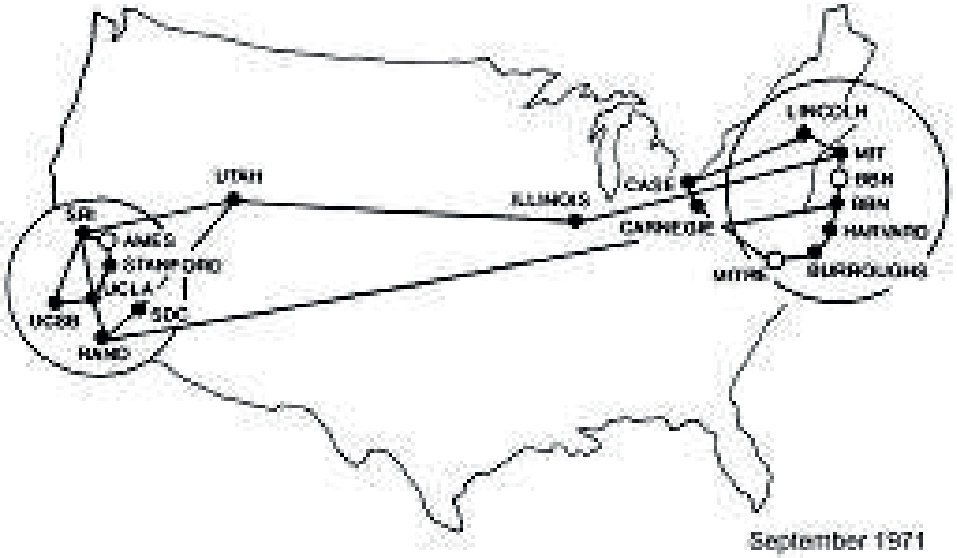
On m’avait promis une utopie, à la place on me surveille :(

« Internet » c'est…

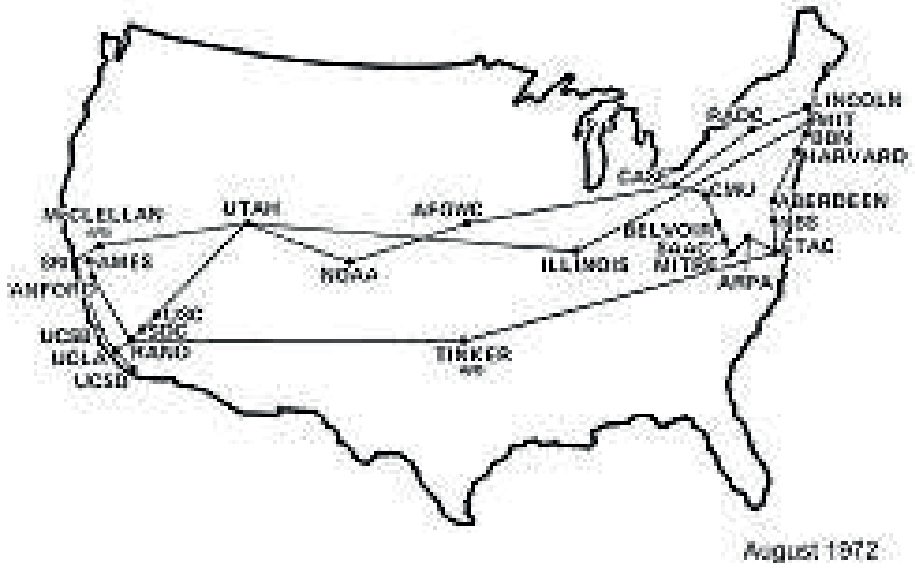
Des ordinateurs.

Connectés entre eux avec des tuyaux, des câbles téléphoniques, des satellites.

Ça existe depuis les années 1970.



September 1971

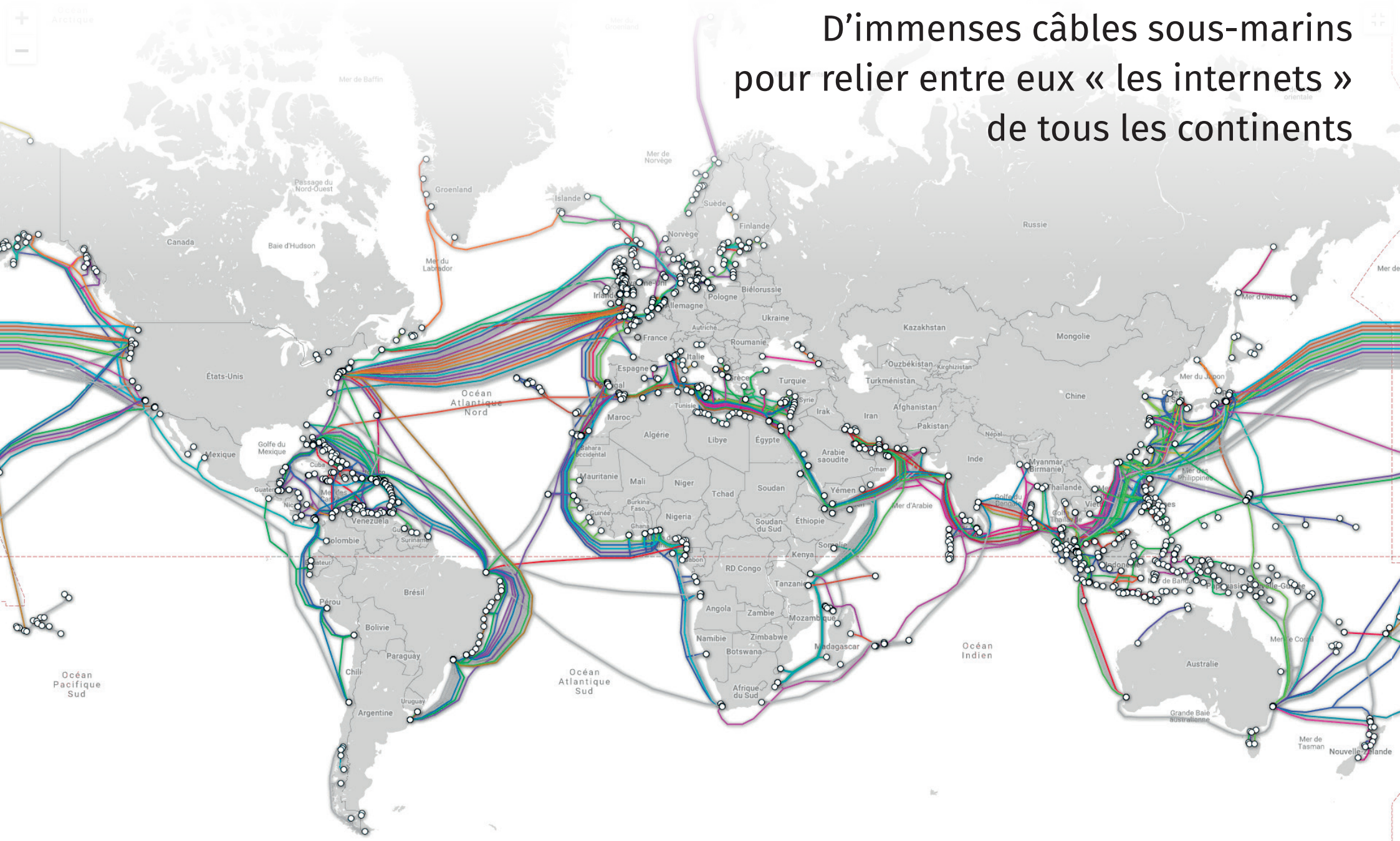


August 1972

June 1975

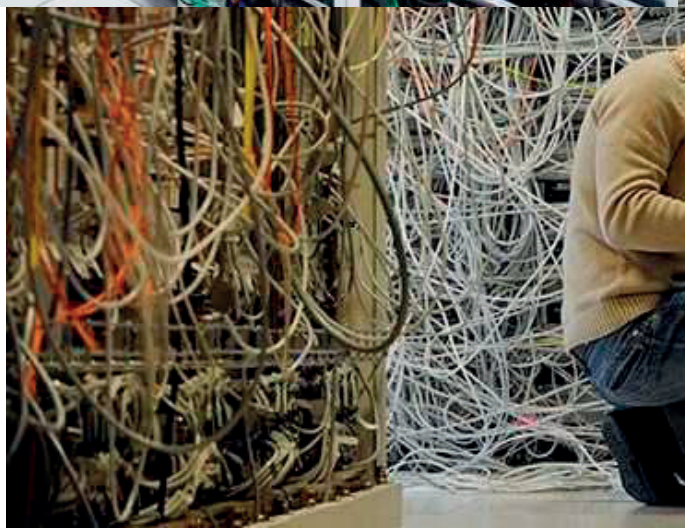
Internet c’est aussi...

