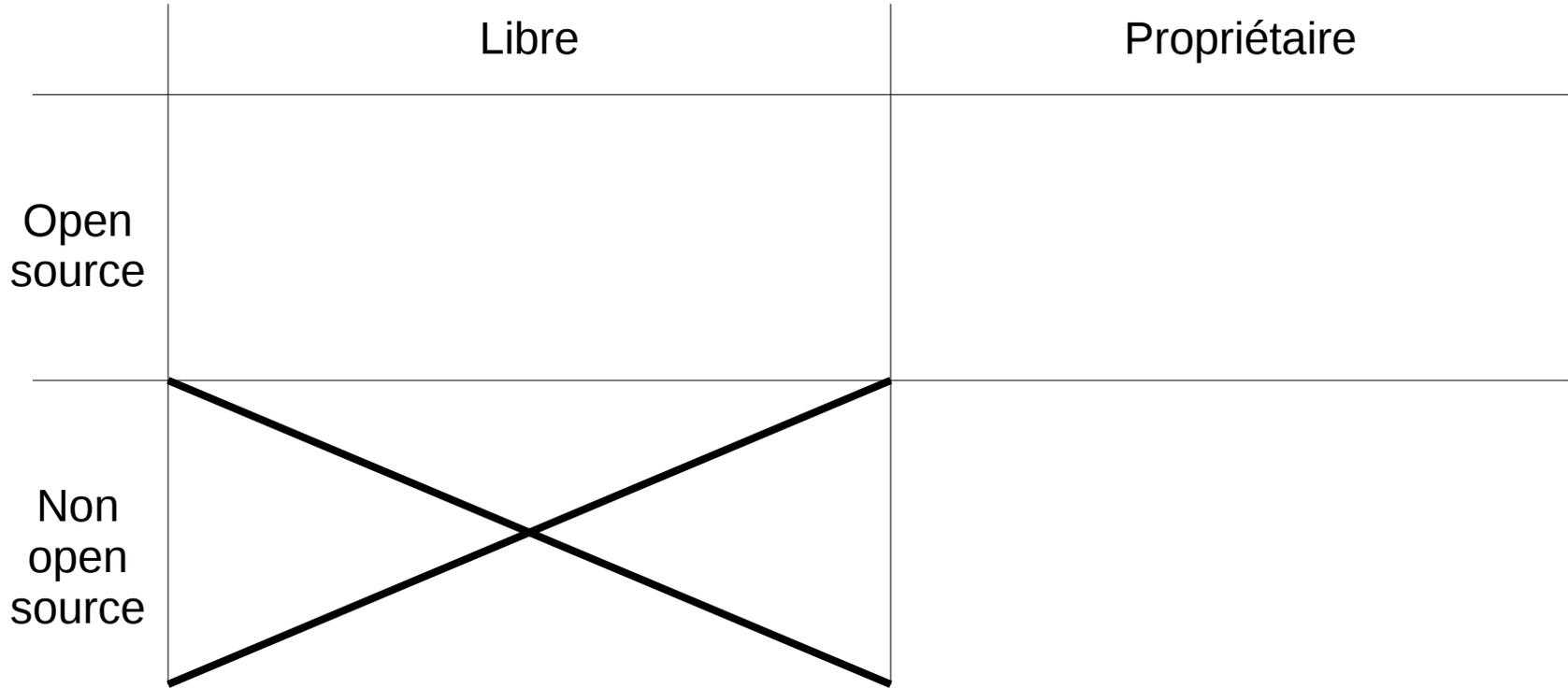


TousAnt  
iCovid

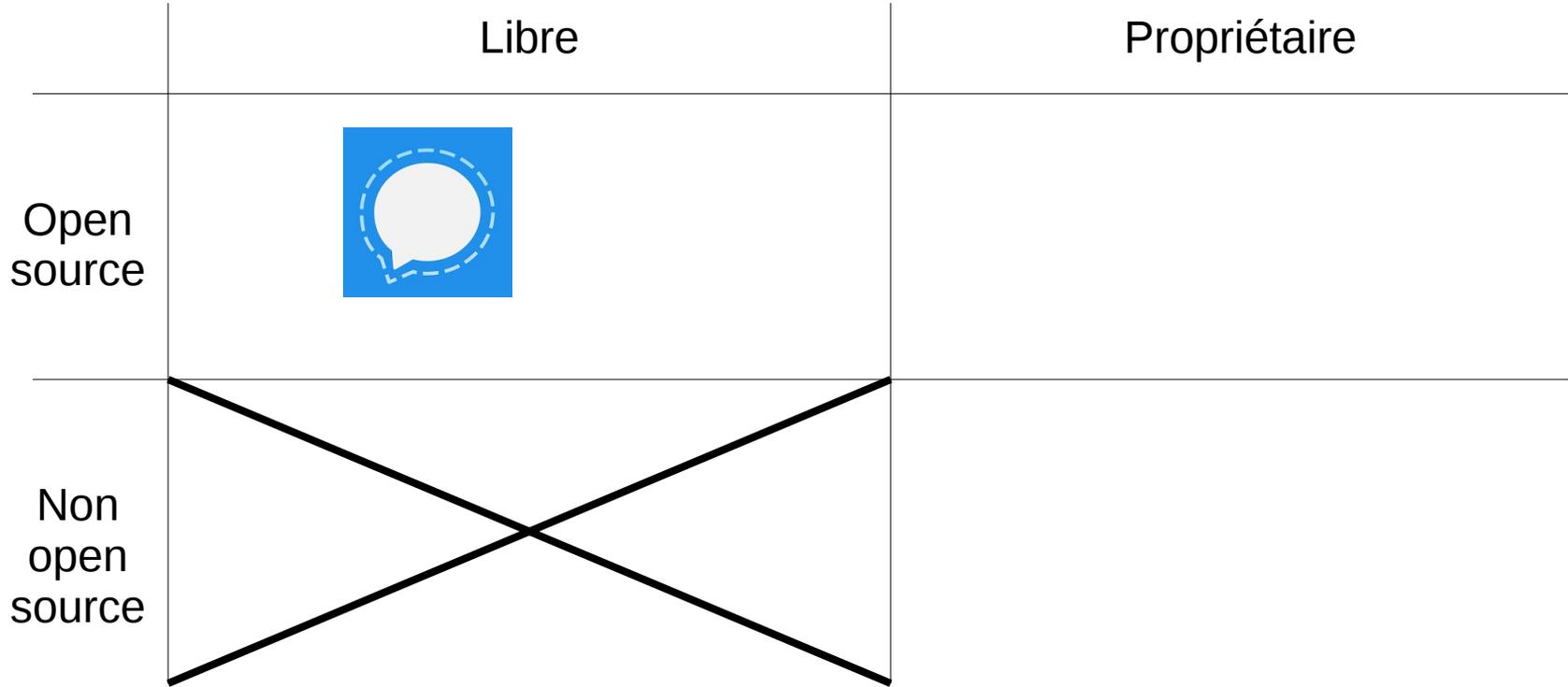


ProtonMail

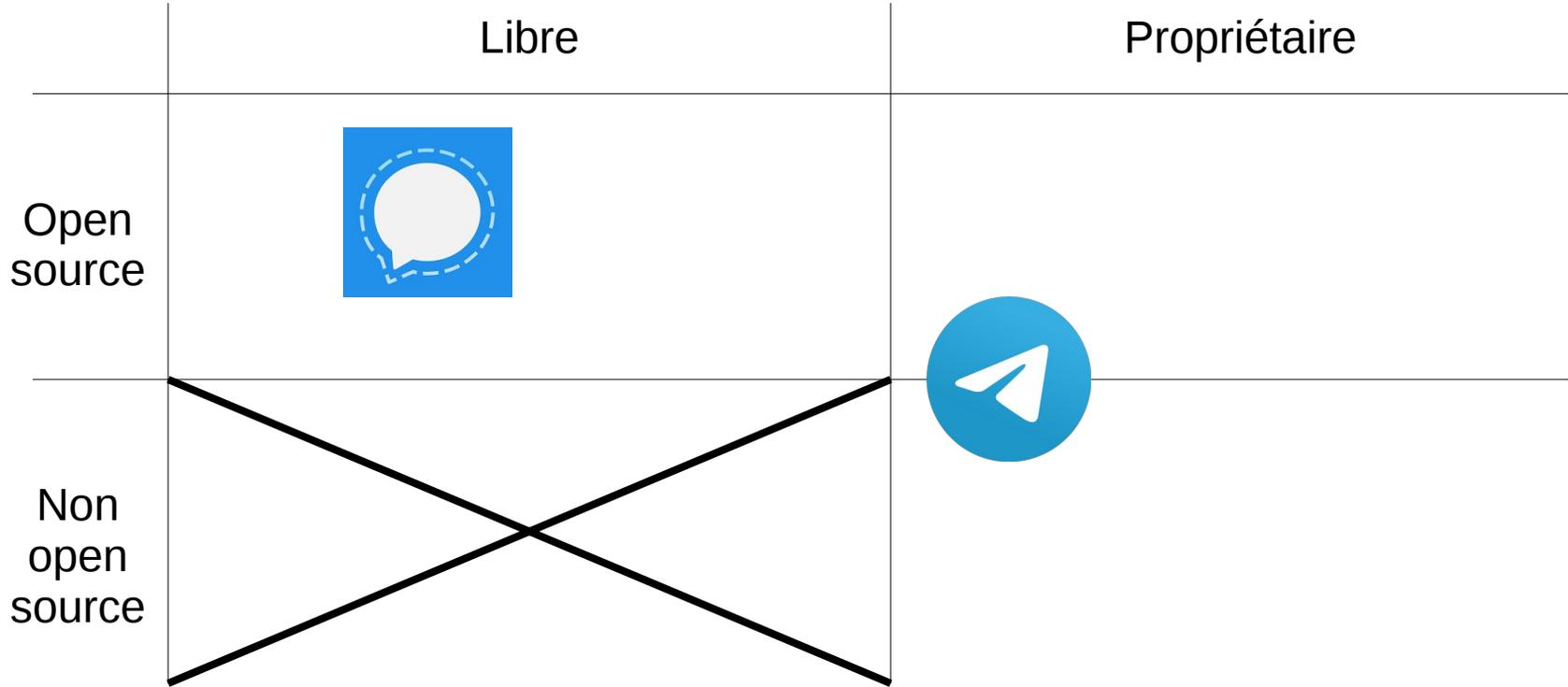
# Différence entre **open-source**, **libre** et **propriétaire**



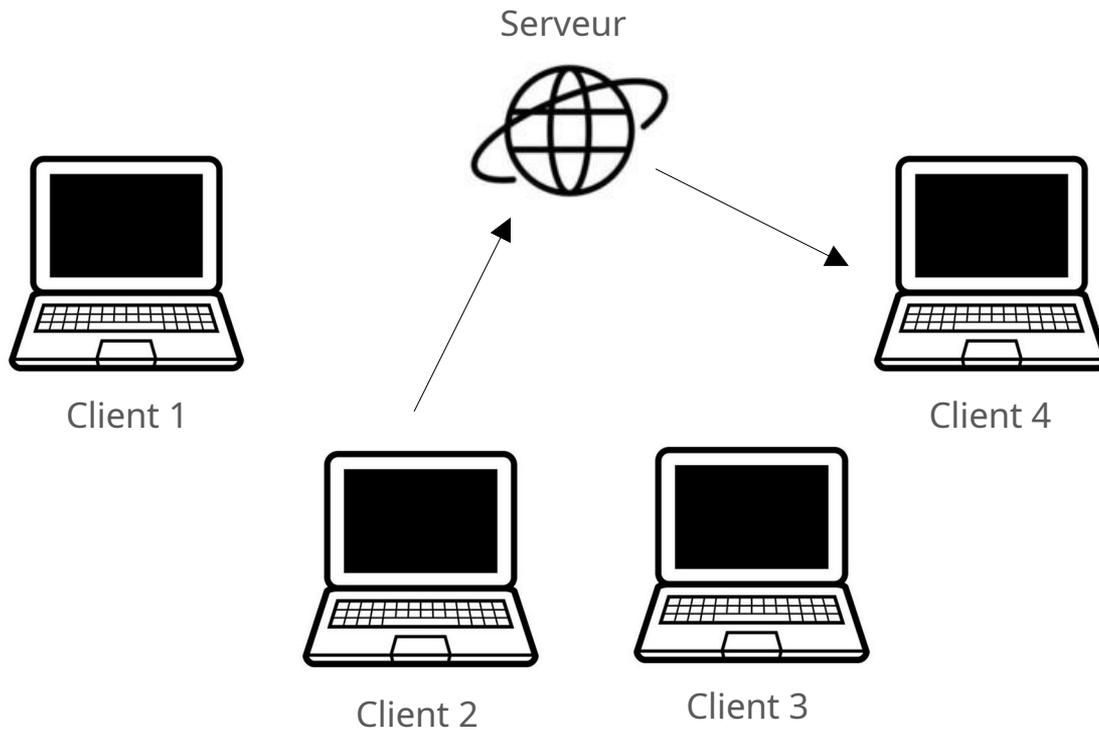
# Différence entre **open-source**, **libre** et **propriétaire**



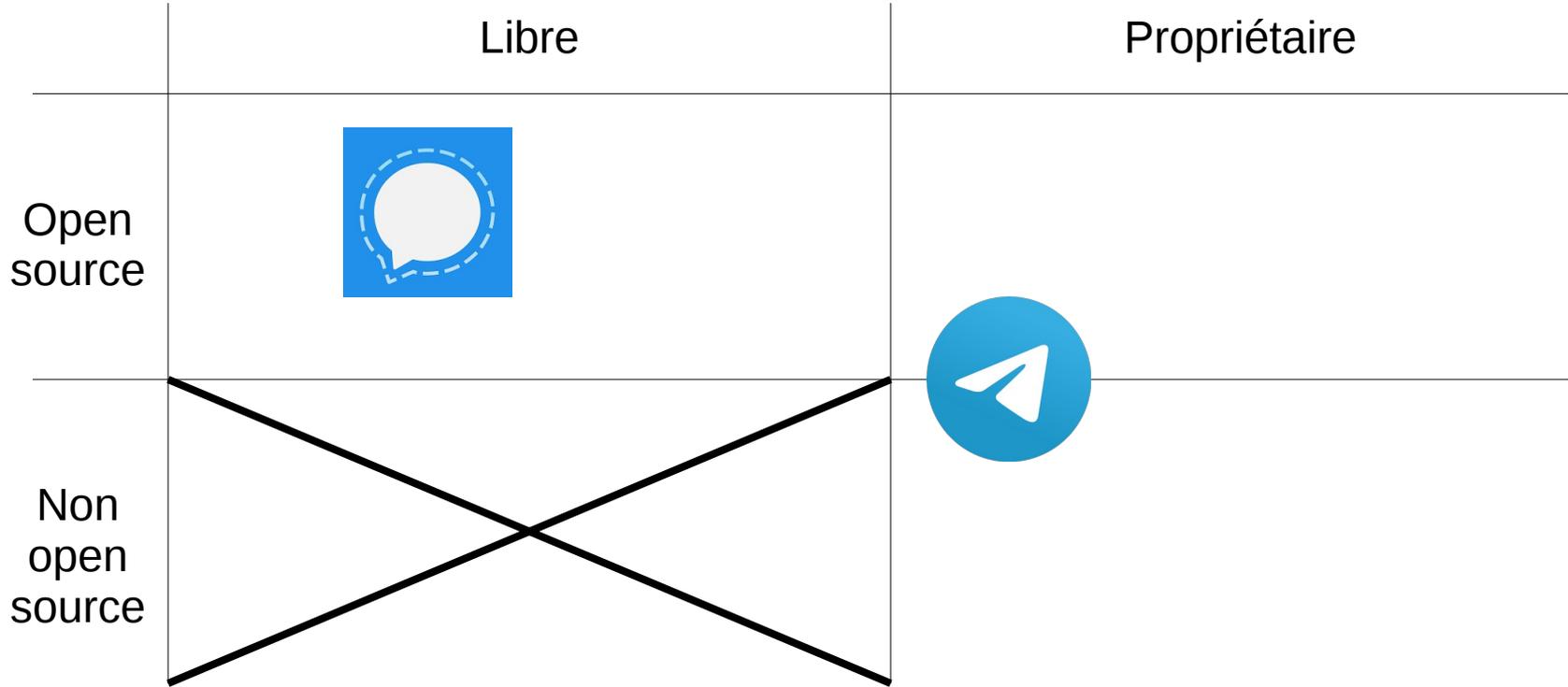
# Différence entre open-source, libre et propriétaire



