Formation à l’auto-défense numérique dans le militantisme

Bernardettes

Qui suis-je ?

Diapos transmises après la formation

Formation en constante évolution grâce à vous

D’où viennent les infos

Sites internet militants/gouvernementaux/autres
Retours d’expériences en ligne et dans la vie réelle
Historique de procédures judiciaires
Discussions plus ou moins techniques durant les formations ou durant d’autres moments 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

« Le smartphone est un appareil d’espionnage ! Il entend tout ce que vous faites, dites, envoyez et prenez en photo. Votre localisation, votre maison… Israël n’a pas besoin de plus que cela. »

Hassan Nasrallah, secrétaire général du Hezbollah

Introduction – les compromis

Outils numériques = risques (et toujours des risques)

Souvent, plus on veut de **sécurité,** plus cela demande de l'**énergie**
→ 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 – modèle de menace

Qui sont nos adversaires potentiels ?

Quels sont leurs moyens ?

Que voulons-nous leur cacher ?

Que risquons-nous si on échoue ?

Quelles difficultés suis-je prêt à rencontrer ?

→ Travail collectif de réflexion

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 un jour vous souhaitez faire des actions plus engageantes ou si vous avez de gros soucis judiciaires, 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 s’intéresser 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 – flirt 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

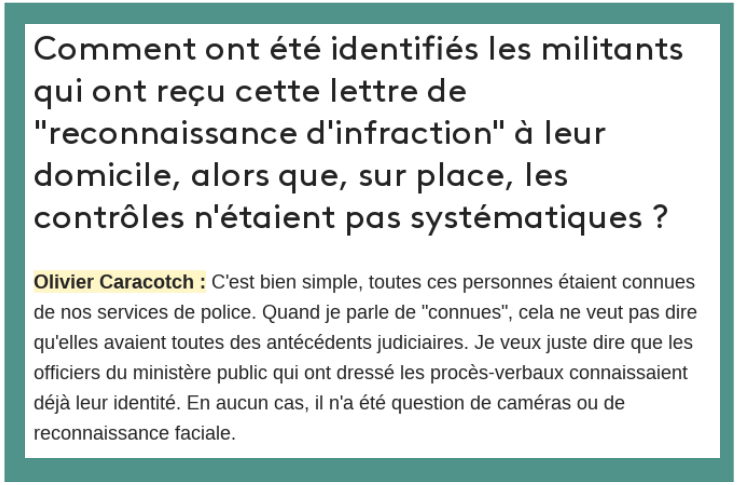
Introduction - Pourquoi se protéger ?

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

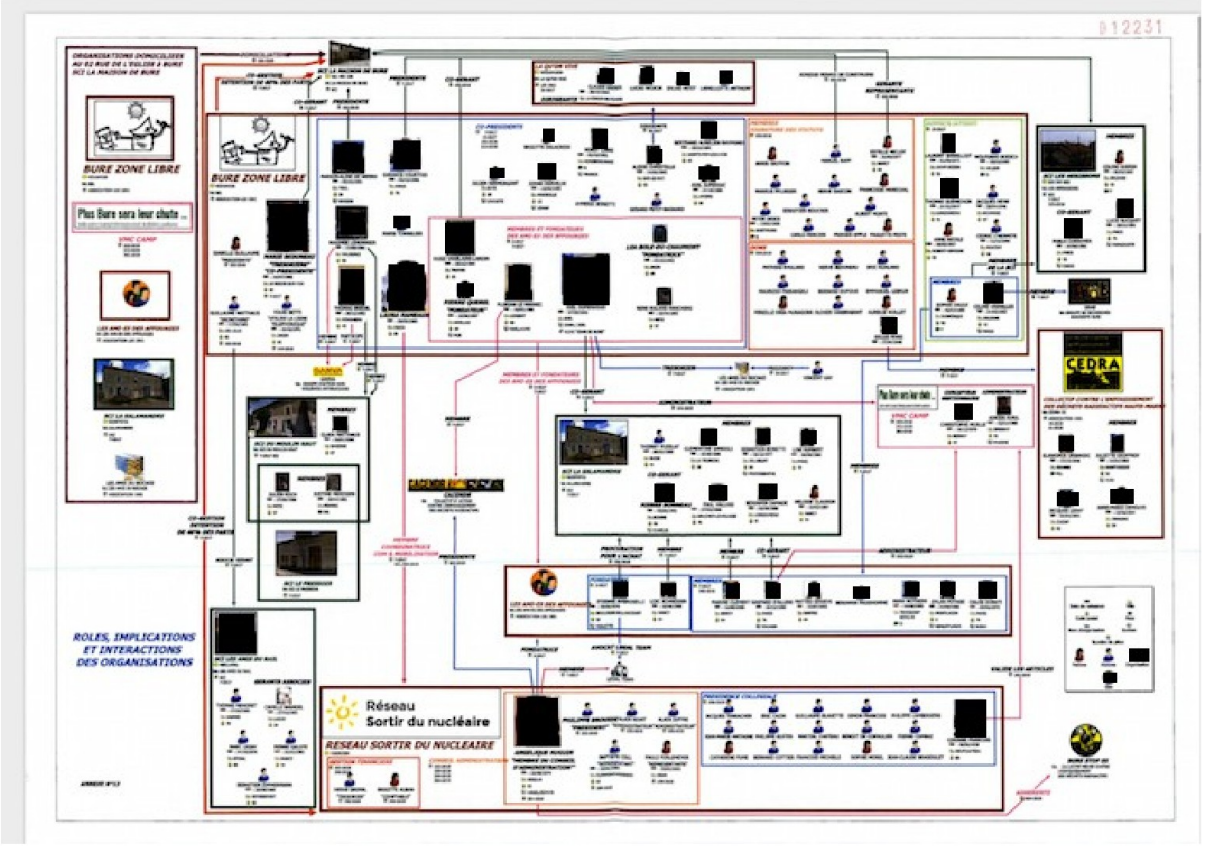
Les impacts d’être fiché·e

- Emploi
- Reconnaissance faciale
- Problème aux douanes
- La police est moins aimable avec vous
- Méprise médiatique (Serge D. Ste Soline, Raphaël Arnault)
- 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

…

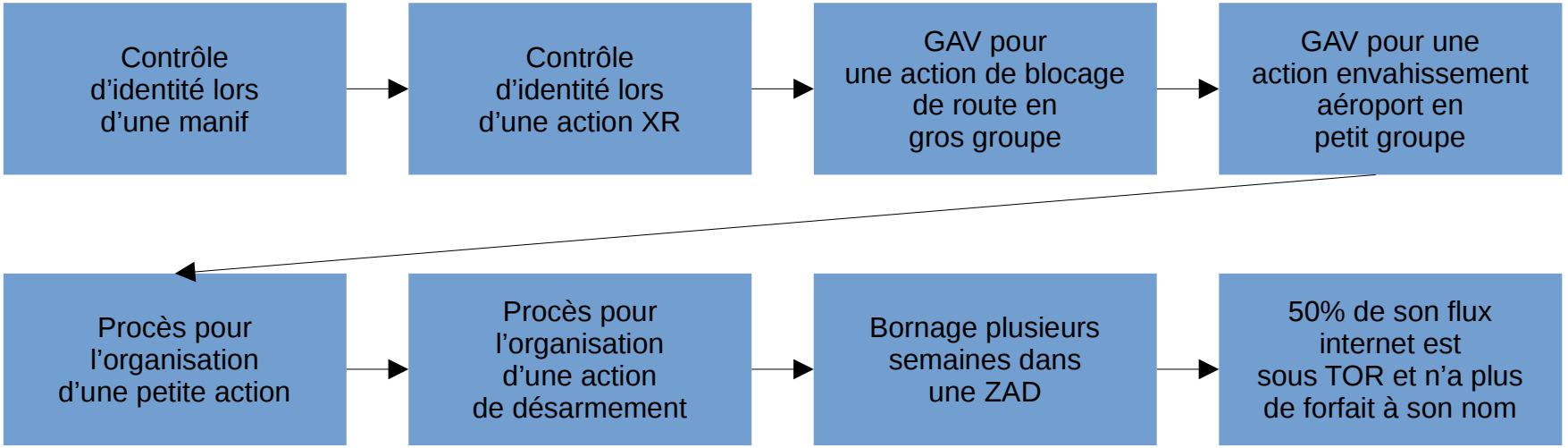


Logiciels d’analyses de données : Mercure, Analyst’s notebook,…



Le parcours de la radicalisation

Exemple :



PROGRAMME DE LA JOURNÉE

MATIN

Signal, 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 perquizs

I – LES OUTILS NUMÉRIQUES DE CHAT

SOMMAIRE - Matin

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

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.

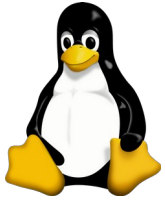
La définition du libre défendue par Richard STALLMAN dès 1980 est constituée de 4 libertés :

- Liberté d'exécuter le programme
- **Liberté d'étudier le fonctionnement du programme**
- Liberté de redistribuer des copies
- Liberté d'améliorer le programme et de publier les améliorations