D’immenses câbles sous-marins
pour relier entre eux « les internets »
de tous les continents



Internet

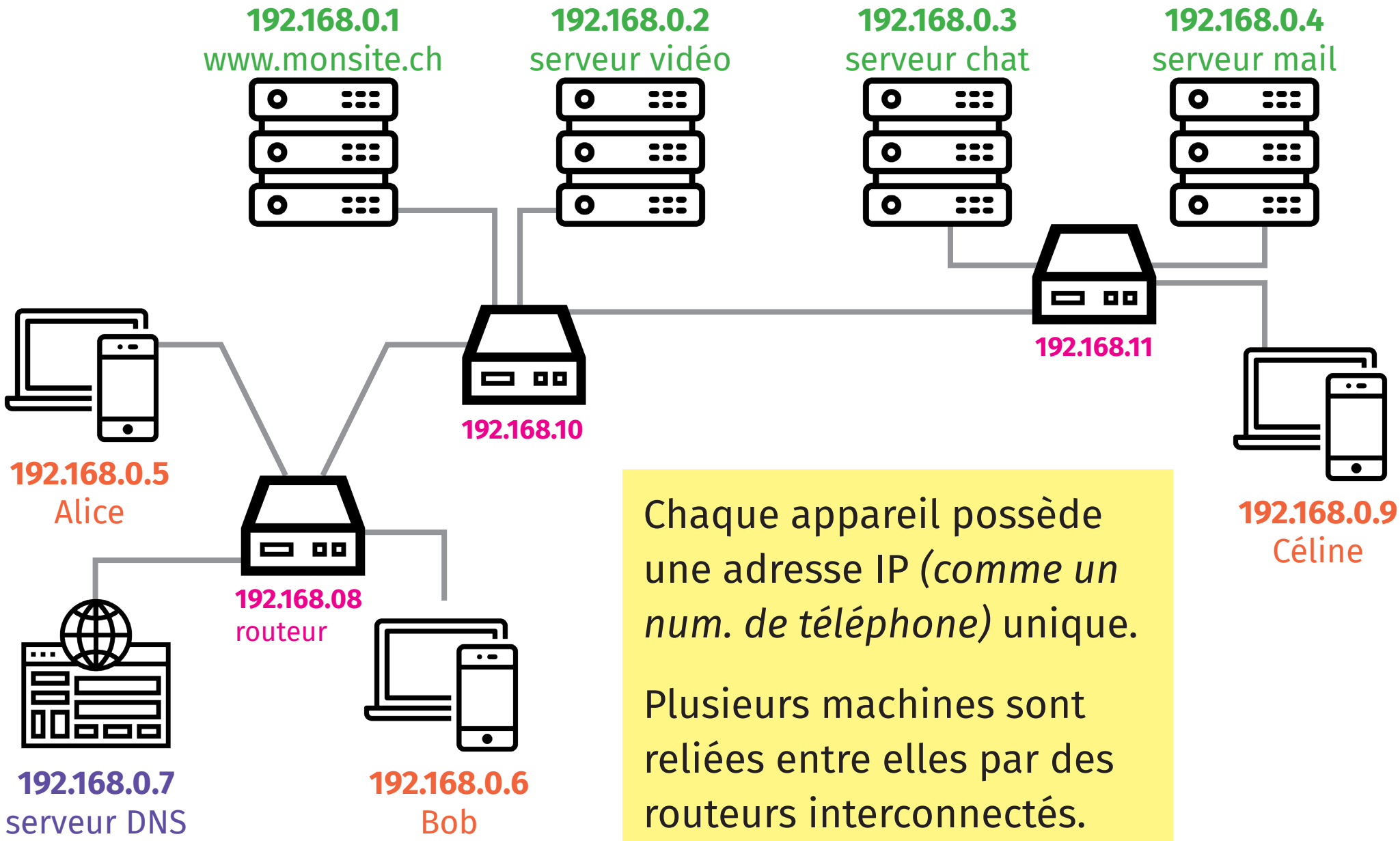
Des ordinateurs
et des câbles. *Plein*.



Internet, plus que des sites web

Nos mails, chats, vidéos à la demande,
partages de fichiers, le cloud… **font partie d'internet**.

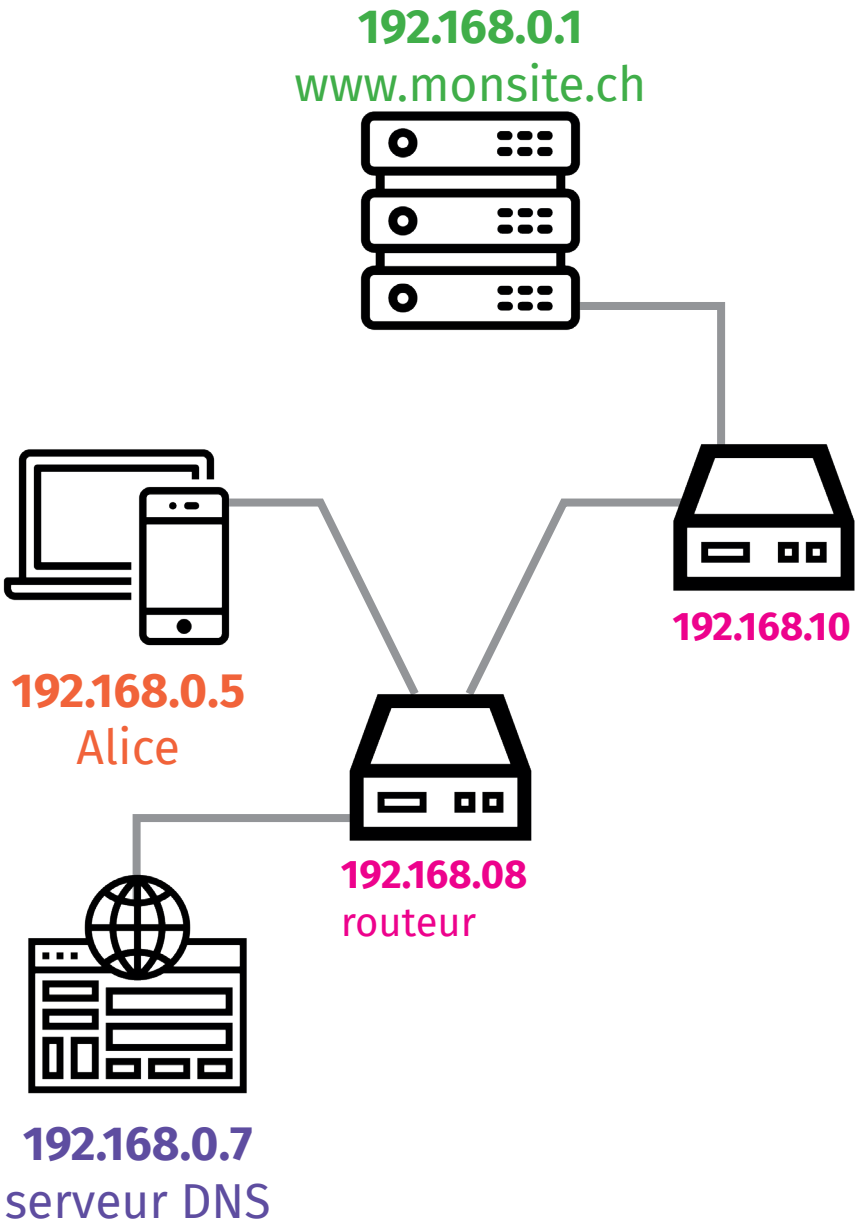
On s'y retrouve comment ?



Chaque appareil possède une adresse IP *(comme un num. de téléphone)* unique.

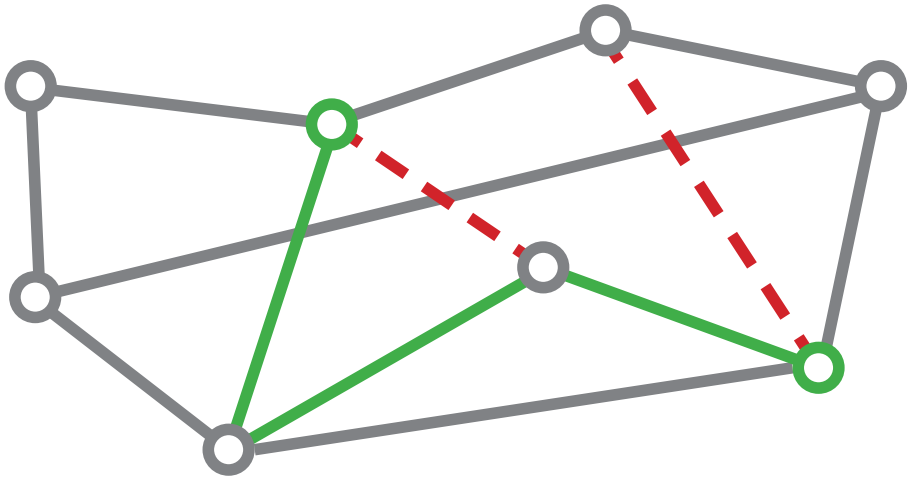
Plusieurs machines sont reliées entre elles par des routeurs interconnectés.