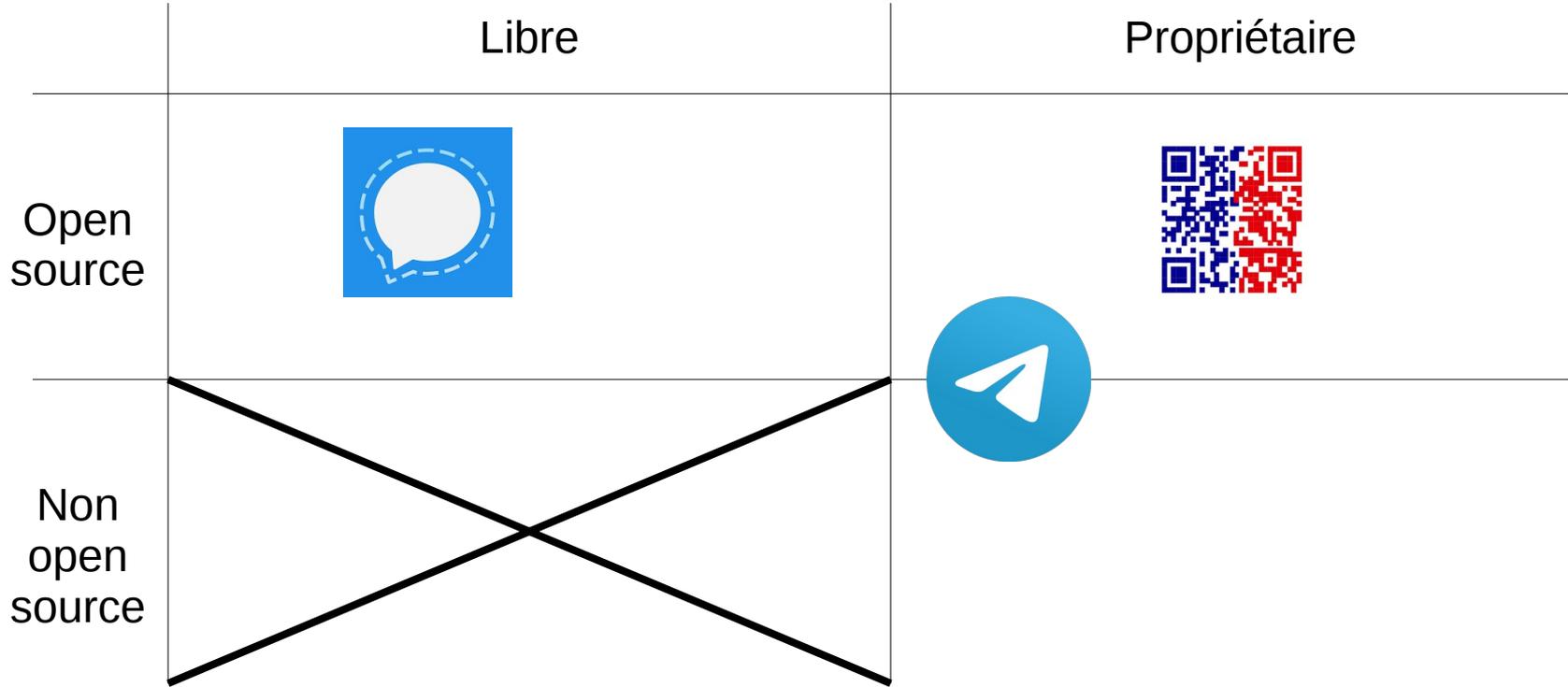
# Serveur et client



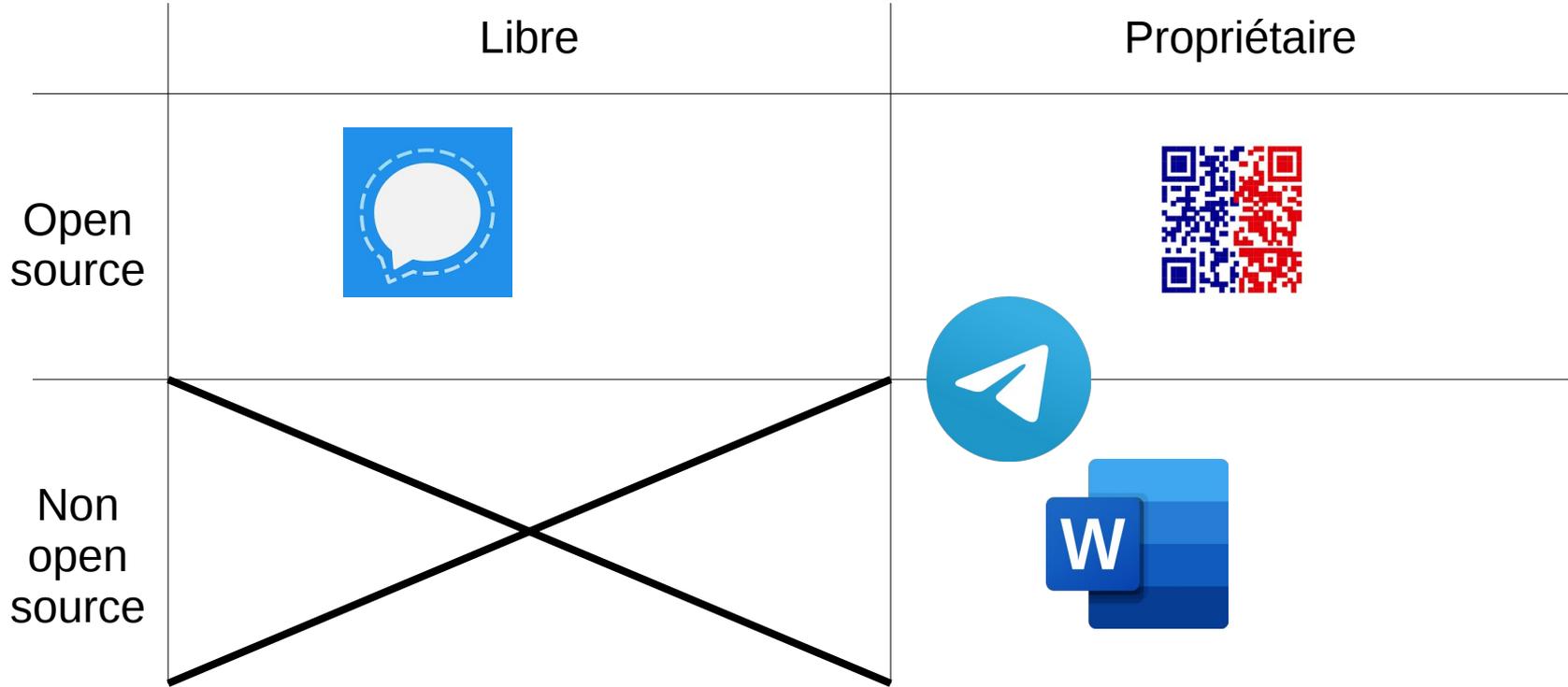
# Différence entre **open-source**, **libre** et **propriétaire**



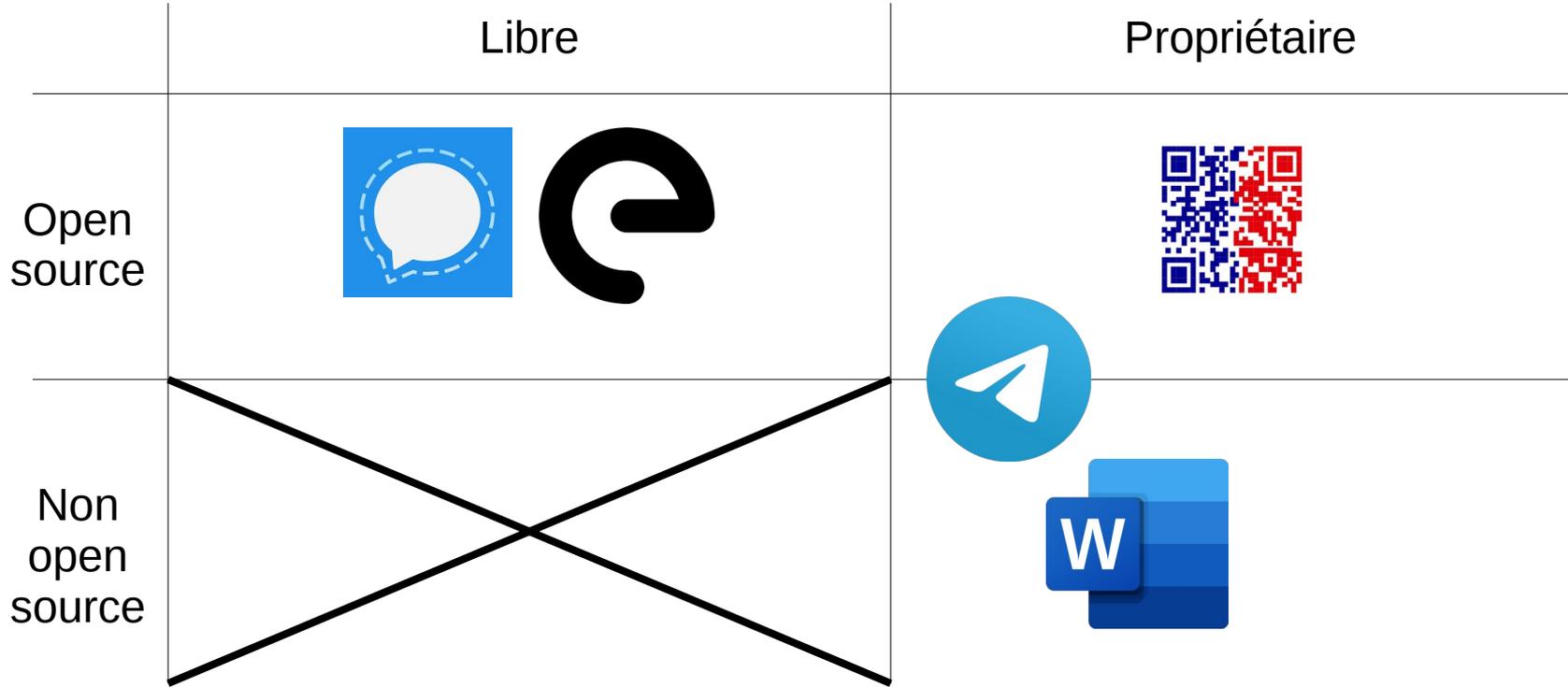
# Différence entre open-source, libre et propriétaire



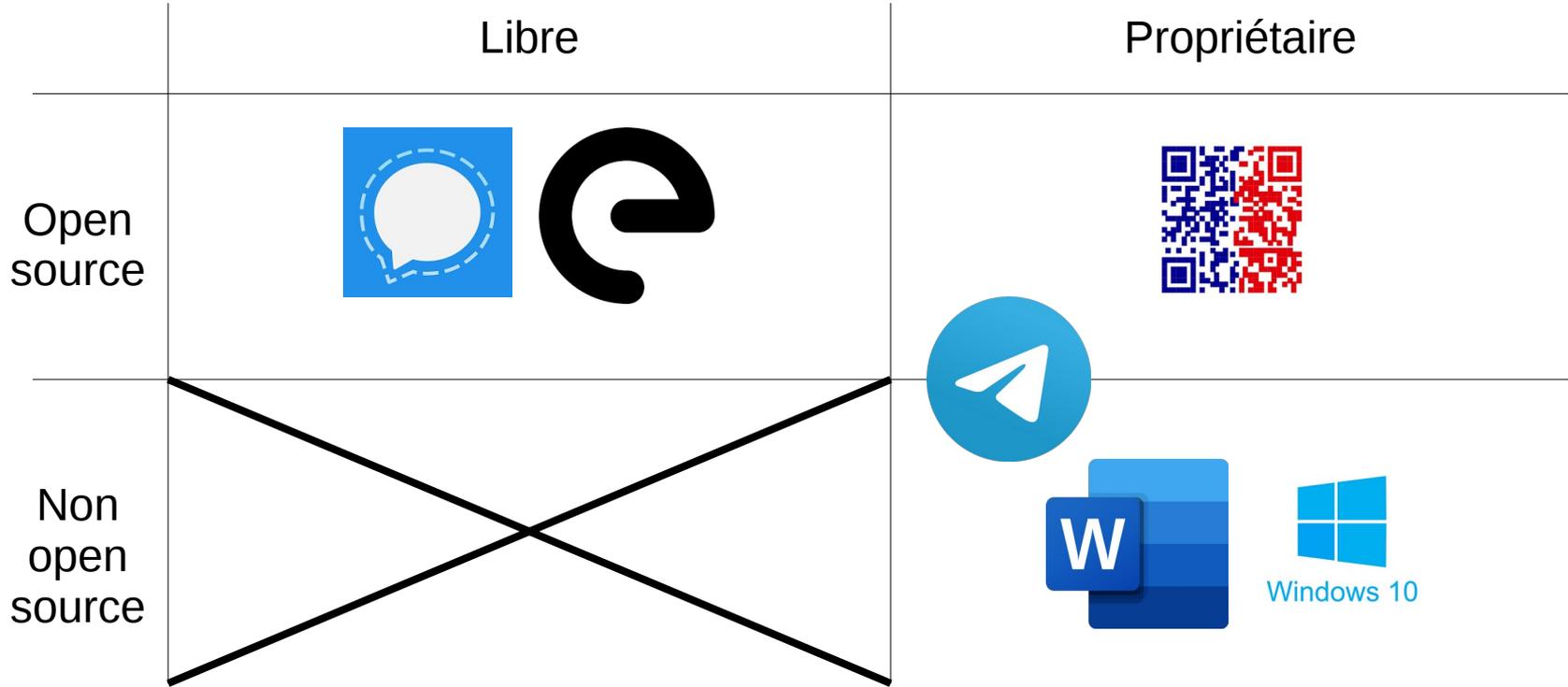
# Différence entre open-source, libre et propriétaire



