POURQUOI UTILISER ET SOUTENIR LES INFRA-STRUCTURES AUTONOMES

FAUT PAS BOIRE LE KOOL-AID MAUVE

montréal 2024

C'est à la fin des années 1990 que l'accès à Internet s'est démocratisé. Le mouvement altermondialiste était alors à son apogée. Beaucoup de militant·e·s ont vu en cette technologie, beaucoup plus décentralisée à ce moment-là, une occasion de communiquer plus facilement, et plus rapidement, entre militant·e·s. Une façon de diffuser des idées plus largement, aussi.

Malheureusement, déjà à l'époque, il y avait peu de services de communications gratuits. Ceux qui l'étaient appartenaient déjà à de grandes corporations qui ne conservaient pas les données de façon sécuritaire. Elles ne respectaient pas la vie privée de ses utilisateur·rices. C'est dans ce contexte que sont nés différents collectifs anarchistes d'informatique à travers le monde. Principalement issus de différents mouvements sociaux et composés de membres ayant différentes compétences (en informatique, mais aussi en rédaction, en graphisme, etc), ces collectifs ont débuté en offrant des services d'hébergement de courriels, de listes de courriels et de sites Web sécuritaires, respectant, surtout, la vie privée de ses utilisateur·rices. Avec les années, les offres de services ont évolué pour accommoder les nouveaux besoins des militant·e·s.

Aujourd'hui, plus de 20 ans plus tard, la majorité de ces collectifs sont toujours actifs et continuent d'offrir des services à des milliers de militant·e·s à travers le monde. Nous avons toutefois l'impression que la nouvelle génération militante accorde moins d'importance à la création et au maintien d'infrastructures autonomes. Se faisant, iels semblent de plus en plus utiliser des services corporatifs ayant comme seul objectif la recherche de profit. Pas d'offrir des outils pour créer un monde meilleur ou, à tout le moins, de permettre aux gens de foutre le bordel en toute sécurité.

Comme à la fin des années 1990 et au début des années 2000, nous voyons beaucoup de militant·e·s jeunes et moins jeunes utiliser des fournisseurs de services corporatifs pour communiquer dans le cadre de différents types d'organisations politiques. Dans les dernières années, en plus de l'habituel Gmail, nous avons pu voir l'émergence de services soi-disant sécuritaires, comme Proton, par exemple.

Nous tenons à rappeler que Proton a fourni, en 2021, l'adresse IP d'un militant de Youth for Climate à la police française. Il a par la suite pu être identifié et arrêté. À l'époque, les militant·e·s écologistes de Youth for Climate s'opposaient à l'embourgeoisement et aux spéculateur·rice·s immobilier·ière·s. Iels ont squatté et occupé des espaces. Plusieurs militant·e·s d'ici pourraient se reconnaître dans leur lutte.

Proton a ensuite fourni, en 2024, l'adresse courriel de récupération, liée à un compte iCloud, d'un de ses utilisateur·rices à la police espagnole. Cela a permis, encore une fois, de l'identifier et de procéder à son arrestation. L'utilisateur·rice était membre présumé·e de l'organisation indépendantiste catalane, Tsunami Démocratique.

Dans la foulée, Proton a rappelé que l'entreprise n'exige pas d'adresse de récupération. L'utilisateurice l'avait ajouté de son propre chef. L'entreprise a également affirmé que le contenu des courriels, des pièces jointes et des fichiers sont chiffrés et ne peuvent pas être lus. C'est bien beau, mais si cela n'empêche pas que les gens se fassent arrêter ou, pire, finissent en prison, cela ne change rien. Bien des collectifs autonomes d'informatique offrent la possibilité de définir une adresse de récupération tout en la conservant de façon sécuritaire, c'est-à-dire qu'elle ne puisse pas être fournie aux forces de l'ordre.