Connexion à une autre machine



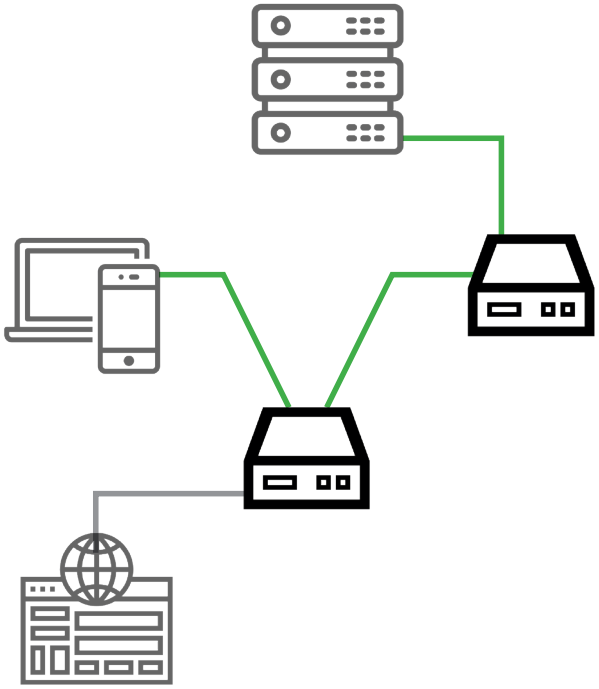
1. **Alice** veut joindre **www.monsite.ch**
2. En passant par **un routeur** elle interroge **un serveur DNS**, un annuaire qui lui indique de contacter **192.168.0.1**
3. La communication est ensuite établie par l'intermédiaire de deux routeurs.

Résilient, pas confidentiel



Internet a été conçu pour continuer de fonctionner si une route disparait.

C'était basé sur la confiance,
pas besoin de confidentialité.



Chaque intermédiaire peut lire
les données en transit s'il le souhaite.

Il conserve aussi une trace
de la connexion dans un journal.

« **192.168.0.5** *contacte* **192.168.0.1** *hier à 10 h.* »

FLASH QUIZZ !

Combien d'intermédiaires
depuis mon ordinateur à la maison
jusqu'au site web d'Amnesty.ch ?

```
> traceroute amnesty.ch
```

192.168.178.1
Maison

routeur

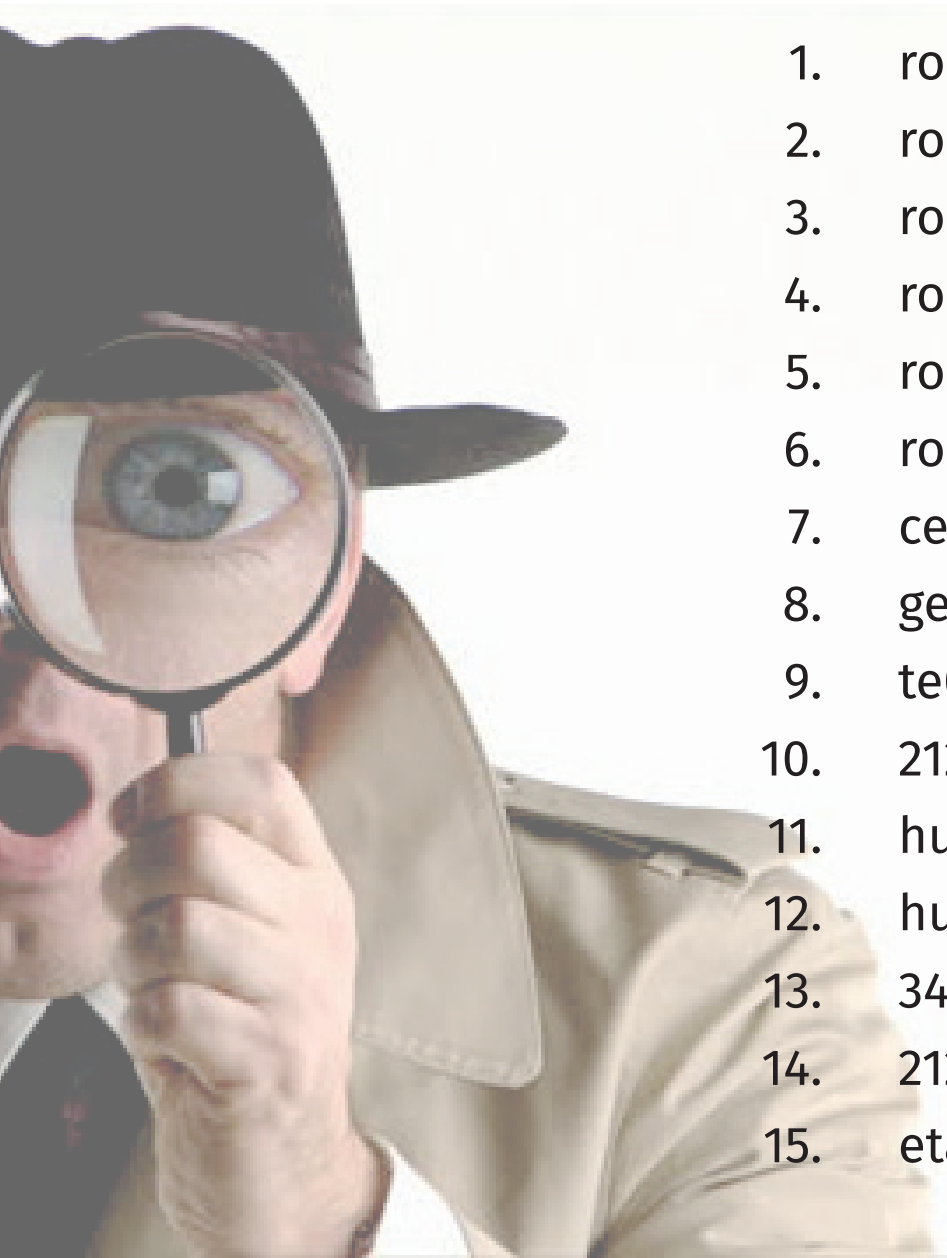
routeur

212.103.66.9
www.amnesty.ch

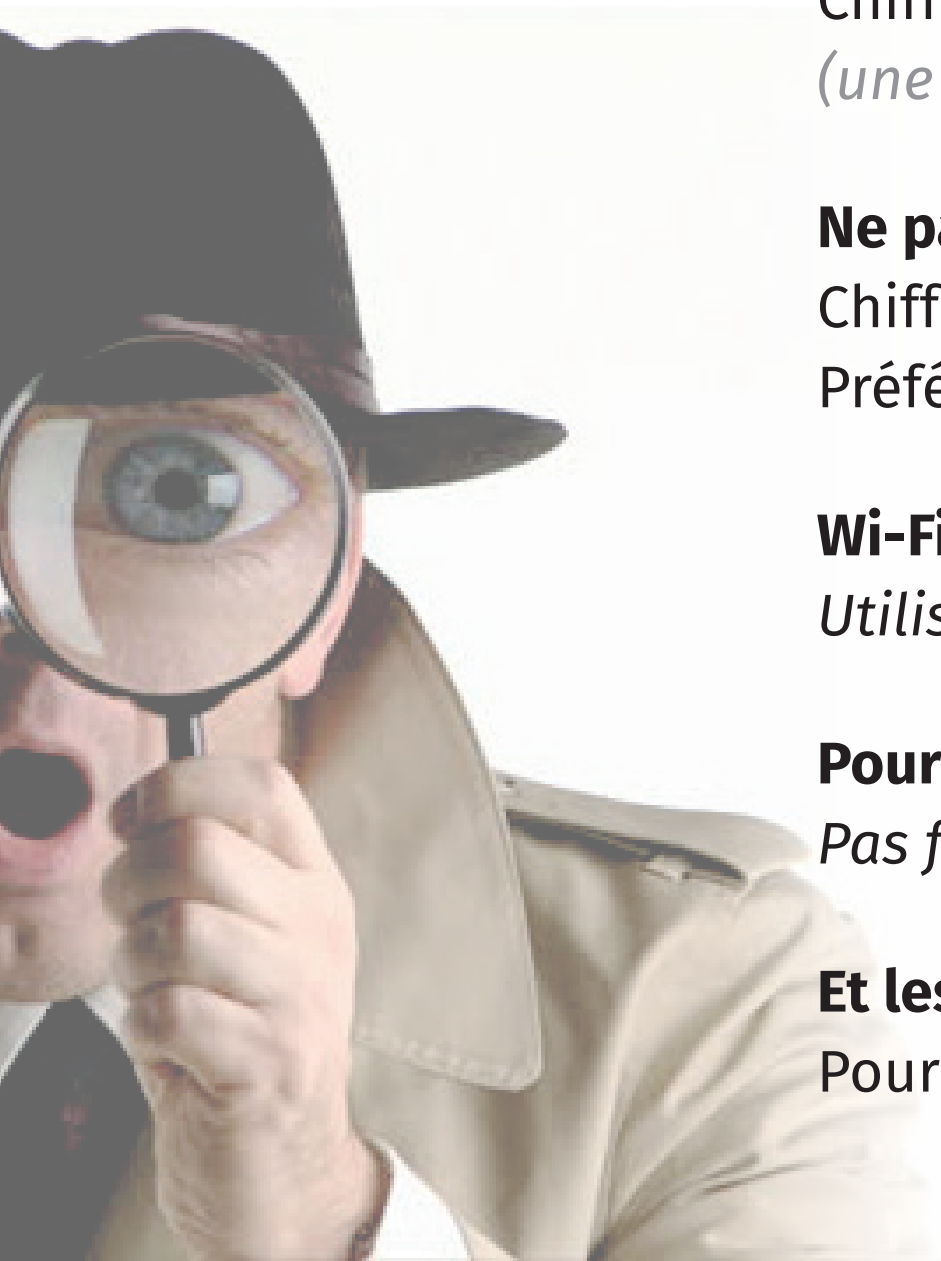
(prenez les paris)

