Comparatif de Sécurité : TeleGuard vs. Olvid, Session, Telegram, Signal et WhatsApp pour les Débutants

1. Résumé Exécutif

Ce rapport compare la sécurité et la confidentialité de six applications de messagerie populaires : TeleGuard, Olvid, Session, Telegram, Signal et WhatsApp. L'objectif est d'aider les utilisateurs débutants, sans connaissances techniques approfondies, à comprendre les différences clés et à choisir l'application qui correspond le mieux à leurs besoins.

Teleguard, en résumé

TeleGuard se présente comme une application de messagerie sécurisée axée sur la protection de la vie privée, développée par l'entreprise suisse Swisscows AG. Cependant, il existe plusieurs préoccupations majeures et raisons pour lesquelles on pourrait envisager d'éviter TeleGuard :

1. **Manque de transparence** : Le code source de TeleGuard est fermé, ce qui signifie que les experts indépendants ne peuvent pas examiner ou vérifier les affirmations de sécurité et de confidentialité faites par l'application. Ce manque de transparence est un inconvénient majeur, car il oblige les utilisateurs à faire confiance aveuglément aux développeurs sans aucune preuve vérifiable.

2. **Absence d'audits de sécurité indépendants** : Il n'existe aucun audit de sécurité indépendant connu pour TeleGuard. Les audits de sécurité sont cruciaux car ils fournissent une revue externe des mesures de sécurité de l'application, aidant à identifier les vulnérabilités et à s'assurer que l'application est sécurisée.

3. **Utilisation d'un protocole de chiffrement non standard** : TeleGuard utilise l'algorithme de chiffrement SALSA20, qui, bien que respecté dans certains contextes, n'est pas un protocole standard pour le chiffrement de bout en bout dans les applications de messagerie. Les détails d'implémentation sur la manière dont SALSA20 est utilisé pour assurer le chiffrement de bout en bout ne sont pas fournis, ce qui rend difficile l'évaluation de la robustesse du chiffrement.

4. **Affirmations contradictoires** : TeleGuard prétend offrir une anonymité totale et ne pas collecter de données utilisateur, y compris les adresses IP. Cependant, il existe des rapports d'utilisateurs sur des comportements inattendus, comme la réapparition de discussions supprimées après une réinstallation, ce qui suggère une certaine forme de stockage ou de liaison de données côté serveur.

5. **Pratiques douteuses** : L'obligation d'acheter un identifiant personnalisé soulève des questions sur la collecte de données et les associations potentielles avec les comptes utilisateurs, malgré les dénégations de l'entreprise. Cette pratique pourrait compromettre les promesses de confidentialité et d'anonymat.

6. **Manque de preuves vérifiables** : Les affirmations fortes de sécurité et de confidentialité faites par TeleGuard ne sont pas soutenues par des preuves vérifiables. Cela rend difficile pour les utilisateurs de faire pleinement confiance à l'application.

7. **Risques potentiels d'une implémentation "maison"** : L'utilisation d'un protocole de chiffrement moins courant et non standard, qui n'a pas été largement validé par la communauté de sécurité, introduit des risques potentiels, surtout si l'implémentation n'a pas été soigneusement vérifiée.

En résumé, bien que TeleGuard fasse des affirmations séduisantes sur la sécurité et la confidentialité, le manque de transparence, d'audits indépendants et de preuves vérifiables, combiné à l'utilisation de protocoles non standard et de pratiques douteuses, en font un choix risqué pour les utilisateurs soucieux de leur vie privée et de leur sécurité.

Principales Conclusions

- **Signal** et **Olvid** sont souvent considérés comme les plus sécurisés globalement. **Signal** offre un chiffrement de bout en bout (E2EE) robuste par défaut pour tous les échanges, collecte très peu de données (métadonnées), est entièrement open source et financé par une fondation à but non lucratif, ce qui inspire confiance[1]. **Olvid** va plus loin en chiffrant également les métadonnées (qui parle à qui) et en utilisant une architecture unique qui ne repose pas sur la confiance dans les serveurs, validée par des certifications françaises (ANSSI) et des experts[2]. Olvid ne nécessite aucun identifiant personnel[3].
- **Session** se distingue par son très haut niveau d'anonymat, ne nécessitant ni numéro de téléphone ni email, et par sa protection avancée des métadonnées grâce à un réseau décentralisé (similaire à Tor)[4]. Cependant, cette architecture peut parfois affecter la vitesse et certaines fonctionnalités sont moins matures[4].
- **WhatsApp**, bien qu'utilisant le même protocole de chiffrement E2EE que Signal par défaut pour les conversations personnelles [5], appartient à Meta (Facebook). Cela soulève des préoccupations majeures car l'application collecte une quantité importante de métadonnées qui sont partagées avec Meta, dont le modèle économique repose sur l'exploitation des données utilisateur[5]. De plus, les sauvegardes des messages dans le cloud ne sont pas chiffrées par défaut[6].
- **Telegram** est très populaire et offre de nombreuses fonctionnalités, mais sa sécurité par défaut est faible : le chiffrement E2EE n'est pas activé pour les discussions normales et est impossible pour les groupes[7]. Il faut utiliser manuellement les "Secret Chats" pour une protection E2EE (limitée aux conversations à deux). Son protocole de chiffrement maison (MTProto) et sa collecte de métadonnées ont été critiqués par des experts[8].

- **TeleGuard** promet un anonymat élevé (pas de numéro de téléphone requis, utilisation d'un ID unique) et des serveurs basés en Suisse[9]. Cependant, l'application manque cruellement de transparence : son code source est fermé et aucun audit de sécurité indépendant n'a été publié[10]. Il est donc impossible de vérifier ses affirmations de sécurité, ce qui représente un risque important. Son protocole de chiffrement (SALSA20) est moins courant pour ce type d'usage[10].

Recommandation Générale pour Novices :

Pour un utilisateur recherchant un bon équilibre entre une sécurité forte et vérifiable, la facilité d'utilisation et une large base d'utilisateurs, **Signal** est souvent le choix le plus recommandé[11]. Pour ceux dont la priorité absolue est la confidentialité maximale et l'anonymat, même au prix de quelques compromis sur la vitesse ou la facilité, **Session** ou **Olvid** sont des options très solides[6]. **WhatsApp** reste pratique en raison de sa popularité, mais implique d'accepter une surveillance significative de ses habitudes par Meta[5]. **Telegram** nécessite une utilisation très prudente (activation systématique des "Secret Chats" pour les conversations sensibles) et comporte des faiblesses structurelles[12]. **TeleGuard** n'apporte pas suffisamment de preuves de sa sécurité pour être recommandé en toute confiance[10].