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 « femer l'application »
        Fermer l'application
```

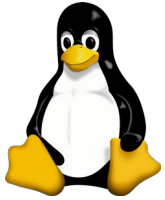
Différence entre open-source, libre et propriétaire








Différence entre open-source, libre et propriétaire



Linux

Firefox

TOR

Framasoft

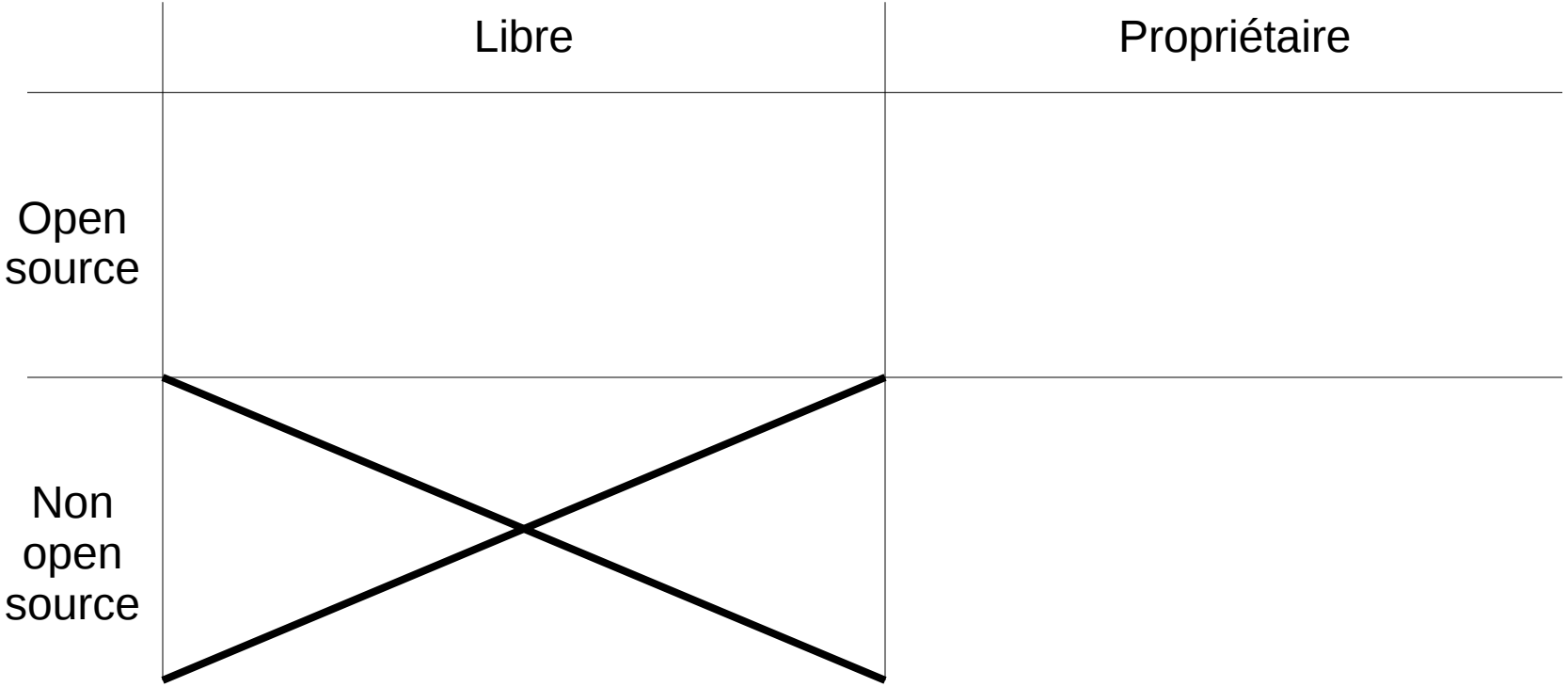
Cryptpad

Jitsi

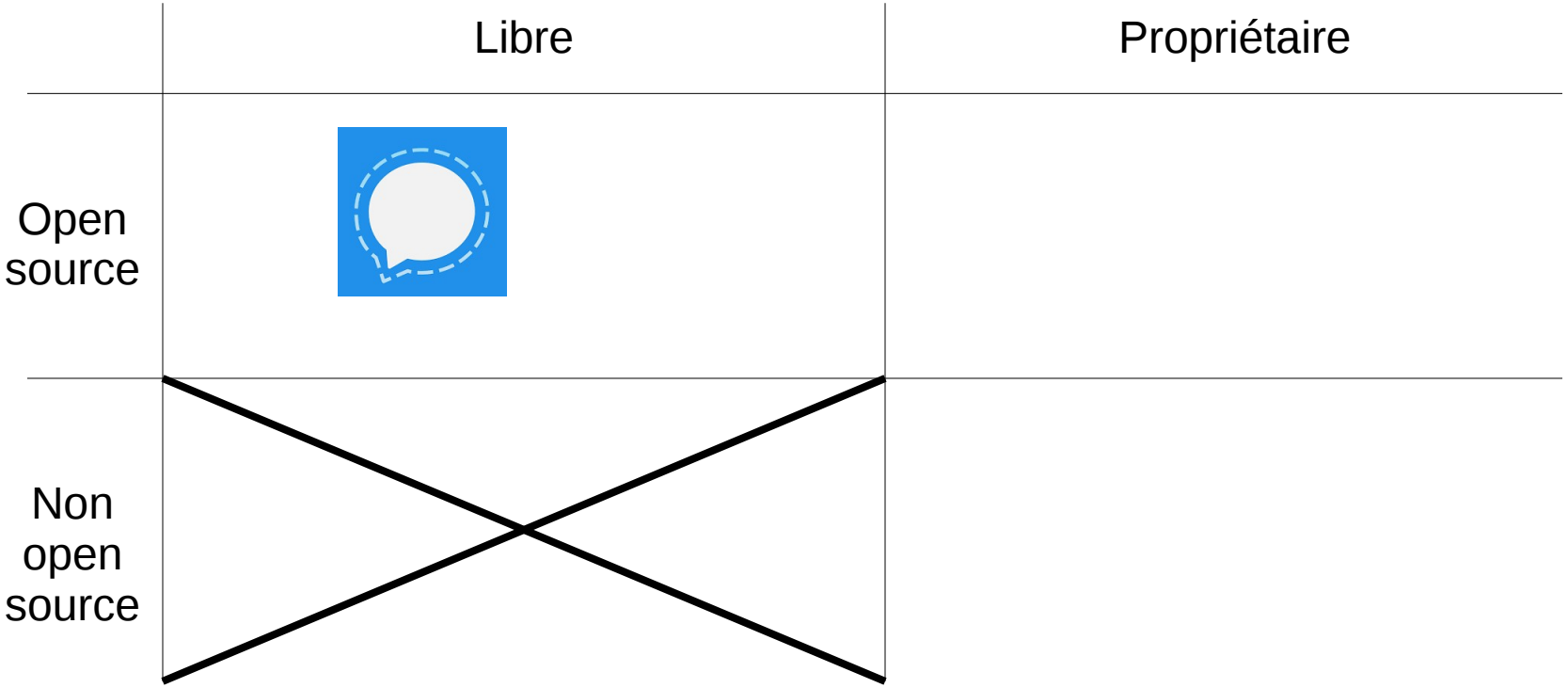
TousAnt
iCovid

ProtonMail

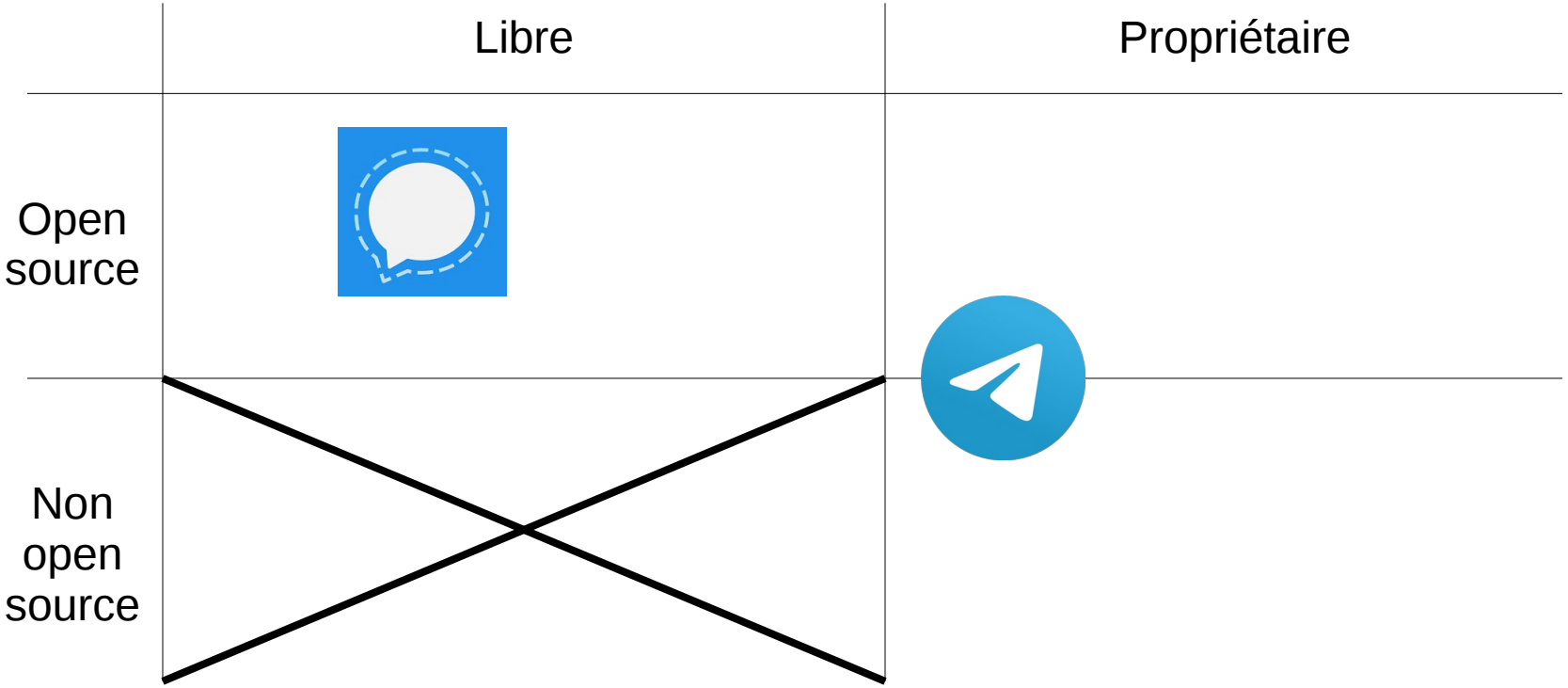
Différence entre open-source, libre et propriétaire



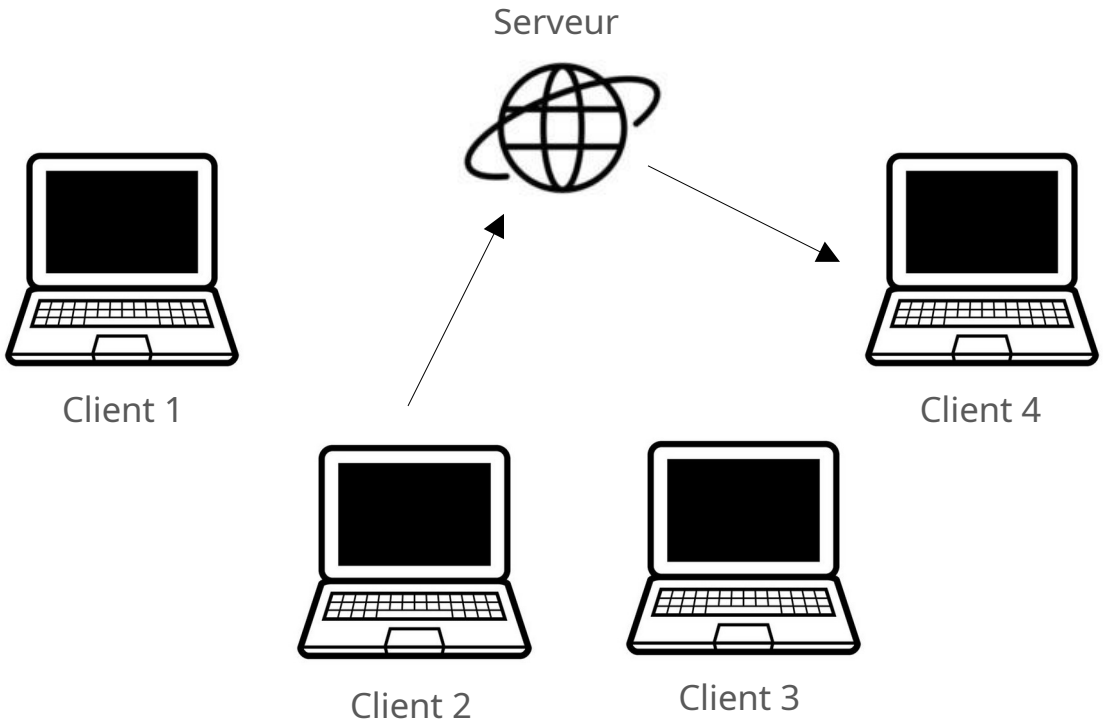
Différence entre open-source, libre et propriétaire



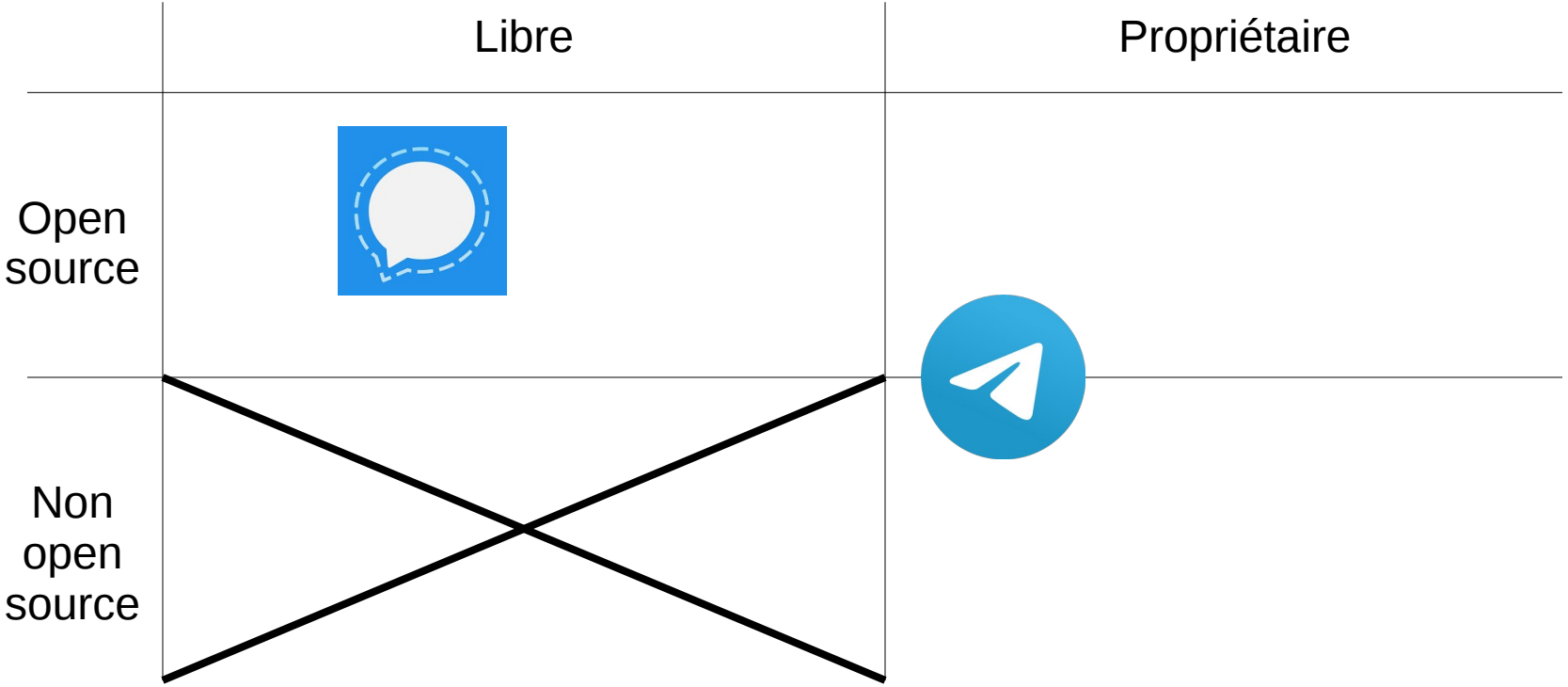
Différence entre open-source, libre et propriétaire



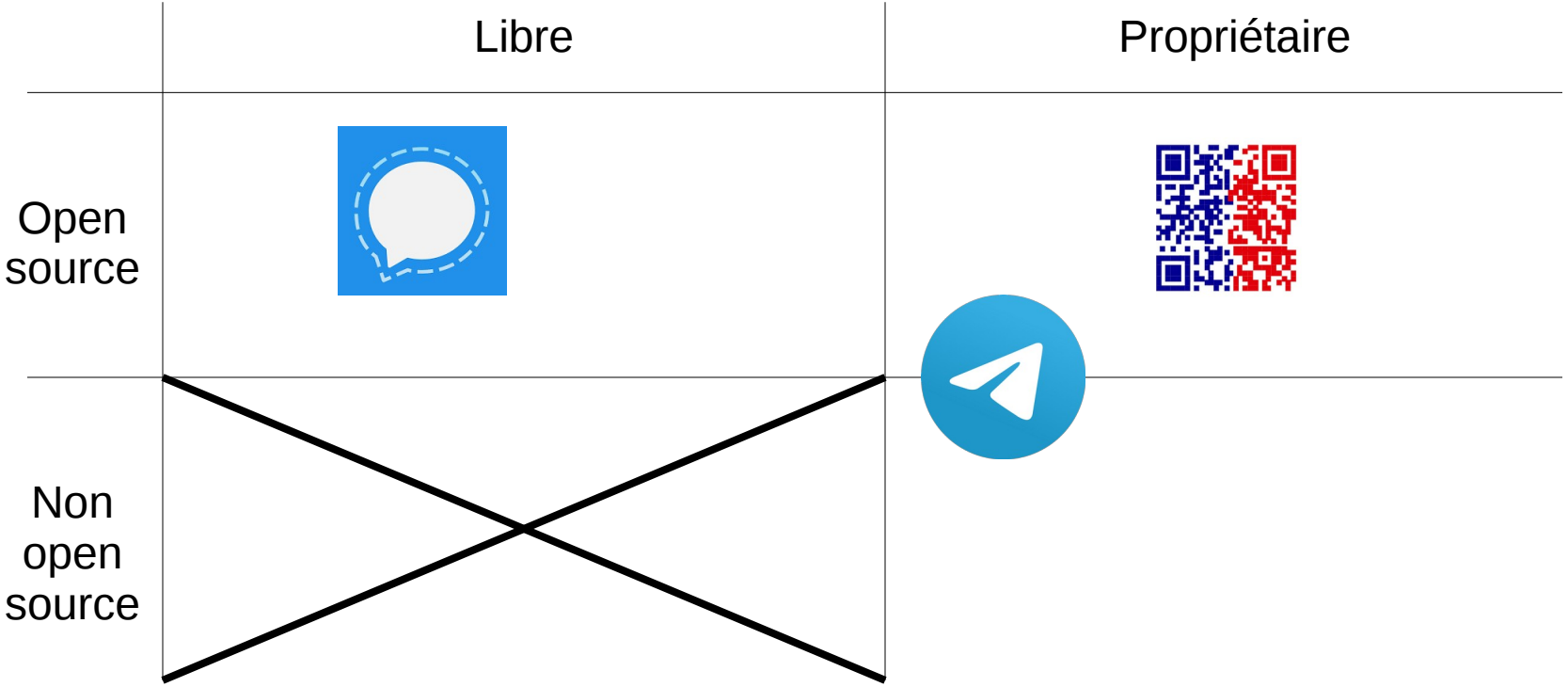
Serveur et client



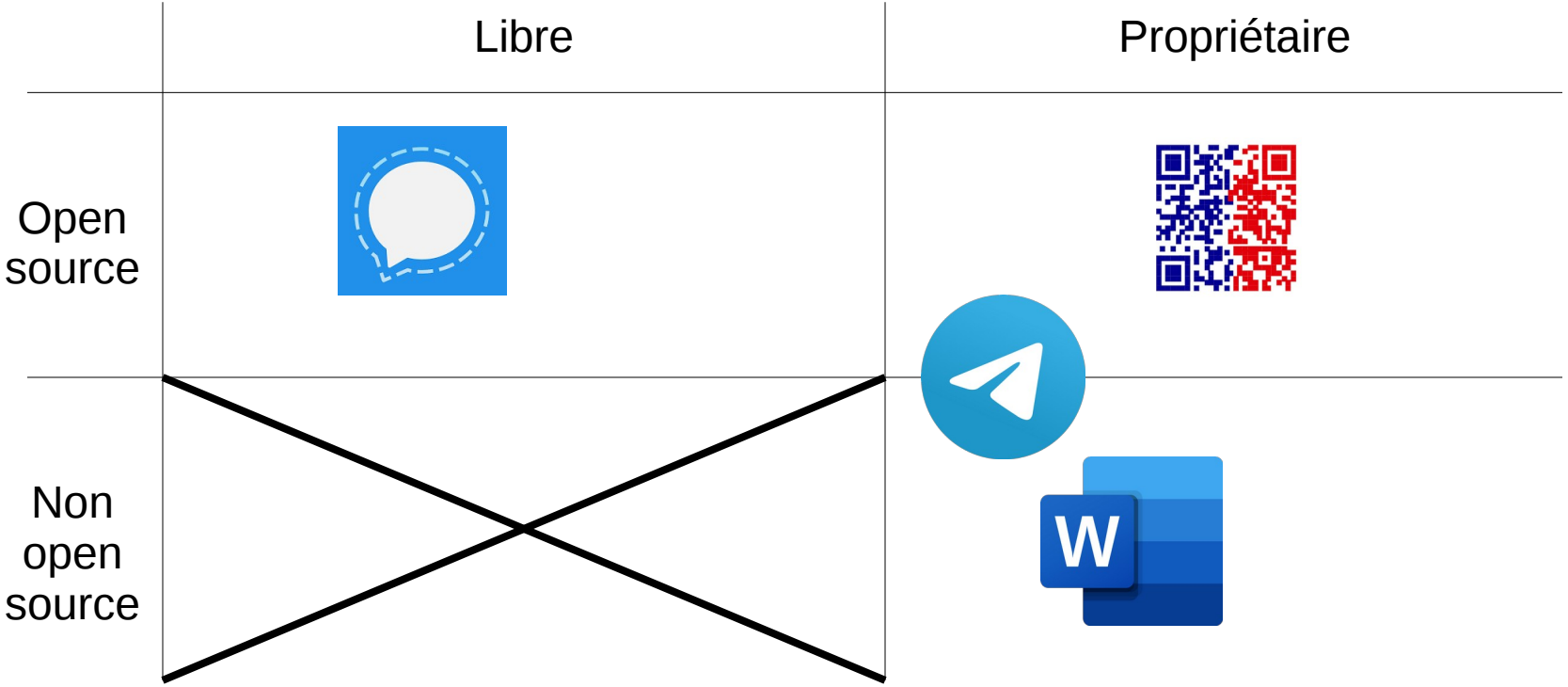
Différence entre open-source, libre et propriétaire



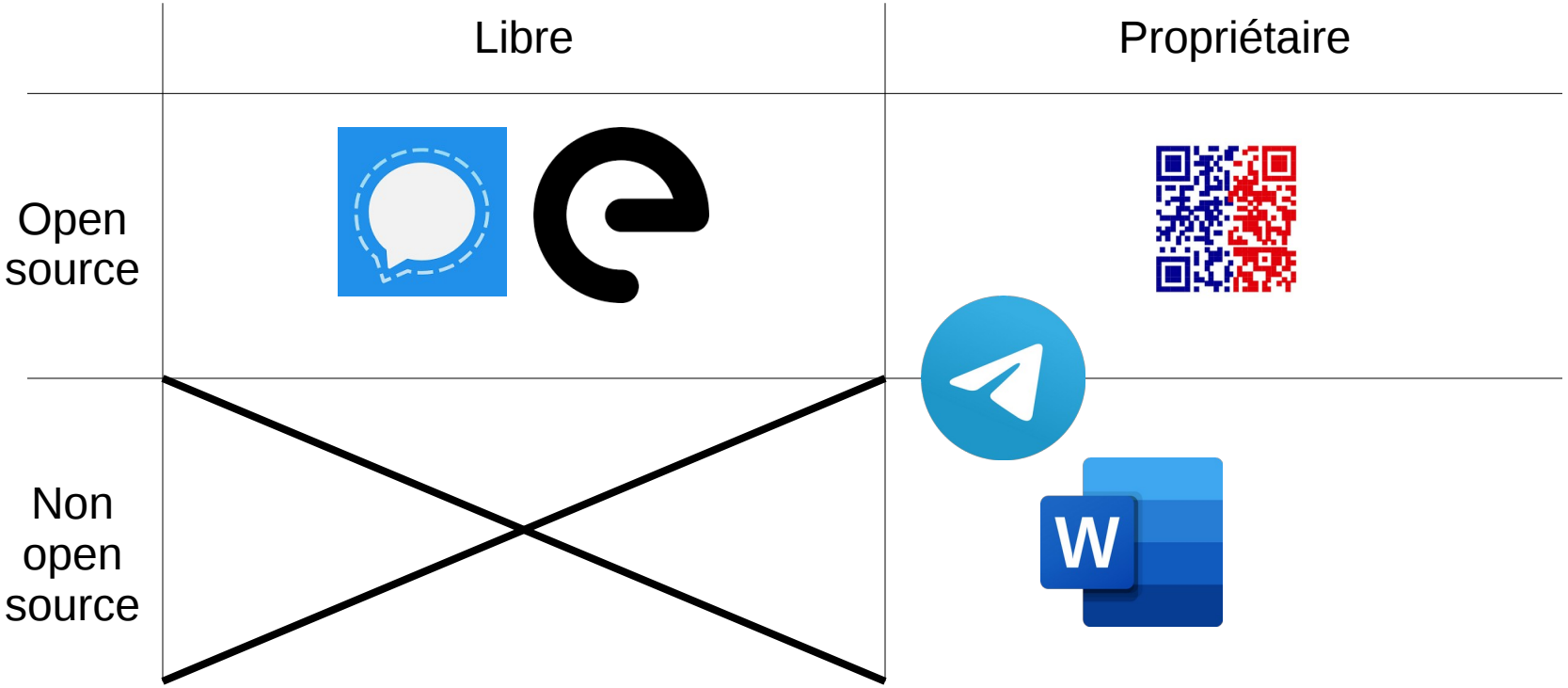
Différence entre open-source, libre et propriétaire



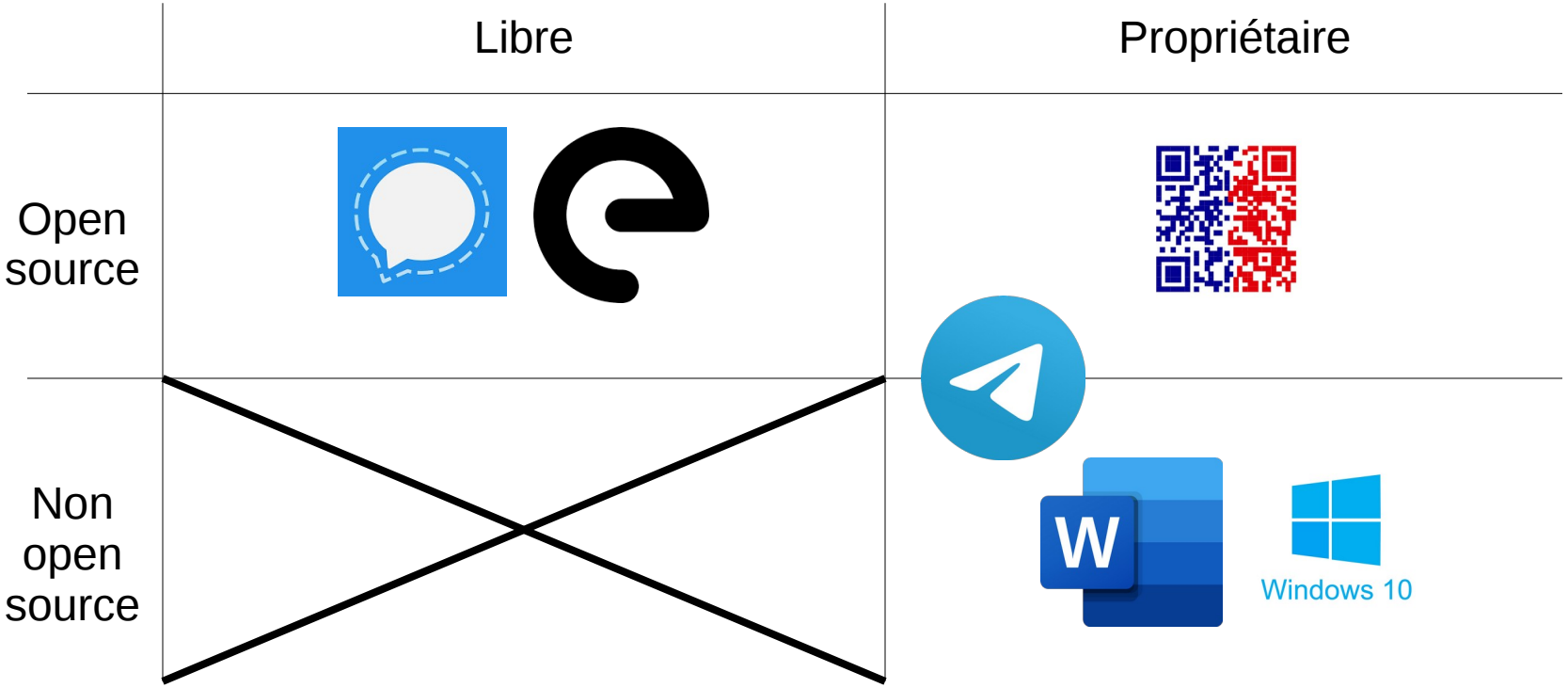
Différence entre open-source, libre et propriétaire



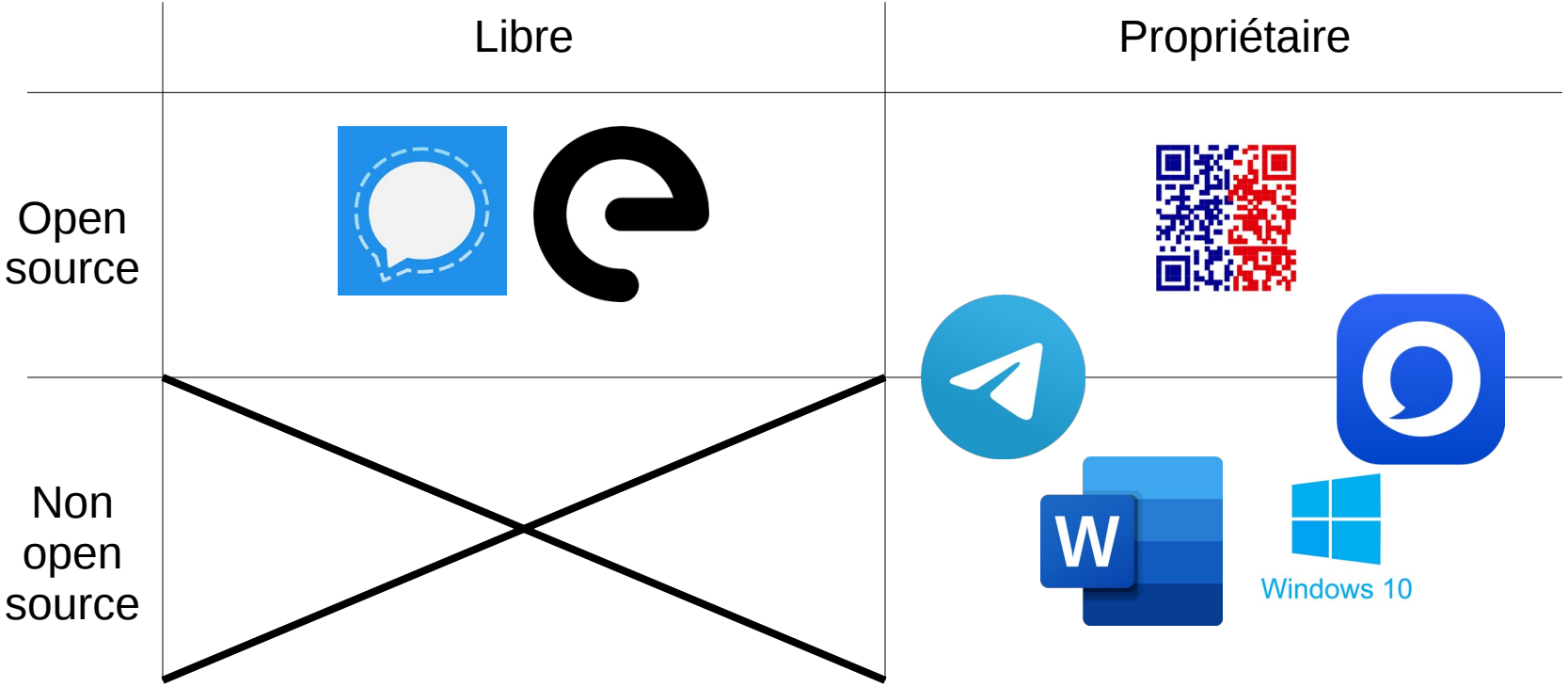
Différence entre open-source, libre et propriétaire



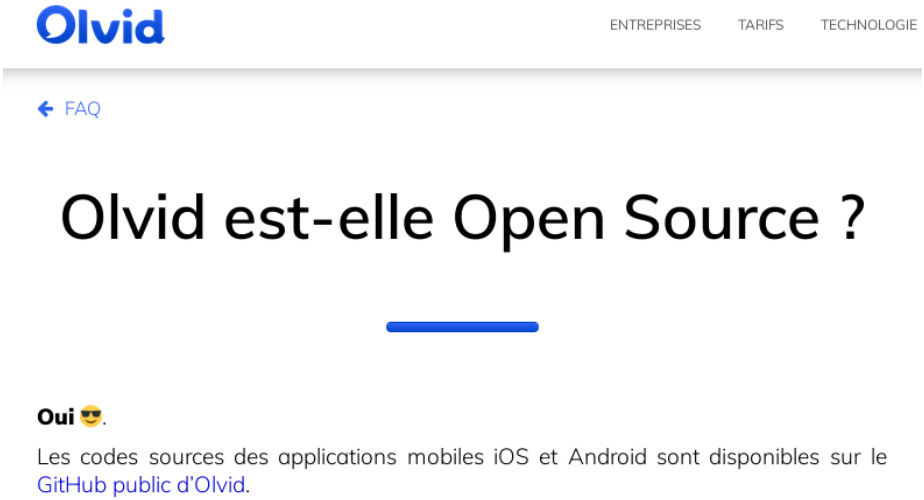
Différence entre open-source, libre et propriétaire



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 :

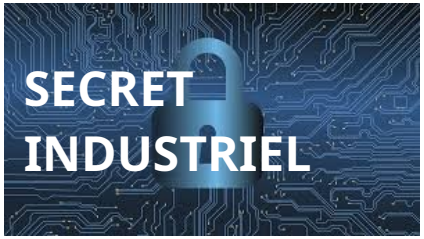
Sera-t'il open source un jour ?

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

Libre et propriétaire

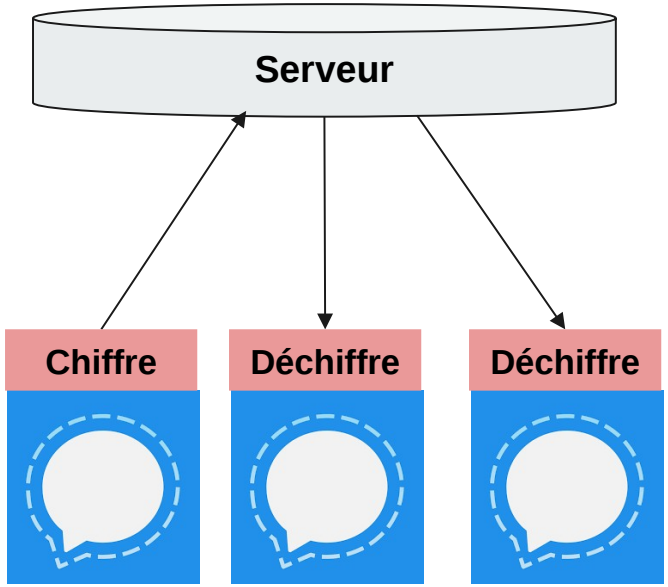
	Open-source ?	Débogage	Financement
	Open-source		Développée par Signal Messenger LLC et financée par la Signal Foundation, une organisation à but non lucratif
	Open-source / Propriétaire		Publicité et Pavel Dourov (créateur de VKontakte le facebook russe)

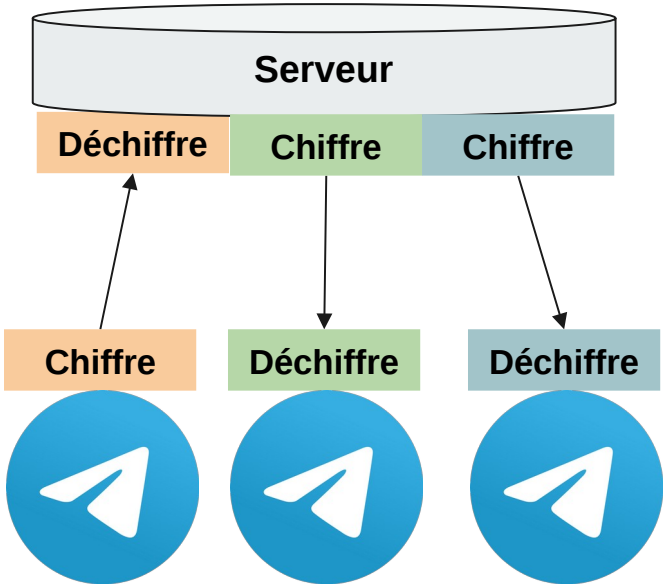
Chiffrement de l’information

Bonjour, je m’appelle Bernardettes

Cpokpvs, kf n’bqqfmmf Cfsobsefuuft

Chiffrement de l’information





Fonctionnalités

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

Fonctionnalités

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

Ne pas mettre son vrai pseudo

Bloquer inscription via NIP si numéro « éphémère »

« Toujours relayer les appels »

Mettre les messages temporaires par défaut

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

Inclusivité technologique

Inclusivité technologique

Militante sans smartphone

Militant pas très à l’aise avec l’utilisation d’un téléphone

Militante sans grosse volonté de se sécuriser

Militant avec peu de temps a consacrer à la lutte et donc peu à la sécurisation

Militant sans téléphone

…

L’inclusivité c’est une démarche, l’inclusivité absolue n’est pas atteignable

Inclusivité technologique

Vivre ensemble

Travailler internationalement

Compartimenter les informations

Avoir des groupes de travail qui ont besoin d’un téléphone et d’autres non

II – BONNES PRATIQUES

SOMMAIRE - Matin

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