Route jusqu'à amnesty.ch

14 intermédiaires *(de confiance ?)*



1. routeur maison *192.168.178.1*
2. routeur 1 fournisseur d'accès *10.0.0.1*
3. routeur 2 fournisseur d'accès *10.0.0.2*
4. routeur 3 fournisseur d'accès *10.0.0.3*
5. routeur 4 fournisseur d'accès *10.0.0.4*
6. routeur 5 fournisseur d'accès *10.0.0.5*
7. cern-fe0-0-bart.gva.router.colt.net *192.65.185.165*
8. ge0-0-0-sar5.zrh.router.colt.net *212.74.65.35*
9. te0-3-0-1-crs2.fra.router.colt.net *212.74.67.72*
10. 212.23.244.242 ..... *212.23.244.242*
11. hu0-0-1-0.01.p.czh.ch.as15576.nts.ch *217.11.214.32*
12. hu0-0-0-0.01.p.cbn.ch.as15576.nts.ch *217.11.211.66*
13. 3462.te101.01.p.cbn.ch.as15576.nts.ch *217.11.216.226*
14. 212.103.70.94 ..... *212.103.70.94*
15. eta.4teamwork.ch **(le site web)** *212.103.66.9*



Que faire pour se protéger ?

Chiffer le traffic, surfer en utilisant **HTTPS://**
(une extension peut vous aider, voir plus loin)

Ne pas envoyer d'informations critiques par mail.
Chiffrer ses mails, idéal mais trop compliqué.
Préférez une messagerie sécurisée Signal.org

Wi-Fi public ? Le traffic n'est **pas sécurisé !**
Utilisez internet avec précaution, https obligatoire !

Pour les internautes avancés : torproject.org
Pas forcément utile pour le surf de tous les jours.

Et les VPN ?
Pourquoi pas, mais il faut leur faire confiance.

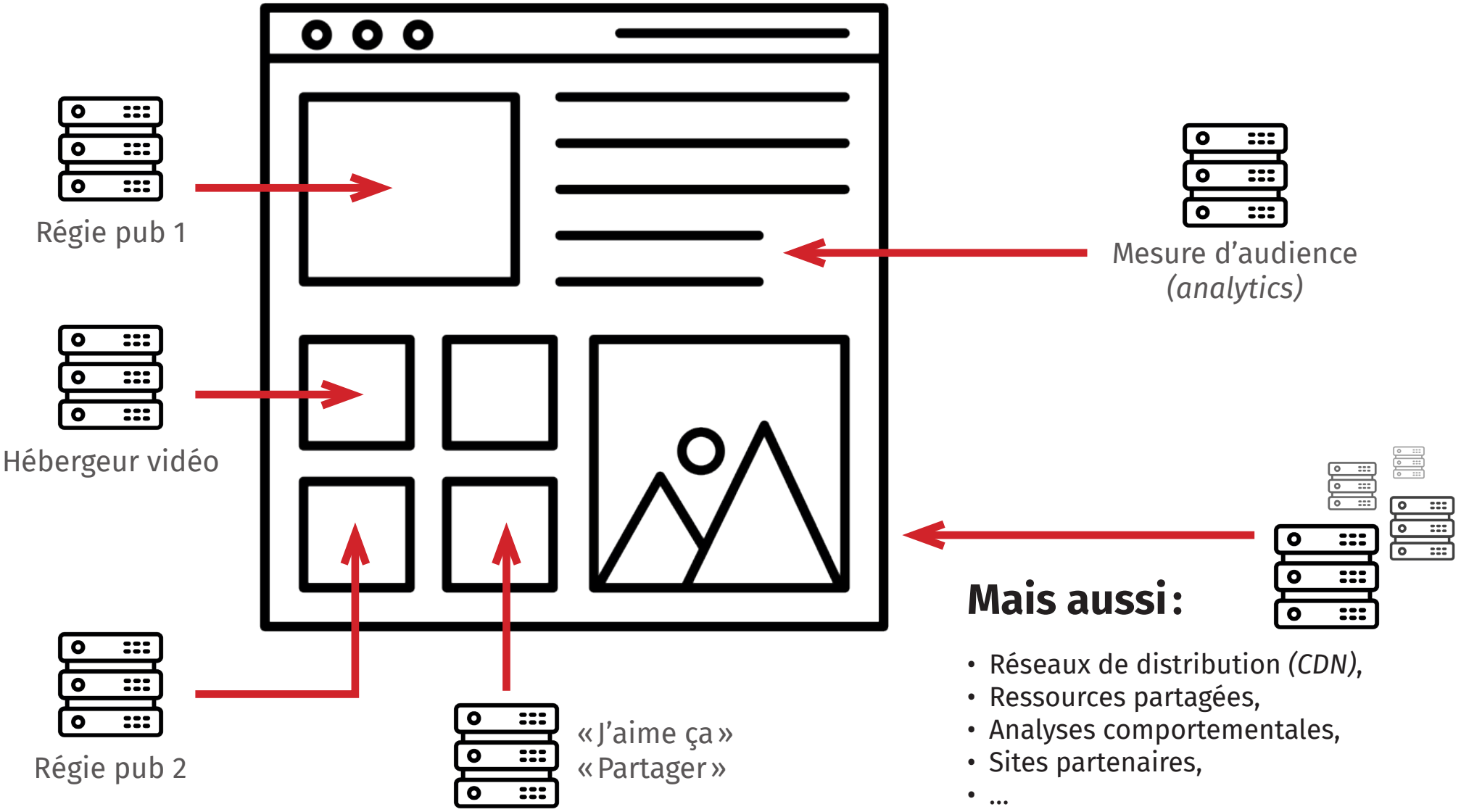
Pistage de la navigation

Juste entre nous...

Je me **connecte sur le site** de mon journal

...et notre public

Je me **connecte sur le site** de mon journal **et aussi à tout ça ?!??**



Mais aussi :

- Réseaux de distribution *(CDN)*,
- Ressources partagées,
- Analyses comportementales,
- Sites partenaires,
- ...

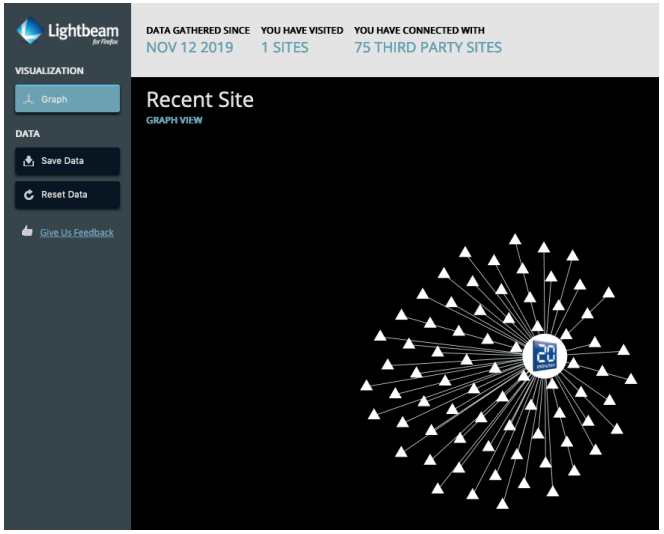
FLASH QUIZZ !

Combien de connexions à des sites externes
si je me connecte sur la page d'accueil du site de 20 Minutes ?