2. Introduction : Pourquoi la Sécurité des Messageries est Importante

Nos conversations quotidiennes passent de plus en plus par des applications de messagerie sur nos smartphones. Qu'il s'agisse d'échanger des nouvelles avec des proches, de discuter de projets professionnels ou de partager des informations personnelles, nous confions beaucoup de données à ces outils. Mais sont-ils vraiment privés?

Les conversations en ligne peuvent être vulnérables. Sans mesures de sécurité adéquates, vos messages pourraient être interceptés par des pirates, lus par l'entreprise qui fournit l'application, ou exposés lors d'une fuite de données. Il est donc essentiel de choisir une application qui protège efficacement vos échanges.

La protection ne concerne pas seulement le *contenu* de vos messages (ce que vous écrivez). Elle concerne aussi les **métadonnées** : ce sont les informations *autour* de vos messages. Par exemple : qui parle à qui, à quelle heure, depuis quel endroit approximatif (via votre adresse IP), et à quelle fréquence. Ces métadonnées peuvent en dire long sur vos habitudes, vos relations et votre vie privée, même si le contenu exact des messages reste secret.

Ce rapport vise à vous éclairer sur la sécurité de six applications de messagerie : TeleGuard, Olvid, Session, Telegram, Signal et WhatsApp. Nous allons les comparer selon plusieurs critères clés, expliqués simplement, pour vous aider à faire un choix informé.

Termes Clés Simplifiés :

- **Chiffrement de bout en bout (End-to-End Encryption - E2EE)** : C'est comme envoyer une lettre dans une boîte verrouillée. Seuls vous et votre destinataire possédez la clé unique pour l'ouvrir. Personne d'autre – pas même le service postal (l'entreprise derrière l'application) – ne peut lire le contenu de la lettre pendant son transport. C'est la meilleure protection pour le contenu de vos messages.
- **Métadonnées (Metadata)** : Ce sont les informations visibles sur l'enveloppe de votre lettre : nom et adresse de l'expéditeur et du destinataire, date d'envoi, cachet de la poste. Elles ne révèlent pas le contenu de la lettre, mais donnent beaucoup d'informations sur l'échange lui-même. Certaines applications protègent le contenu mais collectent beaucoup de métadonnées.
- **Code Source Ouvert (Open Source)** : Imaginez que les plans de construction de la boîte verrouillée et du service postal soient publics. N'importe qui, en particulier les experts en sécurité, peut vérifier comment l'application est construite, s'assurer qu'elle est solide et qu'il n'y a pas de "portes dérobées" cachées. C'est un gage important de transparence et de confiance.
- **Serveurs Centralisés vs. Décentralisés** :
  - *Centralisé* : Tous les messages (ou les informations sur les messages) passent par un centre de données principal contrôlé par l'entreprise (comme une grande poste centrale). C'est plus simple à gérer mais crée un point unique de contrôle et de vulnérabilité.
  - *Décentralisé* : Les messages transitent par un réseau de plusieurs serveurs (ou "nœuds") indépendants, souvent gérés par la communauté (comme un réseau de petites postes locales). Cela rend la surveillance et la censure plus difficiles, car il n'y a pas de point central.
- **Audit de Sécurité Indépendant** : C'est comme faire passer un contrôle technique approfondi à l'application par une entreprise spécialisée en cybersécurité. Ces experts cherchent activement les failles et les faiblesses. La publication de ces audits renforce la confiance dans la sécurité de l'application.

3. Analyse Détaillée par Application

Examinons maintenant chaque application plus en détail, en nous concentrant sur leur sécurité, leur confidentialité et l'organisation qui les soutient.

3.1 TeleGuard

TeleGuard se présente comme un messager sécurisé axé sur la protection de la vie privée, développé par l'entreprise suisse Swisscows AG[9].

- **Sécurité**
  - *Chiffrement* : TeleGuard affirme utiliser le chiffrement de bout en bout (E2EE) pour tous les messages texte, vocaux, ainsi que pour les appels vocaux et vidéo. L'algorithme mentionné est SALSA20, décrit comme "l'un des meilleurs algorithmes de chiffrement actuellement disponibles"[9]. La connexion aux serveurs utilise HTTPS[9]. SALSA20 est un

chiffrement de flux conçu par Daniel J. Bernstein, reconnu pour sa vitesse[13]. Bien que l'algorithme lui-même soit respecté (la version complète Salsa20/20 résiste bien aux attaques connues [14]), son utilisation pour l'E2EE dans une messagerie est moins standard que d'autres protocoles comme le Signal Protocol. De plus, TeleGuard ne fournit aucun détail technique sur la manière dont SALSA20 est implémenté pour garantir l'E2EE (gestion des clés, authentification, forward secrecy, etc.)[10]. Ce manque d'information rend difficile l'évaluation de la robustesse réelle du chiffrement.

- *Collecte de Métadonnées* : L'application prétend ne collecter aucune donnée utilisateur, y compris l'adresse IP, et ne pas enregistrer les navigateurs ou systèmes d'exploitation utilisés[9]. Les messages seraient supprimés des serveurs immédiatement après leur livraison[9]. Ces affirmations sont très fortes mais sont mises à mal par l'absence de preuves vérifiables. Des utilisateurs ont rapporté des expériences contradictoires, comme la réapparition de discussions supprimées après réinstallation ou la réattribution du même ID, suggérant une forme de stockage ou de liaison de données côté serveur[15]. La politique de confidentialité mentionne la collecte d'e-mail et d'informations de paiement pour des actions sur le *site web* (comme l'achat d'un ID personnalisé [9]), mais affirme que ces données ne sont pas liées à l'activité dans l'application[16].
- *Identifiant et Anonymat* : TeleGuard n'exige ni numéro de téléphone ni adresse e-mail pour utiliser l'application[9]. Chaque utilisateur reçoit un "TeleGuard ID" unique (un numéro à 9 chiffres et un QR code) qui sert d'identifiant pour ajouter des contacts[9]. Il est possible d'acheter un ID personnalisé[9]. L'application revendique un anonymat total[9]. Ne pas lier l'application à un numéro de téléphone est un avantage pour l'anonymat[17]. Cependant, le TeleGuard ID reste un identifiant unique et persistant lié à l'utilisateur[17]. L'achat d'un ID personnalisé soulève des questions sur la collecte de données de paiement et leur potentielle association au compte, malgré les dénégations de l'entreprise[18].
- *Architecture des Serveurs* : Les serveurs sont centralisés et situés dans des centres de données en Suisse[9]. TeleGuard affirme que cette localisation les exempte des lois sur la protection des données de l'UE/USA, tout en étant conforme au RGPD (Règlement Général sur la Protection des Données européen)[9]. La localisation en Suisse est souvent vue comme positive pour la vie privée[19]. Cependant, l'architecture centralisée implique une confiance totale envers l'opérateur (Swisscows AG). L'affirmation d'être conforme au RGPD tout en n'étant pas soumis aux lois de l'UE semble contradictoire[9].
- *Code Source et Audits* : Le code source de TeleGuard n'est pas public (closed source)[10]. Aucun audit de sécurité réalisé par une entreprise indépendante n'a été publié ou même mentionné[10]. C'est un inconvénient majeur. Sans accès au code et sans audits, il est impossible de vérifier de manière indépendante les affirmations de sécurité et de confidentialité de TeleGuard. Les utilisateurs doivent se fier entièrement aux déclarations du développeur.