Mise sur écoute classique

Problème :
La police peut vous mettre sur écoute dans le cadre d’une enquête

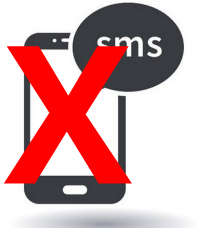
Elle peut écouter vos échanges téléphoniques non chiffrés, vos SMS et vos méta-données internet (quels sites vous consultez mais pas ce que vous y faites dessus, et quelles applications vous utilisez)

 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)

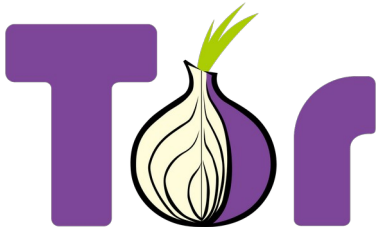
Mise sur écoute classique

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

!!! TRES RARE !!!

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, sans action de sa part

« Aucun appareil connecté à internet n'est sécurisé », a encore mis en garde le directeur exécutif de SMEX (une ONG libanaise de défense des droits humains dans les espaces numériques). « Nous ne pouvons pas faire grand-chose contre Pegasus. »

Le monde du libre

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

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

NSO GROUP

Prevenir le concepteur	**Faire de l'argent en exploitant cette faille (faire un exploit)**	**Revendre la faille à une entreprise ou a quelqu'un qui fait de l'exploitation de faille**
Rémunération sous forme de bug bounty (peut se compter en millions d'euro) + éthique	Possibilité de faire beaucoup d'argent illégalement	NSO = entreprise israellienne qui fournit un logiciel permettant a des entités éthatiques de suveiller leur population

!!! TRES RARE !!!

Piratage de votre appareil

Solutions :

Mises à jour régulières de vos appareils et applications

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

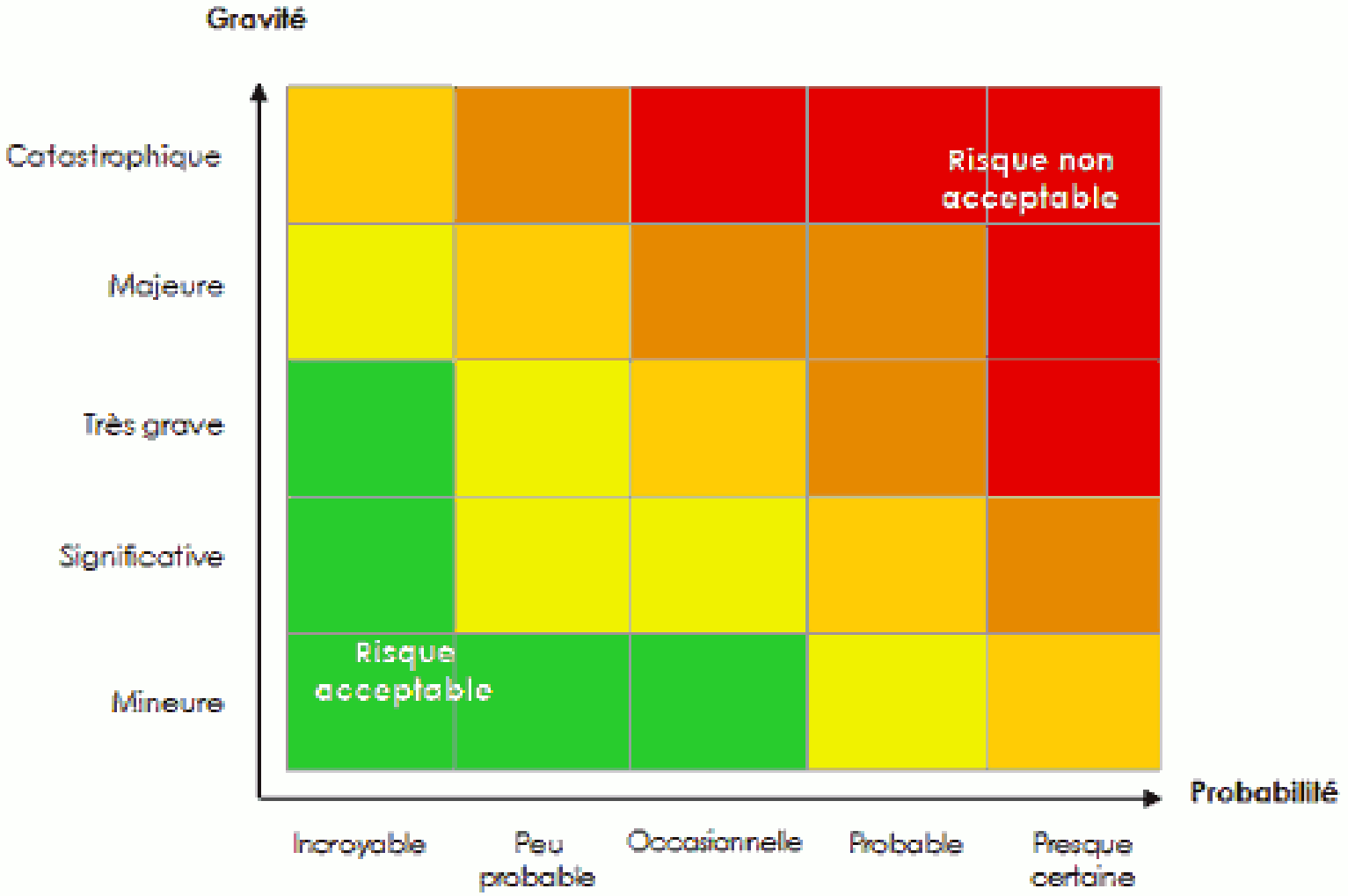
+ vos applications ont des droits sur votre téléphone + vous avez de failles de sécurité

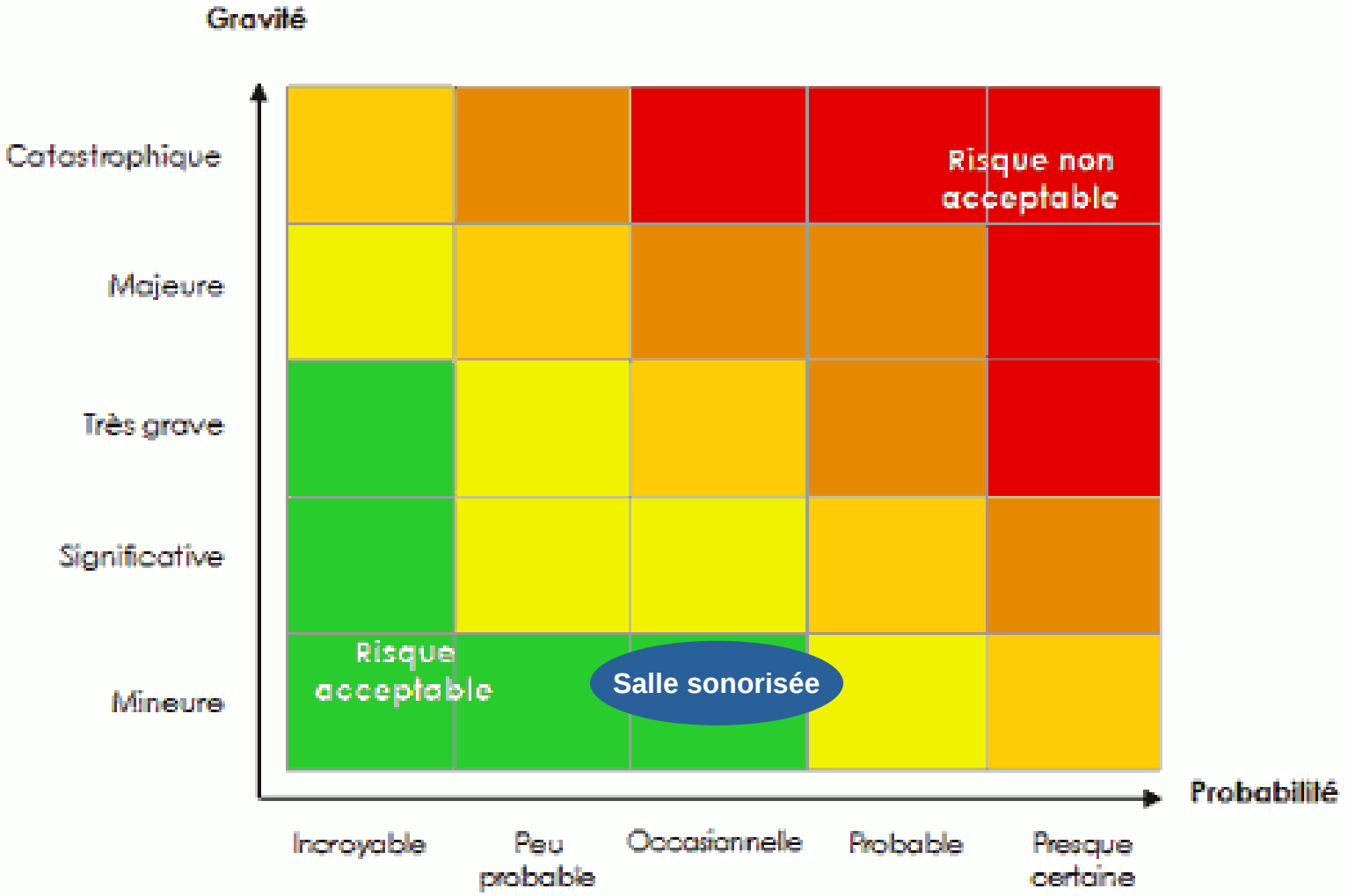
Déconnecter physiquement le micro (très difficile)

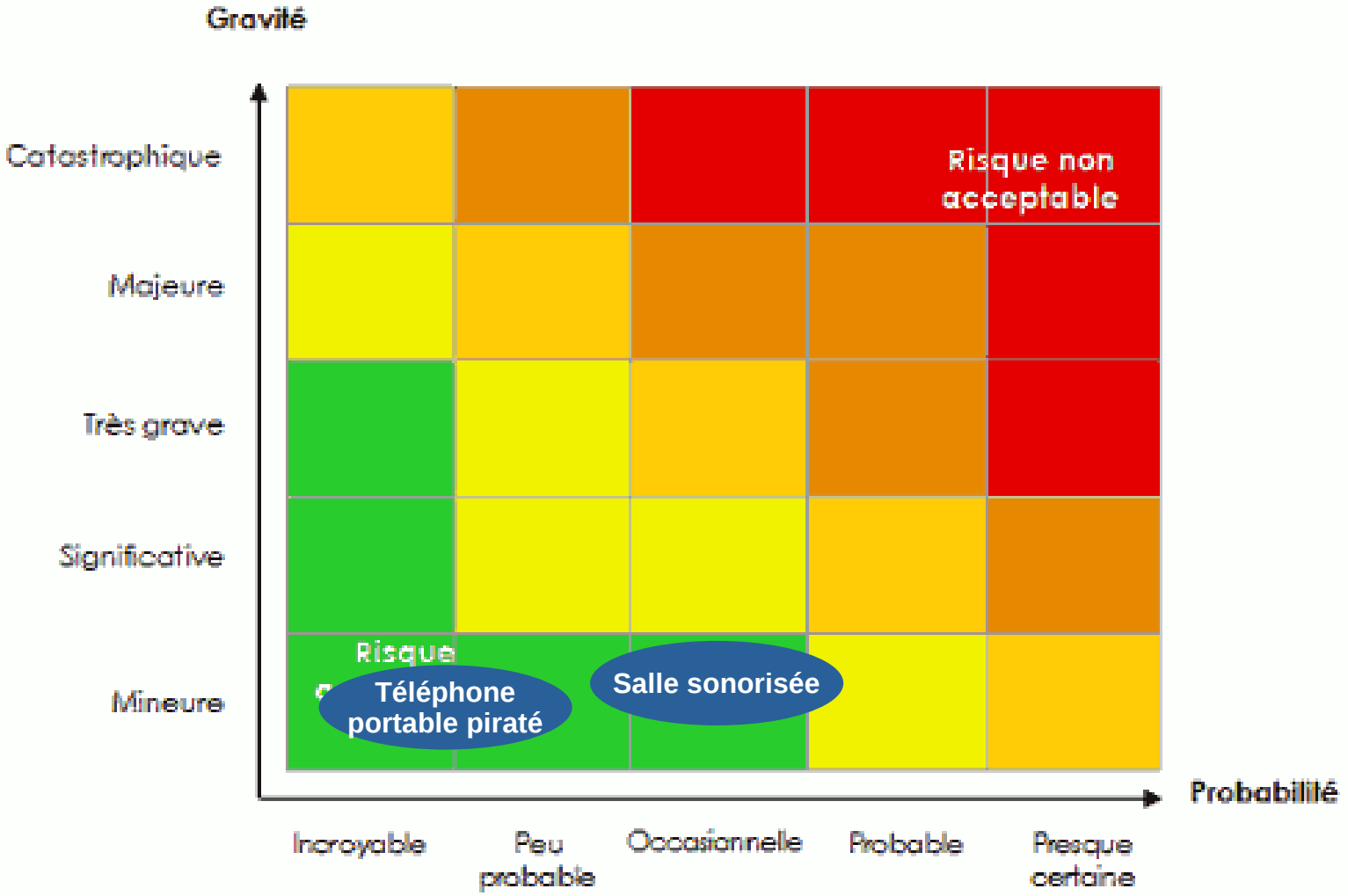
Mettre un cache sur la webcam

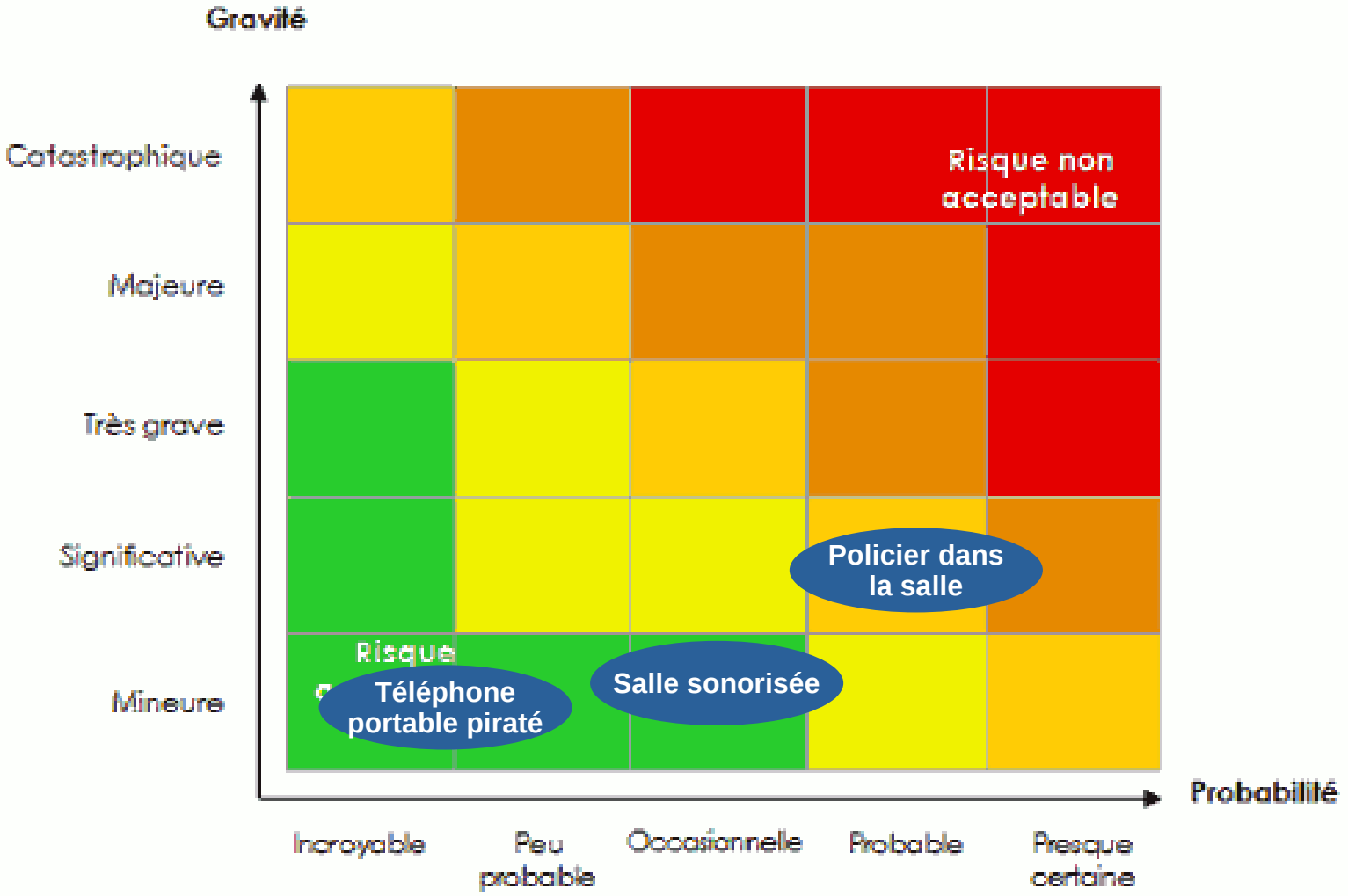
Ne pas avoir son portable avec soit lorsque l’on parle de choses incriminantes

Très cher pour la police mais très difficilement évitable


Gravité
Catastrophique
Majeure
Très grave
Significative
Mineure
Risque non acceptable
Risque acceptable
Probabilité
Incroyable
Peu probable
Occasionnelle
Probable
Presque certaine


Gravité
Catastrophique
Majeure
Très grave
Significative
Mineure
Risque non acceptable
Risque acceptable
Salle sonorisée
Probabilité
Incroyable
Peu probable
Occasionnelle
Probable
Presque certaine


Gravité
Catastrophique
Majeure
Très grave
Significative
Mineure
Risque non acceptable
Risque
Téléphone portable piraté
Salle sonorisée
Probabilité
Incroyable
Peu probable
Occasionnelle
Probable
Presque certaine


Gravité
Catastrophique
Majeure
Très grave
Significative
Mineure
Risque non acceptable
Policier dans la salle
Salle sonorisée
Téléphone portable piraté
Incroyable
Peu probable
Occasionnelle
Probable
Presque certaine
Probabilité

B . Bornage