Lightbeam
for Firefox

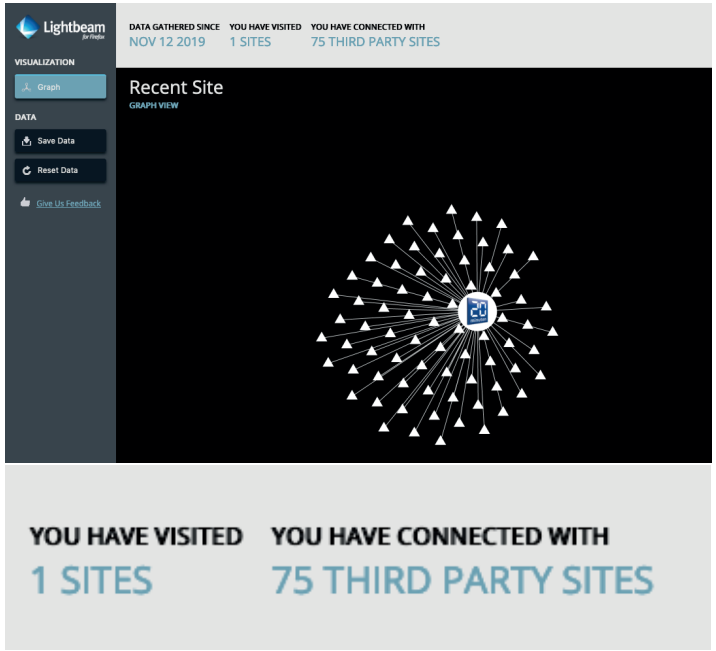
Si vous voulez tester
https://addons.mozilla.org/fr/firefox/addon/lightbeam-3-0/
(uniquement disponible pour Firefox)

On n’est pas seuls



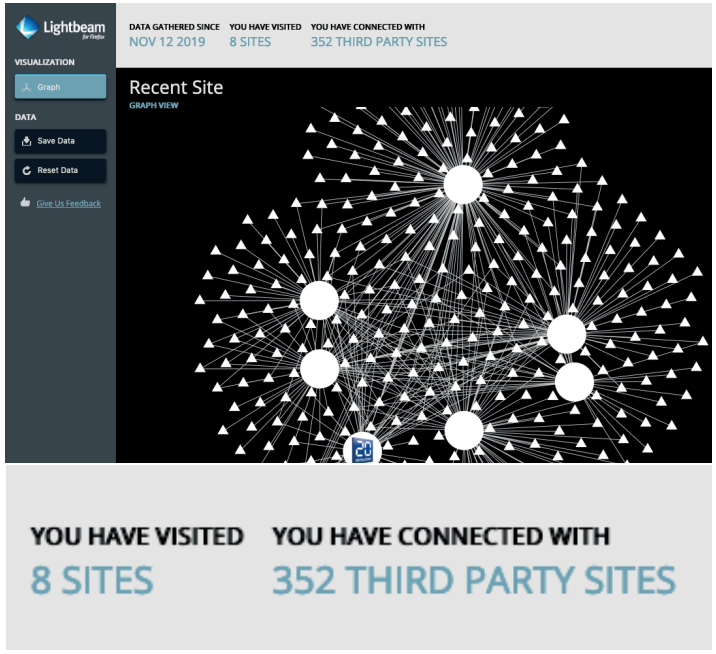
Et si on visite plus qu’un site ?

On n’est vraiment pas seuls



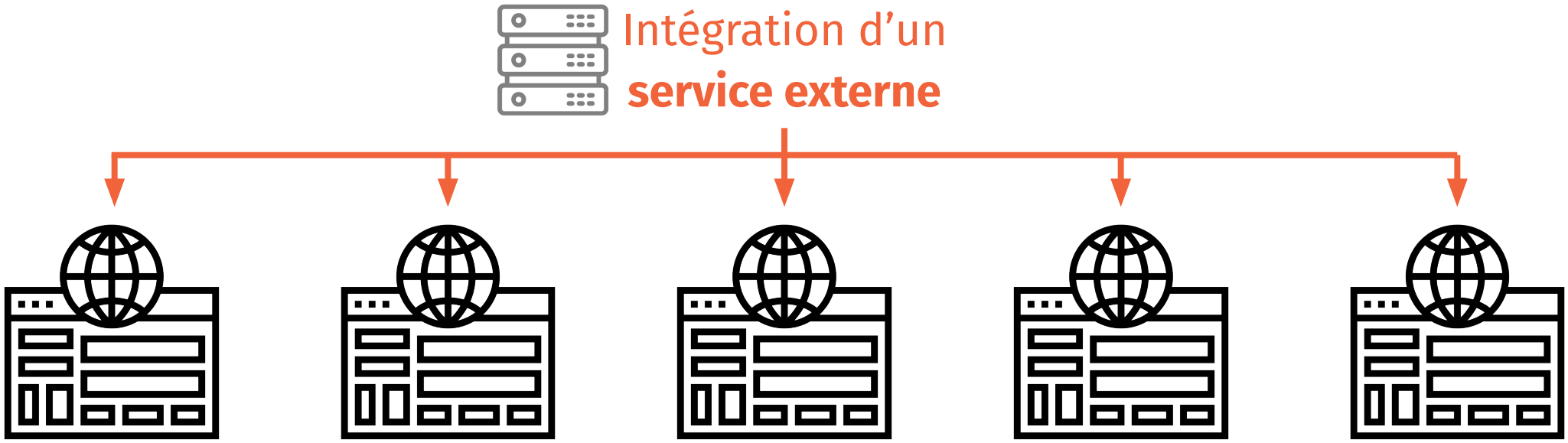
Rajoutons les sites suivants

Le Temps, RTSInfos, 24 Heures,
Le Matin, La Liberté, Le Monde, Le Figaro



Mais ne paniquez pas tout de suite...

C’est pas fini !



Un service externe peut savoir où il est intégré. Il peut également laisser un identifiant unique sur l’ordinateur du visiteur.

C’est ainsi possible de suivre la navigation des internautes !

FLASH QUIZZ !

Qu’est-ce qu’un cookie ?

1. Délicieux *biscuit sec*
   aux pépites de chocolat

2. *Jeu vidéo* de plates-formes
   publié en 1983

3. *Fichiers permettant* aux
   sites web que nous visitons
   de se souvenir de nous.

4. *Film* réalisé en 2012
   par Léa Fazer

Comment on nous piste ?

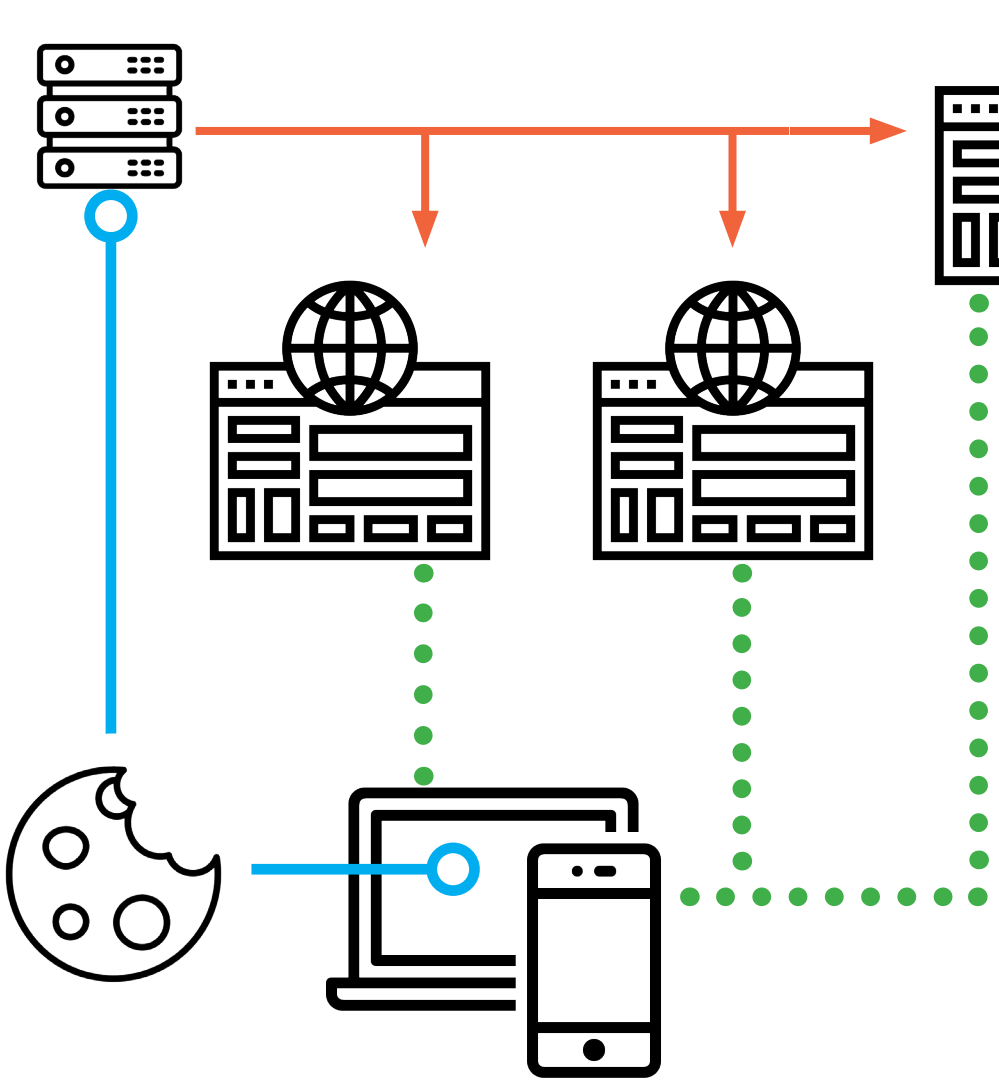
Empreintes numériques déposée dans

- un **cookie**,
- le LocalStorage du navigateur,
- un `<canvas>`.

