Messagerie instantanée et autodéfense informatique

En terme de vie privée et de sûreté, communiquer non-publiquement n'est pas anodin. En effet, le contenu des échanges n'est pas destiné à n'importe qui et on ne voudra que certaines personnes (individuelles ou morales) y aient accès, les méta-données (qui communique avec qui, à quelle fréquence, quand, etc.) révèlent aussi beaucoup de choses, dépendre d'un point central est problématique (il pourrait disparaitre, il peut collecter un certain nombre d'informations d'une manière concentrée, etc.), le ou les intermédiaires peuvent trafiquer les messages, etc.

Les moyens utilisés pour communiquer ne sont donc pas à négliger. Nous proposons ci-dessous une liste non-exhaustive de messageries instantanées, pour aider à s'y retrouver vis-à-vis de la vie privée et de sûreté dans ce domaine.

- ☹ Mauvais (privateur ☹, centralisé ☹, à la merci du profit et des États ☹)
  - Facebook : Messenger et WhatsApp
  - Microsoft : Skype
  - Google : Hangouts
  - Discord, Slack, Snapchat
- ☺ Plutôt bon
  - **Signal** (libre ☺, centralisé ☹, chiffrement ☺, dépend d'une organisation 😐)
  - **Silence** (libre ☺, basé sur le MMS 😐, chiffrement ☺, F-Droid ☺)
  - **Mattermost** (libre ☺, pas de fédéralisme 😐, pas de chiffrement de bout-en-bout 😐)
  - **Rocket.Chat** (libre ☺, pas de fédéralisme 😐, pas de chiffrement de bout-en-bout 😐)
- 😀 Très bon (libre ☺, fédéré ☺, chiffrement ☺)
  - **XMPP** / Jabber + **OMEMO** (même chiffrement que Signal ☺)
    - Gajim (GNU/Linux, *BSD, macOS, Windows),
    - Conversations (Android, disponible via F-Droid)
    - Dino (GNU/Linux, FreeBSD),
    - Monal (iOS et macOS) et Siskim IM (iOS)
  - **SIP** + **TLS** + **zRTP**
    - Linphone (GNU/Linux, *BSD, Android, macOS, Windows, iOS)
    - Jitsi (GNU/Linux, *BSD, Windows)
  - **Tox** (GNU/Linux, *BSD, macOS, Windows), Antox (Android), Antidote (iOS)
  - **Jami** (GNU/Linux, *BSD, Android, macOS, Windows)

Pour aller plus loin :

- `https://prism-break.org/fr/all/#instant-messaging`
- Chiffrement de messagerie quasi instantanée : à quel protocole se vouer ? (ANSSI, 2017)