VPN

ce qu'il voit, ce qu'il cache, et ce qu'il vous coûte

Comprendre qui observe votre activité en ligne, et pourquoi un VPN gratuit n'est jamais gratuit

Livre blanc by ChallengeMyProject

À qui s'adresse ce document ?

À toute personne qui veut savoir ce qu'un VPN change vraiment : qui voit son activité en ligne, ce que le VPN voit à son tour, et pourquoi un service gratuit n'est jamais sans contrepartie. Aucun prérequis technique.

01

Le problème : votre trafic n'est pas privé

Qui peut voir ce que vous faites en ligne ?

Quand vous ouvrez un site, votre connexion ne va pas directement de votre appareil au site. Elle traverse d'abord le réseau de votre fournisseur d'accès à Internet (FAI) : Orange, Free, SFR, Bouygues, ou l'opérateur du Wi-Fi du café où vous êtes assis.

Ce fournisseur est un intermédiaire obligatoire, et il voit passer deux choses : votre adresse IP, qui identifie votre connexion, et le nom des sites que vous consultez. Selon la réglementation applicable, il est même tenu de conserver une partie de ces informations pendant plusieurs mois, et de les communiquer sur réquisition.

À cela s'ajoutent les administrateurs des réseaux que vous empruntez : l'entreprise, l'université, l'hôtel, l'aéroport. Chacun voit, à son niveau, une partie de votre activité.

Le VPN (Virtual Private Network, « réseau privé virtuel ») ne fait pas disparaître ce problème : il le déplace. Au lieu que votre fournisseur d'accès voie tout, c'est le fournisseur de VPN qui voit. Toute la question — et c'est l'objet de ce livre blanc — est donc de savoir à qui vous choisissez de faire confiance, et sur quels critères.

02

Le tunnel chiffré

Ce qu'un VPN change concrètement à votre connexion

Un VPN crée un tunnel chiffré entre votre appareil et un serveur exploité par le fournisseur. Tout votre trafic y passe, et devient illisible pour qui l'observe de l'extérieur.

Concrètement, trois choses changent en même temps.

Votre fournisseur d'accès perd la visibilité. Il ne voit plus que deux éléments : que vous êtes connecté à un serveur VPN, et le volume de données échangé. Ni les sites consultés, ni leur contenu.

Les sites que vous visitez ne voient plus votre adresse IP réelle. Ils voient celle du serveur VPN, et vous localisent donc là où se trouve ce serveur. C'est ce qui permet d'accéder à des contenus restreints à un pays — mais c'est aussi ce qui montre les limites de l'exercice : le site ne sait plus où vous êtes, le fournisseur de VPN, lui, le sait toujours.

Le fournisseur de VPN prend la place de votre FAI. C'est le point le plus important de ce document, et le plus souvent passé sous silence par le marketing. En chiffrant votre trafic jusqu'à ses serveurs, le VPN devient le nouvel intermédiaire obligatoire : il achemine vos connexions et reçoit vos requêtes DNS, c'est-à-dire la liste des noms de domaine que votre appareil demande à résoudre.

Un VPN ne supprime donc pas l'observateur. Il le déplace, et vous laisse le choisir.

03

Ce que voit votre FAI, ce que voit votre VPN

Le même trafic, deux points d'observation différents

Poser la question dans les deux sens est le meilleur moyen de comprendre ce qu'on gagne et ce qu'on perd.

Sans VPN, votre fournisseur d'accès voit votre adresse IP réelle, les noms des sites que vous consultez, les horaires et la durée de vos connexions, et le volume de données échangé.

Avec un VPN, ce même fournisseur d'accès ne voit plus qu'une connexion chiffrée vers une adresse appartenant au VPN. La liste des sites disparaît de son champ de vision.

Mais le fournisseur de VPN est désormais en position de voir ce que votre FAI voyait : votre adresse IP réelle, les serveurs auxquels vous vous connectez, et vos requêtes DNS. Techniquement, rien ne l'en empêche.