Pixel espion, **images invisibles**.

Dans le cas des apps :
Elles sont capables d'analyser leur utilisation.
Un navigateur web sans scrupule pourrait
épier l'intégralité de votre activité.

Comment ça fonctionne ?



Je me connecte sur un site utilisant un service tiers.

Celui-ci me dépose **un cookie**, avec un **identifiant unique**.

Je me connecte ensuite à un autre site utilisant le même service tiers qui lit mon cookie et me reconnait.

Pistage

Pour bâtir un profil et ainsi mieux connaitre nos habitudes, nos goûts, anticiper nos envies.

Avec ça je peux, par exemple:

- *optimiser le contenu* en fonctions des visites,
- proposer de la *publicité* ciblée,
- *influencer* l'opinion,
- savoir quelle *décision* prendre concernant des *sujets sensibles*.

Se protéger

Mozilla Firefox

Privilégie et respecte
votre vie privée.

Protection contre le pistage
intégrée par défaut.

FIREFOX.COM

pour Mac, PC, iOS, Android

Pourquoi pas les autres ?

RAPPEL

Les apps sont capables d'analyser leur utilisation.
Un navigateur web sans scrupule pourrait épier l'intégralité de votre activité.

Voulez-vous vraiment leur faire confiance pour ne jamais nous épier ?

- Google *(Chrome)*
- Microsoft *(Edge)*
- Apple *(Safari)*
- Samsung *(Internet Browser)*

Aller plus loin

Les **modules complémentaires** *suivants peuvent aussi vous aider*:

uBlock Origins *(bloqueur de publicités)*
https://addons.mozilla.org/fr/firefox/addon/ublock-origin/

DecentralEyes *(ressources partagées mise en cache local)*
https://addons.mozilla.org/fr/firefox/addon/decentraleyes/

Facebook Containter *(isole Facebook du reste du navigateur)*
https://addons.mozilla.org/fr/firefox/addon/facebook-container/

HTTPS Everywhere *(force une connexion sécurisée si disponible)*
https://addons.mozilla.org/fr/firefox/addon/https-everywhere/

Le Cloud

FLASH QUIZZ !

Où trouver le Cloud ?

- Dans le ciel
- En regardant le radar météo
- Aux bonnes adresses Internet
- Sur l’ordinateur de quelqu’un d’autre

« Le Cloud, c'est les ordinateurs de quelqu'un d'autre »

Et tant d'autres...

Risques du cloud

Que font les compagnies avec les données stockées dans leur cloud ?

Rien ne garanti que certains pratiques n’apparaîtront pas dans le futur.

Des *companies*, jugées aujourd’hui sûres, seraient demain *forcées de partager des informations en notre défaveur*.

Autant des états comme d’autres sociétés pouraient en profiter.

Risques du cloud

Sans compter que

- une telle richesse *attire les convoitises* des pirates
- une *fuite de donnée*, et nos informations se retrouvent publiques

Nous y déposons un trésor

Recommandations

Evitez d'y déposer :

- des fichiers administratifs sensibles *(assurances, dossier médicaux, facturation)*
- des scans de pièces d'identité ou autres documents officiels
- des documents compromettants *(critiques de l'autorité, questionnements sur son identité, relations à cacher, nus, ...)*

Nous y synchronisons peut-être aussi...

Photos
qui peuvent être analysées pour contribuer à notre profil, ou être compromettantes

Contacts
à partir desquels on déduit nos relations et nos cercles d'intérêt

Agenda
pour tout savoir de nos déplacements et de notre emploi du temps

Données de santé
et journaux d'activité physique, qui feraient le bonheur de notre assurance

Notes et listes de tâches

Liste non-exhaustive

Le Cloud, quelles solutions ?

Le Cloud personnel, pour reprendre le contrôle.

A installer soi-même
(mais c'est technique):

- ownCloud – owncloud.org
- **nextCloud** – nextcloud.org
- YUNOhost – yunohost.org

Des services qui vous respectent
(et c'est plus simple):

- **Cozy** – cozy.io
- CHATONS – chatons.org

Réseaux sociaux, une note

Chaque info sur Facebook ou discussion Twitter est utilisée pour construire notre profil.

- Ce qu'on **aime**,
- les gens avec qui on **interagit**,
- nos **commentaires**,
- les **liens que nous publions**
- même nos **photos** *(reconnaissance d'images)*

Un p’tit like et puis s’en va

«Une fois qu’on a liké, on n’y pense plus.

Mais **pour les algorithmes** qui vont traiter ces informations, **ça révèle** beaucoup plus sur ce que nous sommes, ce que nous aimons ou pas, notre comportement, **ce que l’on est profondément**.»

https://www.rts.ch/info/sciences-tech/10847789-facebook-la-fin-du-like-ou-comment-rendre-moins-dependant.html

Un p’tit like et puis s’en va

«Quand un site web intègre ce bouton like sur ses pages web,
le simple fait que vous accédiez au site web et **que le bouton like se charge transmet déjà des informations à Facebook**»

https://www.rts.ch/info/sciences-tech/10847789-facebook-la-fin-du-like-ou-comment-rendre-moins-dependant.html

Internet n’oublie jamais

tout ce que vous publiez sera retenu contre vous

Photos compromettantes (*ébriété, nus, …)*

Voyages, emploi du temps

Critiques (*de son employeur, de l’autorité)*

État de santé

…

Et pourtant,
nous partageons ça de notre plein gré

Le modèle de menace

C’est l’**ensemble des risques** auxquels on se pense être exposé.

Il varie selon les individus.

Y **réfléchir** permet de mettre sur pieds des **solutions** en réponse aux problèmes identifiés.

Exemples de menaces

Vol de son ordinateur
ou son téléphone

Accès non-autorisé
à un appareil ou à un compte

Fuite de données

Pistage numérique

Profil comportemental

Écoutes de masse

Attaques ciblées *(spear-phishing)*

…

A quoi vos élèves sont-ils vulnérables

quand leurs données personnelles sont exposées ?

A quoi vos élèves sont-ils vulnérables

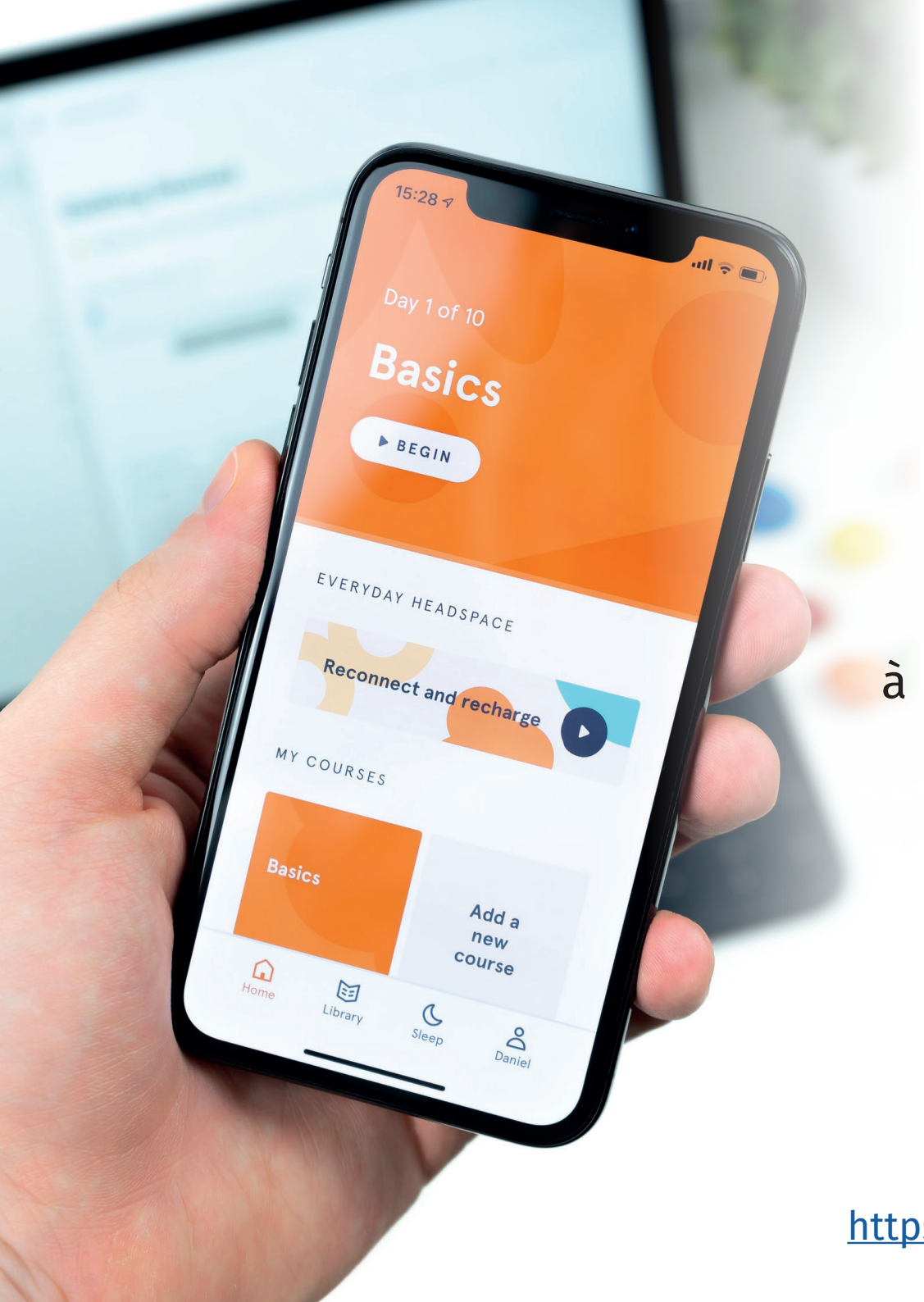
quand leurs données personnelles sont exposées ?