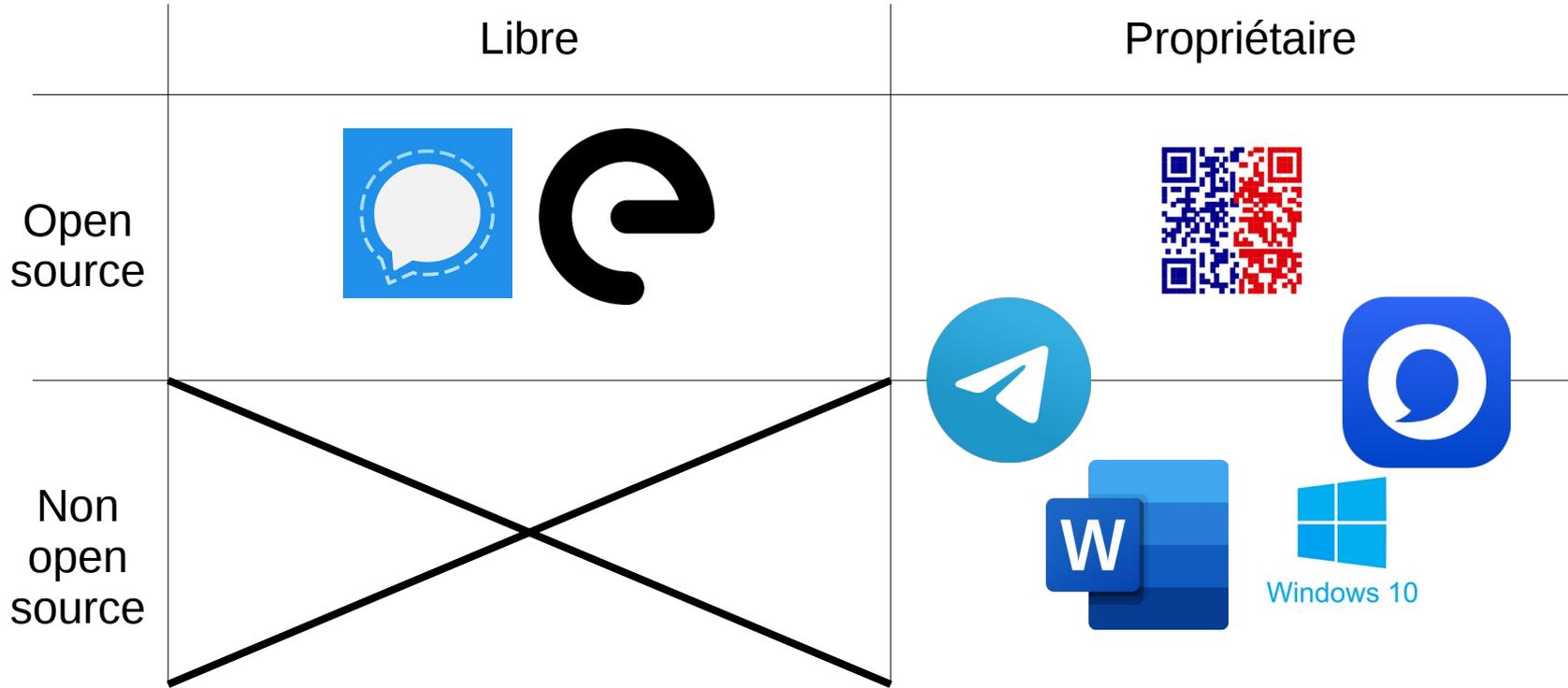
# Différence entre **open-source**, **libre** et **propriétaire**



# Différence entre **open-source**, **libre** et **propriétaire**



# Différence entre **open-source**, **libre** et **propriétaire**



# Savoir si l'outil est **open-source** ou **propriétaire**

**Olvid**

ENTREPRISES   TARIFS   TECHNOLOGIE

← FAQ

## Olvid est-elle Open Source ?

---

**Oui** 😊.

Les codes sources des applications mobiles iOS et Android sont disponibles sur le [GitHub public d'Olvid](#).

### Le code du serveur est-il open source ?

L'intégralité du code des clients est open-source. Ce code, une fois compilé, permet de produire des clients iOS et Android qui pourront communiquer avec notre serveur en production (le même que celui utilisé par les applications clients téléchargées sur l'App Store ou Google Play), et donc d'entrer en relation et de discuter avec tous les autres utilisateurs d'Olvid.

Pour le moment, nous avons néanmoins choisi de ne pas publier le code source du serveur par lequel transitent les messages et ce, pour quatre raisons :

### Sera-t'il open source un jour ?

Oui, quand les API seront stabilisées et que nous serons prêts. Mais pour toutes les raisons expliquées précédemment, ça ne sera probablement pas la version AWS que nous ouvrirons, mais plutôt une version « standalone » (par exemple un Docker), facile à déployer et plus adaptée pour un « petit » nombre d'utilisateurs (quelques centaines).

# B . Différences entre Signal et Telegram

## SOMMAIRE - Matin

### I – LES OUTILS NUMÉRIQUES DU CHAT

A . Le monde du libre

B . Différences entre Signal et  
Telegram

### II – BONNES PRATIQUES

A . Écoute

B . Bornage

# Libre et propriétaire



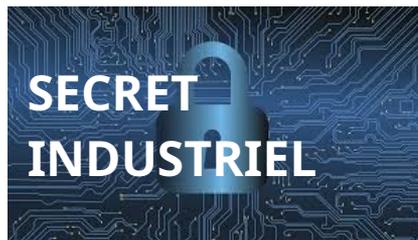
Open-source ?

Open-source



Open-source /  
Propriétaire

Débogage



Financement

Développée par Signal Messenger LLC et financée par la Signal Foundation, une organisation à but non lucratif

Publicité et Pavel Durov (créateur de VKontakte le facebook russe)

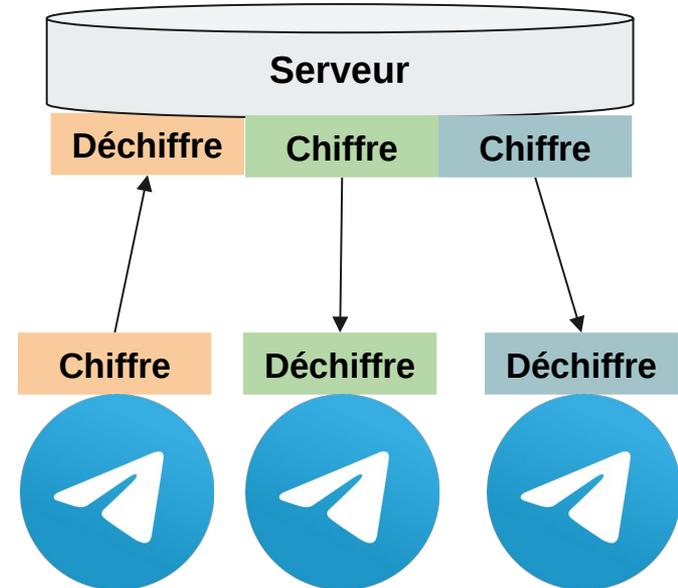
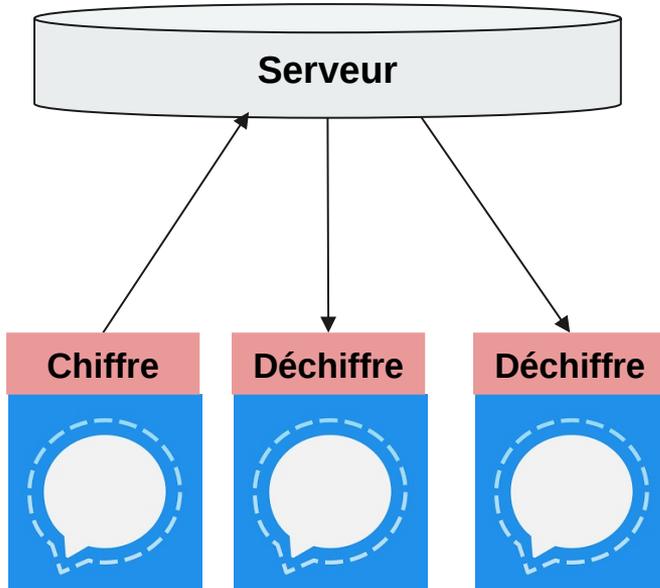
# Chiffrement de l'information

Bonjour, je m'appelle Bernardettes



Cpokpvs, kf n'bqqfmmf Cfsobsefuuft

# Chiffrement de l'information



# Fonctionnalités



Open source	Oui	Client seulement	Client seulement
Chiffrement client/client	Oui	Conv secrète indiv	Oui (+mdp/pgp)
Messages temporaires	Oui	Oui	Oui
Inclusivité technologique	Non	Oui	Oui
Utilité	Petit groupe	Gros groupe	Préparation

# Fonctionnalités



Affichage du numéro de téléphone

Oui

Inclusivité technologique

Non

Utilité

Petit groupe

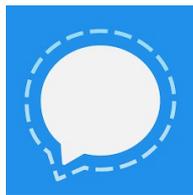
Chiffrer client/client

Oui

Messages temporaires

Oui

# Fonctionnalités



Affichage du numéro de téléphone	Oui
Inclusivité technologique	Non
Utilité	Petit groupe
Chiffrer client/client	Oui
Messages temporaires	Oui

**Ne pas mettre son  
vrai pseudo  
Ou  
Avoir un numéro  
militant**

**Bloquer inscription  
via NIP**

**Toujours relayer les  
appels**

**Mettre les messages  
temporaires par  
défaut**

# Fonctionnalités



Affichage du numéro de téléphone	Non
Inclusivité technologique	Oui
Utilité	Préparation
Chiffrer client/client	Oui (+mdp/pgp)
Messages temporaires	Oui et non

**D'autres applications existes**



# Choisir un outil

- Financement (Fondation, entreprise, publicité...)
- Sécurité fonctionnelle (Chiffrement client-client, message éphémère, numéro de tel)
- Fondateur/Conseil d'administration
- Historique
- Notoriété
- Décentralisation/Juridiction
- Militant
- Open-source
- Inclusivité sécuritaire & anti-tech & facilité

# II – BONNES PRATIQUES



## SOMMAIRE - Matin

### I – LES OUTILS NUMÉRIQUES DU CHAT

- A . Le monde du libre
- B . Différences entre Signal et Telegram

### II – BONNES PRATIQUES

- A . Écoute
- B . Bornage

**Comment éviter les écoutes téléphoniques, sécuriser ses transferts et ses stockages de données ?**

**Ne jamais se fier au software,  
travaillez hardware !**

# A . Écoute



## SOMMAIRE - Matin

### I – LES OUTILS NUMÉRIQUES DU CHAT

- A . Le monde du libre
- B . Différences entre Signal et Telegram

### II – BONNES PRATIQUES

- A . Écoute
- B . Bornage

# Mise sur écoute classique

## Problème :

La police peut vous mettre sur écoute dans le cadre d'une enquête

Elle peut écouter vos échanges téléphonique non chiffrés, vos sms et vos méta-données internet (quels sites vous consultez mais pas ce que vous y faites dessus, et quels applications vous utilisez)



Potentiellement un détecteur de mots clefs (loi renseignement 2021)

Exemple : Affaire de sabotage à Bure (16 ans d'écoutes en cumulé, 29 personnes et lieux mis sur écoute)

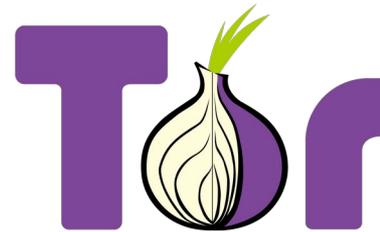
# Mise sur écoute classique

Solution :



Utilisez des messageries chiffrées au lieu des sms et des appels téléphoniques classiques

Signal, Telegram, Whatsapp...



Utilisez TOR ou un VPN

Sur votre ordinateur et sur votre portable

# Piratage de votre appareil

## Problème :

La police n'a pas le droit d'utiliser votre micro ou votre caméra à votre insu (Loi d'orientation de la justice 2023)

Mais les services de renseignements le font souvent : « *Eric Dupond-Moretti soulignait que le déclenchement à distance d'appareils connectés est déjà utilisé par "les services de renseignement", sans l'autorisation du juge, qui devait être ici indispensable* »

Avec Pegasus il suffisait parfois d'avoir son numéro de téléphone pour pirater une personne instantanément

# Cybersécurité : les ministres français invités à désinstaller les applications de messagerie comme Whatsapp, Signal ou Telegram

## Le monde du libre

Selon Elisabeth Borne, ces applications de messageries instantanées "ne sont pas dénuées de failles de sécurité et ne permettent donc pas d'assurer la sécurité des informations" échangées. **franceinfo:**



Je trouve une faille de sécurité



Prevenir le concepteur

Rémunération sous forme de bug bounty (peut se compter en millions d'euro)  
+ éthique

Faire de l'argent en exploitant cette faille (faire un exploit)

Possibilité de faire beaucoup d'argent illégalement

Revendre la faille à une entreprise qui fait de l'exploitation de faille

NSO = entreprise israélienne qui fournit un logiciel permettant a des entités étatiques de surveiller leur population

# Piratage de votre appareil

## Solution :

Mises à jour régulières de vos appareils et applications

+ vous avez d'applications + vous avez de failles de sécurité

+ vos applications ont des droits sur votre téléphones + vous avez de failles de sécurité

Déconnecter physiquement le micro (très difficile)

Mettre un cache sur la webcam

**Ne pas avoir son portable avec soit lorsque l'on parle de choses incriminantes**

# B . Bornage



## SOMMAIRE - Matin

### I – LES OUTILS NUMÉRIQUES DU CHAT

- A . Le monde du libre
- B . Différences entre Signal et Telegram

### II – BONNES PRATIQUES

- A . Écoute
- B . Bornage**

## **Journée habituelle**

La police vous arrête, elle cherche à prouver que vous n'étiez pas là où vous dites que vous étiez, quel(s) moyen(s) technologique(s) a-t-elle pour le prouver ?

# Journée habituelle

Bornage téléphone portable

Utilisation de la CB

Connexion banque en ligne via ordinateur portable

Autoroute/radar plaque immatriculation

Reconnaissance faciale

Carte de transport

# Problématique

La police peut suivre la localisation d'un téléphone portable de différentes façons, cela est effectué de différentes façon, plus ou moins précise, et leur demandant plus ou moins d'efforts

**Comment votre téléphone peut prévenir la police que vous êtes sur place ?**

	<b>Vise une personne</b>	<b>Vise un lieu</b>
<b>En temps réel</b>	<b>Piratage GPS</b>	<b>IMSI Catcher</b>
<b>A posteriori</b>	<b>Fadettes</b>	<b>Evènements réseaux</b>

## Comment votre téléphone peut prévenir la police que vous êtes sur place ?

	Vise une personne	Vise un lieu
En temps réel	<b>Piratage GPS</b>	<b>IMSI Catcher</b>
A posteriori	<b>Fadettes</b>	<b>Evènements réseaux</b>

# Bornage : piratage GPS

On pirate votre portable pour utilisé sa fonction GPS (Loi d'orientation de la justice 2023)

Comme précédemment nécessite une faille de sécurité

Peut être précis au mètre près

Fonctionne en mode avion et probablement pas lorsque le portable est éteint

**Comment votre téléphone peut prévenir la police que vous êtes sur place ?**

	<b>Vise une personne</b>	<b>Vise un lieu</b>
<b>En temps réel</b>	<b>Piratage GPS</b>	<b>IMSI Catcher</b>
<b>A posteriori</b>	<b>Fadettes</b>	<b>Evènements réseaux</b>

