Protégez vos communications mobiles avec Telegram

Mai 2019 – LePoissonLibre - CC-By-Sa

Messagerie instantannée

I. La messagerie instantanée

- **Principe**
  - S’échanger des messages sous forme de conversations
  - À deux ou en groupe
  - Interactivité forte à rapprocher du SMS
  - Un usage différent du mail

I. La messagerie instantanée

- **Histoire**
  - IRC : 1988
  - ICQ : 1996
  - Jabber : 1998
  - MSN : 1999

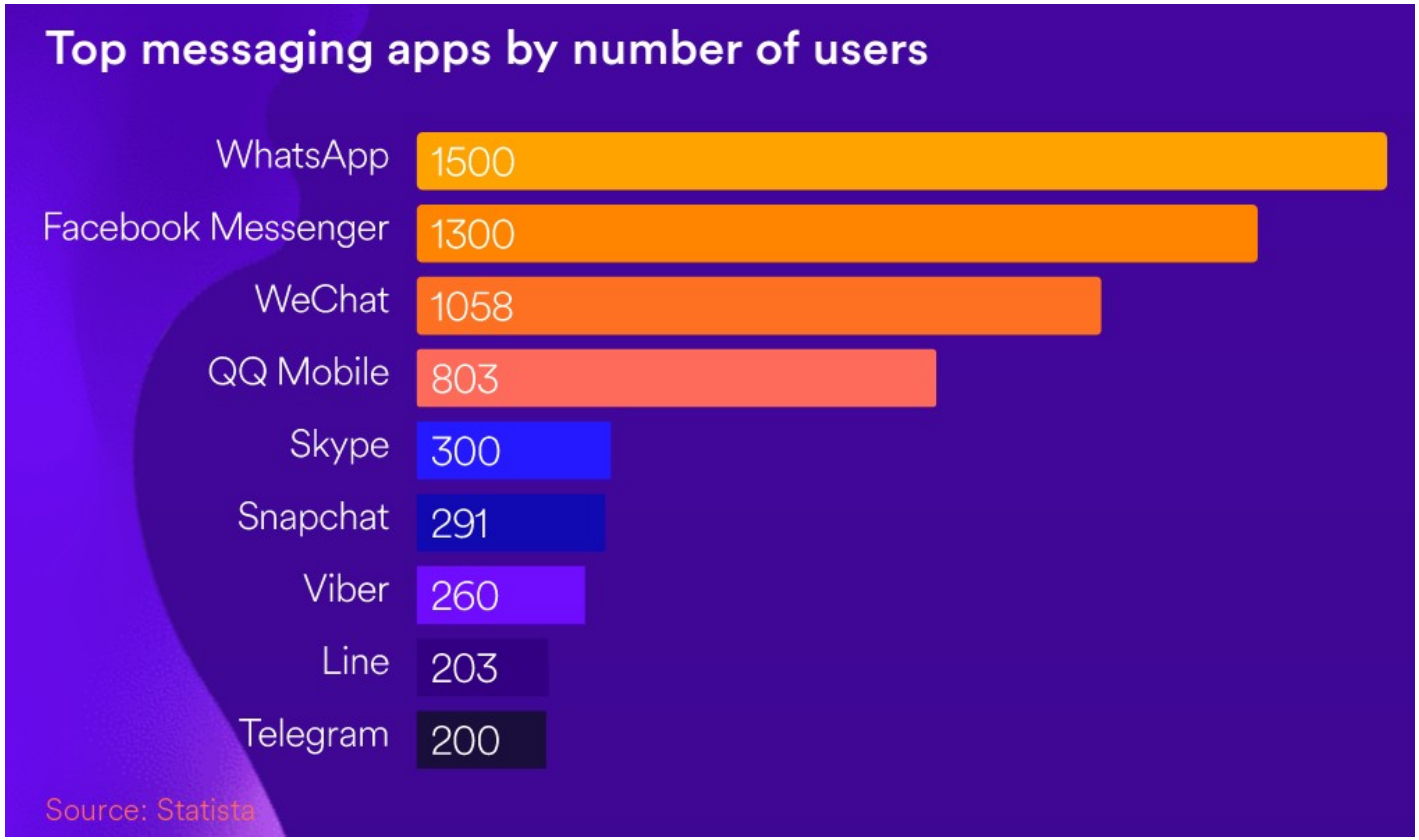
Soudain, le smartphone

WhatsApp : 2009

Facebook Messenger : 2014

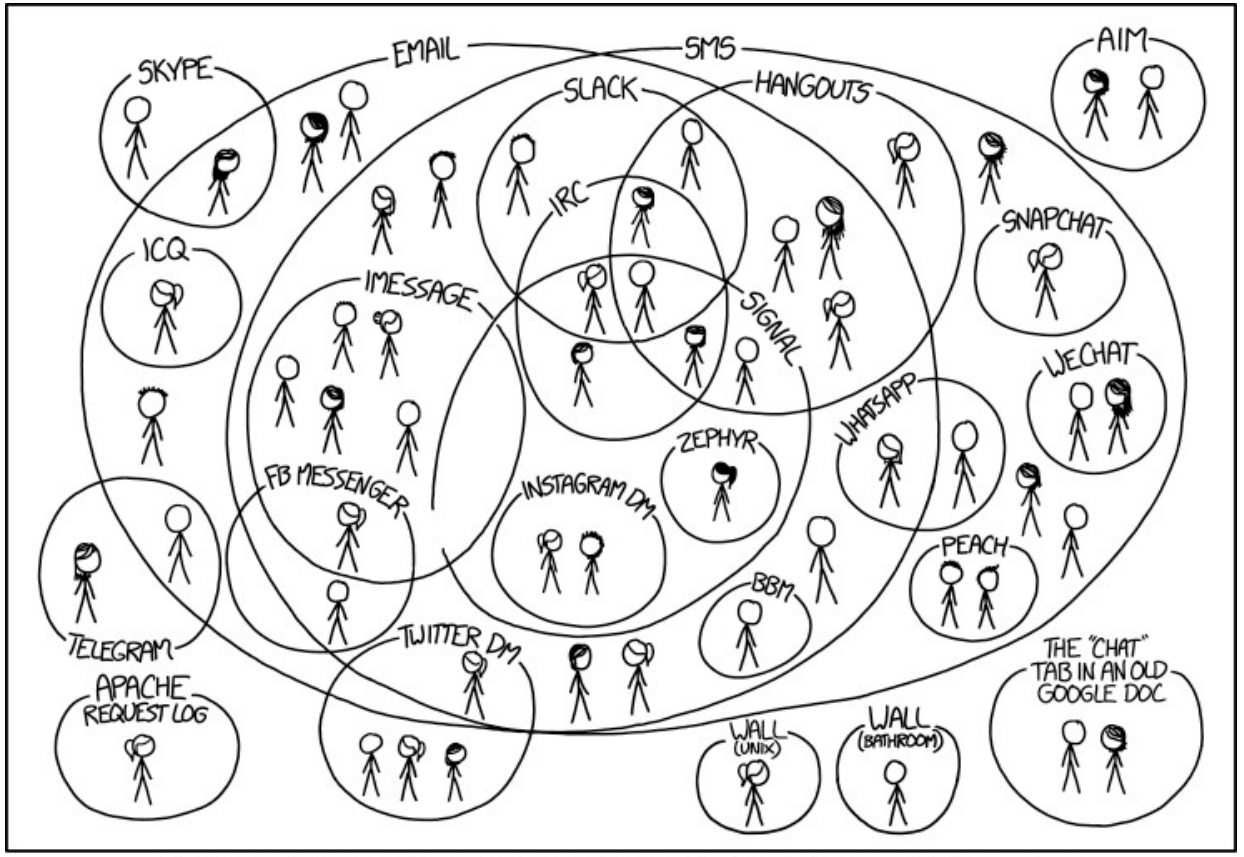
I. La messagerie instantanée

- **Aujourd'hui**



I. La messagerie instantanée

- **Effet de réseau**



I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.

I. La messagerie instantanée

- **Traitement des données personnelles**
  - La CNIL met en demeure WhatsApp pour transfert illégal de données personnelles https://www.lesechos.fr/2017/12/la-cnil-met-en-demeure-whatsapp-pour-transfert-illegal-de-donnees-personnelles-190038#1vIZFtDH3tO8Hrm8.99
  - Facebook scanne vos conversations Messenger https://www.clubic.com/internet/facebook/actualite-843096-facebook-lit-conversations-messenger.html

- **Problèmes de sécurité**
  - WhatsApp : une faille exploitée à des fins d'espionnage https://www.numerama.com/tech/512797-mettez-a-jour-whatsapp-tout-de-suite-pour-corriger-une-faille-exploitee-a-des-fins-despionnage.html
  - Facebook a conservé des centaines de millions de mots de passe de manière non sécurisée https://www.lemonde.fr/pixels/article/2019/03/21/facebook-a-conserve-des-centaines-de-millions-de-mots-de-passe-de-maniere-non-securisee_5439366_4408996.html
  - WhatsApp : des chercheurs découvrent un défaut de sécurité dans les discussions de groupe https://www.lemonde.fr/pixels/article/2018/01/11/whatsapp-des-chercheurs-decouvrent-un-defaut-de-securite-dans-les-discussions-de-groupe_5240314_4408996.html
  - Facebook a diffusé en mode public les conversations privées de 14 millions de ses membres https://www.latribune.fr/technos-medias/internet/bug-facebook-a-diffuse-en-mode-public-les-conversations-privees-de-14-millions-de-ses-membres-781146.html