- **Structure et Modèle Économique**
  - *Organisation* : TeleGuard est un produit de Swisscows AG, une société anonyme suisse[9]. Swisscows AG appartient elle-même à Hulbee AG, également suisse et dirigée par

Andreas Wiebe[19]. Swisscows exploite aussi un moteur de recherche qui se veut respectueux de la vie privée[9].

- *Financement et Gouvernance* : Le financement provient de dons faits à Swisscows, de la vente potentielle d'ID TeleGuard personnalisés, et d'une future version professionnelle de TeleGuard[9]. Le modèle repose sur l'écosystème global de Swisscows[9]. Un financement par dons et services premium est généralement mieux aligné avec la vie privée qu'un modèle publicitaire. Toutefois, la structure d'entreprise privée implique des objectifs commerciaux.

- Évaluation des Affirmations de TeleGuard TeleGuard construit son image sur des promesses très fortes d'anonymat et de sécurité : pas de numéro de téléphone, pas de collecte de métadonnées, serveurs en Suisse, chiffrement solide[9]. Ces promesses sont séduisantes. Cependant, l'absence totale de transparence – code source fermé, aucun audit de sécurité publié – crée une contradiction fondamentale[10]. Les utilisateurs sont invités à faire une confiance aveugle à Swisscows AG, sans aucune preuve vérifiable. C'est un pari risqué dans le domaine de la sécurité, surtout quand on compare avec des alternatives open source et auditées. Les témoignages d'utilisateurs faisant état de comportements inattendus de l'application [15] ne font que renforcer ce scepticisme. De plus, le choix de l'algorithme SALSA20 [9] est inhabituel pour une messagerie E2EE moderne. Les leaders du domaine privilégient des protocoles complets et éprouvés comme le Signal Protocol ou des bibliothèques comme libsodium. Bien que SALSA20 soit un algorithme de chiffrement de flux respecté [13], son implémentation correcte pour l'E2EE (qui va bien au-delà du simple chiffrement) est complexe et n'est absolument pas documentée par TeleGuard[10]. On peut se demander si ce choix technique est justifié ou s'il reflète un manque d'alignement avec les meilleures pratiques reconnues, introduisant un risque potentiel lié à une implémentation "maison" non validée.

3.2 Olvid

Olvid est une application de messagerie développée en France, qui met en avant un modèle de sécurité unique et des garanties cryptographiques fortes[2].

- **Sécurité**
  - *Chiffrement* : Olvid utilise le chiffrement E2EE par défaut pour absolument tous les échanges : messages, pièces jointes (peu importe la taille), appels audio et vidéo (individuels et de groupe dans la version premium)[2]. Chaque message et fichier utilise une clé de chiffrement différente et à usage unique, assurant la confidentialité persistante (Forward Secrecy)[2]. Fait unique, Olvid chiffre également les **métadonnées**, empêchant ainsi même les serveurs Olvid de savoir "qui parle à qui"[2]. Olvid utilise ses propres protocoles cryptographiques, conçus par ses fondateurs cryptologues et validés scientifiquement par des chercheurs externes (Michel Abdalla, CNRS, IACR)[2]. L'application se prépare également à l'ère post-quantique[2]. Le chiffrement des métadonnées est un avantage majeur en termes de confidentialité par rapport à presque toutes les autres messageries.

- *Collecte de Métadonnées* : Olvid affirme ne collecter aucune donnée personnelle et ne laisser aucune trace sur ses serveurs. Grâce au chiffrement des métadonnées et à son architecture, le serveur ne peut techniquement pas savoir qui communique avec qui[2].
- *Identifiant et Anonymat* : L'application ne requiert ni numéro de téléphone, ni adresse e-mail pour fonctionner[3]. L'identité des contacts est établie et vérifiée directement entre les utilisateurs, soit en scannant un QR code, soit via un annuaire d'entreprise sécurisé dans la version payante[3]. Il n'y a pas d'annuaire central d'utilisateurs[6]. Cela offre un très haut niveau d'anonymat. L'ajout de contacts est plus manuel que sur d'autres applications, ce qui peut être perçu comme moins pratique mais renforce la sécurité en évitant les risques liés à la synchronisation des carnets d'adresses.
- *Architecture des Serveurs* : Olvid utilise une architecture révolutionnaire qui ne repose pas sur la confiance accordée aux serveurs ("No trust in servers")[2]. Les serveurs agissent comme de simples relais de messages chiffrés, sans jamais pouvoir accéder ni au contenu, ni aux métadonnées. Même en cas de piratage des serveurs Olvid, les communications resteraient confidentielles et les identités protégées, car la sécurité repose entièrement sur la cryptographie côté client[2]. Des sources tierces mentionnent l'utilisation d'infrastructures cloud comme Amazon Web Services [20], mais le modèle de sécurité d'Olvid est conçu pour rendre cette localisation non pertinente pour la confidentialité des données. Ce modèle est théoriquement supérieur aux architectures centralisées et même décentralisées classiques.
- *Code Source et Audits* : Les applications client Olvid (iOS, Android) sont open source, publiées sous licence AGPLv3[2]. Le code côté serveur reste propriétaire[20]. Olvid est la seule messagerie à ce jour à avoir reçu deux **Certifications de Sécurité de Premier Niveau (CSPN)** délivrées par l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information française), pour ses versions iOS et Android[2]. Les protocoles ont été validés scientifiquement [2] et l'entreprise participe à un programme public de chasse aux bugs (bug bounty)[20]. Cette combinaison (open source client, certifications gouvernementales de haut niveau, validation scientifique, bug bounty) offre un niveau de transparence et d'assurance exceptionnel.