# Bornage : fadettes

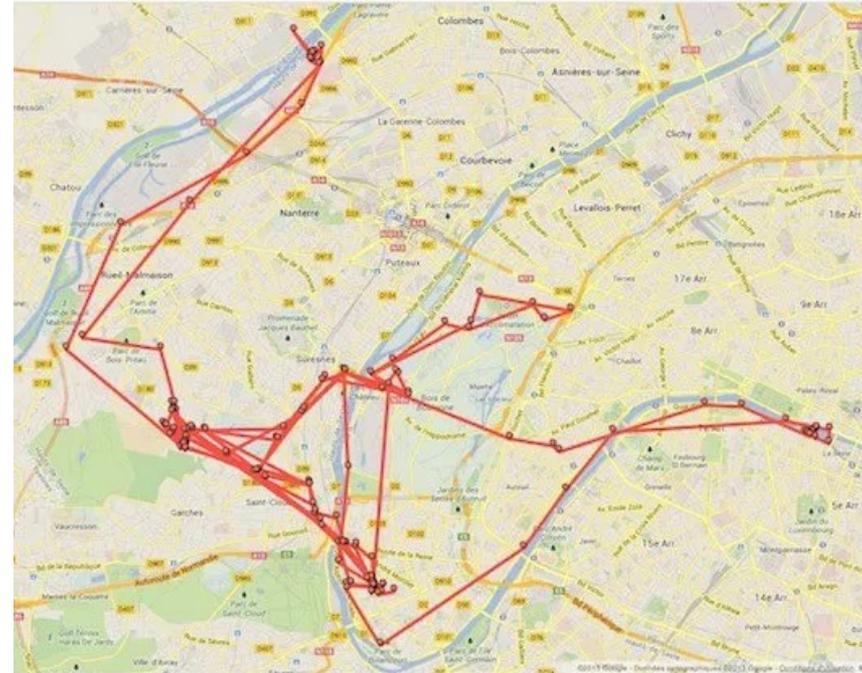
Liste des appels et SMS envoyés et reçus avec la localisation de l'antenne relais

La précision varie : de 1 pâté de maison en ville à plusieurs kilomètres à la campagne

Obligation des opérateurs de garder ces données pendant 1 an

Permet de savoir où vous étiez et des fois qui vous êtes

Première chose regardé par la police en cas d'enquête → garder ses habitudes



**Comment votre téléphone peut prévenir la police que vous êtes sur place ?**

	<b>Vise une personne</b>	<b>Vise un lieu</b>
<b>En temps réel</b>	<b>Piratage GPS</b>	<b>IMSI Catcher</b>
<b>A posteriori</b>	<b>Fadettes</b>	<b>Evènements réseaux</b>

# Bornage : IMSI Catcher

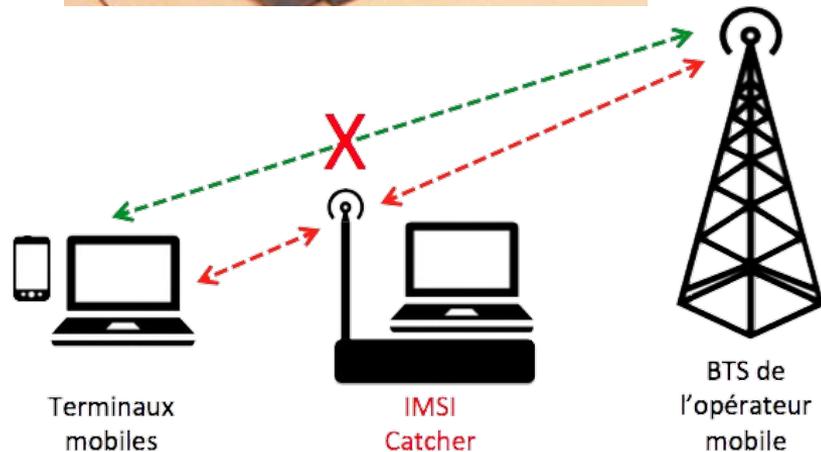
Dispositif permettant de savoir quels portables sont dans les « environs » en direct

Très précis

Déployer en amont

Exemple de moment où il y a des IMSI catcher :

- Sainte Soline
- Jour d'affrontement en ZAD
- Pour découvrir le deuxième portable d'une militante



Brochure : Affaire « Lafarge » Les moyens d'enquêtes utilisés et quelques attentions à en tirer

[https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables\\_4605827\\_4408996.html](https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables_4605827_4408996.html)

**Comment votre téléphone peut prévenir la police que vous êtes sur place ?**

	<b>Vise une personne</b>	<b>Vise un lieu</b>
<b>En temps réel</b>	<b>Piratage GPS</b>	<b>IMSI Catcher</b>
<b>A posteriori</b>	<b>Fadettes</b>	<b>Evènements réseaux</b>

## **Bornage : évènements réseaux**

On demande à une antenne quels téléphones portables sont passés dans le coin et ce qu'ils y ont fait

Contrairement aux fadettes, marche même si on ne reçoit et envoie rien

Contrairement à l'IMSI catcher, est utilisé a posteriori

Grace à la triangulation : précis à quelques metres près

## Comment votre téléphone peut prévenir la police que vous êtes sur place ?

	Vise une personne	Vise un lieu
En temps réel	Piratage GPS	IMSI Catcher
A posteriori	Fadettes	Evènements réseaux

# **Bornage : quel est le résultat de mettre tout les portables dans un micro-ondes**

Tout les portables s'éteignent en même temps à un endroit précis

Cela peut permettre à la police de savoir qui participe à une réunion

C'est plus dangereux que de ne rien faire du tout

# Bornage : solution

Téléphone portable allumé <

Téléphone portable en mode avion <

Téléphone portable éteint <

Téléphone portable sans batterie <

Téléphone portable dans une cage de faraday <

## Pas de téléphone portable

Possibilité de le mettre mode avion + wifi : le mettre en mode avion bien avant d'arriver sur place



FARADAY FABRIC KIT



INCLUDES

① TITANRF FABRIC ② TITANRF TAPE ③ INSTRUCTION CARD

## **Petit quiz !**

Qu'est ce que :  
Un IMSI Catcher  
Un logiciel libre  
Signal ou Télégram ?

## Le petit mémo !

On utilise Signal pour les petits groupes, Telegram pour les gros, Mattermost et Protonmail pour l'avant et l'après

On n'emmène pas son portable ni au brief, ni en action (sauf médiactivistes)

Sur signal : pseudo différent, avoir un NIP + verrouillage inscription, mettre par défaut les messages éphémère, toujours relayer les appels

## Liste de tâches à faire

- Ajouter un VPN à son téléphone et son ordinateur
- Supprimer des conversations pour virer l'historique d'appel
- Avoir les bons réglages sur Signal
- Mettre un cache sur tes webcams

**Des questions ?**

# I – AVOIR SON TEL EN ACTION



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# B . Avoir 2 téléphones / SIM



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM**
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

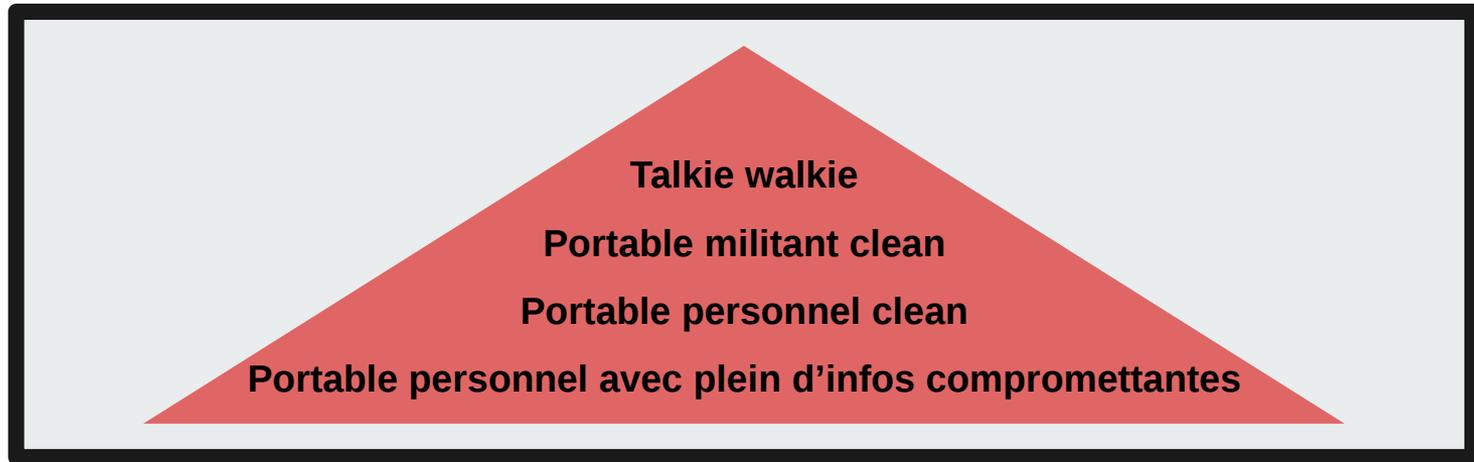
## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Un portable ou pas de portable en action ?



## Les identifiants d'un smartphone

IMEI : numéro de série de la carte réseau gérant votre carte SIM

- un portable avec plusieurs emplacements SIM a plusieurs numéros IMEI mais facilement reliable grace à la géolocalisation

IMSI : le numéro de série de la carte SIM

- change à chaque fois que vous changez de carte SIM

Les deux sont envoyés à une antenne lorsque votre portable tente de se connecter

Les opérateurs gardants les fadettes pendant 1 an, vous ne pouvez pas utiliser un ancien portable personnel comme portable activiste

## Burner phone ou Bigo

Téléphone pas chère utilisé temporairement

Avantage :

- Pas chère
- Rapide à mettre en place
- Inconnu pour sur des services de police

Inconvénients :

- Echange non sécurisé donc facilement écoutable par la police si connu
- Vos fadettes seront très intéressantes car pas de chiffrement

L'objectif étant de l'utiliser que sur une très courte période pour être sur de ne pas être écouté puis de s'en séparer



# Achat portable et carte SIM

## Le portable :

- Acheter soit neuf dans un magasin, soit d'occasion dans un magasin type "cash affaire"
- Payer en cash
- Impossible d'utiliser leboncoin avec TOR, donc si vous souhaitez l'utiliser ça sera avec un wifi public ou avec une carte SIM déjà prépayée

## La carte SIM :

- Toujours prépayée à moins que vous ayez un compte aux îles Cayman
- Opérateur favoris : Lyca, Syma
- Au besoin : remplissez le formulaire avec une « fausse » identité

# Avoir un numéro de portable activiste : les opérateurs



# Avoir un numéro de portable anonyme : les risques

« Avoir une cagoule dans un foule »

Ne pas perdre son portable sinon on perd son compte Signal

# A . Perquisitions



## I – AVOIR SON TEL EN ACTION

### A . Perquisitions

- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Quand est ce que ca se produit ?

Arrestation lors d'une action : Appareils sur vous ou perquisition chez vous pendant la garde à vue

Perquisition chez vous à 6h du matin

# Infos sensibles

Conversation signal, **contacts**, SIM/IMEI, comptes déjà authentifiés, photos...



# Suppression de données

Rarement efficace car les données sont souvent déréférencées et non supprimées

Aucun logiciel ou appli ne permet un effacement efficace d'une image/vidéo/document

Attention ! Supprimer une app de votre portable ne veut pas forcément dire supprimer ses données (Signal c'est le cas)

Sur ordinateur, supprimer l'entièreter du disque dur est quelque chose d'efficace

La meilleure solution c'est **le chiffrement**

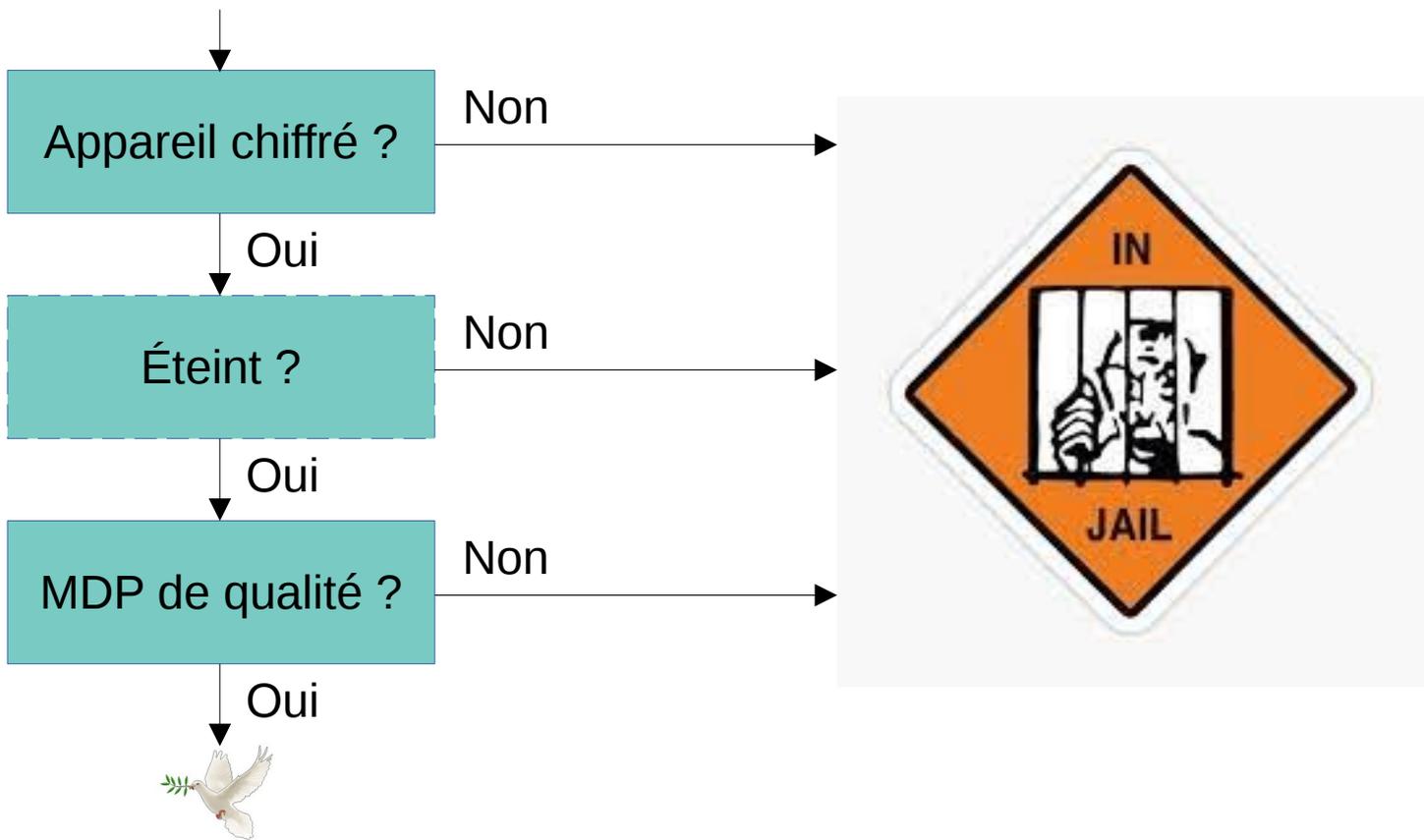
Pour les documents secret défense, la NSA recommande la transformation des disques durs en particules de maximum 2mm à l'aide d'un puissante mixeur