Manipulations comportementales : publicité et achats compulsifs, orientation d'opinion.

Risques pour le futur basé sur des **traces de leur comportement actuel** : travail, assurances, location, crédit, ...

Révélations forcées : grossesse, identité de genre, orientation sexuelle, ...

Cyberharcèlement / extorsion *(par exemple à cause de sexting)*



Le téléphone roi

Sur leurs 2 heures de surf quotidien,
les 15-24 ans en passent
les trois quarts sur leur mobile.

Ils sont d'ailleurs **6 sur 10**
à utiliser **exclusivement leur smartphone**
pour naviguer sur internet.

https://www.mediametrie.fr/fr/lannee-internet-2018

Le téléphone roi

Les mobinautes visitent
en moyenne 56 sites par mois
contre **18 applications**.

Ces dernières concentrent
90% du temps passé sur mobile.

https://www.mediametrie.fr/fr/lannee-internet-2018

Le téléphone roi

Les **réseaux sociaux** s'imposent comme **1ère activité** sur internet.

Ils représentent
⅕ du temps passé sur internet
et **⅓ chez les 15-24 ans**.

https://www.mediametrie.fr/fr/lannee-internet-2018

FLASH QUIZZ !

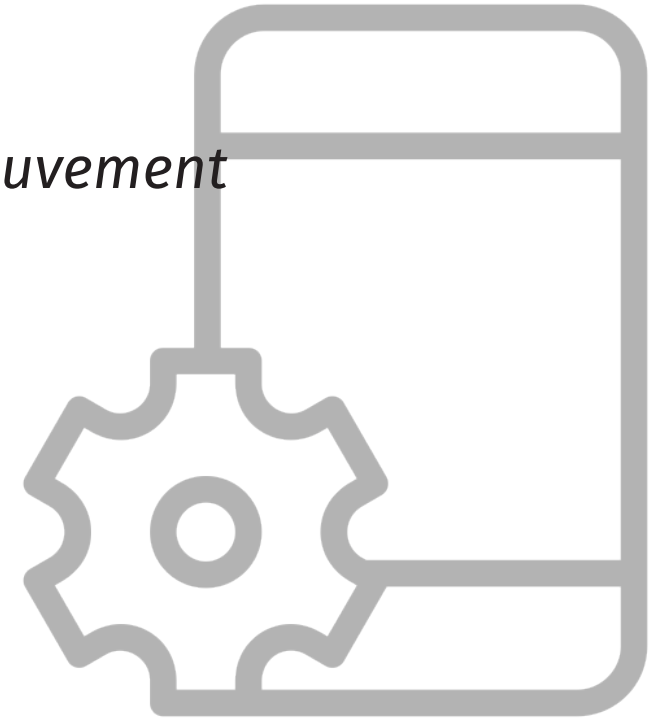
Pourquoi ces apps requierent-elles ces permissions ?

Calculatrice – *accès à internet*

Recettes de cuisine – *accès aux contacts*

Traffic routier – *accès à la géolocalisation*

Assurance maladie – *accès aux données de mouvement*

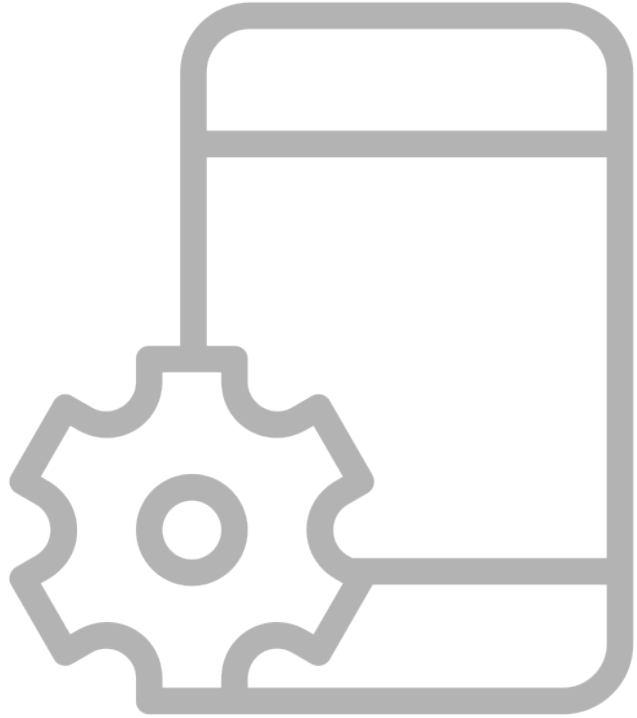


FLASH QUIZZ !

Pourquoi ces apps requierent-elles ces permissions ?

Calculatrice – *accès à internet*
Consulte les taux de change pour les conversions de monnaie
et affiche de la **publicité**

Recettes de cuisine – *accès aux contacts*
Partage vos coups de coeurs avec vos amis
et les abonne de force à des **newsletters**

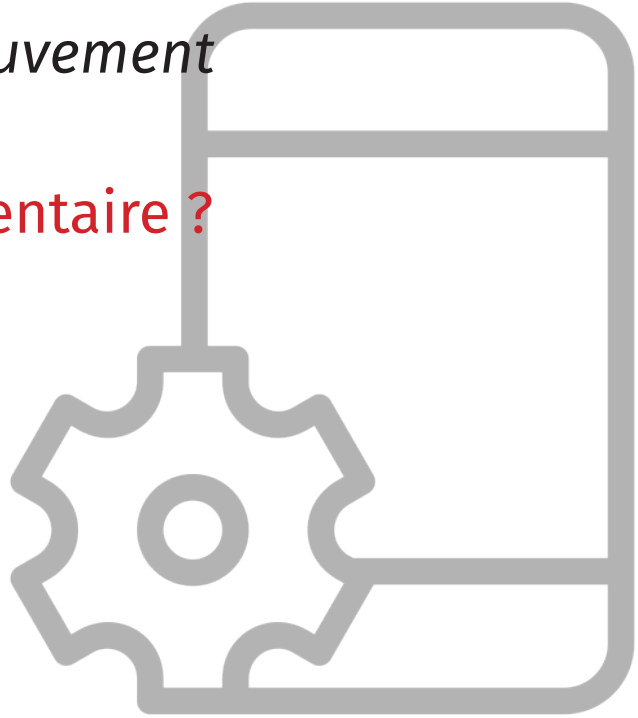


FLASH QUIZZ !

Pourquoi ces apps requierent-elles ces permissions ?

Traffic routier – *accès à la géolocalisation*
Signale les ralentissements sur votre route
et **dénonce vos excès de vitesse** à votre assurance

Assurance maladie – *accès aux données de mouvement*
Vous **accorde un rabais** dès 10’000 pas par jour
et **refuse de vous assurer** si vous être trop sédentaire ?