- **Structure et Modèle Économique**
  - *Organisation* : Olvid est développé par Olvid SAS, une société privée française basée à Paris, fondée en 2017/2019 par des experts en cryptographie[20].
  - *Financement et Gouvernance* : Olvid utilise un modèle économique **freemium**. Les fonctionnalités essentielles (messagerie texte E2EE, pièces jointes, groupes, réception d'appels sécurisés) sont gratuites. Des fonctionnalités avancées, principalement destinées aux professionnels et aux entreprises (initier des appels audio/vidéo de groupe, utiliser Olvid sur plusieurs appareils simultanément, console d'administration pour déploiement et gestion centralisée), sont payantes via Olvid Enterprise[3]. Olvid a également reçu des financements d'investisseurs, dont BNP Paribas et Wavestone[21]. Ce modèle freemium, axé sur la valeur ajoutée pour les clients payants, est structurellement aligné avec les promesses de confidentialité. Il n'y a pas d'incitation à exploiter les

données des utilisateurs gratuits pour générer des revenus, contrairement aux modèles basés sur la publicité.

- Évaluation d'Olvid Olvid se positionne comme offrant les garanties de sécurité les plus fortes et les mieux prouvées du marché actuel, grâce notamment au chiffrement des métadonnées, à son modèle sans serveur de confiance, et à ses validations externes crédibles (ANSSI, recherche scientifique, code client open source)[2]. Cet accent mis sur une sécurité mathématiquement démontrable est son principal atout. Cependant, cette excellence a des contreparties potentielles : une base d'utilisateurs plus restreinte que les géants comme WhatsApp ou Telegram, ce qui peut limiter son utilité si vos contacts ne l'utilisent pas (effet réseau), et un processus d'ajout de contact qui demande une action volontaire (échange de QR code), moins immédiat que la synchronisation automatique du carnet d'adresses[6]. Le choix d'Olvid représente donc un arbitrage clair : une sécurité et une confidentialité maximales et vérifiables, en échange d'une popularité et d'une commodité potentiellement moindres. Son modèle économique freemium [3] renforce sa crédibilité en matière de vie privée. En tirant ses revenus des licences professionnelles et des fonctionnalités avancées, Olvid n'a pas besoin de monétiser les données de ses utilisateurs gratuits. Ce modèle économique est donc en parfaite cohérence avec sa mission affichée de protection absolue de la confidentialité, le distinguant des plateformes dont les revenus dépendent intrinsèquement de la collecte de données utilisateur[5].

3.3 Session

Session est une application de messagerie axée sur l'anonymat et la protection des métadonnées, utilisant un réseau décentralisé[4].

- **Sécurité**
  - *Chiffrement* : Session utilise le chiffrement E2EE par défaut pour les messages individuels et de groupe[4]. Il se base sur le "Session Protocol", lui-même construit sur la bibliothèque cryptographique reconnue libsodium[4]. Les appels vocaux et vidéo sont également chiffrés E2EE, mais ils utilisent une connexion directe entre les utilisateurs (peer-to-peer, P2P). Ce mode P2P, contrairement aux messages, ne passe pas par le réseau d'anonymisation et peut donc révéler les adresses IP des participants l'un à l'autre[4]. C'est un compromis important à connaître pour les appels.
  - *Collecte de Métadonnées* : La conception de Session vise à minimiser radicalement la collecte de métadonnées. L'application ne demande ni numéro de téléphone, ni email, ni données de localisation, ni informations sur l'appareil[4]. Son principal atout est l'utilisation d'un réseau décentralisé de serveurs ("Service Nodes") et d'un système de **routage en oignon** ("onion routing"), similaire à celui de Tor[4]. Ce système fait transiter les messages par plusieurs nœuds intermédiaires, de sorte qu'aucun nœud unique ne connaît à la fois l'expéditeur et le destinataire. Cela permet de masquer l'adresse IP de l'utilisateur et de protéger le "graphe social" (qui communique avec qui)[4]. C'est une protection des métadonnées supérieure à celle des messageries centralisées.

- *Identifiant et Anonymat* : Session offre un très haut niveau d'anonymat. Aucun numéro de téléphone ou email n'est requis pour créer un compte[4]. L'identifiant est un "Session ID", une longue chaîne de caractères générée aléatoirement[22]. Les utilisateurs choisissent un nom d'affichage qui peut être un pseudonyme[4]. Pour sauvegarder et restaurer un compte (par exemple, en changeant de téléphone), l'utilisateur doit impérativement conserver une **phrase de récupération** (recovery phrase) secrète[4]. La sécurité du compte repose entièrement sur la bonne gestion de cette phrase par l'utilisateur.
- *Architecture des Serveurs* : Session utilise une architecture **décentralisée**. Les messages sont relayés par un réseau de "Service Nodes" opérés par une communauté mondiale d'opérateurs[4]. Ce réseau utilise le routage en oignon pour protéger la vie privée[4]. Les messages qui ne peuvent être livrés immédiatement sont stockés temporairement (14 jours maximum) par un groupe de nœuds ("swarm") avant d'être supprimés[4]. Les pièces jointes sont chiffrées et stockées sur un serveur de fichiers dédié (Oxen File Server), mais l'accès à ce serveur est également protégé par le routage en oignon pour masquer l'IP[4]. Cette décentralisation renforce la résistance à la censure et évite un point de défaillance unique[23]. Cependant, elle peut parfois entraîner une certaine latence dans la livraison des messages, notamment si l'option "slow mode" est utilisée[4].
- *Code Source et Audits* : Les applications Session (pour ordinateur, Android et iOS) sont entièrement **open source**[4]. Le réseau de nœuds repose sur le projet Oxen, également open source. Session a fait l'objet d'un audit de sécurité par l'entreprise spécialisée Quarkslab en 2021. L'audit n'a révélé aucune vulnérabilité critique, mais quelques problèmes mineurs qui ont été corrigés[4]. L'open source et cet audit renforcent la confiance, bien qu'un audit plus récent serait bienvenu.

- **Structure et Modèle Économique**
  - *Organisation* : Session était initialement gérée par l'Oxen Privacy Tech Foundation (OPTF), une fondation australienne[24]. Fin 2023/début 2024, face à un environnement réglementaire jugé moins favorable en Australie, la gestion a été transférée à la **Session Technology Foundation** (Session Technology Stiftung), une fondation à but non lucratif basée en **Suisse**[4]. Ce choix de la Suisse vise à bénéficier d'un cadre juridique plus protecteur pour la vie privée et le chiffrement[25].
  - *Financement et Gouvernance* : Le fonctionnement du réseau décentralisé de Session repose sur des incitations économiques liées à une cryptomonnaie. Les opérateurs des Service Nodes doivent immobiliser ("stake") une certaine quantité du token **$SESH** (Session Token) pour participer au réseau et sont récompensés en $SESH pour leur contribution[4]. Ce mécanisme vise à assurer la robustesse et la décentralisation du réseau. Le développement de l'application elle-même est soutenu par la fondation et potentiellement par de futures fonctionnalités premium qui pourraient être achetées en $SESH ou en monnaie traditionnelle[26]. Ce modèle basé sur une cryptomonnaie est unique parmi les applications comparées ici.
- Évaluation de Session Session se distingue par son engagement radical en faveur de l'anonymat et de la protection des métadonnées, grâce à l'absence d'identifiant personnel à l'inscription et à son architecture décentralisée utilisant le routage en oignon[4]. C'est son