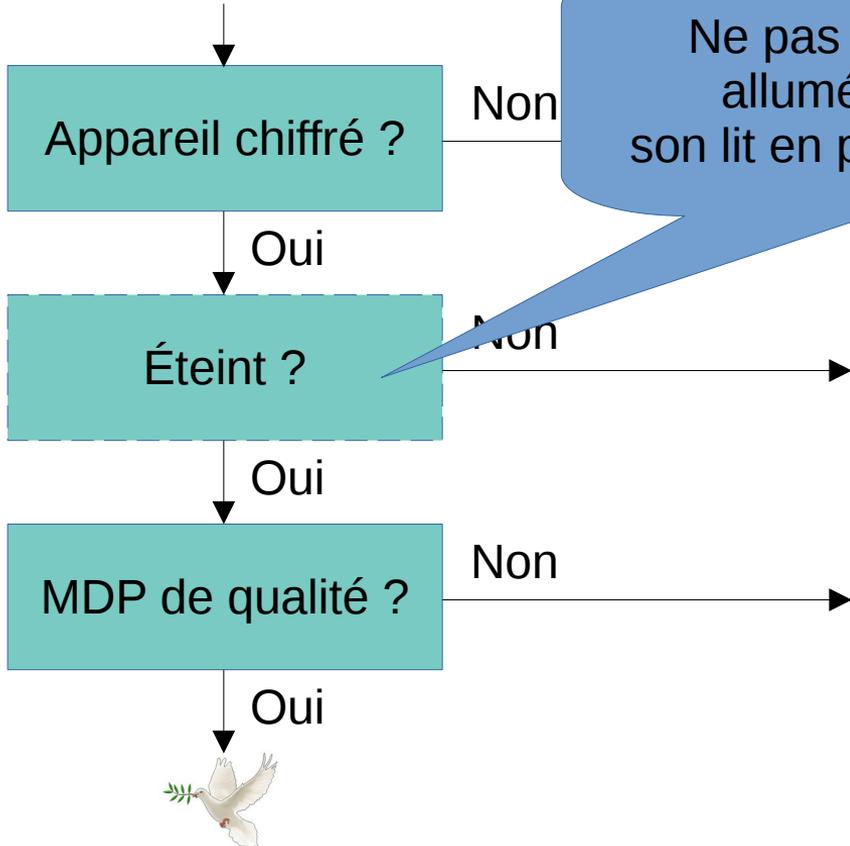
# Aspirateur à données



# Chiffrez votre appareil (Ordi/Téléphone)



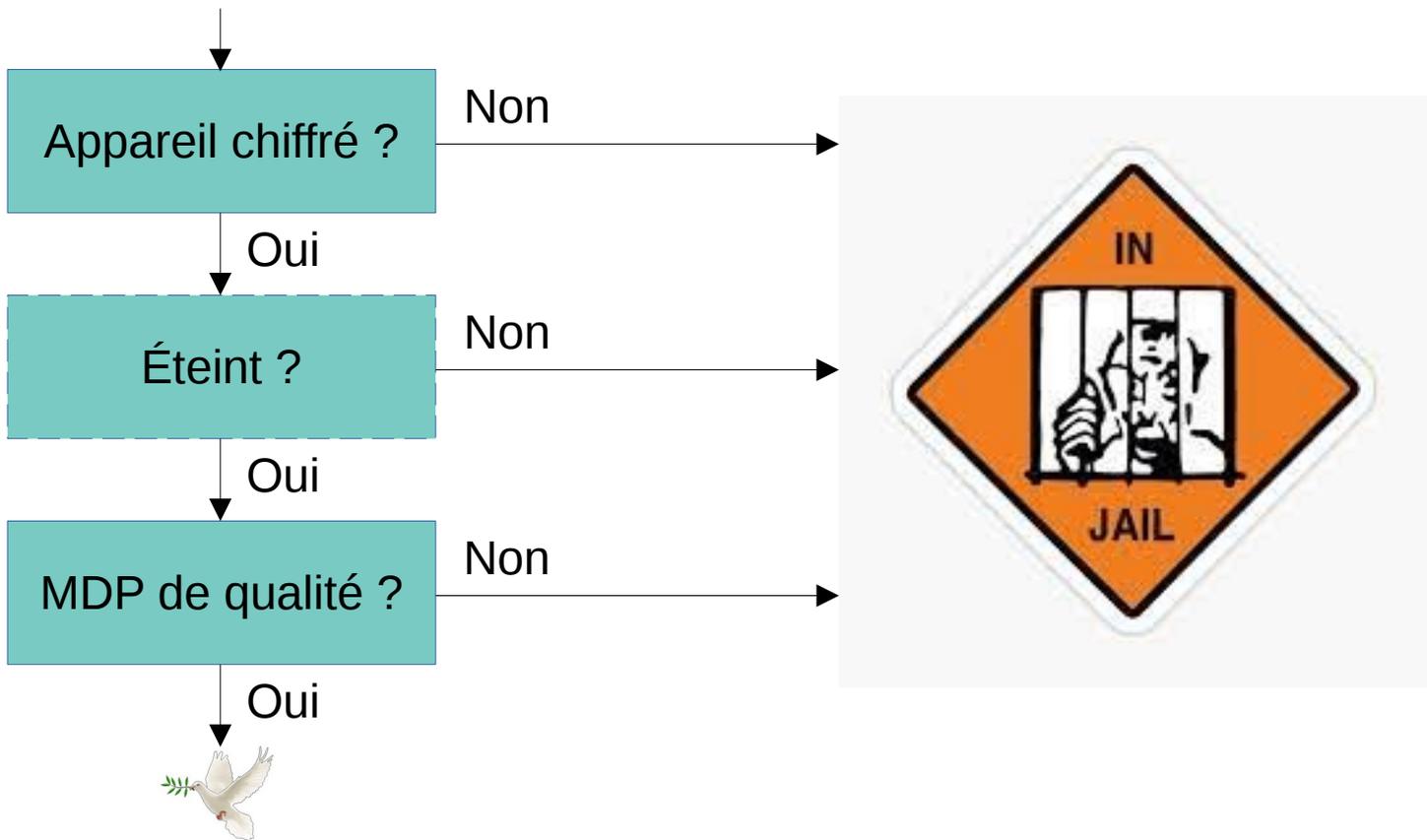
# Chiffrez votre appareil (Ordi/Téléphone)



Ne pas laisser son ordi allumé et ouvert sur son lit en partant en action...



# Chiffrez votre appareil (Ordi/Téléphone)



# Chiffrez son ordiphone

Virer le deverouillage par empreinte digital et reconnaissance faciale

Niveau de chiffrement dépendant de votre modèle de menace

## **Modèle de menace bas :**

Mettre un mot de passe basique avec 4 chiffres

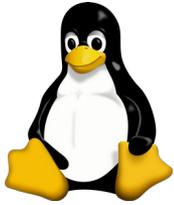
## **Modèle de menace élevé :**

Mettre un mot de passe avec 16 chiffres

Possibilité de mettre un temps d'inactivité neccessaire (30 minutes par exemple)

# Chiffrez votre ordinateur

Chiffrement du système d'exploitation = chiffrement du disque entier



Chiffrement à faire à l'installation



Chiffrement possible à l'installation et une fois installé (réinstallation)



Chiffrement officiel (BitLocker) possible seulement sur certaines versions et vraiment pas très efficaces  
Solution : utiliser Veracrypt

Autre possibilité : chiffrer vos données et pas votre OS en entier

Ralentissement très léger

# Refus de PIN/Mot de passe

L'article 434-15-2 du Code pénal :

Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.

Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.

## Refus de PIN/Mot de passe

Il n'est pas possible de condamner l'auteur du refus s'il ne s'est pas vu notifier formellement le risque pénal que son comportement peut engendrer

Il faut prouver que vous avez connaissance de la convention secrète de déchiffrement →  
Si vous êtes crédible, vous pouvez plaider la non-connaissance du MDP

Chiffrement par déni plausible

# Médiactiviste

Problématique :

Durant une action, le.a médiactiviste possède très souvent un ordiphone avec des photos prises pendant l'action, ielle risque l'arrestation ce que peut engendrer :

- La suppression des images par les FDO
- La confiscation de l'appareil pour le temps de la procédure et donc l'indisponibilité des images et vidéo durant une longue période
- L'utilisation des photos/vidéos prises comme preuves par les FDO

L'objectif :

Réussir à prendre des photos, à les conserver sans que les FDO ne puissent les voir et les supprimer

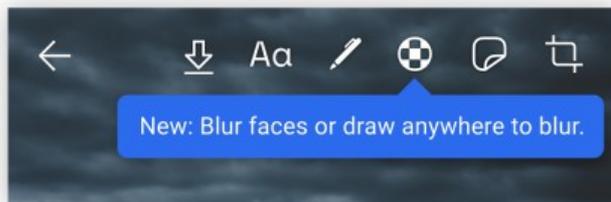
**Scénario :**  
**Ils ont réussi à**  
**déchiffrer votre**  
**téléphone portable**

# Solution

Ne rien stocké sur son téléphone

# Scénario mediactiviste

Signal avec message éphémère à 1h maximum



Signal

# C . Rôles médiactiviste



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste**
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# D . Rôles BAC



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# La BAC (Base arrière communication)

Lieu en dehors de l'action et des risques

Disponible tout le long de l'action

Missions :

- Recevoir les images et vidéos
- Les anonymiser
- Les publier sur les réseaux sociaux (pendant ou après l'action)

# Recevoir les photos et vidéos

Via Signal, sauvegardé sur le portable, puis transfert via câble USB vers l'ordinateur

Ou reçus par la suite pour les photos plus qualitatives

# Ne pas laisser de trace sur l'ordinateur



## Who uses Tails



### Activists

use Tails to hide their identities, avoid censorship, and communicate securely.



### Journalists and their sources

use Tails to publish sensitive information and access the Internet from unsafe places.



### Domestic violence survivors

use Tails to escape surveillance at home.



### You

whenever you need extra privacy in this digital world.

# Anonymiser les photos

Vérifier qu'on ne voit pas de visage (consentement) ou les flouter

Supprimer les métas-données

# Les métag-données

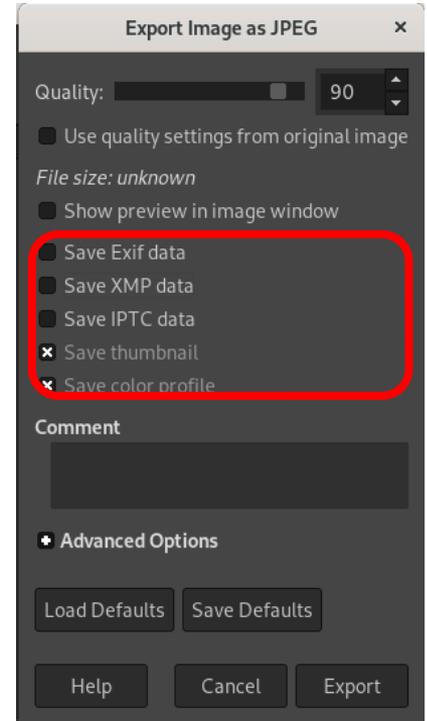
Qu'est ce que c'est ?

# Les métas-données

Date de création de l'image  
Identifiant de l'appareil photos  
Localisation de la prise de la photo  
...

A supprimer avant tout transfert de données non sécurisé et surtout tout post sur les réseaux

Mat2 difficile à utiliser ou disponible sur TAILS



# II – SÉCURISER SES AUTHENTIFICATIONS



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

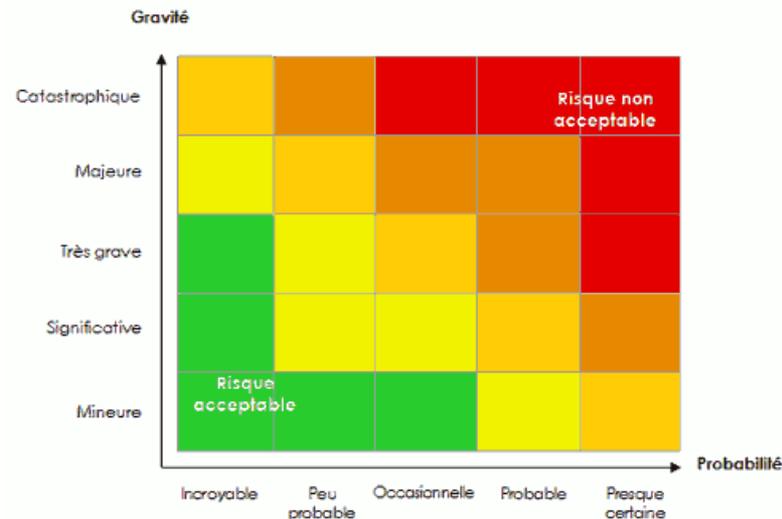
# Qui a le plus de risques de se faire “pirater”/surveiller ?

Personnes ayant potentiellement accès à des informations/média importantes soit car elles :

- Incriminent quelqu'un
- Sont confidentielles et en lien avec un évènement important (par exemple une cible)
- Permettent d'établir la criticité d'un risque

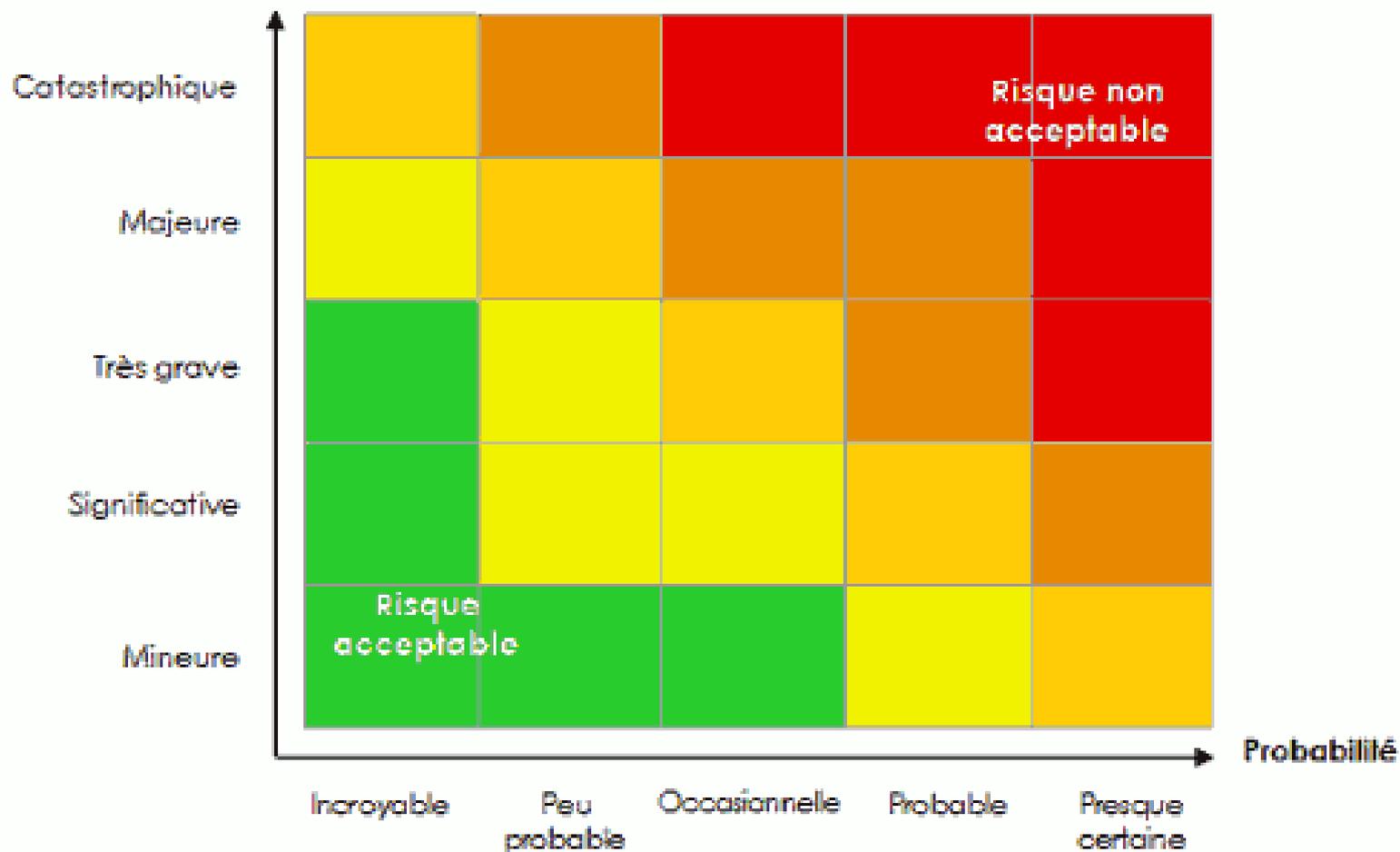
Les personnes souvent à risques sont donc :