Vie privée

II. Vie privée

- **Chiffrement**
  - Rendre illisible un message pour qui n’a pas le droit d’y accéder

Un algorithme : la façon dont on rend illisible

Des clés : pour chaque personne, à fournir à l’algorithme

  - Exemple : le code de César, décalage dans l’alphabet
    - BONJOUR → CPOKOVS
    - Clé : 1

II. Vie privée

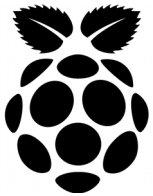
- **Chiffrement classique**
  - Les intermédiaires ont accès aux messages
    - Exemple : le mail

- **Chiffrement bout-en-bout**
  - Aucun intermédiaire n’a accès aux messages
  - Mais la synchronisation plus difficile
  - Basé sur un système de clé publique, demande vérification d’identité
    - Car la phase la plus critique est l’établissement de la communication, où une interception est problématique

II. Vie privée

- **Client – Serveur**
  - Client : l'application, le logiciel qui permet d'accéder au service


  - Serveur : l'intermédiaire qui transmet (et stocke parfois) les messages

II. Vie privée

- **Réseau centralisé**
  - Un seul et unique fournisseur de service
    - Facebook
    - Youtube
    - ...

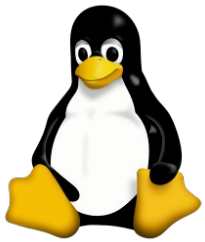
- **Réseau décentralisé**
  - On peut choisir son fournisseur
    - Mail : Orange, Gmail, Outlook, Net-Courrier..
    - Mastodon : Framapiaf, Mamot...
  - Fédération : communiquer entre serveurs
    - Via une adresse : utilisateur@fournisseur

II. Vie privée

- **Logiciel libre**
  - 4 libertés :
    - Exécuter
    - Étudier
    - Redistribuer
    - Améliorer
  - Code source disponible
    - Relisible par tous
    - Permet de repérer les portes dérobées et failles
  - Souvent communautaire
    - Pas de ciblage publicitaire
    - Pas d’utilisation commerciale des données







II. Vie privée

- **F-Droid : pour les utilisateurs Android**
  - Même principe que Google Play
  - Seulement des applications libres
  - f-droid.org
  - Critères strictes pour y figurer
  - Fourni certaines application avec moins de pisteurs à l'intérieur : Firefox, Telegram...

Telegram

III. Telegram

- **Créé en 2013**
  - Disponible sur tous systèmes confondus
  - Vraiment accessible à tous
  - Rapide et léger

- **N’est pas parfait (cf plus loin)**
  - Mais a l’avantage de contrer l’effet de réseau
    - Une base d’utilisateurs déjà grande
    - Des fonctionnalités modernes

III. Telegram

- **Essayons ensemble !**
  - Installez Telegram sur n’importe quel appareil
  - Ajoutez vous un nom d’utilisateur
    - Est utile pour identifier une personne
      - Commence par un @
    - Paramètres > Nom d’utilisateur
  - Débutez une conversation avec moi
    - @linkTheFish
  - Créons un groupe !

III. Telegram

- **Échange classique (« cloud »)**
  - Non bout-en-bout
    - Le secret est partagé avec Telegram
    - Synchronisation entre appareils
  - À deux ou en groupe
  - Des groupes très très grands
    - Avec des fonctions d'administration avancées
      - Admin
      - Épingler des messages
      - Sondages anonymes

III. Telegram

- **Échange secret**
  - Bout-en-bout
    - Personne à part vous et votre correspondant n’a accès
    - Pas de synchronisation
  - Seulement à deux

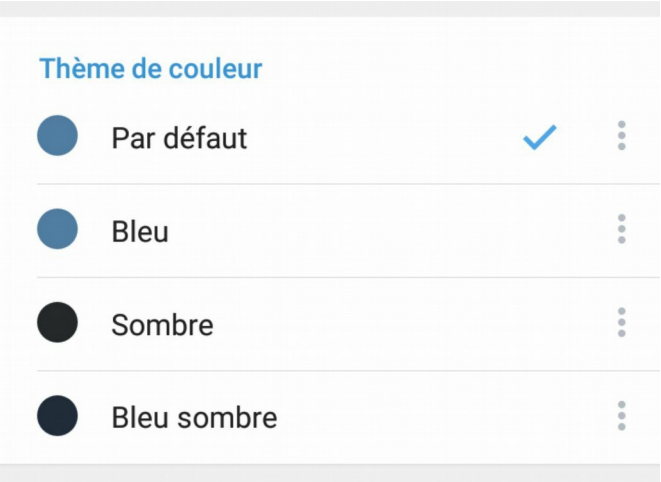
  - Délai d’autodestruction
  - Vérification de la clé de chiffrement par image
  - Interdiction des captures d’écran sur Android