Deux mécanismes limitent ce qu'il peut réellement en faire.

Le premier est technique : le chiffrement HTTPS, sur lequel nous revenons en section 04, empêche aussi bien le FAI que le VPN de lire le contenu de vos échanges.

Le second est contractuel et juridique : la politique de journalisation du fournisseur, et le droit du pays dans lequel il est établi. C'est l'objet de la section 05.

Retenez la formule : **un VPN ne vous rend pas invisible, il change qui vous regarde.**

04

HTTPS : la couche que le VPN ne remplace pas

Ce que même votre VPN ne peut pas lire

Le petit cadenas de la barre d'adresse n'est pas un détail cosmétique. C'est lui qui protège le contenu de ce que vous faites, y compris vis-à-vis de votre VPN.

HTTPS chiffre les échanges entre votre navigateur et le site consulté, de bout en bout. Ni votre fournisseur d'accès, ni le réseau Wi-Fi que vous empruntez, ni votre fournisseur de VPN ne peuvent lire ce qui circule à l'intérieur.

La distinction est fine mais décisive : un intermédiaire voit que vous vous connectez à un domaine — par exemple impots.gouv.fr. Il ne voit ni la page que vous ouvrez, ni ce que vous y saisissez, ni ce que le site vous répond.

Trois conséquences pratiques.

Vos mots de passe et vos coordonnées bancaires sont protégés par HTTPS, pas par le VPN. C'est vrai même sur un réseau public, et même avec un VPN médiocre. La crainte du Wi-Fi de gare ou d'hôtel repose largement sur une menace que la généralisation de HTTPS a désormais neutralisée.

Ce qui reste exposé, c'est la liste de ce que vous consultez, pas son contenu. C'est cette donnée-là — vos centres d'intérêt, vos habitudes, votre santé, vos opinions — qu'un VPN soustrait à votre FAI, et qu'un mauvais VPN peut exploiter à sa place.

Les requêtes DNS échappent souvent à HTTPS. Avant d'ouvrir une connexion chiffrée, votre appareil demande l'adresse du domaine. Si cette requête part en clair, elle trahit la liste de vos visites. Un fournisseur sérieux résout le DNS lui-même, à l'intérieur du tunnel, et protège contre les fuites DNS et IPv6.

05

Les logs et la juridiction

Les deux critères qui décident de tous les autres

Puisqu'un VPN est techniquement capable de tout voir, la seule protection réelle consiste à savoir ce qu'il enregistre, et quel droit s'applique à ce qu'il enregistre.

La politique « no-logs ». Les fournisseurs sérieux s'engagent à ne conserver aucun enregistrement de l'activité de navigation : ni sites visités, ni horodatages associés à un utilisateur, ni adresses IP d'origine. L'engagement n'a de valeur que s'il est vérifiable — d'où l'importance d'audits indépendants, publiés et renouvelés, plutôt que d'une mention marketing sur la page d'accueil.

La juridiction. Un engagement contractuel ne pèse rien face à une obligation légale. Le pays où le fournisseur est établi détermine ce qu'un État peut lui imposer : conservation obligatoire, réquisition, et surtout possibilité de le contraindre au silence. Aux États-Unis, les national security letters permettent d'exiger une surveillance tout en interdisant d'en parler. À l'inverse, des juridictions comme la Suisse offrent un cadre nettement plus protecteur : Proton VPN, établi à Genève, met en avant l'impossibilité, en droit suisse, d'être contraint de journaliser l'activité de ses utilisateurs.

Attention à la distinction entre siège social et infrastructure. Beaucoup de fournisseurs sont domiciliés dans des juridictions permissives — Panama, îles Caïmans, îles Vierges britanniques — mais exploitent physiquement des serveurs dans des pays aux exigences bien plus strictes.