- Les coordos de grosses actions
- Les modérateurices / administrateurices (statistiques, accès à beaucoup d'infos... )
- Les rebelles ayant des posture de meneuse
- Les rebelles faisant des rôles à gros risques

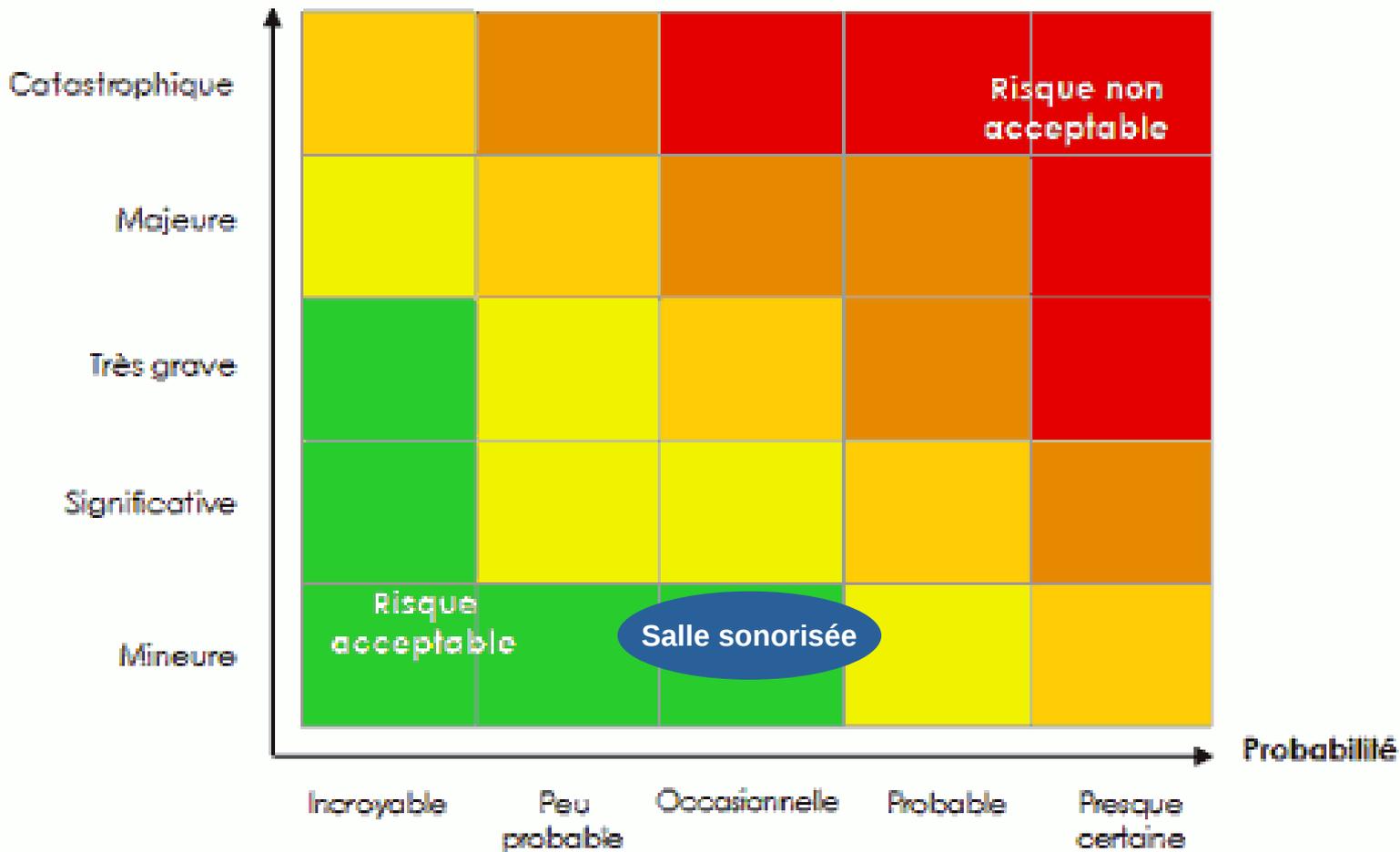


Criticité d'un risque

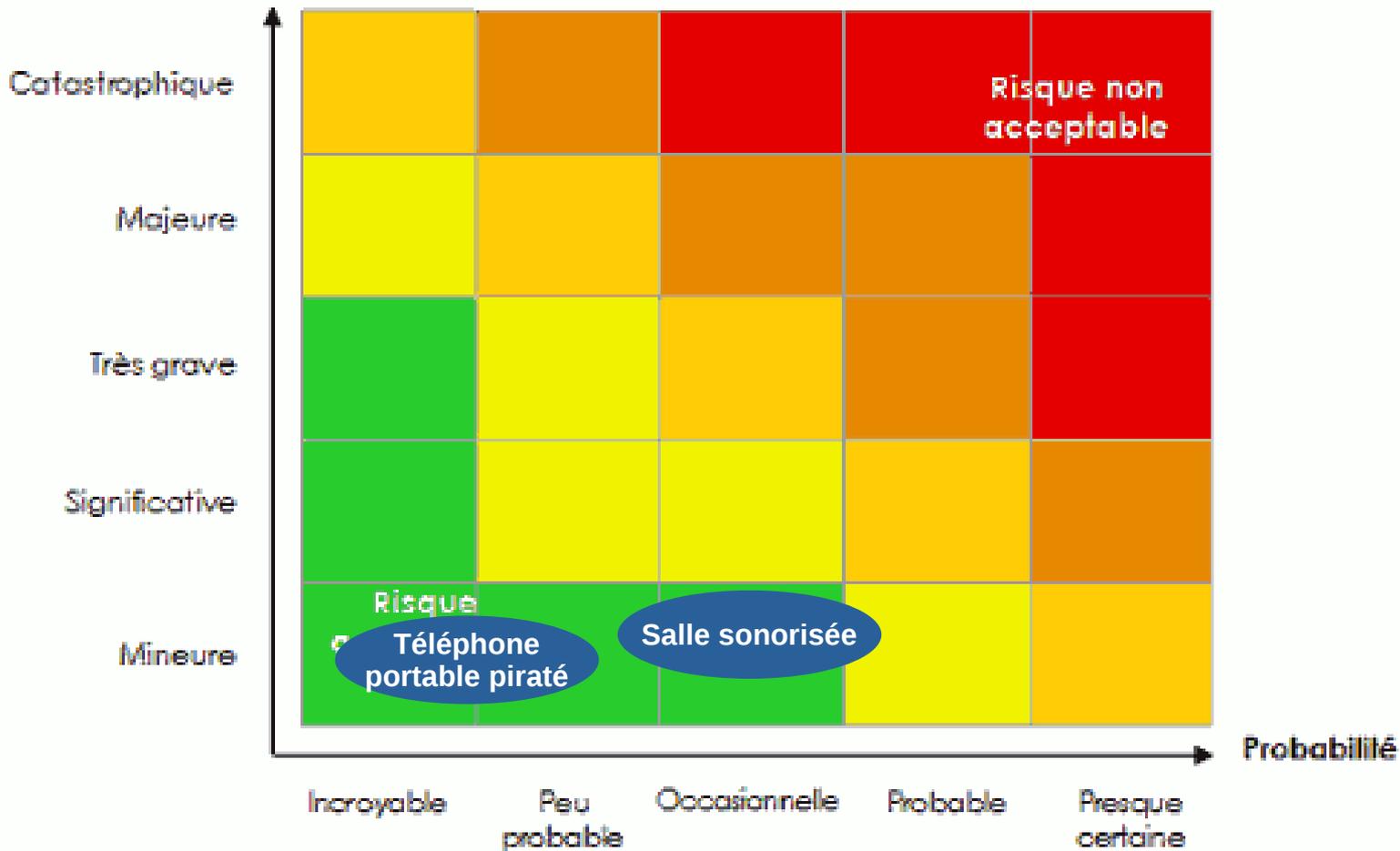
Gravité



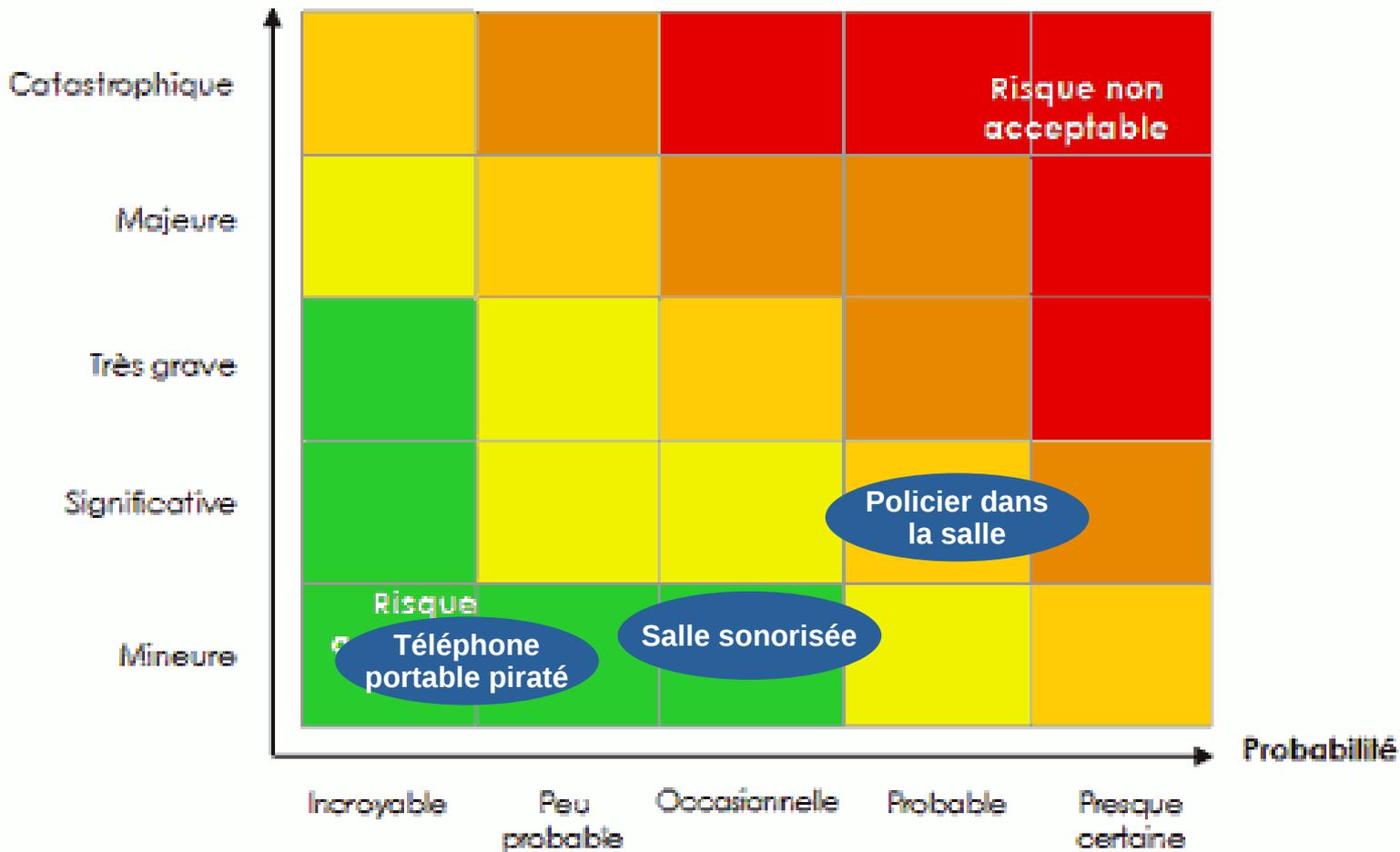
Gravité



Gravité



Gravité



# A . Mots de passe



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Les caractéristiques d'un bon mot de passe

Atelier par petit groupe pour "comment se définir un bon mot de passe ?"

- Faire une liste de choses à faire attention
- Faire 1 mots de passe à retenir

# Les caractéristiques d'un bon mot de passe

Beaucoup de caractères (min 12 caractères) -> phrase de passe

Chiffres, lettres, majuscule/minuscule, caractères spéciaux

Pas de données logiques : date de naissance, prénom, abcde, azerty

Pas d'entrée de dictionnaire

Ni même avec des remplacement de lettres par des caractères d'apparence similaire (\$€rv1ette, cou\$\$1... )

Variété de mot de passe

# La sûreté d'un mot de passe - une solution

Choisir une phrase ou une chanson qui nous fait penser à l'outil

Prendre les premières lettres

Faire des remplacement de lettres par des caractères d'apparence similaire

Exemple, la Marseillaise :

**A€2lpLj2g€@Cn2ltL'€s€l**

- 22 caractères
- 4 lettres majuscules
- 9 lettres minuscules
- 6 caractères spéciaux
- 3 chiffres
- facilement retenable
- incompréhensible

# La sûreté d'un mot de passe - gestionnaire de mdp

Centralisation de tous les mots de passe

Différent type de gestionnaire de mot de passe :

- Fichier chiffré en local
- Application chiffré sur un cloud disponible via :
  - le navigateur web sous forme d'une page web
  - Le navigateur web via un plugin (rempli les champs tout seul)
  - une application mobile

Création du mot de passe maître avec la méthode puis autres automatiquement



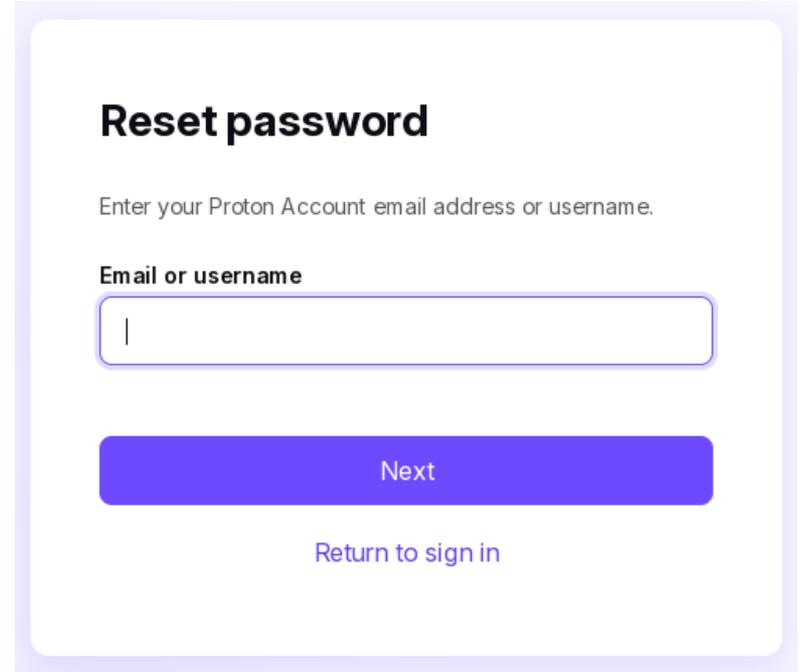
# Les backups

Concerne les authentications mais aussi les données parfois (Mattermost envoie des mail à votre mail...