III. Telegram

- **Canaux**
  - Diffusion d’informations par une personne ou un groupe personnes
    - @ISISwatch
    - @durov
    - @JLMelenchon
    - @francoisruffin
    - @enmarchefr
    - @elysee
    - @LeMonde_et_Liberation
    - @LeFigaroFr
    - …

III. Telegram

- **Thèmes**
  - Tous les clients sont complètement personnalisables
  - Paramètres > Paramètres des échanges
  - Canaux intéressants :
    - @AndroidThemes
    - @themes
    - @LinebeckThemes
    - @DMJ_Themes



III. Telegram

- **Réglages de vie privée**
  - Paramètres > Confidentialité et Sécurité
  - Auto-destruction de compte
  - Désactiver la synchronisation des contacts
  - Suppression des contacts synchronisés

- **Réglages d’économie de données**
  - Données et stockage

III. Telegram

- **Lecteur de musique intégré**
  - Shuffle, dans l’odre, en arrière-plan…
  - ogg, mp3, flac…
  - Canal @cctracks pour une démo

- **Gestion facile des documents**
  - Classés par catégorie pour chaque conversation

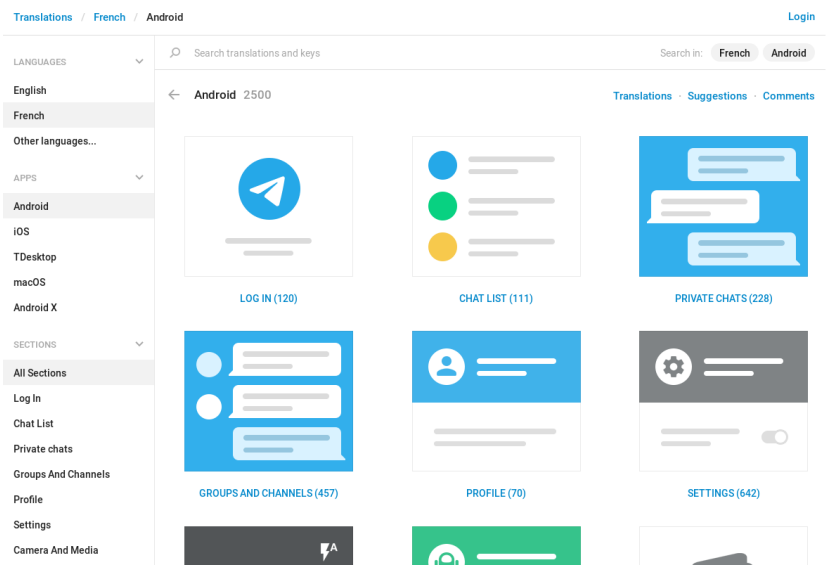
III. Telegram

- **Appel audios**
  - Chiffrés de bout-en-bout
  - Vérifiables par simple comparaison d’émojis
  - Seulement à deux pour l’instant

- **Des bots**
  - Comptes gérés par un programme
  - Permette d’effectuer des actions simples
  - Deux catégories :
    - En conversation : nécessite de leur parler
      - @gmailbot
      - @vote
    - En « ligne » : simplement les mentionner en écrivant un message
      - @gif
      - @pic
      - @imdb

III. Telegram

- **Traduction**
  - Collaborative
  - Pour chaque client
  - En ligne : translations.telegram.org



III. Telegram

- **Chat avec soi-même**
  - Pour prendre des notes
  - Sauvegarder des documents
  - De la musique

- **En vrac**
  - Envoi de message audio et vidéo
  - Envoi de localisation

- **Autocollants**
  - Énormément de jeux différents
  - Associés à des émojis

III. Telegram

- **Désavantages**
  - Pas de code source du serveur
  - Développé de façon unilatérale
  - Financement par son fondateur uniquement
  - Stockage illimité : et écologie alors ?
  - Basé sur le numéro de téléphone

Les alternatives

IV. Les alternatives

- **Signal**
  - Code source des clients ET du serveurs
  - Constamment en bout-en-bout
  - Centralisé
  - Dépendance aux services Google pour l’acheminement des messages

IV. Les alternatives

- **Riot**
  - Décentralisé
  - Basé sur le réseau Matrix
  - Complètement bout-en-bout

IV. Les alternatives

- **XMPP**
  - Décentralisé
  - Historique : Jabber
  - LaQuadratureDuNet : jabber.lqdn.fr
  - Pas de synchronisation

Merci !