Proton se fait toujours un point d'honneur à mentionner que ses services offrent la confidentialité. Ce qu'il ne faut pas oublier, ici, est que Proton fournit la « confidentialité par défaut », et non pas l'anonymat par défaut.

Proton, qui se présente comme « le plus grand service de messagerie sécurisée au monde », prétend être sécuritaire « grâce » aux lois suisses, mais en théorie (ou plutôt en réalité) « [des] informations peuvent être demandées par les autorités suisses dans les cas de terrorisme, et cette décision est généralement prise par l'Office fédéral de la justice suisse. » Une compagnie ne peut pas flancher dans ce cas-là.

Dans les faits, ce qui permet de déterminer si un fournisseur de services est sécuritaire, c'est la quantité de données permettant à l'État d'identifier une personne ou non. À ce niveau, de nombreux services de communications autonomes ont fait leurs preuves. Riseup est en un, mais il en existe un tas d'autres, dont Disroot, Systemli, Immerda, Autistici/Inventati ou encore Espora. Vous pouvez consulter https://riseup.net/radical-servers pour une liste plus complète.

C'est pourquoi nous pensons que les militant·e·s, peu importe le type de travail politique dans lequel iels sont impliqué·e·s, devraient utiliser des services de communications hébergés par des collectifs issus des mêmes milieux qu'elleux. C'est très important pour la sécurité des militant·e·s et de leurs communautés. Ce l'est aussi pour les collectifs eux-mêmes. Plus un collectif a d'utilisateur·ice·s, plus il sera capable de maintenir ses services. Il sera mieux outillé pour offrir de l'aide à ses différent·e·s utilisateur·rices, aussi.

Il faut garder à l'esprit qu'un collectif d'informatique est comme n'importe quel autre projet politique ; plus sa communauté est grande, et plus elle s'enracine dans les différentes sphères de la société. Il devient alors difficile pour l'Etat de l'attaquer.

Finalement, nous pensons qu'il faut soutenir les différents projets collectifs des communautés militantes : les infoshops, les centres sociaux ou de sports de combat et les infrastructures plus abstraites comme les services de communications ou d'hébergement Web. Ce sont ces infrastructures qui font en sorte que les communautés militantes n'ont pas toujours à recommencer le travail à zéro. Les infrastructures autonomes sont importantes pour maintenir des mouvements de résistance plus forts d'une lutte à l'autre. Elles permettent aux réseaux militants et à ses communautés de subsister.

Nous vivons encore tristement dans un monde capitaliste où l'argent est nécessaire pour maintenir des infrastructures. Il faut donc continuer de soutenir les projets collectifs de toutes les façons possibles, mais aussi monétairement parlant. Que celleux capables de donner un peu de sous, ne serait-ce qu'un 5-10 $ / mois aux 4-5 projets qui facilitent leur organisation politique, puissent le faire. Il est aussi souhaitable que les personnes capables d'organiser un spectacle ou un party de financement, sérigraphier une batch de t-shirts ou préparer de la bouffe avec des ami·e·s pour un évènement-bénéfice, puissent le faire. Ce sont toutes de très bonnes choses à faire pour permettre aux communautés militantes de rester vibrantes.


AS-TU UNE ADRESSE ★RISEUP?
DEHORS GILLES LOGI
AUX CONTENE
J'AI PROTON.
(SOUPIR...)
RISEUP N'A MÊME PAS UNE APP.
UNE NUIT
DÉSARMEMENT, MON AMOUR!
SNAPPITY SNAP!
LE LENDEMAIN
COMMUNIQUÉ. CETTE NUIT DU 3 MARS, 3 ENGINS DE CHANTIER FURENT DÉSARMÉS
TAP TAP
HA, HA. ÇA NOUS A PRIS 20 MINUTES.
QUELQUES MOIS PLUS TARD...
TOC. TOC. TOC.
?
BLAM!
C'EST LA POLICE!
DING.
SUPER ACTION. TU NOUS REJOINS AU PARC?
"POUAN" POUAN
POLICE
POLICE

WHY USE & SUPPORT AUTONOMOUS INFRASTRUCTURES

DON'T DRINK THE PURPLE KOOL-AID

montréal 2024

The popularization of the Internet began in the late 1990s. The anti-globalization movement was at its height. Many activists saw in this technology, more decentralized at the time, an opportunity to communicate more easily and rapidly between activists. It was also a way of spreading ideas more widely.