Option supprimable souvent

La sécurité de l'authentification d'un compte est égale à la plus faible sécurité de l'authentification de ce compte et des comptes de récupération

Il faut donc avoir un très bon mot de passe protonmail si il est relié à plusieurs autres outils



The image shows a screenshot of a web form titled "Reset password". The form is enclosed in a light purple border. At the top, the title "Reset password" is displayed in a bold, black font. Below the title, there is a subtitle: "Enter your Proton Account email address or username." Underneath this, the label "Email or username" is positioned above a text input field. The input field is empty and has a vertical cursor on the left side. Below the input field is a large, rounded rectangular button with a purple gradient, labeled "Next". At the bottom of the form, there is a link that says "Return to sign in" in a blue, underlined font.

**B . 2 FA**



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

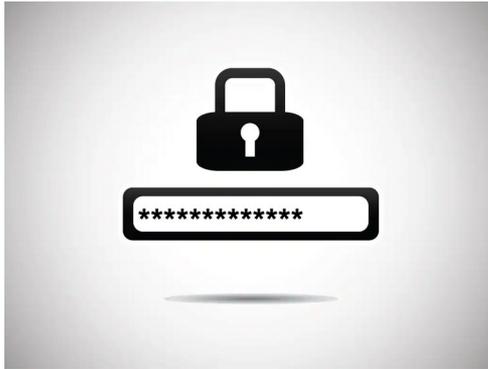
- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Authentification à deux facteurs (2FA)

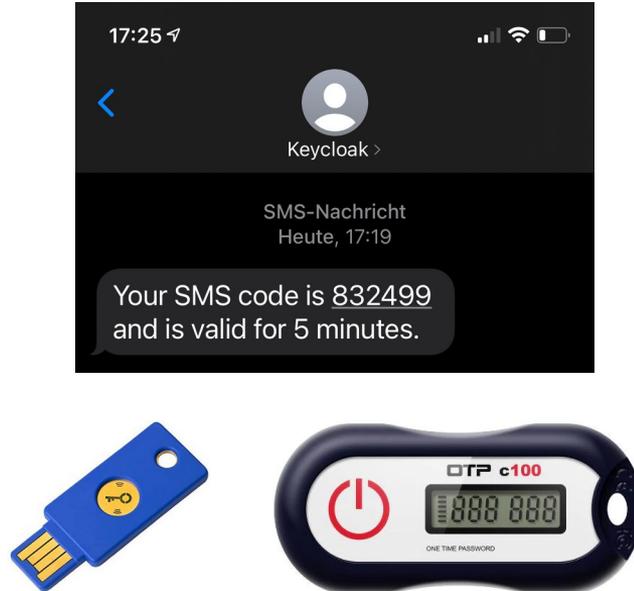
Qu'est ce que c'est ?

# Authentication à deux facteurs (2FA)

Savoir



Avoir



Être



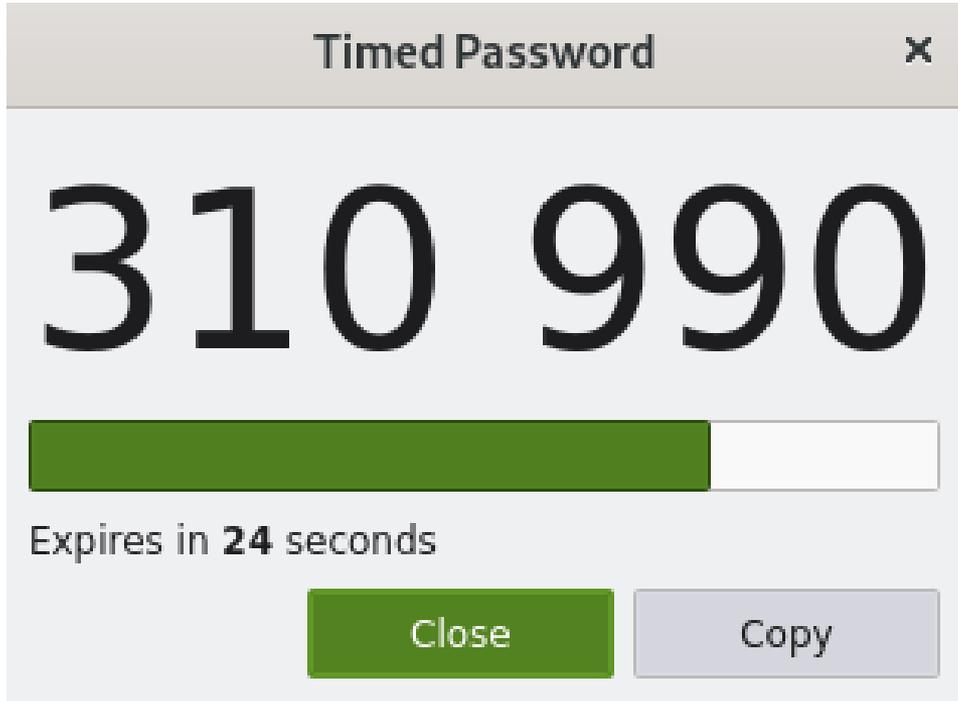
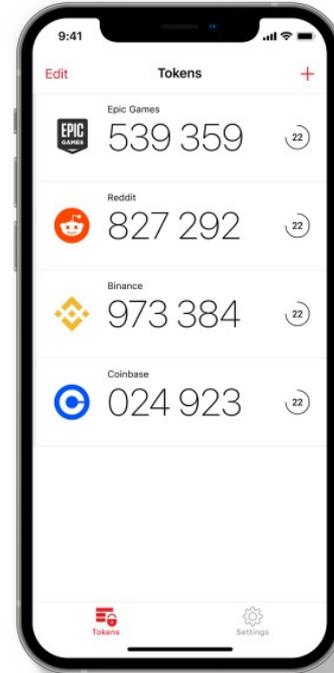
# Time-Based One Time Password (TOTP)

Timed Password ✕

310 990

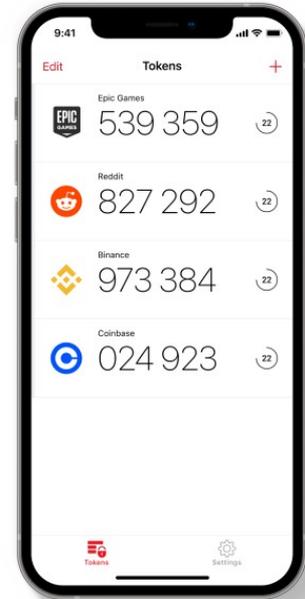
Expires in 24 seconds

Close Copy

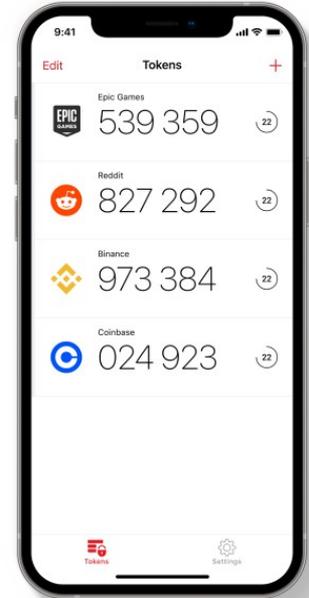
A screenshot of a mobile application dialog box titled "Timed Password" with a close button (✕) in the top right corner. The main content displays the large numbers "310 990" in a dark font. Below the numbers is a green progress bar that is approximately 40% full, indicating the remaining time. Underneath the progress bar, the text "Expires in 24 seconds" is shown. At the bottom of the dialog, there are two buttons: a green "Close" button and a grey "Copy" button.

# Time-Based One Time Password (TOTP)

Comment faire si on perd son portable ?



# Time-Based One Time Password (TOTP)



# III – NAVIGATION WEB ET STOCKAGE DE DONNÉES



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# A . Navigation web

## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Naviguer incognito avec son ordi

Pourquoi un ordi ?

Pourquoi naviguer incognito ?

# L'IP

Numéro d'identification unique attribué à votre box internet

Le police cherche à identifié un utilisateur

→ Ils demandent à l'entreprise gérant les serveurs de leur donner l'IP

→ Selon la politique de confidentialité de l'outil, l'entreprise à + ou - d'infos vous concernant (no logs)

→ Elle leur donne votre IP

→ La police identifie votre FAI (fournisseur d'accès à internet) et lui demande votre identité

→ Votre FAI donne votre identité

Utilisable dans des procédures pour trouver les utilisateurs de : formulaire, boite mail, compte facebook, propriétaire d'un blog...



Reporterre

Le média de l'écologie

## Réputé sûr, Protonmail a livré à la police des informations sur des militants climat

En vertu de la loi suisse, Proton peut être contraint de collecter des informations sur des comptes appartenant à des utilisateurs faisant l'objet d'une enquête pénale suisse. Cela n'est évidemment pas fait par défaut, mais seulement si Proton obtient un ordre légal pour un compte spécifique. En aucun cas, cependant, notre chiffrement ne peut être contourné, ce qui signifie que les emails, pièces jointes, calendriers, fichiers et autres ne peuvent être compromis par des demandes légales.

--- Pour faire suite à la réquisitin adressée à PROTONMAIL ainsi qu'à la réponse obtenue le vingt-six janvier deux mil vingt-et-un, nous demandant d'utiliser le canal INTERPOL ou EUROPOL pour faire parvenir nos réquisitions, ---  
--- Mentionnons avoir adressé à l'unité en charge de la coopération internationale à la Préfecture de Police notre réquisition datant du vingt-six janvier deux mil vingt-et-un afin que soit utilisé la messagerie EUROPOL dédiée, ---  
--- Constatons être destinataire d'une réponse EURPOL que nous exploitons comme suit : ---  
--- Il appert que la société PROTONMAIL nous informe que l'adresse mail a été créée le [REDACTED]. L'adresse IP reliée au compte est la suivante [REDACTED].  
--- Le support utilisé est un appareil [REDACTED] identifié sous le numéro : [REDACTED].  
--- Il s'agit des seules données transmises par la société requise du fait de la politique de confidentialité de PROTONMAIL TECHNOLOGIES. ---  
--- Dont procès-verbal, ---

L'Officier de Police Judiciaire

# Protonmail : militant ?

## Rapport de transparence

De temps à autre, l'entreprise Proton peut être légalement tenue de communiquer aux autorités suisses certaines informations relatives aux utilisateurs, comme indiqué dans notre Politique de confidentialité. Cela peut se produire en cas de violation de la loi suisse. Comme indiqué dans notre Politique de confidentialité, l'ensemble des messages, fichiers et invitations sont chiffrés, et nous n'avons aucun moyen de les déchiffrer.

En vertu de l'article 271 du Code pénal suisse, Proton ne peut transmettre directement aucune donnée à des autorités étrangères, et nous refusons donc toute demande émanant de telles autorités. Les autorités suisses peuvent, de temps à autre, assister les autorités étrangères dans leurs demandes, à condition qu'elles soient valides dans le cadre des procédures d'assistance juridique internationale et qu'elles soient jugées conformes au droit suisse. Dans ces cas, le critère de légalité est également basé sur le droit suisse. En général, les autorités suisses n'aident pas les autorités étrangères des pays ayant un passé de violations des droits de l'homme.

Vous trouverez ci-dessous des statistiques agrégées sur les ordonnances légales que nous avons reçues :

2022

Nombre d'ordonnances légales : 6 995  
Ordonnances contestées : 1 038  
Ordonnances respectées : 5 957

2021

Nombre d'ordonnances légales : 6 243  
Ordonnances contestées : 1 323  
Ordonnances respectées : 4 920

2020

Nombre d'ordonnances légales : 3 767  
Ordonnances contestées : 750  
Ordonnances respectées : 3 017

2019

Nombre d'ordonnances légales : 1 594  
Ordonnances contestées : 110  
Ordonnances respectées : 1 484

2018

Nombre d'ordonnances légales : 340  
Ordonnances contestées : 4  
Ordonnances respectées : 336

2017

Nombre d'ordonnances légales : 26  
Ordonnances contestées : 3  
Ordonnances respectées : 23

## Framaform: militant ?

Nous en recevons une ou deux par an et les respectons quand elles sont en bonnes et dues formes

Framasoft répond positivement aux requêtes de police judiciaire qui lui sont adressées en bonne et due forme, et dont le motif est légitime et correspond à une réelle infraction. Par exemple, si vous ou l'un de vos utilisateurs utilise Framaspace pour héberger (à notre insu) des fichiers pédopornographiques et que nous sommes contactés par les services de police, nous agissons sans délai avec lesdits services pour régler la situation. Après avoir vérifié l'authenticité de la requête, nous collaborerons avec la police ou la gendarmerie et leur communiquerons les informations qu'ils nous demanderont (dans les limites fixées par la loi) et supprimerons les fichiers incriminés.

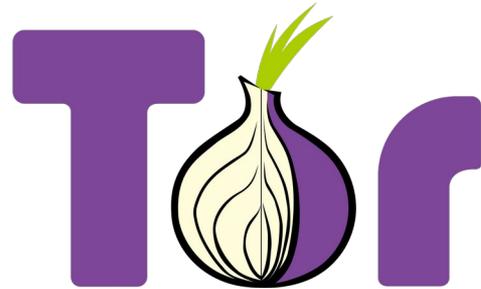
En cas de requête manifestement illégitime, nous refuserons de répondre, en argumentant l'illégitimité de la requête.

En cas de requête tendancieuse ou motivée par des motifs flous, nous agissons au cas par cas, selon l'interprétation de nos juristes concernant la légitimité de la demande.

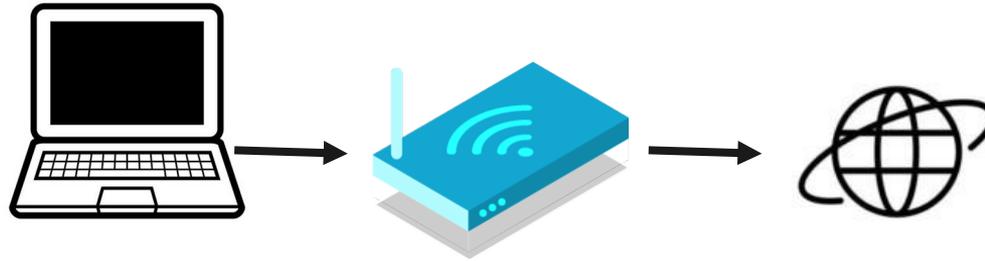


La police dit ne pas envoyer de réquisitions à Riseup par peur qu'ils ne préviennent les personnes concernées, et considérant que Riseup ne leur répondra probablement jamais. Cela semble confirmer que l'utilisation de fournisseurs mail militantes mettant en œuvre un certain nombre de protections et de système de chiffrement tels que Riseup leur pose beaucoup plus de problèmes d'accès que dans le cas de fournisseurs commerciaux <sup>[5]</sup>. (Il va sans dire que l'utilisation de clés de chiffrement PGP pour les échanges de mails ajoute une couche de protection supplémentaire).