La bonne question n'est donc pas « ce VPN conserve-t-il des journaux ? », mais « **que se passera-t-il le jour où on lui en demandera ?** ».

06

Masse ou ciblée : deux surveillances

Contre quoi un VPN protège, et contre quoi il ne peut rien

La surveillance de masse consiste à collecter indistinctement les données de tout le monde. C'est le modèle des obligations de conservation imposées aux fournisseurs d'accès, et celui des grands programmes d'interception de trafic.

Contre cette forme-là, un VPN sans journaux établi dans une juridiction protectrice est efficace : il n'y a tout simplement plus rien à collecter chez votre fournisseur d'accès, et rien d'exploitable chez le fournisseur de VPN.

La surveillance ciblée est d'une autre nature. Une autorité judiciaire s'intéresse à une personne précise et adresse une injonction au fournisseur, qui doit s'y conformer. Mais il ne peut transmettre que ce qu'il possède : un fournisseur qui n'enregistre rien ne livrera que ce qu'il commencera éventuellement à enregistrer à partir de la date de l'injonction.

À retenir : un VPN est un outil de confidentialité, pas d'impunité. Il élève très efficacement le coût de la surveillance indiscriminée, et déplace la confiance vers un acteur que vous choisissez. Il ne protège pas une personne spécifiquement visée par une enquête, et ne prétend pas le faire.

07

VPN gratuit : d'où vient l'argent ?

Quand vous ne payez pas, quelqu'un paie à votre place

Faire fonctionner un réseau mondial de serveurs coûte cher. Un VPN illimité, rapide et entièrement gratuit n'existe pas sans contrepartie : la question n'est pas de savoir s'il y a un piège, mais lequel.

Quatre modèles financent les applications gratuites, et un seul est honnête.

La publicité et le profilage. L'application insère des publicités, et surtout observe votre navigation pour constituer un profil revendable. C'est précisément la donnée que vous cherchiez à soustraire à votre fournisseur d'accès.

La revente de votre bande passante. Votre connexion est mise à disposition de tiers, qui sortent sur Internet par votre adresse IP. Le cas d'école reste Hola VPN, dont le réseau d'utilisateurs a été commercialisé en 2015 auprès de clients dont certains s'en sont servis pour mener des attaques.

La collecte assumée. L'application est un instrument de mesure. Onavo, racheté par Facebook, analysait le trafic de ses utilisateurs pour observer l'usage des applications concurrentes ; il a été retiré des magasins d'applications en 2019.

La version limitée d'un service payant. Le fournisseur bride le volume, le débit ou le choix des serveurs, et espère vous convertir. C'est le seul modèle dont le financement est identifiable, et donc le seul recommandable.

Ce que mesurent les études indépendantes

Le sujet est documenté par la recherche académique, et le constat est d'une constance frappante.

En 2016, une étude du CSIRO australien, menée avec l'université de Nouvelle-Galles du Sud et Berkeley, a analysé 283 applications VPN Android : 38 % contenaient un code malveillant ou publicitaire intrusif, et 18 % ne chiffraient tout simplement pas le trafic qu'elles prétendaient protéger.

En février 2026, une étude présentée au symposium NDSS, conduite par des chercheurs des universités du Michigan, du Nouveau-Mexique et de l'IIT Delhi, a porté sur 281 applications totalisant 2,4 milliards d'installations : 22 % transmettaient encore des données en clair, et plus de 80 % contactaient des serveurs publicitaires ou de traçage.

Les signaux d'alerte

Un nom générique, sans éditeur identifiable : ni entreprise, ni pays, donc personne à qui confier son trafic.

Aucune politique de confidentialité lisible, ou une politique qui autorise le partage de données avec des « partenaires ».

Aucun audit indépendant, ou un audit ancien dont le rapport n'est pas public.

Des permissions étrangères à la fonction : contacts, localisation précise, usage des autres applications.

Une note anormalement élevée, portée par des avis génériques et récents.