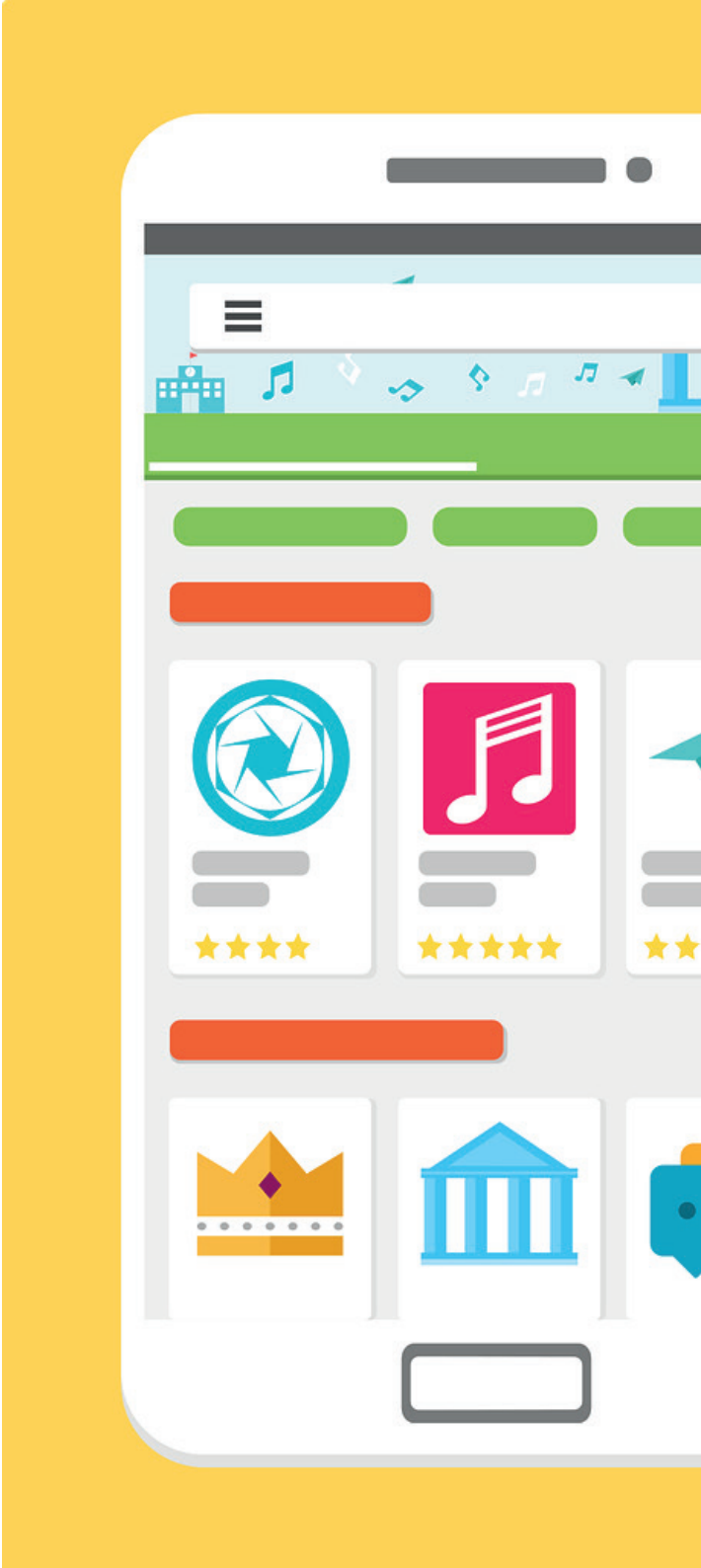
Applications mobiles

Souriez, vous êtes pistés !

exodus

La plateforme d'audit de la vie privée des applications Android

https://reports.exodus-privacy.eu.org/fr/



Chasseur chassé

Pokémon GO

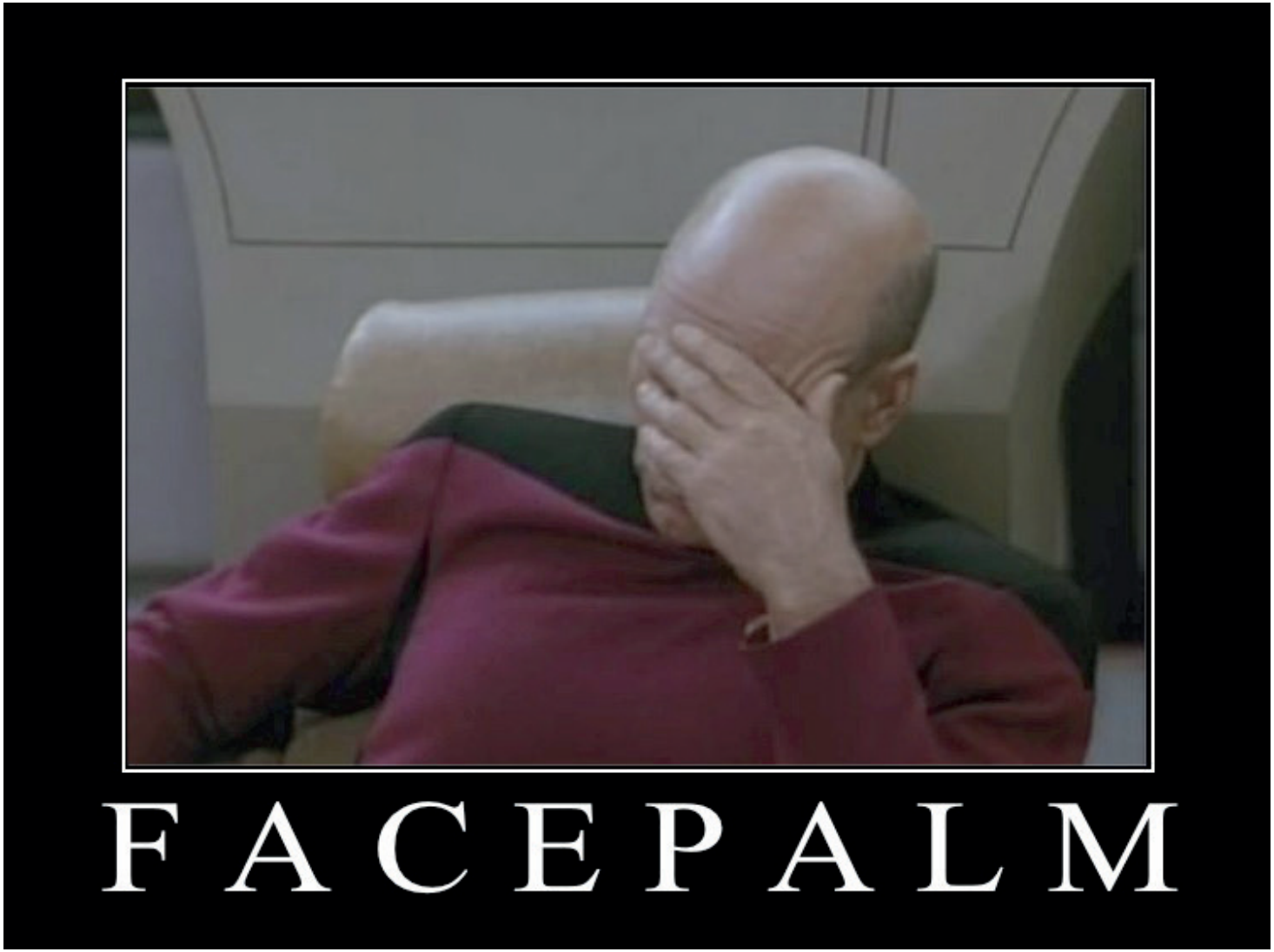
9 pisteurs dans cette application :

1. Adjust
2. Braze (formerly Appboy)
3. Facebook Analytics
4. Facebook Login
5. Facebook Share
6. Google AdMob
7. Google CrashLytics
8. Google Firebase Analytics
9. HelpShift

Et 24 permissions!

https://reports.exodus-privacy.eu.org/fr/reports/com.nianticlabs.pokemongo/latest/

Comment je m’en sors ?



Comment je m’en sors ?

Minimiser le nombre d’applications installées

Éviter les applications aux
permissions trop gourmandes

Ne pas installer n’importe quoi :
modèle économique 100% "gratuit",
sources inconnues, …

Vérifier les permissions, retirer celles inutiles
iOS : *Paramètres > Confidentialité*
Android : *Paramètres > Applications > Autorisations*
ou *Paramètres > Sécurité > Autorisations*

Conclusion

J’ai accès

- à ton compte facebook,
- à l’intégralité de ton téléphone
- à tes mails.

Mais c’est cool, parce que
tu n’as rien à cacher,
n’est-ce pas ?

MERCI DE VOTRE ATTENTION

Une présentation de Jonas Boni

—

https://www.daoro.net/pres/internetsurveillance.pdf

https://www.daoro.net
https://twitter.com/daoro

Crédits photos

Icônes par the Noun Project

- Server by Creative Stall
- Router by Lero Keller
- Responsive by Xinh Studio
- Domain by Eucalyp
- Webpage by Vectors Point
- Cookies by Graphic Tigers
- Check list by Robiul Alam
- Health by Guilherme Furtado
- Pictures by Atif Arshad
- Calendar by AlePio
- Contacts by Template
- Contact by Icons Producer
- Aoo settings by shuai tawf

Images

Pixabay.com
Wikimedia Commons
Domaine Public.
Unsplash

- Smartphone, by Daniel Korpai
- Gray steel chain locked on gate, by John Salvino
- Person using black iPad, by NordWood Themes
- Facebook button pins, by NeONBRAND

Clouds paint by Colorsark on DeviantArt.
Memes are considered parody.