avantage comparatif majeur. Cependant, cette approche implique des compromis. La décentralisation et le routage en oignon peuvent parfois réduire la vitesse de livraison des messages par rapport aux systèmes centralisés[11]. Les appels vocaux/vidéo, bien que chiffrés E2EE, ne bénéficient pas de l'anonymisation du réseau et exposent les adresses IP entre les participants[4]. L'anonymat total reporte sur l'utilisateur la responsabilité cruciale de la gestion de sa phrase de récupération[4]. Enfin, le modèle de financement basé sur une cryptomonnaie ($SESH) est innovant mais peut sembler complexe ou volatil pour certains utilisateurs[26]. Le transfert récent de la gestion de Session vers une fondation basée en Suisse [25] est un signal fort et positif. Il aligne la structure juridique de l'application avec sa mission de protection de la vie privée, en choisissant une juridiction réputée pour ses lois favorables[25]. Cela renforce la crédibilité de Session et sa posture de résistance potentielle face aux demandes d'accès aux données, la différenciant des applications basées dans des pays aux lois de surveillance plus étendues. Session représente donc un choix solide pour ceux qui privilégient l'anonymat et la protection des métadonnées avant tout, et qui sont prêts à accepter les compromis associés en termes de performance ou de gestion.

3.4 Telegram

Telegram est une application de messagerie extrêmement populaire, connue pour sa rapidité, son interface et ses nombreuses fonctionnalités, notamment les grands groupes et les canaux de diffusion[11].

- **Sécurité**
  - *Chiffrement* : C'est le point le plus controversé de Telegram. Par défaut, les discussions normales ("Cloud Chats") **ne sont PAS chiffrées de bout en bout (E2EE)**[7]. Elles utilisent un chiffrement entre le client et le serveur, puis entre le serveur et le client. Cela signifie que **Telegram a accès aux clés de chiffrement et peut lire le contenu de ces messages** sur ses serveurs[7]. Pour bénéficier de l'E2EE, il faut **activer manuellement** l'option **"Secret Chat"** pour chaque conversation individuelle[7]. Cette option n'est **pas disponible pour les discussions de groupe**[7]. Les appels vocaux et vidéo semblent, eux, être E2EE par défaut[27]. Telegram utilise son propre protocole de chiffrement, **MTProto**, développé en interne[28]. Ce protocole a été critiqué par de nombreux experts en cryptographie pour son caractère "maison", son manque initial d'audits publics et certaines faiblesses ou choix de conception jugés risqués, bien que des améliorations aient été apportées (MTProto 2.0) et que certaines analyses récentes soient plus nuancées[8]. L'absence d'E2EE par défaut pour la majorité des échanges est un inconvénient majeur par rapport aux autres applications de cette comparaison.
  - *Collecte de Métadonnées* : Telegram collecte un certain nombre de métadonnées, notamment le **numéro de téléphone** utilisé pour l'inscription, les **contacts** de l'utilisateur (si l'autorisation est donnée pour les synchroniser), l'**adresse IP**, les informations sur les **appareils** utilisés, et l'historique des changements de nom d'utilisateur[7]. Ces données peuvent être conservées jusqu'à 12 mois[29]. Telegram affirme ne pas utiliser ces données à des fins publicitaires ciblées [29], mais elles sont néanmoins collectées et stockées, et pourraient être accessibles à Telegram ou divulguées sur demande légale[30].

    - *Identifiant et Anonymat* : Un **numéro de téléphone valide est obligatoire** pour créer un compte Telegram[31]. Ce numéro est l'identifiant principal lié au compte. Il est possible de le cacher dans les paramètres de confidentialité pour qu'il ne soit pas visible par les utilisateurs qui ne sont pas dans vos contacts[7]. On peut également définir un nom d'utilisateur public (@username) qui permet d'être contacté sans partager son numéro. L'anonymat est donc limité par la nécessité de fournir un numéro de téléphone.
    - *Architecture des Serveurs* : Telegram utilise une architecture **centralisée**, avec des serveurs répartis dans différents centres de données à travers le monde pour des raisons de performance et de disponibilité[29]. Les clés de chiffrement des "Cloud Chats" (non-E2EE) sont également stockées par Telegram, bien que de manière distribuée pour des raisons de sécurité interne[29]. Cette centralisation, combinée au chiffrement faible par défaut, donne à Telegram un contrôle et un accès considérables aux données des utilisateurs.
    - *Code Source et Audits* : Les applications client de Telegram (mobiles, bureau, web) sont **open source**, ce qui permet une certaine transparence[11]. Cependant, le **code côté serveur n'est pas open source**[27]. Concernant le protocole MTProto, bien que des analyses académiques aient été menées [32], Telegram ne publie pas régulièrement d'audits de sécurité formels et indépendants de l'ensemble de son système, contrairement à Signal par exemple[27]. Les critiques sur la conception de MTProto persistent[8].
- **Structure et Modèle Économique**
    - *Organisation* : Telegram a été fondé par les frères russes Pavel et Nikolai Durov[33]. Pavel Durov en est le PDG et la figure publique[34]. L'entreprise (souvent enregistrée sous des noms comme Telegram Messenger LLP) est généralement considérée comme basée à Dubaï, bien que sa structure légale exacte reste opaque[7]. Pavel Durov a quitté la Russie après des conflits avec les autorités concernant son précédent réseau social, VKontakte[33].
    - *Financement et Gouvernance* : Historiquement, Telegram a été financé par la fortune personnelle de Pavel Durov[34]. Une tentative majeure de financement via une levée de fonds en cryptomonnaie (ICO pour le projet TON/Gram) a échoué en raison de problèmes réglementaires, notamment avec les autorités américaines[34]. Depuis, Telegram s'est tourné vers la monétisation via un abonnement **Telegram Premium** offrant des fonctionnalités supplémentaires, et une plateforme publicitaire discrète diffusée uniquement dans les grands canaux publics (Telegram affirme que ces publicités sont basées sur le sujet du canal et non sur les données personnelles des utilisateurs)[29]. Ce modèle est potentiellement moins intrusif que la publicité ciblée classique, mais introduit une logique commerciale. L'opacité de la structure de l'entreprise et sa base à Dubaï rendent la gouvernance difficile à évaluer.
- Évaluation de Telegram Telegram illustre un paradoxe : il est extrêmement populaire et souvent perçu comme une "messagerie sécurisée", notamment par ceux qui cherchent une alternative à WhatsApp[8]. Cependant, cette réputation est largement surfaite ou basée sur une mauvaise compréhension de son fonctionnement réel[12]. La réalité technique est que la sécurité par