Unfortunately, even back then, there weren't many free online communication services. Those that did exist belonged to big corporations that didn't store data securely and didn't respect their users' privacy. This is why many anarchist tech collectives have sprung up around the world. Coming from different social movements and made up of members with different skills (in computing, but also in writing, graphic design, etc.), these collectives began by offering secure e-mail hosting, e-mail lists and websites, respecting, above all, the privacy of its users. Over the years, these services have evolved to meet the changing needs of activists.

Over 20 years later, the majority of these collectives are still active and continue to provide services to thousands of activists around the world. However, we find that today's activists attach less and less importance to creating and maintaining autonomous infrastructures. We have a feeling that activists are once again using corporate services whose only goal is to make a profit. Not to offer tools to create a better world or, at the very least, to enable people to do direct action in total safety.

As in the late 1990s and early 2000s, we see many activists of all ages using corporate service providers to communicate across different types of political organizations. In recent years, in addition to the usual Gmail, we've seen the explosion of so-called secure communication, like Proton, for example.

We'd like to remind you that Proton provided in 2021 the IP address of a Youth for Climate activist to the French police. He was then identified and arrested. At the time, radical environmentalists from Youth for Climate were fighting against gentrification and real estate speculation. They squatted and occupied spaces. A lot of current's activists can identify with their struggle.

In 2024, Proton then provided the recovery email address, linked to an iCloud account, of one of its users to the Spanish police. Once again, this enabled the user to be identified and arrested. The user was a suspected member of the Catalan pro-independence organization, Tsunami Democràtic.

Following this story, Proton reiterated that the company does not require a recovery address. The user had added it on her own initiative. The company also asserted that the contents of e-mails, attachments and files are encrypted and cannot be read. Well, that's nice, but if it doesn't prevent people from getting arrested or, worse, ending up in jail, it doesn't change a thing. Many autonomous tech collectives offer the possibility of defining a recovery address while keeping it secure, i.e. so that it cannot be provided to the state.

To sum up, we believe in supporting the various collective projects of activist communities: infoshops, social or combat sports centers, and more abstract infrastructures such as communication tools or web hosting. It's these infrastructures that ensure that activist communities don't always have to start from scratch. Autonomous infrastructures are important for maintaining stronger resistance movements from one struggle to the next. They enable activist networks and their communities to survive.

Sadly, we still live in a capitalist world where money is needed to maintain infrastructures. So we must continue to support collective projects in any way we can, even monetarily. People who are able to give money, even if it's only $5-10/month to 4-5 projects that that help their political organization, should do so. People who can organize a show or a fund-raising party, silk-screen a batch of t-shirts or cook food with friends for an event, should also be able to do so. These are all great things to do to keep activist communities vibrant.


DO YOU HAVE A RISEUP ACCOUNT?
DEHORS GILLES LOGI
I HAVE PROTON.
(SIGH...)
RISEUP DOESN'T HAVE AN APP.
ONE NIGHT
♪ WORKIN' ON OUR NIGHT MOVES ♪
SNAPPITY SNAP!
THE NEXT DAY
PRESS RELEASE. ON THE NIGHT OF MARCH 4TH, 3 CONSTRUCTION MACHINES WERE DISARMED...
TAP TAP
HA, HA. IT TOOK US AROUND 20 MINUTES.
A FEW MONTHS LATER...
TOC. TOC. TOC.
?
BLAM!
THIS IS THE POLICE!
DING.
GREAT ACTION. MEET US AT THE PARK?
"POUAN POUAN"
POLICE
POLICE