SOMMAIRE - Matin

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

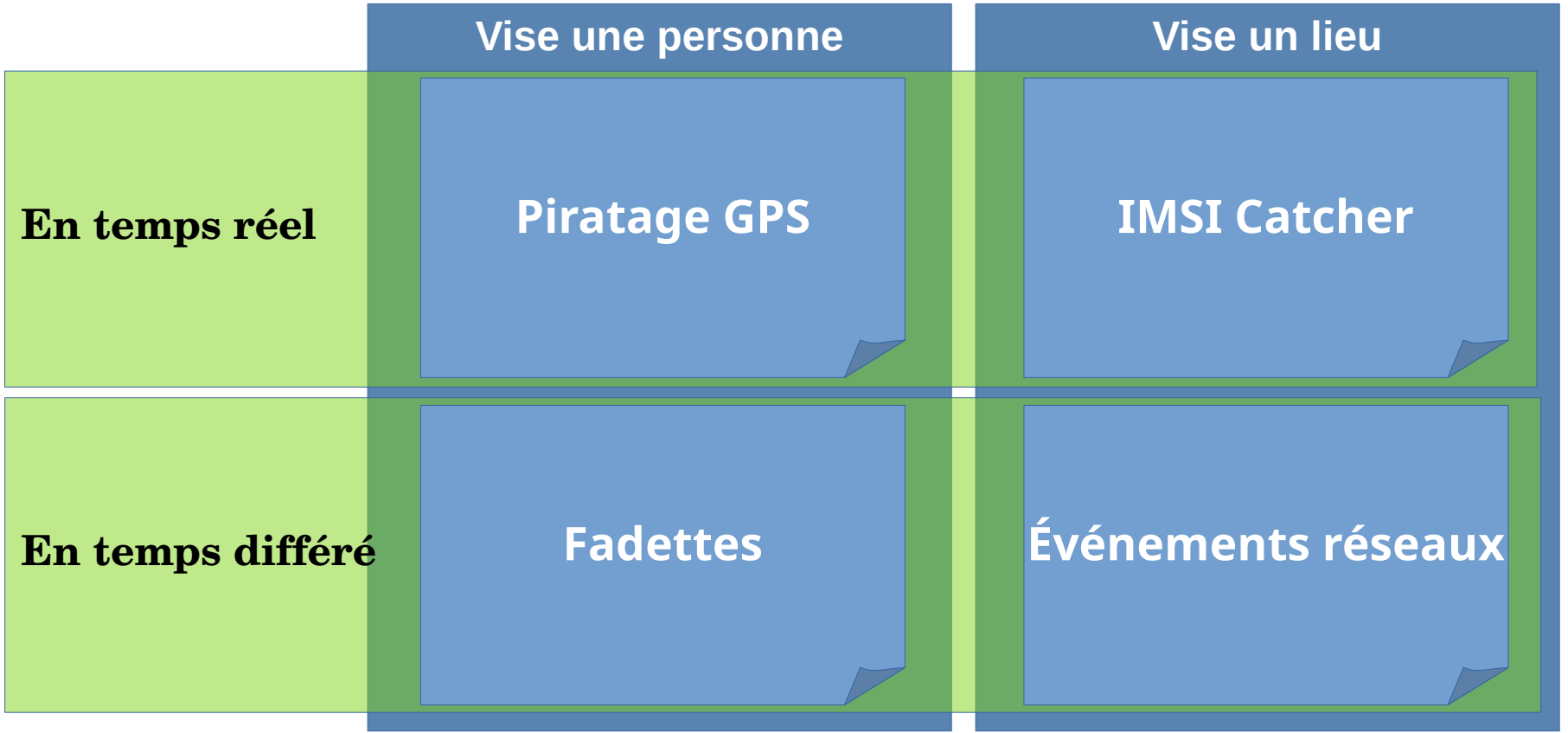
Reconnaissance faciale

Carte de transport

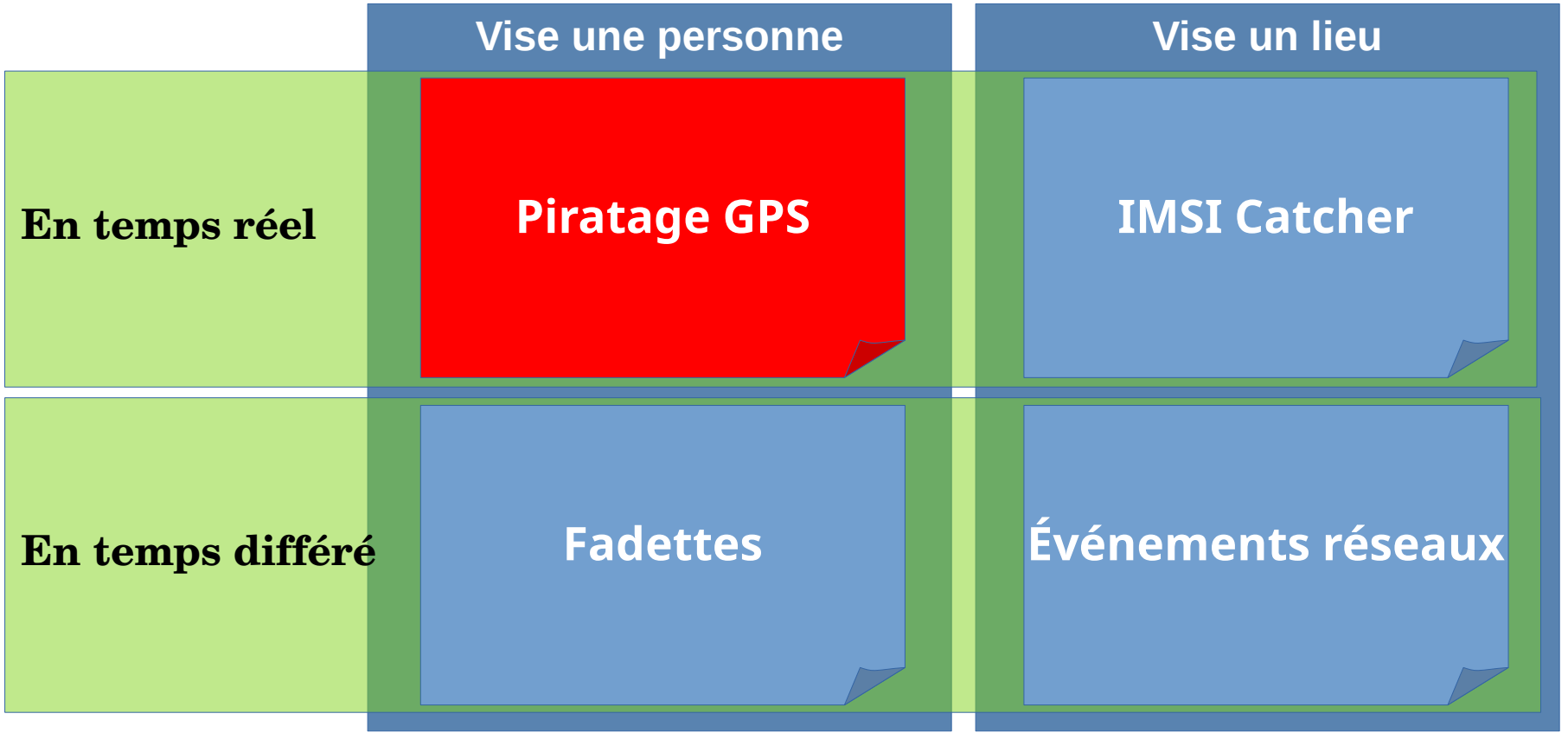
Problématique

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 ?



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



Bornage : piratage GPS

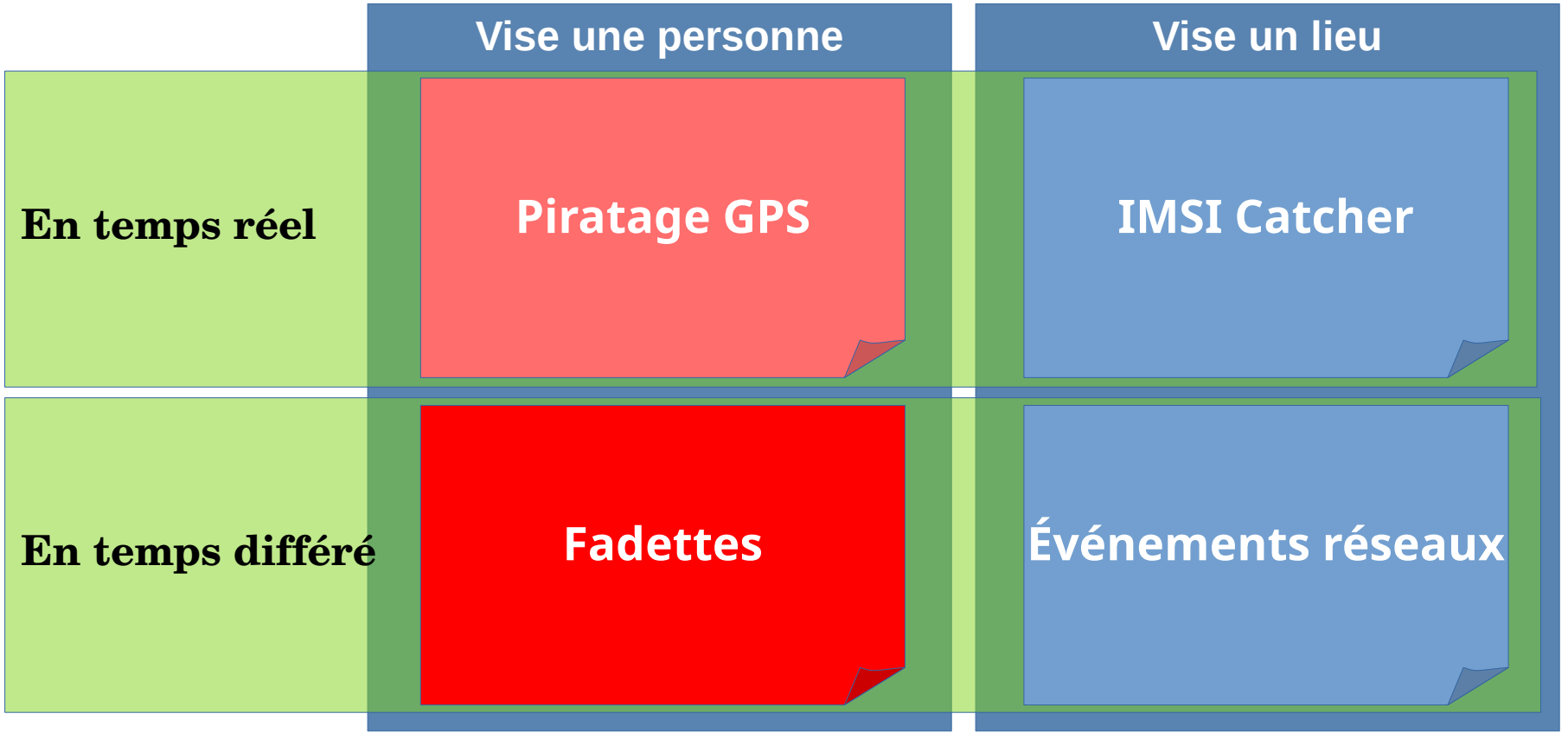
On pirate votre portable pour utiliser sa fonction GPS (Loi d’orientation de la justice 2023)

Comme précédemment, cela 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 ?



Bornage : fadettes

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

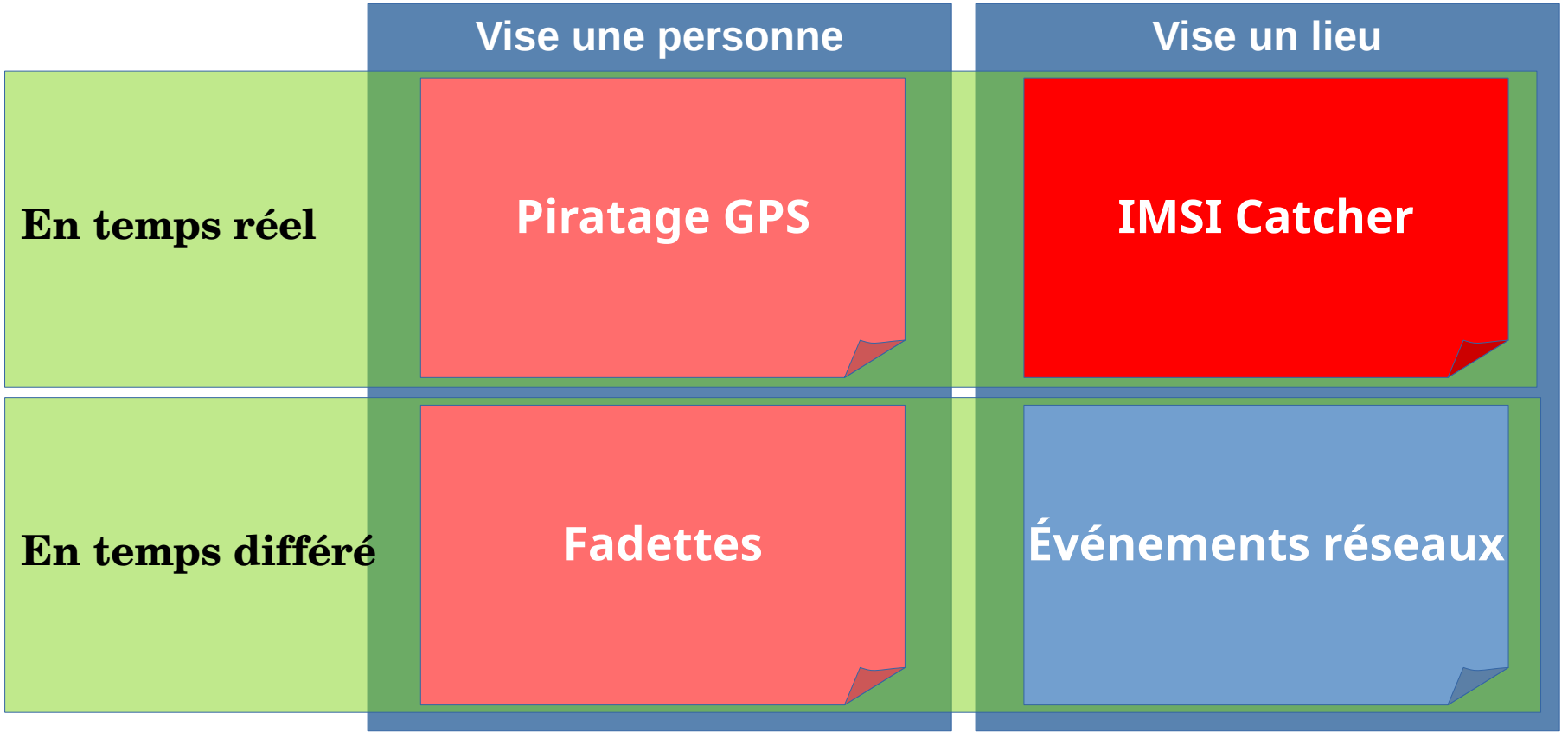
La précision varie : de 1 patté de maisons en ville à plusieurs kilomètres à la campagne

Obligation des opérateurs de garder ces données pendant 1 an

Permet de savoir où vous étiez et parfois qui vous êtes

Première chose regardée par la police en cas d’enquête → garder ses habitudes

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



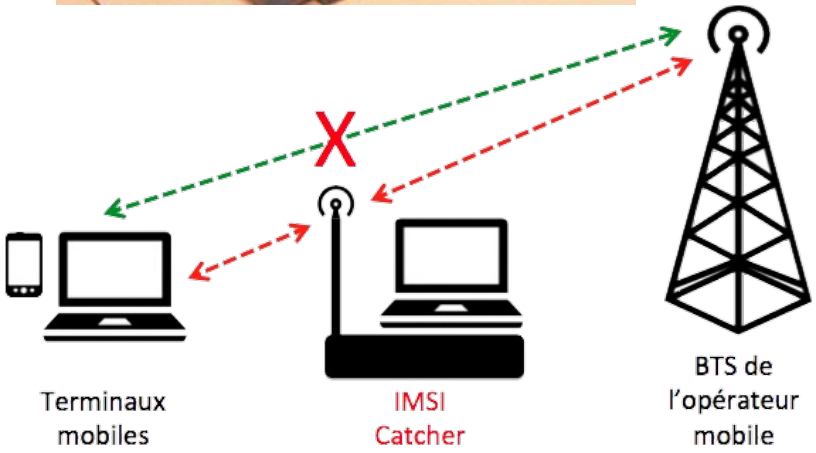
Bornage : IMSI Catcher

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

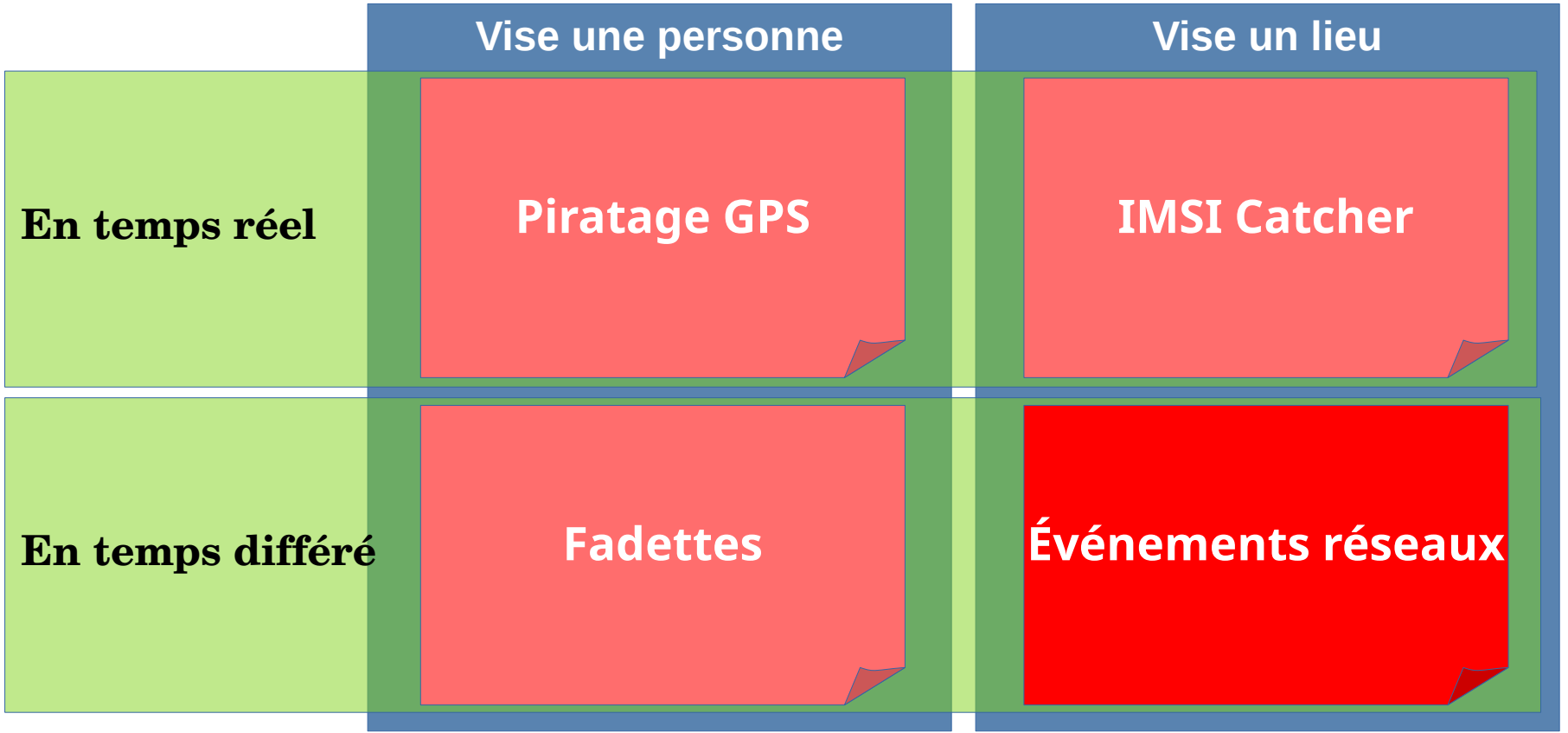
Très précis

Déployer en amont

Exemple de moment où il y a des IMSI catcher :
- Sainte Soline
- Jour d'affrontement en ZAD
- Pour decouvrir le deuxième portable d'une militante



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



Bornage : événements réseaux

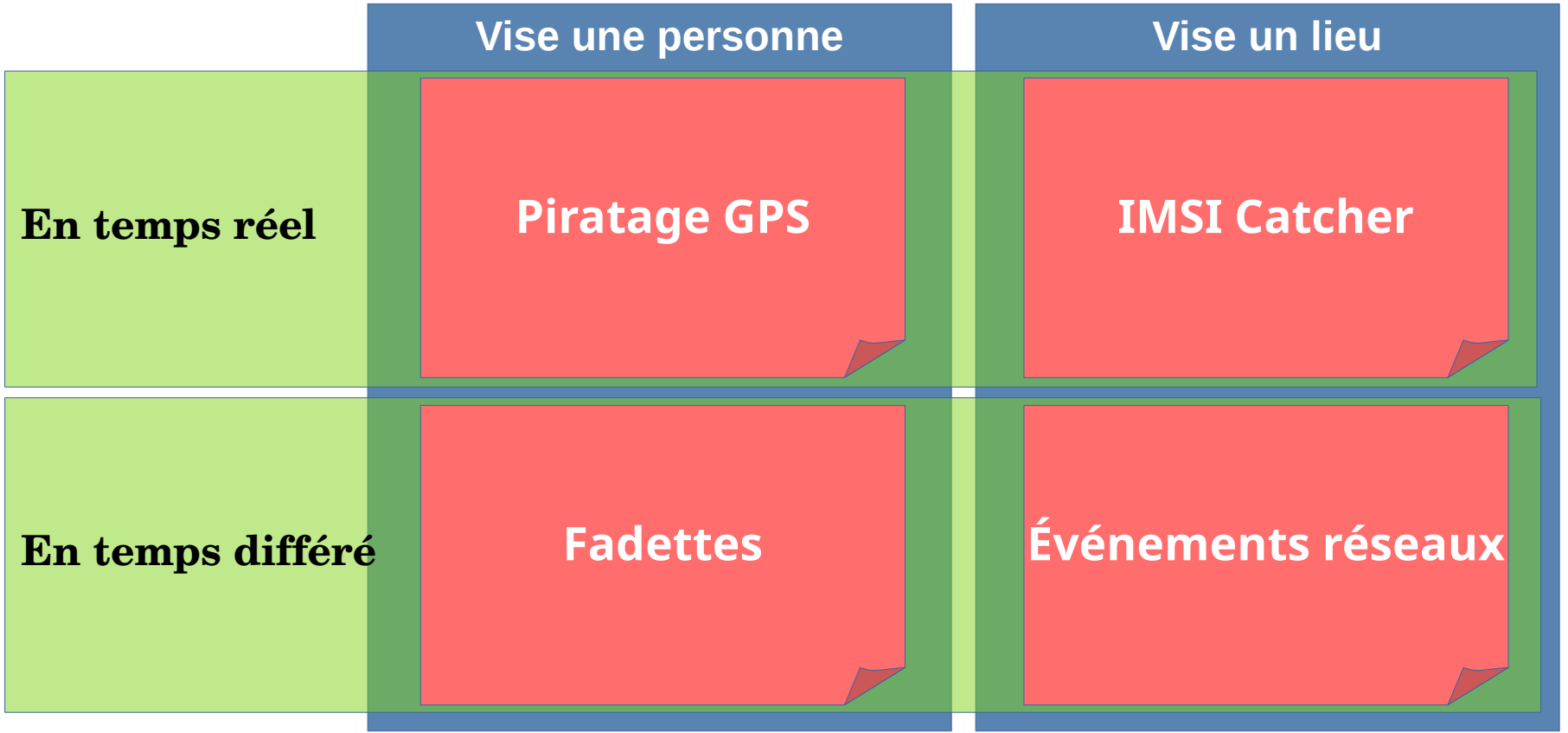
On demande à une antenne quels téléphones portables sont passés dans le coin et ce qu’ils y ont fait

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

Contrairement à l’IMSI catcher, est utilisé a posteriori

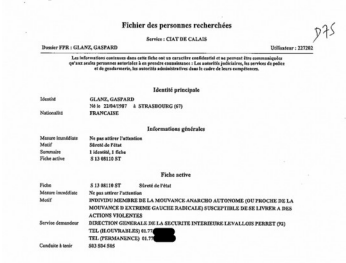
Grace à la triangulation : précis à quelques mètres près

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



Exemple : affaire Bouc Bel air, LaFarge

Après des contrôles d'identité, des GAV, des infos de RT, la police récolte plein d'infos sur José



Fichier des personnes recherchées

Service : CIAT DE CALAIS

Dossier FPR : GLANZ, GASPARD — Utilisateur : 237202

Identité principale

Identité — GLANZ, GASPARD

Né le 21/04/1987 à STRASBOURG (67)

Nationalité — FRANCAISE

Informations générales

Mesure immédiate — Ne pas attirer l'attention

Motif — Sûreté de l'Etat

Fiche active — S 13 08110 ST

Fiche active

Fiche — S 13 08110 ST — Sûreté de l'Etat

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)

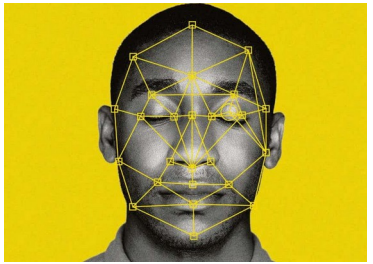
TEL (BUREAU/CELL) : 01.71.[redacted]

TEL (PERMANENCE) : 01.71.[redacted]

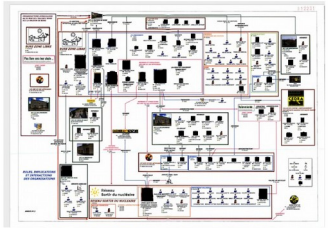
Conduite à tenir — 803 854 986

José participe à l'action sans qu'il n'y ait le moindre contrôle de police

La police identifie un des militants grâce aux caméras (TAJ) ou aux événements réseaux



Elle utilise les infos qu'elle a déjà pour identifier de potentiels complices dont José