défaut de Telegram est faible car elle n'utilise pas le chiffrement E2EE pour la majorité des conversations (Cloud Chats et tous les groupes)[7]. L'utilisateur doit activement choisir les "Secret Chats" (limités aux discussions à deux) pour obtenir une protection E2EE[7]. De plus, son protocole maison MTProto, bien qu'amélioré, a fait l'objet de critiques et ne bénéficie pas du même niveau de confiance que des standards comme le Signal Protocol[8]. Enfin, Telegram collecte des métadonnées non négligeables[29]. Sa popularité semble donc davantage due à son interface rapide, ses fonctionnalités riches (grands groupes illimités, canaux, bots, partage de fichiers volumineux) et son image "rebelle" qu'à une sécurité intrinsèquement supérieure à celle de concurrents comme Signal ou Olvid. Le choix de développer et maintenir son propre protocole cryptographique, MTProto, plutôt que d'adopter des standards éprouvés, reste un point fondamental de débat et de risque perçu[8]. Même si MTProto 2.0 est considéré comme plus robuste [30], l'histoire du protocole, les failles passées (même théoriques) et le manque d'audits tiers réguliers et complets [27] maintiennent une incertitude. Pour un utilisateur novice, cela pose la question de la confiance : faut-il se fier à un protocole "maison" moins éprouvé ou privilégier des solutions basées sur des standards largement validés par la communauté internationale des experts en sécurité? Utiliser Telegram pour des communications sensibles sans activer systématiquement les "Secret Chats" revient à faire confiance à Telegram pour ne pas accéder à vos messages.

3.5 Signal

Signal est une application de messagerie largement reconnue pour son engagement fort en faveur de la sécurité et de la confidentialité, développée par une fondation à but non lucratif[1].

- **Sécurité**
  - *Chiffrement* : Signal utilise le **chiffrement E2EE par défaut pour absolument toutes les communications** : messages individuels, messages de groupe, appels audio, appels vidéo, pièces jointes et même les autocollants (stickers)[1]. Il utilise le **Signal Protocol**, un protocole de chiffrement open source considéré comme l'état de l'art en matière de sécurité pour la messagerie[1]. Ce protocole est si respecté qu'il a été adopté et implémenté par d'autres acteurs majeurs comme WhatsApp, Google (pour les messages RCS) et Skype[35]. La robustesse et la fiabilité du chiffrement de Signal sont largement reconnues par les experts.
  - *Collecte de Métadonnées* : Signal est conçu dès le départ pour **collecter le minimum absolu de métadonnées** nécessaires à son fonctionnement[1]. L'application ne stocke pas d'informations sur vos contacts, les groupes auxquels vous appartenez, votre profil, ou avec qui vous communiquez. Les seules informations que Signal admet conserver sur ses serveurs sont techniques : essentiellement, le numéro de téléphone enregistré (stocké sous forme de hash cryptographique), la date de création du compte et la date de la dernière connexion au service[36]. Signal a même prouvé lors de requêtes judiciaires (subpoenas) qu'il ne pouvait fournir quasiment aucune donnée utile sur ses utilisateurs[37]. Des techniques avancées comme "Sealed Sender" sont utilisées pour tenter de masquer l'expéditeur d'un message même aux serveurs de Signal.

    - *Identifiant et Anonymat* : Historiquement, Signal nécessitait un **numéro de téléphone** pour l'inscription, ce qui était son principal point faible en termes d'anonymat[36]. Cependant, Signal a récemment introduit des fonctionnalités majeures pour répondre à cette critique : la possibilité de créer et d'utiliser des **noms d'utilisateur (usernames)** pour être contacté, et la fonction **"Phone Number Privacy"** qui permet de masquer son numéro de téléphone à ses contacts et à Signal lui-même dans la mesure du possible[37]. Bien qu'un numéro de téléphone soit toujours requis pour l'enregistrement initial (pour éviter le spam), il n'est plus nécessaire de le partager pour communiquer. Cela améliore considérablement le potentiel d'anonymat sur Signal.
    - *Architecture des Serveurs* : Signal utilise une architecture **centralisée**, gérée par la Signal Foundation[38]. Cependant, les serveurs sont conçus pour être des relais "ignorants" : grâce au chiffrement E2EE et à la minimisation extrême des métadonnées, ils n'ont pas accès au contenu des communications ni à la plupart des informations contextuelles[36]. Le principal risque lié à la centralisation est donc une éventuelle interruption de service plutôt qu'une violation de la confidentialité via les serveurs.
    - *Code Source et Audits* : Signal est un modèle de transparence : **l'intégralité de son code, à la fois pour les applications client (iOS, Android, Desktop) et pour le code serveur, est open source** et disponible publiquement pour examen[1]. De plus, le protocole et les applications Signal ont fait l'objet de **multiples audits de sécurité indépendants** au fil des années, réalisés par des entreprises de cybersécurité reconnues[27]. Les résultats de ces audits sont souvent discutés publiquement. Cette transparence maximale et ces validations externes répétées inspirent une très grande confiance.
- **Structure et Modèle Économique**
    - *Organisation* : Signal est développé par Signal Messenger LLC, une entité détenue à 100% par la **Signal Technology Foundation**, une **fondation américaine à but non lucratif** (enregistrée sous le statut 501(c)(3))[1]. Elle a été co-fondée par Moxie Marlinspike (le cryptographe à l'origine de Signal) et Brian Acton (co-fondateur de WhatsApp, qui a quitté Facebook/Meta par désaccord sur la vie privée)[35]. L'actuelle présidente est Meredith Whittaker, une défenseure reconnue de la vie privée[35].
    - *Financement et Gouvernance* : Signal est financé **exclusivement par des dons** de ses utilisateurs et des subventions[1]. Brian Acton a fourni un don initial substantiel de 50 millions de dollars pour lancer la fondation[35]. Il n'y a **aucune publicité, aucun investisseur extérieur cherchant un retour financier, et aucune vente de données utilisateur**[1]. La structure à but non lucratif garantit que la mission de protection de la vie privée et de la sécurité prime sur toute considération de profit. La fondation publie ses déclarations financières (Form 990 aux États-Unis), offrant une transparence sur ses revenus et dépenses[37]. Ce modèle est considéré comme le plus aligné avec les objectifs de confidentialité.
- Évaluation de Signal Signal s'est solidement établi comme la référence en matière de messagerie sécurisée E2EE. Son principal atout réside dans la combinaison d'une technologie de chiffrement (le Signal Protocol) reconnue comme l'état de l'art, open source et largement auditée, avec une application qui applique ce chiffrement par défaut à tous les échanges[1]. Le

fait que ce protocole soit adopté par des acteurs majeurs comme WhatsApp et Google témoigne de sa robustesse[35]. La transparence totale de Signal (code client et serveur open source, audits réguliers [37]) et sa structure de financement à but non lucratif via une fondation dédiée à la vie privée [38] renforcent considérablement la confiance. Signal ne se contente pas de promettre la sécurité, il fournit les preuves et les mécanismes pour la vérifier. La critique historique concernant l'obligation d'utiliser un numéro de téléphone, qui limitait l'anonymat, a été largement adressée par l'introduction récente des noms d'utilisateur et de la fonction "Phone Number Privacy"[37]. Cette évolution majeure montre que Signal écoute sa communauté et cherche activement à améliorer la protection de la vie privée au-delà du chiffrement du contenu. Signal réussit de mieux en mieux à offrir un équilibre entre une sécurité de très haut niveau, une confidentialité solide des métadonnées, une transparence exemplaire et une facilité d'utilisation qui lui permet de toucher un public large et pas seulement les experts en sécurité[11].