# Naviguer incognito avec son ordi

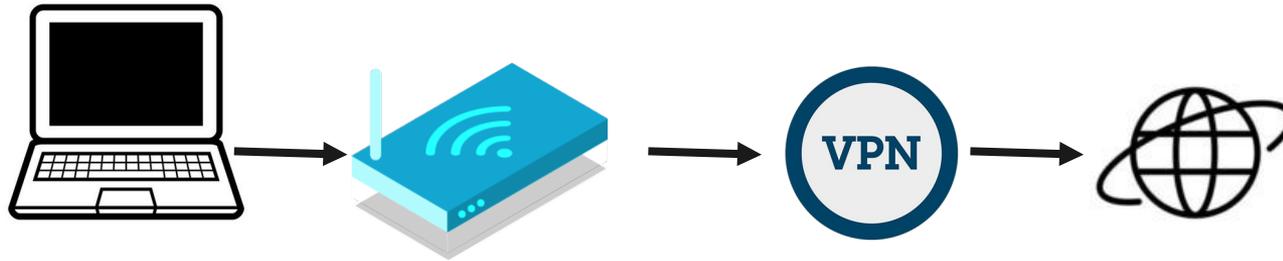


# Sans VPN/TOR



Votre FAI	Le site internet
Sait sur quel site vous allez Ne sait pas ce que vous y faites	Sait et enregistre que vous vous êtes connecté.e

## Avec un VPN



Votre FAI	Votre VPN	Le site internet
Sait seulement que vous utilisez un VPN	Sait sur quel site vous allez Ne sait pas ce que vous y faites	Sait et enregistre qu'un VPN s'est connecté.e et peut l'identifier

## Naviguer incognito avec son ordi



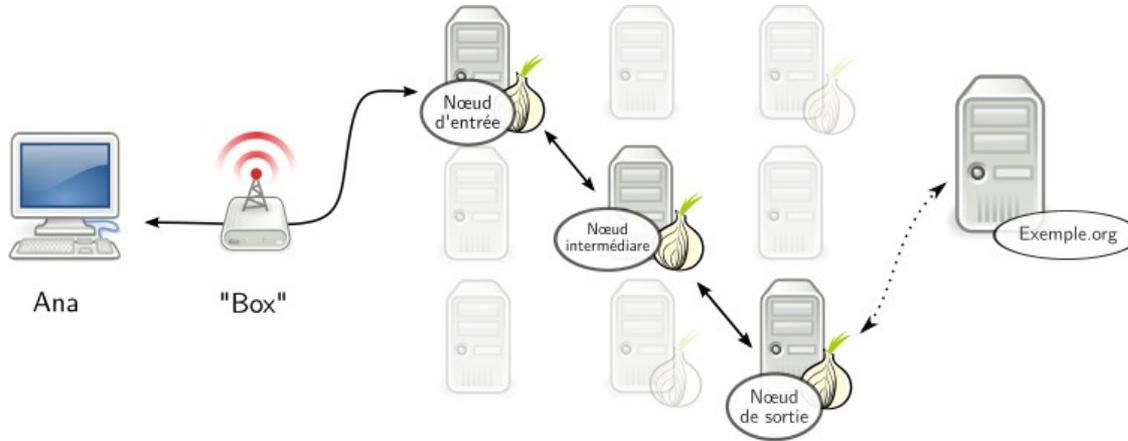
**RISEUP VPN**



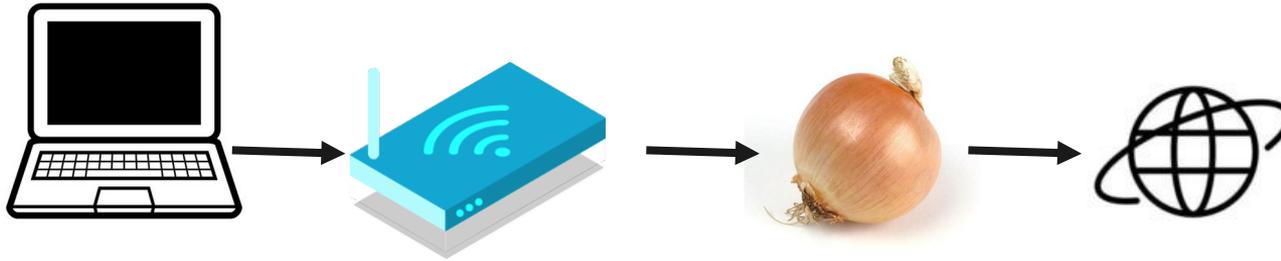
# Avec

Tor est un réseaux informatique et un navigateur web qui permet l'anonymat

Tor est disponible sur toutes les plateformes : Pc, Mac, Android, iOS...



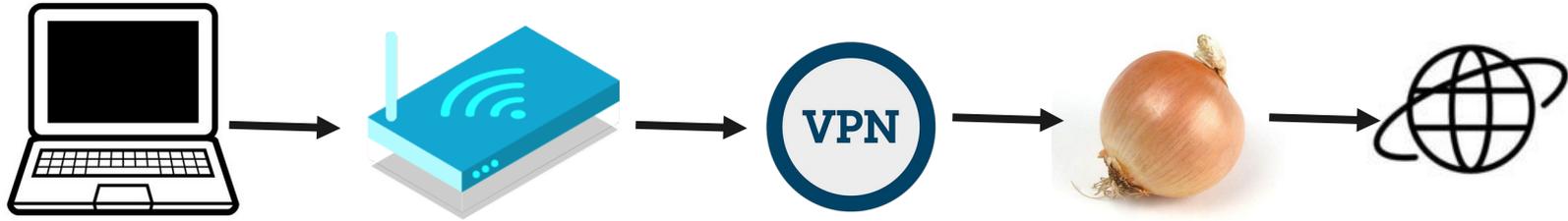
## Avec un VPN



Votre FAI	TOR	Le site internet
Sait seulement que vous utilisez TOR	Ne sait rien	Sait et enregistre que quelqu'un.e s'est connecté.e avec TOR

## Naviguer incognito avec son ordi

TOR + VPN afin d'éviter que votre opérateur ne sache que vous passez par TOR et afin que le VPN ne sache pas où vous allez



Votre FAI	Votre VPN	TOR	Le site internet
Sait seulement que vous utilisez un VPN	Sait seulement que vous utilisez TOR	Ne sait rien	Sait et enregistre que quelqu'un.e s'est connecté.e avec TOR

# Naviguer incognito avec son ordi - bonnes pratiques

Pas d'agrandissement de la fenêtre

Ne pas mélanger ces identités, surtout sur le même site

<https://coveryourtracks.eff.org/>

# Les limites

Il y a de nombreuses failles tel que :

- Les attaques par confirmation :

Considérons que des adversaires aient des raisons de penser que c'est Ana qui publie sur tel blog anonyme. Pour confirmer leur hypothèse, elles pourront observer le trafic qui sort de la connexion fibre d'Ana et le trafic qui entre sur le serveur qui héberge le blog. Si elles observent les mêmes motifs de données en comparant ces deux trafics, elles pourront être confortées dans leur hypothèse.

Tor protège Ana contre des adversaires qui cherchent à déterminer qui publie sur le blog anonyme. Mais il ne protège pas contre des adversaires ayant davantage de moyens qui essaient de confirmer une hypothèse en surveillant aux bons endroits dans le réseau puis en faisant la corrélation.

# B . Stockage de données



## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# Faire du repérage sans faille



## Sécuriser le stockage : la solution



+



# Sécuriser le stockage : la solution



## Who uses Tails



### Activists

use Tails to hide their identities, avoid censorship, and communicate securely.



### Journalists and their sources

use Tails to publish sensitive information and access the Internet from unsafe places.



### Domestic violence survivors

use Tails to escape surveillance at home.



### You

whenever you need extra privacy in this digital world.

# Sécuriser le stockage : la solution



N'a pas de stockage persistant

Pleins de logiciels utiles pour travailler :

- Chiffrement de message
- Écrasement par dessus données
- LibreOffice
- Suppression des meta données

Passer par TOR pour tous les flux internet

Code source vérifiable

# Sécuriser le stockage : la solution



Chiffrée

Utilisé seulement quand on en a besoin

Verrouillée le reste du temps

**Avoir des sauvegardes cachées en cas de perquisitions**



Gnome disk



**LUKS**  
Linux Unified Key Setup

# Sécuriser le stockage : la solution



# Sécuriser le stockage : la solution - DEMO

Les différentes options de démarrage de Tails  
Montrer circuits onion

# IV – AUTRES

## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles

# A . Enquête judiciaire

## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles



# Enquête judiciaire

Sources ouverte = la police trouve les informations sans utiliser leur pouvoir légal

Réquisitions = la police utilise la loi pour demander des informations à des tiers

Surveillance de masse = la police cherche à savoir toutes les personnes qui vont dans une ZAD

Surveillance ciblée = la police vous surveille pour savoir si vous allez dans une ZAD

€€€ Une enquête ça a un coûts €€€

# Enquête judiciaire

Requisitions parfois mensongères

# Quel niveau de sécurité choisir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je vais manifester pacifiquement à Ste Soline

Risques **avant** la manif ?

# Je vais manifester pacifiquement à Ste Soline

Risques **avant** la manif :

- IMSI catcher
- Controle de police

# Je vais manifester pacifiquement à Ste Soline

Risques **avant** la manif :

- IMSI catcher
- Contrôle de police

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je vais manifester pacifiquement à Ste Soline

Risques **avant** la manif :

- IMSI catcher
- Contrôle de police

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je vais manifester pacifiquement à Ste Soline

Risques **pendant** la manif ?

# Je vais manifester pacifiquement à Ste Soline

Risques **pendant** la manif :

- IMSI catcher
- arrestations -> fouille pas très minutieuse du téléphone

# Je vais manifester pacifiquement à Ste Soline

Risques **pendant** la manif :

- IMSI catcher
- arrestations -> fouille pas très minutieuse du téléphone

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je vais manifester pacifiquement à Ste Soline

Risques **pendant** la manif :

- IMSI catcher
- arrestations -> fouille pas très minutieuse du téléphone

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je fais du sabotage

Risques **pendant/après** l'action ?

# Je fais du sabotage

Risques **pendant/après** l'action :

- arrestation -> fouille très minutieuse du portable
- enquête avec fadettes/bornage...

# Je fais du sabotage

Risques **pendant/après** l'action :

- arrestation -> fouille très minutieuse du portable
- enquête avec fadettes/bornage...

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Je fais du sabotage

Risques **pendant/après** l'action :

- arrestation -> fouille très minutieuse du portable
- enquête avec fadettes/bornage...

Quel est le minimum à avoir ?

Téléphone portable  
**personnel** avec carte  
**SIM personnelle**

Téléphone portable  
**personnel** avec carte  
**SIM militante**

Téléphone **militant**  
avec carte SIM militante  
**avec bornage** au domicile

Téléphone **militant**  
avec carte SIM militante  
**sans bornage** au domicile

# Enquête judiciaire

Quelles informations sur un suspect va chercher la police lors d'une enquête pour sabotage ? (par ordre de fréquence)

Filature

Piratage du téléphone portable

Fadettes

Connexion banque/  
service gouvernementaux

Relevé de comptes bancaires

Ecoutes téléphonique

Fichage/antécédents judiciaires

Carte de transport

# Enquête judiciaire

Quelles informations sur un suspect va chercher la police lors d'une enquête pour sabotage ? (par ordre de fréquence)

Fichage/antécédents judiciaires

Fadettes

Relevé de comptes bancaires

Carte de transport

Connexion banque/  
services gouvernementaux

Ecoutes téléphoniques

Filature

Piratage du téléphone portable  
à distance

# B . Attention aux Rts

## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts**
- C . Identités contextuelles



# L'histoire

**Comment ils ont eu mon identité ?**

**Comment ont-ils eu mon identité ?**

**Quelles erreurs ai-je fait ?**

**Comment ont-ils eu mon identité ?**

**Quelles erreurs ai-je fait ?**

- Parler avec un RT
- Mettre des données dans mon portable après cette rencontre
- Avoir donné mon numéro perso à un activiste
- Accepter les contacts dans telegram

# Les deux tactiques de base des RT

Vous complimenter (vous ou votre mouvement)

Vous dénigrer ou complimenter d'autres mouvements

# C . Identités contextuelles

## I – AVOIR SON TEL EN ACTION

- A . Perquisitions
- B . Avoir 2 téléphones / SIM
- C . Rôles médiactiviste
- D . Rôles BAC

## II – SÉCURISER SES AUTHENTIFICATIONS

- A . Mots de passe
- B . 2 FA

## III – NAVIGATION WEB ET STOCKAGE DE DONNÉES

- A . Navigation web
- B . Stockage de données

## IV – AUTRES

- A . Enquête judiciaire
- B . Attention aux Rts
- C . Identités contextuelles



# Identités contextuelles

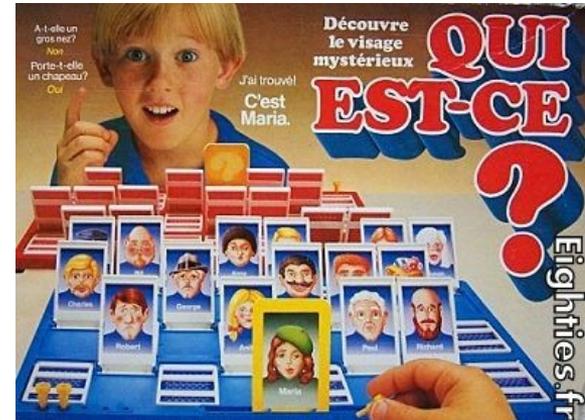
- l'anonymat, c'est ne pas laisser apparaître de nom
- le pseudonymat, c'est choisir et utiliser un nom différent de son identité civile.

Lien entre l'identité contextuelle et l'identité civile → Le recouplement

Corrélation temporelle

Stylométrie

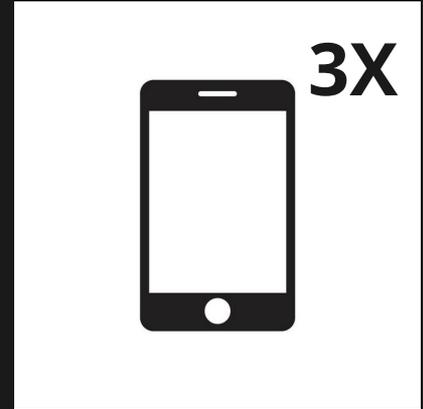
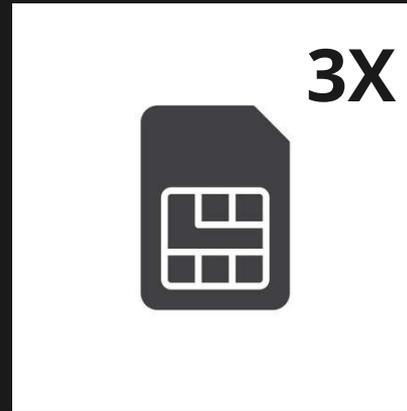
La compartimentation



# Activiste parano STARTER PACK



# Activiste parano STARTER PACK



**FIN !**

# Ouverture

# Petit quiz !

Qu'est ce que :

TOR

Authentification à deux facteur (2FA)

Tails

VPN

**Pour être anonyme vous devez penser à toutes les façons que le gouvernement a pour vous tracer, pour cela il faut connaître très bien tout ce que l'on utilise, ce qui est impossible pour la plupart des gens**

**→ Ayez un groupe/une personne qui s'occupe essentiellement de ça**

## Liste de tâches à faire

- Se faire un portable militant
- Créer un groupe responsable de la sécurité dans votre collectif
- Refaire l'authentification de ses comptes (2FA, backup, gestionnaire de mdp... ) voir même se refaire une identité propre
- Changer son numéro Signal pour en avoir un anonyme
- Acheter/Fabriquer une cage de faraday
- Avoir un clef TAILS et savoir un minimum l'utiliser

**Des questions ?**

# Phase pratique sécu numérique

Objectif : créer un compte Protonmail de la façon la plus anonyme et sécur' possible

## Le petit mémo !

On utilise Signal pour les petits groupes, Telegram pour les gros, Mattermost et Protonmail pour l'avant et l'après

On n'emmène pas son portable ni au brief, ni en action (sauf médiactivistes)

Sur signal : pas de pseudo, avoir un NIP + verrouillage inscription, mettre par défaut les messages éphémère

Ne pas stocker de photos/vidéos sur son portable

Chiffrer son portable