Elle réquisitionne auprès des opérateurs téléphoniques, les fadettes de José

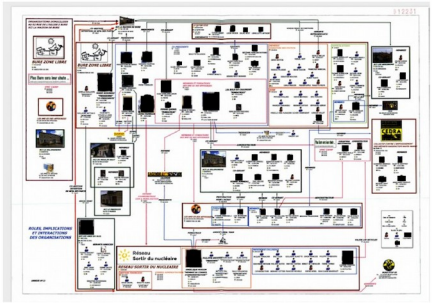
Fadettes

Elle se rend compte que José avait son portable allumé toute l'année sauf ce week-end précis

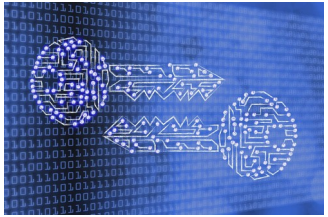
Exemple : affaire Bouc Bel air, LaFarge

Avec les fadettes de José et de trois autres suspects, la police identifie le lieu du briefing

Des militants qui avait fait attention aux fadettes pour l'action mais pas pour le briefing sont alors identifiés



Une perquisition chez les suspects permet d'avoir accès a des conversations signal, permettant d'identifier d'autres militants et d'inculper tout le monde



Bornage : quel est le résultat de mettre tous 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 en mode avion + wifi : le mettre en mode avion bien avant d’arriver sur place

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 éphémères, toujours relayer les appels

Liste de tâches à faire

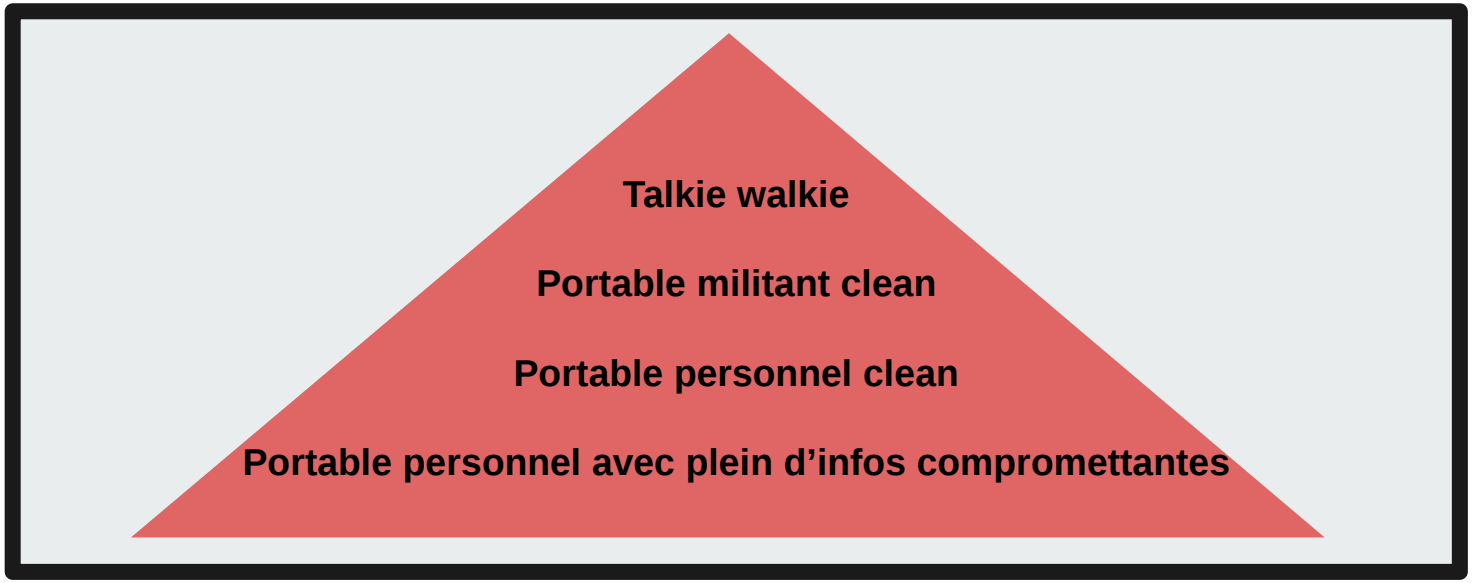
- [ ] Ajouter un VPN à son téléphone et son ordinateur
- [ ] Supprimer des conversations pour virer l’historique d’appel
- [ ] Avoir les bons réglages sur Signal
- [ ] Mettre un cache sur tes webcams

Des questions ?

I – AVOIR SON TEL EN ACTION

A . Avoir 2 téléphones / SIM

Un portable ou pas de portable en action ?



Les identifiants d’un smatphone

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 grâce 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 gardant les fadettes pendant 1 an, vous ne pouvez pas utiliser un ancien portable personnel comme portable activiste

Burner phone ou Bigo

Téléphone pas cher utilisé temporairement

Avantage :
- Pas cher
- Rapide à mettre en place
- Inconnu pour sûr des services de police

Inconvénients :
- Échanges non sécurisés donc facilement écoutables 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 sûr de ne pas être écouté puis de s’en séparer

Achat portable et carte SIM

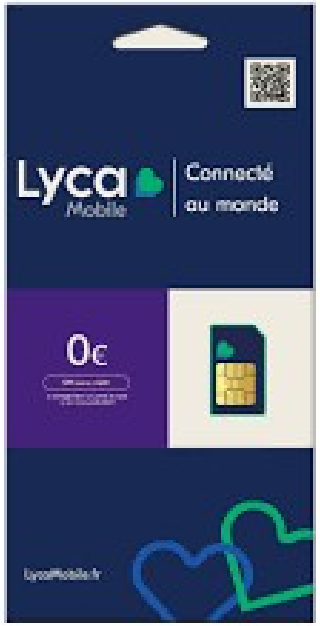
Le portable :

- 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
- Opérateurs 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 une foule »

Ne pas perdre son portable sinon on perd son compte Signal

Potentiellement, ne pas allumer son portable chez soi

B . Perquisitions

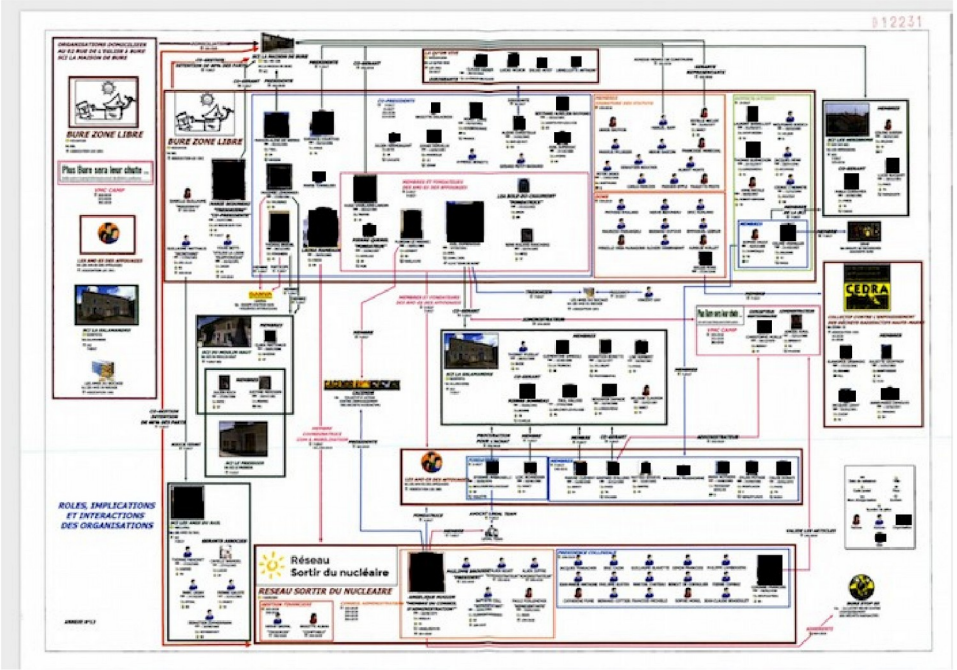
Quand est ce que ça se produit ?

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…



Expert forensic

L’analyse scientifique de cas, appelée par calque de l'anglais science forensique ou la forensique, regroupe l'ensemble des méthodes d'analyse fondées sur les sciences (chimie, physique, biologie, neurosciences, informatique, mathématique, imagerie, statistique) afin de servir au travail d'investigation de manière large.

Suppression de données

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'entièreté 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)

Appareil chiffré ?

Non

Oui

Éteint ?

Non

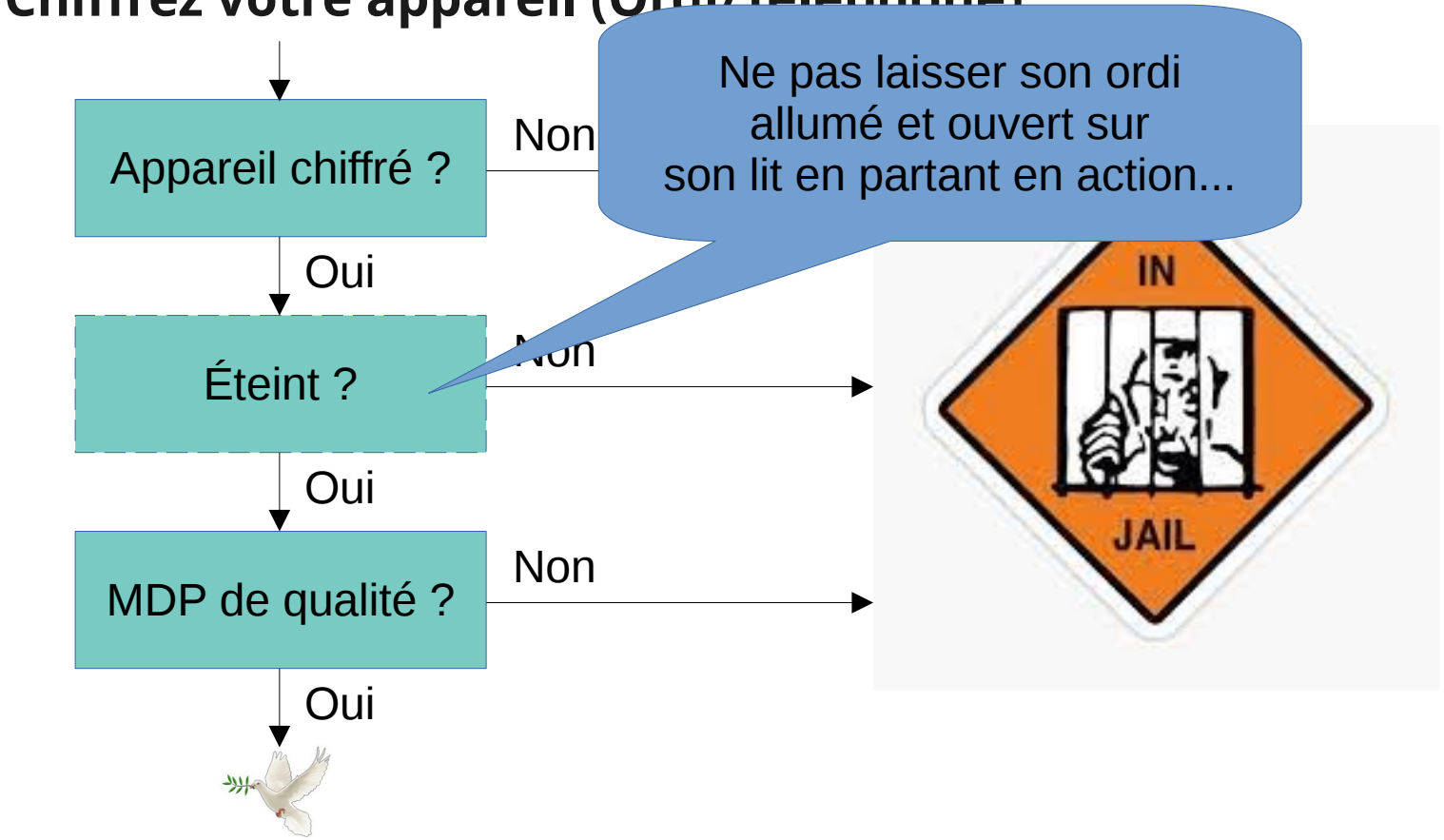