3.6 WhatsApp

WhatsApp est l'application de messagerie la plus utilisée au monde, appartenant à Meta (anciennement Facebook)[11].

- **Sécurité**
  - *Chiffrement* : WhatsApp utilise le **chiffrement E2EE par défaut** pour la plupart des communications entre utilisateurs individuels : messages texte et vocaux, appels audio et vidéo, photos, vidéos, documents, mises à jour de statut et partage de localisation en direct[5]. L'application utilise une implémentation du **Signal Protocol**, le même protocole robuste que Signal[5]. Cependant, il y a des exceptions importantes : les messages échangés avec des **comptes professionnels** peuvent ne pas être E2EE[11]. Plus critique encore, les **sauvegardes (backups) de l'historique des discussions sur le cloud (Google Drive pour Android, iCloud pour iOS) ne sont PAS chiffrées E2EE par défaut**[6]. Bien qu'une option existe pour activer le chiffrement E2EE des sauvegardes, elle doit être **activée manuellement** par l'utilisateur et nécessite la création d'un mot de passe ou d'une clé spécifique[39]. Sans cette activation manuelle, tout l'historique des messages, bien que chiffré pendant l'échange, devient accessible en clair à Google/Apple ou à quiconque accède à ces comptes cloud.
  - *Collecte de Métadonnées* : C'est le **point faible majeur** de WhatsApp en matière de confidentialité. L'application **collecte une quantité très importante de métadonnées**[5]. Cela inclut : votre numéro de téléphone, les numéros de téléphone de vos contacts (si vous autorisez l'accès au carnet d'adresses), votre nom de profil et photo, des informations sur votre utilisation (quand vous utilisez l'application, quelles fonctionnalités, avec qui vous interagissez le plus fréquemment), des informations techniques sur votre appareil et votre connexion (modèle, OS, niveau de batterie, force du signal, **adresse IP**), votre localisation approximative (déduite de l'IP) ou précise (si vous partagez votre localisation), des informations sur les transactions si vous utilisez les fonctions de paiement, et des données sur vos interactions avec les comptes professionnels[5]. Ces métadonnées sont **partagées avec la société mère, Meta (Facebook)**, et utilisées pour

divers objectifs, notamment l'amélioration des services Meta, la sécurité, et potentiellement pour le ciblage publicitaire sur les autres plateformes de Meta (Facebook, Instagram)[5].

- *Identifiant et Anonymat* : L'utilisation de WhatsApp nécessite **obligatoirement un numéro de téléphone** valide pour l'enregistrement et le fonctionnement[5]. Ce numéro est l'identifiant principal de l'utilisateur et est généralement visible par ses contacts. Il n'y a **aucune possibilité d'anonymat** ni vis-à-vis de WhatsApp/Meta, ni vis-à-vis de ses contacts.
- *Architecture des Serveurs* : WhatsApp utilise une architecture **centralisée**, gérée par Meta[5]. Les serveurs agissent comme des relais pour les messages chiffrés E2EE (ils ne peuvent pas lire le contenu), mais ils collectent, stockent et traitent activement la grande quantité de métadonnées mentionnée ci-dessus[5]. La centralisation chez Meta est une source de préoccupation en raison du modèle économique de l'entreprise[40].
- *Code Source et Audits* : Le code source de l'application WhatsApp est **fermé (closed source)**[41]. Bien que le protocole de chiffrement sous-jacent (Signal Protocol) soit open source, l'implémentation spécifique faite par WhatsApp n'est pas publique, ce qui empêche une vérification indépendante complète[41]. Meta réalise probablement des audits de sécurité internes, mais ne les publie pas de manière transparente comme le font Signal ou Olvid.

- **Structure et Modèle Économique**
  - *Organisation* : WhatsApp Inc. est une **filiale de Meta Platforms, Inc.**, l'un des géants mondiaux de la technologie[5]. Facebook a racheté WhatsApp en 2014 pour la somme colossale de 19 milliards de dollars[40].
  - *Financement et Gouvernance* : L'application WhatsApp est gratuite pour les utilisateurs finaux. Sa valeur pour Meta réside dans son intégration à l'écosystème global de l'entreprise. Les métadonnées collectées par WhatsApp sont utilisées pour **améliorer les autres produits Meta** (comme Facebook et Instagram) et pour **affiner le ciblage publicitaire** sur ces autres plateformes[5]. Meta développe également des **services payants pour les entreprises** via l'API WhatsApp Business, qui leur permet de communiquer avec leurs clients via WhatsApp[39]. Il est important de noter que les fondateurs originaux de WhatsApp, Jan Koum et Brian Acton, ont tous deux quitté Meta/Facebook après l'acquisition, citant des désaccords profonds concernant la stratégie de monétisation et l'affaiblissement de la protection de la vie privée des utilisateurs[35].
- Évaluation de WhatsApp WhatsApp incarne le compromis le plus répandu pour des milliards d'utilisateurs à travers le monde. Il offre d'un côté une sécurité considérée comme bonne pour le contenu des messages personnels, grâce à l'utilisation par défaut du solide Signal Protocol pour le chiffrement E2EE[5]. De l'autre côté, il offre une facilité d'utilisation et une popularité inégalées : il est très probable que la majorité de vos contacts utilisent déjà WhatsApp, ce qui le rend extrêmement pratique[11]. Cependant, ce confort et cette sécurité apparente ont un coût élevé en termes de confidentialité des métadonnées. En utilisant WhatsApp, vous acceptez que Meta (Facebook) collecte une quantité massive d'informations sur vos habitudes

de communication (qui, quand, où, comment) et les utilise à ses propres fins commerciales[5]. Pour un utilisateur novice, le choix est donc clair : privilégier la facilité de connexion avec son réseau existant, ou refuser la surveillance de ses métadonnées par l'un des plus grands collecteurs de données au monde. Un point technique crucial, souvent négligé, concerne les **sauvegardes dans le cloud**. Par défaut, elles ne sont pas chiffrées E2EE[6]. Cela signifie que si vous utilisez la fonction de sauvegarde (très pratique pour ne pas perdre ses messages en changeant de téléphone), tout votre historique de conversation, bien que protégé pendant l'échange initial, devient vulnérable une fois stocké sur les serveurs de Google ou d'Apple. Activer manuellement l'option de **sauvegarde chiffrée E2EE** [39] est une étape **absolument essentielle** pour maintenir un semblant de confidentialité sur le long terme avec WhatsApp. Sans cette action, la protection offerte par le chiffrement E2EE est largement annulée dès la première sauvegarde.