Les extensions de navigateur présentées comme des VPN gratuits sont un cas à part : ce sont souvent de simples proxys, qui ne couvrent que le trafic du navigateur. Le risque est moindre, la protection aussi.

Si votre budget est nul, préférez la version gratuite bridée d'un éditeur identifiable à une application illimitée dont vous ne savez rien.

08

Les limites : ce qu'un VPN ne protège pas

Ce que le marketing n'écrit jamais en gras

Un livre blanc honnête doit dire où l'outil s'arrête. Un VPN protège le transport de vos données. Il ne protège ni ce que vous publiez, ni ce que vous installez, ni ce que vous acceptez.

Il ne vous rend pas anonyme. Vous restez identifié dès que vous vous connectez à un compte, et le fournisseur de VPN, lui, connaît votre moyen de paiement et votre adresse IP réelle.

Il n'empêche pas le pistage publicitaire. Cookies, empreinte de navigateur, identifiants publicitaires mobiles et comptes connectés continuent de fonctionner à l'identique. Masquer l'adresse IP ne masque pas le reste.

Il ne remplace pas un antivirus. Un fichier malveillant téléchargé dans un tunnel chiffré reste un fichier malveillant.

Il ne protège pas de l'hameçonnage. Si vous saisissez vos identifiants sur un faux site, le tunnel les y achèmine parfaitement.

Il ne protège pas votre appareil. Un téléphone compromis expose vos données avant même qu'elles entrent dans le tunnel.

Il n'est pas neutre en performance. Le chiffrement et le détour par un serveur distant coûtent du débit et de la latence.

En résumé : le VPN traite un problème précis — la visibilité de votre trafic par les intermédiaires réseau — et le traite bien. Attendre de lui une confidentialité globale, c'est se tromper d'outil.

Checklist : choisir un VPN

Onze points à vérifier avant de s'abonner

- [ ] **Éditeur identifiable : raison sociale, siège, dirigeants**
- [ ] **Juridiction connue, distincte du seul pays d'hébergement**
- [ ] **Politique no-logs explicite, datée et lisible**
- [ ] **Audit indépendant publié, récent et renouvelé**
- [ ] **Modèle économique clair : vous payez, ou vous savez qui paie**
- [ ] **Protection contre les fuites DNS et IPv6 par défaut**
- [ ] **Kill switch : coupure du trafic si le tunnel tombe**
- [ ] **Protocoles modernes (WireGuard, OpenVPN), jamais PPTP**
- [ ] **Résolution DNS assurée par le fournisseur, dans le tunnel**
- [ ] **Aucune permission mobile étrangère à la fonction VPN**
- [ ] **Rapport de transparence et réquisitions publiés**

Conclusion

Déplacer la confiance, en connaissance de cause

Un VPN ne fait pas disparaître l'observateur : il le remplace. Votre fournisseur d'accès cesse de voir votre activité, et le fournisseur de VPN prend sa place. Tout le bénéfice de l'opération tient donc à une seule question : cet acteur mérite-t-il davantage votre confiance que le précédent ?

Trois éléments permettent d'y répondre sans être technicien : un éditeur identifiable, une politique de journalisation auditée, et une juridiction qui rend cette politique tenable. Un service gratuit qui ne remplit aucune de ces trois conditions ne vous protège pas — il change simplement qui exploite vos données.

C'est ce que ce document visait à vous donner : de quoi choisir, et de quoi comprendre ce que vous choisissez.

Ce livre blanc a été rédigé par les équipes de ChallengeMyProject.

David Patiashvili

Fondateur, président & CTPO

E-mail :
david.patiashvili
@challengemyproject.com

Téléphone :
+ 33 (7) 69 40 60 43

Visio / RDV :
challengemyproject.com

David Patiashvili
Fondateur | Directeur technique

+33 (0)7 69 40 60 43
david.patiashvili@challengemyproject.com