Oui

MDP de qualité ?

Non

Oui

Chiffrez votre appareil (Ordi/Téléphone)



Chiffrez votre appareil (Ordi/Téléphone)

Appareil chiffré ? — Non → 

Oui ↓

Éteint ? — Non →

Oui ↓

MDP de qualité ? — Non →

Oui ↓

Chiffrez son ordiphone

Virer le déverrouillage par empreinte digital et reconnaissance faciale

Niveau de chiffrement dépendant de votre modèle de menace

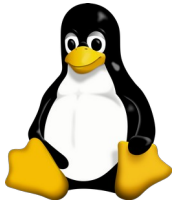
Modèle de menace bas :
Mettre un mot de passe basique avec 4 chiffres

Modèle de menace élevé :
Mettre un mot de passe avec 16 chiffres

Possibilité de mettre un temps d’inactivité nécessaire (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 mediactiviste possède très souvent un ordiphone avec des photos prisent 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

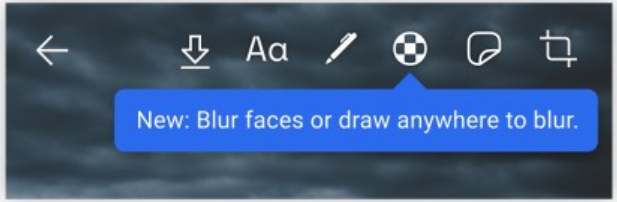
Scénario :
Ils ont réussis à déchiffrer votre téléphone portable

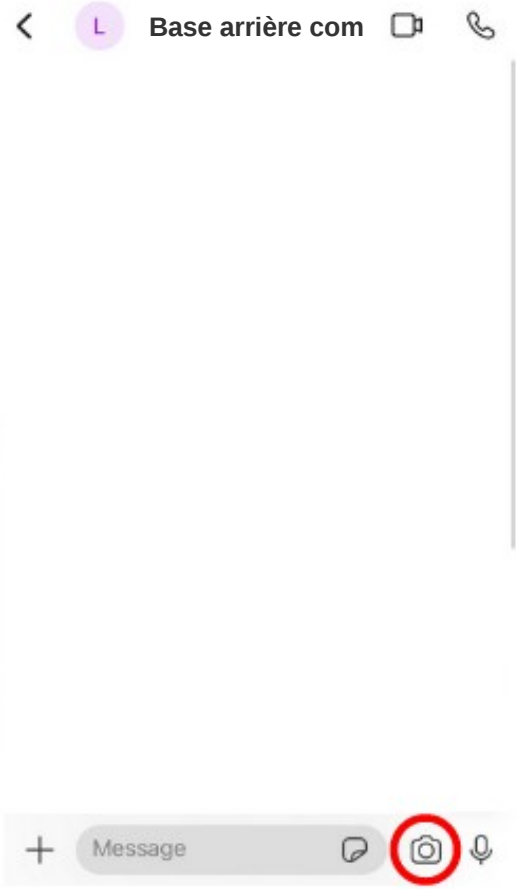
Solution

Ne rien stocker sur son téléphone

Scénario mediactiviste

Signal avec message éphémère à 1h maximum





Signal

C . BAC

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 l’ordinateur via le logiciel

Ou reçus par la suite pour les photos plus qualitatives

Ne pas laisser de trace sur l'ordinateur

Tails

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

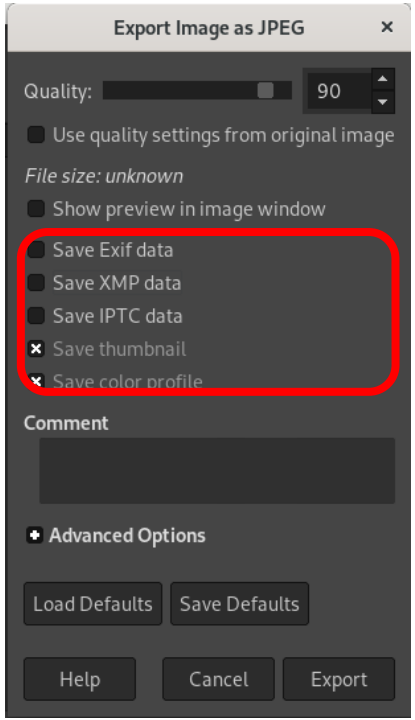
Supprimer les métas-données

Les métas-données

Qu’est ce que c’est ?

Les métas-données

GIMP



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

D . Mots de passe

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

La sûreté d’un mot de passe - gestionnaire de mdp

https://haveibeenpwned.com/

Centralisation de tous les mots de passe

Différent type de gestionnaire de mot de passe :

- Fichier chiffré en local
- Application chiffrée 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

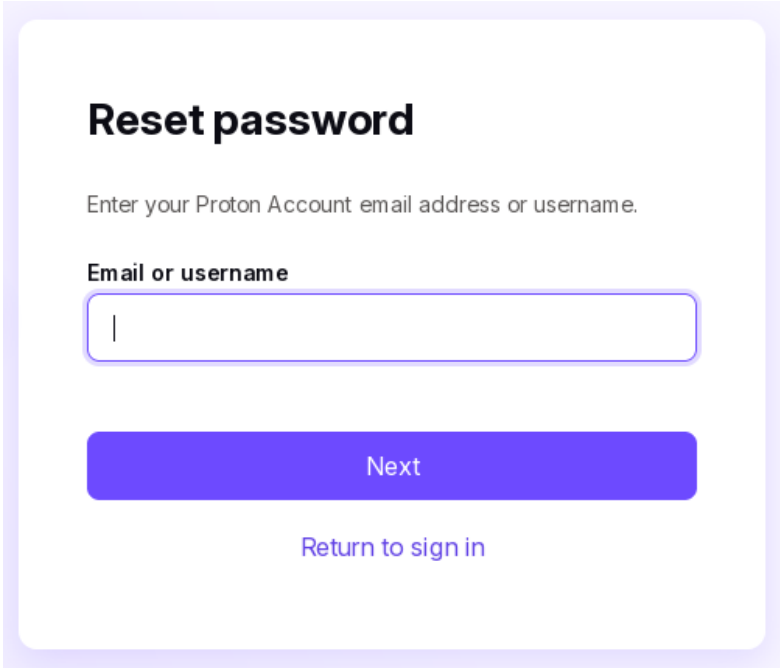
Les backups

Concerne les authentifications mais aussi les données parfois (Mattermost envoies 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



II – NAVIGATION WEB

Naviguer incognito avec son ordi

Pourquoi un ordi ?

Pourquoi naviguer incognito ?

L’IP

Numéro d’identification unique attribué à votre box internet

La police cherche à identifier 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

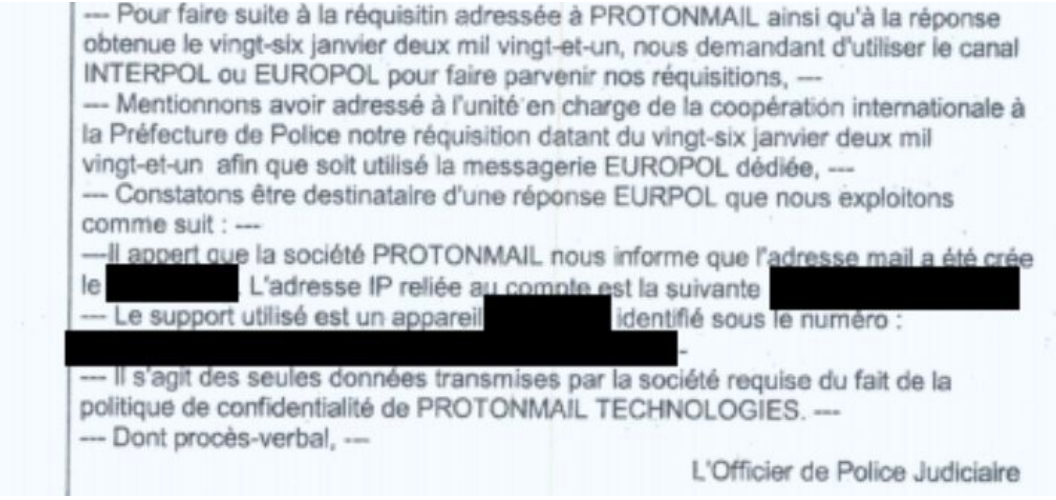
Utilisable dans des procédures pour trouver les utilisateurs de : formulaire, boite mail, compte facebook, propriétaire d’un blog…

Reporterre
Le média de l'écologie

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

Un militant identifié par son adresse e-mail de récupération Proton

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. 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 crée 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 :

2023 Nombre d'ordonnances légales : 6 378 Ordonnances contestées : 407 Ordonnances respectées : 5 971 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

Protonmail : militant ?

Entreprise → se soumet à la loi

Privilégiez les acteurs associatifs militants de confiance aux entreprises « militantes »

Proton Mail et Wire : collabos comme les autres

Publié le 2 juin 2024 | Maj le 16 juin
Analyses > Dispositifs de contrôle
Brochure — Surveillance

Ou pourquoi on doit arrêter d'utiliser les services de Proton pour les trucs répréhensibles et préférer des alternatives anarchistes et autogestionnaires.

Proton Mail peut être un choix cohérent si l'on souhaite simplement **éviter la surveillance de masse** des GAFAM — bien que Proton AG reste une entreprise capitaliste — mais **en aucun cas lorsque l'on souhaite réduire les risques liés à la repression** d'État.

Un outil sécurisé est sécurisé seulement si on l'utilise de la bonne façon et pour les bonnes raisons

Apprenez à utilisez des outils sécurisés, ne pensez pas être en sécurité seulement parce que votre outil est « sécurisé »

Telegram : militant ?

Laure Beccuau, procureure de Paris : « Ce qui a fait nous intéresser à la plateforme Telegram, ça a été le fait que cette plateforme, lorsqu'elle était saisie pour un certain nombre de réquisitions, il n'y avait pas de retours à ses réquisitions. Elle ne réagissait pas. »

Pavel Durov a été arrêté le 24 août 2024, à sa descente d'avion au Bourget

« Nous avons clarifié le fait que les adresses IP et les numéros de téléphone portables de ceux qui violent nos règles pourront être communiqués aux autorités en réponse aux requêtes judiciaires valides » Pavel Durov

En 2024, Telegram a collaborer 893 fois avec la police française, à propos de 2072 utilisateurices, fournissant leur adresse IP et leur numéro de téléphone
Nombre de requêtes françaises répondu par Telegram

Janvier → Avril : 4

Avril → Juillet : 6

Juillet → Octobre : 210

Octobre → Décembre : 673

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 agirons 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.

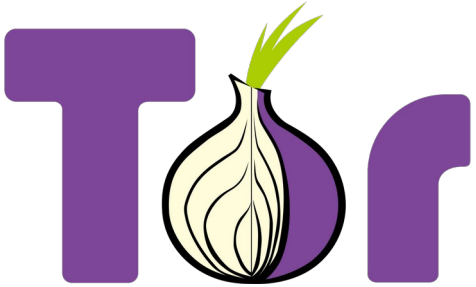
En cas de requête manifestement illégitime, nous refuserons de répondre, en argumentant l'illégitimité de la requête.

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

Autistici

La police dit ne pas envoyer de réquisitions à Riseup par peur qu'iels 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 [5]. (Il va sans dire que l'utilisation de clés de chiffrement PGP pour les échanges de mails ajoute une couche de protection supplémentaire).

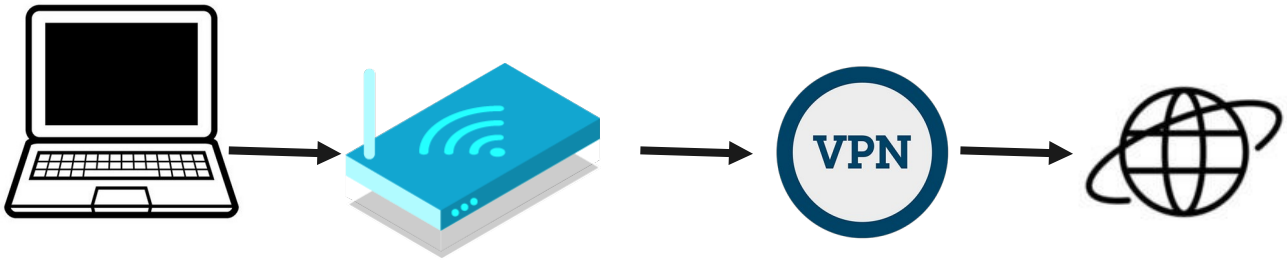
Naviguer incognito avec son ordi



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 peux l'identifier

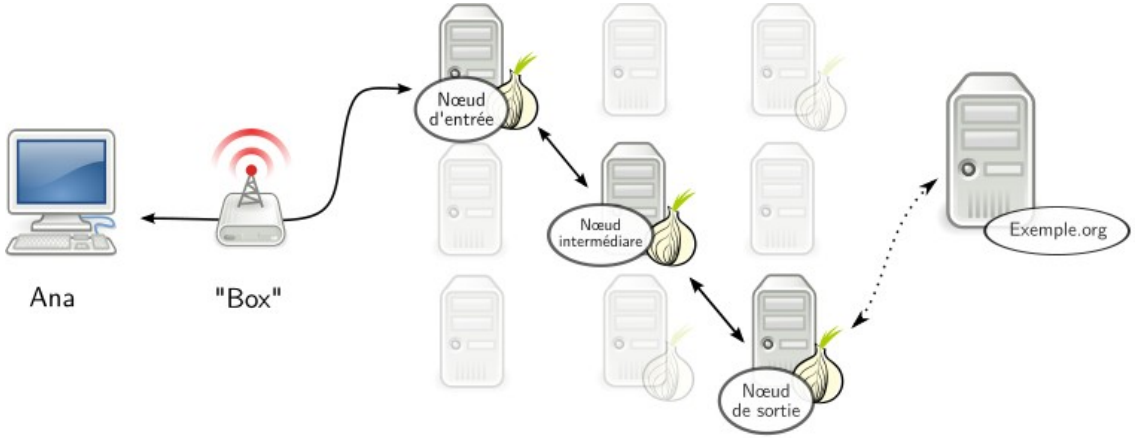
Naviguer incognito avec son ordi

RISEUP VPN

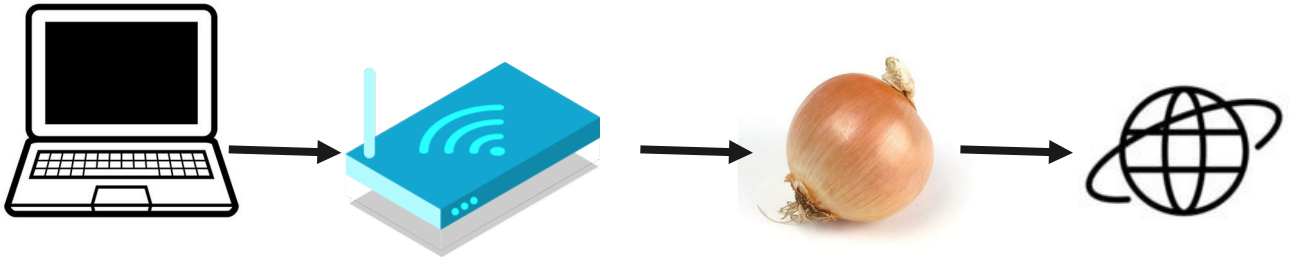
Avec Tor

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

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



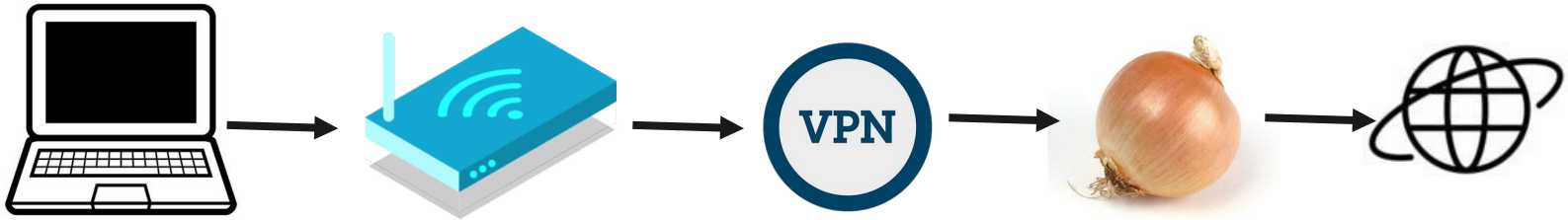
Avec un VPN



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 ses 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 essayent de confirmer une hypothèse en surveillant aux bons endroits dans le réseau puis en faisant la corrélation.

Les limites de la formation

Avec une formation d’une journée, nous considérons que vous avez beaucoup de connaissance mais pas suffisamment pour utiliser des outils numériques en tant que coordo d’une action importante ou en tant que participante à une action très risquée

III – STOCKAGE DE DONNÉES

Faire du repérage sans faille

Sécuriser le stockage : la solution

Tails

+

Sécuriser le stockage : la solution

Tails

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 persistent par défaut

Plein de logiciels utiles pour travailler :

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

Passe par TOR pour tous les flux internet

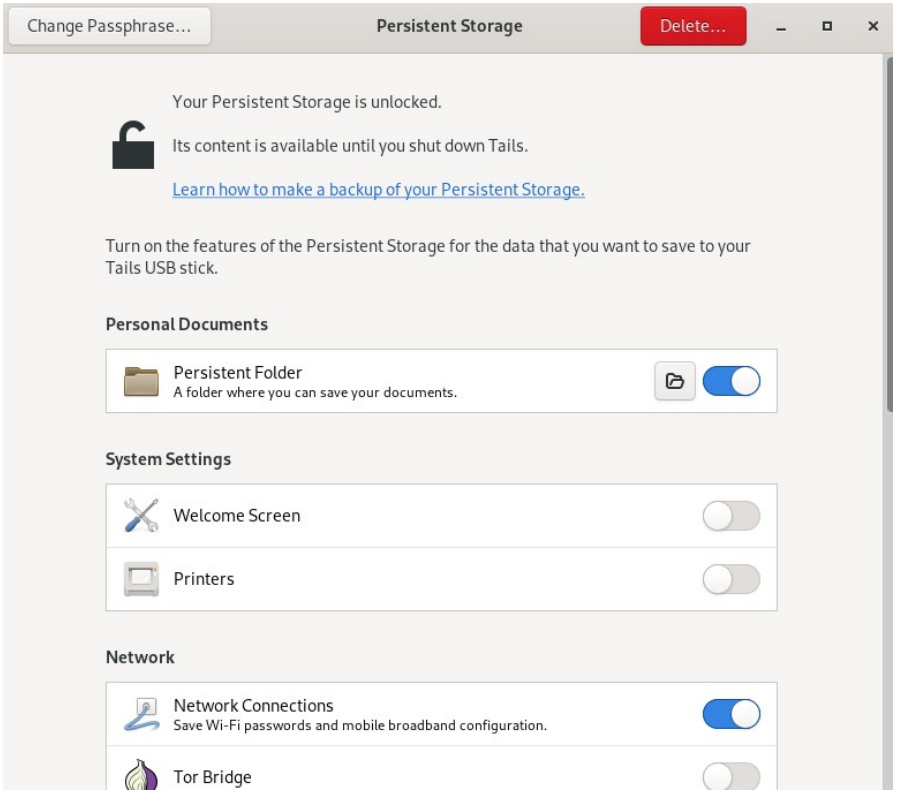
Code source vérifiable

Sécuriser le stockage : la solution

1ère solution :
Activer le stockage persistant sur Tails

- fichiers
- compte Thunderbird
- wifi
...

LUKS
Linux Unified Key Setup



Sécuriser le stockage : la solution

2ème solution :

Clef usb chiffrée annexe

Gnome disk

LUKS

Linux Unified Key Setup

VeraCrypt

Sécuriser le stockage : la solution

Dans les deux cas :

Avoir des sauvegardes cachées en cas de perquisitions

Sécuriser le stockage : la solution

Sécuriser le stockage : la solution - DEMO

Les différentes options de démarrage de Tails
Montrer circuits onion

IV – AUTRES

Qui, quoi, où, comment, pourquoi...

Réfléchir à quelles informations il est intéressant de communiquer, à qui, où ça, comment, quelles sont les raisons...

Identités contextuelles

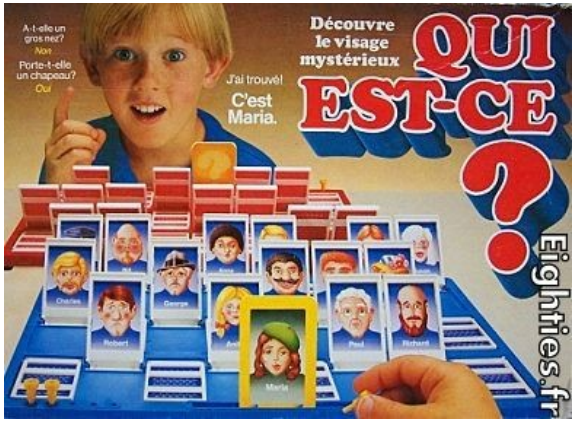
- l’anonymat, c’est ne pas laisser apparaître de nom
- le pseudonymat, c’est choisir et utiliser un nom différent de son identité civile.

Lien entre l’identité contextuelle et l’identité civile → Le recoupement

Corrélation temporelle

Stylométrie

La compartimentation



Enquête en source ouverte (OSINT)

Vos photos sur Facebook

Votre planning de connexion à Mattermost

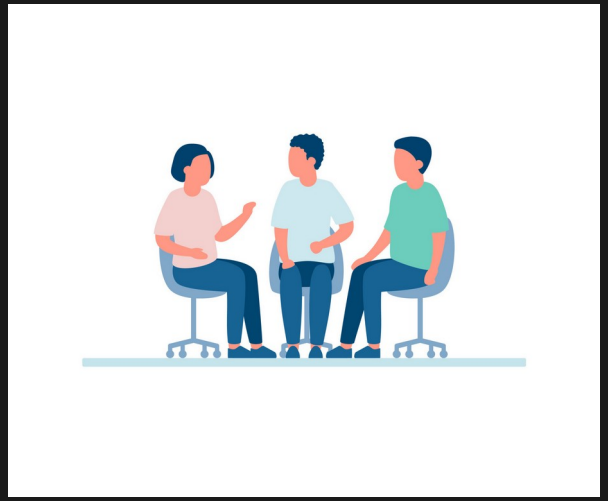
Les canaux sur lesquels vous êtes sur Mattermost et des statistiques

Les stickers sur votre ordi

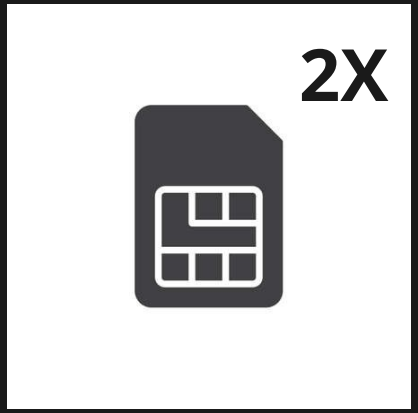
Des articles de journaux, des vidéos d’un journaliste dans un lieu militant

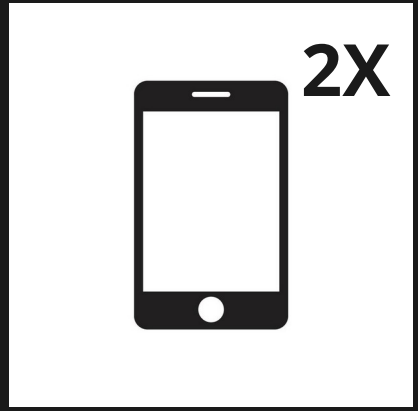
...

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 a 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 + utilisé le moins d’outils numérique possible

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 (backup, gestionnaire de mdp…) voir même se refaire une identité propre
- [ ] Acheter/Fabriquer une cage de faraday
- [ ] Avoir un clef TAILS et savoir un minimum l’utiliser
- [ ] Se faire une clef de sauvegarde

Des questions ?

Phase pratique sécu numérique

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