4. Comparaison Systématique

Après avoir examiné chaque application individuellement, comparons-les directement sur les aspects clés de la sécurité et de leur structure.

4.1 Tableau Comparatif : Fonctionnalités de Sécurité

Le tableau suivant résume les caractéristiques de sécurité techniques de chaque application.

Caractéristique	TeleGuard	Olvid	Session	Telegram	
E2EE par Défaut	Revendiqué Oui [9]	Oui [2]	Oui (Messages) [4]	Non (Cloud Chats) / Oui (Secret Chats) [7]	Oui [
Protocole Chiffrement	SALSA20 (Propriétaire/Non standard) [9]	Protocoles custom (Validés) [2]	Session Protocol (Libsodium) [4]	MTProto (Propriétaire, critiqué) [28]	Signa (Star
Chiffrement Métadonnées	Non	Oui [2]	Partiel (Routage Oignon) [4]	Non [29]	Parti avan
Collecte Métadonnées Clés	Revendiqué Non (IP, etc.) [16]	Non (Pas de données perso) [3]	Très faible (Pas de Tél/Email/IP msg) [22]	Oui (Tél, IP, Contacts, Usage) [29]	Très date

Caractéristique	TeleGuard	Olvid	Session	Telegram	
Identifiant Requis	TeleGuard ID [9]	Aucun (Vérification directe) [3]	Session ID [22]	Numéro Tél. [29]	Num masc [36]
Niveau d'Anonymat Possible	Élevé (Revendiqué)	Très Élevé	Très Élevé	Faible/Moyen	Moye user
Architecture Serveurs	Centralisée [9]	Sans Confiance (Relais) [2]	Décentralisée (Service Nodes) [4]	Centralisée [29]	Cent Conf
Localisation Serveurs	Suisse [9]	Non Pertinent (Modèle Crypto)	Globale (Communauté)	Globale (Distribués) [29]	USA
Code Source Client	Fermé [10]	Ouvert (AGPLv3) [42]	Ouvert [23]	Ouvert [11]	Ouve
Code Source Serveur	Fermé	Fermé [20]	Ouvert (Oxen)	Fermé [27]	Ouve
Audits Sécurité Indépendants	Non connus [10]	Oui (ANSSI, Scientifique, Bug Bounty) [2]	Oui (Quarkslab 2021) [4]	Limités / Non réguliers [8]	Oui (Régu
Certifications	Aucune connue	ANSSI CSPN (iOS,	Aucune connue	Aucune connue	Aucu

Ce tableau met en évidence les différences techniques fondamentales. Olvid et Session se distinguent par leur approche de l'anonymat et des métadonnées. Signal brille par son protocole standardisé, sa transparence et son E2EE par défaut. WhatsApp partage le bon protocole de Signal mais échoue sur les métadonnées et la transparence. Telegram est à la traîne sur l'E2EE par défaut et son protocole. TeleGuard fait des promesses sans preuves vérifiables.

4.2 Tableau Comparatif : Structures et Modèles Économiques

La sécurité d'une application ne dépend pas que de sa technologie, mais aussi de qui la contrôle et comment elle gagne de l'argent.

Application	Structure Propriétaire	Juridiction Principale	Modèle Économique / Financement	Transparence (Code, Audits, Finances)	Impact Potentiel sur Vie Privée / Conflit d'Intérêt
TeleGuard	Entreprise Privée (Swisscows AG)	Suisse [19]	Dons, ID premium, Business (futur) [18]	Très Faible (Code fermé, pas d'audits)	Moyen (Objectifs commerciaux inconnus)
Olvid	Entreprise Privée (Olvid SAS)	France [21]	Freemium (Base gratuite, Enterprise payant) [3]	Élevée (Client ouvert, audits ANSSI)	Faible (Modèle aligné avec vie privée)
Session	Fondation (Session Tech Found.)	Suisse [25]	Crypto ($SESH Staking, Premium futur) [4]	Élevée (Code ouvert, audit Quarkslab)	Faible (Fondation, modèle décentralisé)
Telegram	Entreprise Privée (Durov)	Dubaï (?) [7]	Fortune Durov, Premium, Pub (canaux) [29]	Moyenne (Client ouvert, serveur fermé)	Moyen/Élevé (Opacité, collecte métadonnées)
Signal	Fondation (Signal Foundation)	USA [38]	Dons, Subventions [35]	Très Élevée (Tout ouvert, audits, 990)	Très Faible (Non-profit, mission alignée)
WhatsApp	Filiale Tech Géante (Meta)	USA [40]	Écosystème Meta (Données -> Pub), Business API [40]	Très Faible (Code fermé, collecte données)	Très Élevé (Conflit d'intérêt majeur)

Ce tableau montre clairement comment la structure et le financement peuvent influencer la confiance. Signal, avec sa fondation à but non lucratif financée par dons, présente le moins de conflits d'intérêts. Olvid et Session, avec leur modèle freemium ou crypto/fondation en Suisse,

semblent également bien alignés. À l'opposé, WhatsApp, en tant que filiale de Meta dont le cœur de métier est l'exploitation des données, présente un conflit d'intérêt structurel majeur. Telegram et TeleGuard se situent entre les deux, avec une certaine opacité ou des objectifs commerciaux qui pourraient potentiellement primer sur la vie privée.

4.3 Analyse Comparative Détaillée

- **Chiffrement** : Signal, Olvid, Session et WhatsApp (pour les chats perso) offrent l'E2EE par défaut, ce qui est la meilleure pratique. Telegram et TeleGuard sont en retrait, Telegram ne l'offrant qu'en option limitée, et TeleGuard utilisant un protocole non standard et non vérifiable. Olvid se distingue par le chiffrement des métadonnées, offrant une couche de protection supplémentaire.
- **Métadonnées** : C'est un champ de bataille crucial. Olvid et Session sont conçus pour en collecter le moins possible, voire pas du tout pour Olvid. Signal minimise activement leur collecte. TeleGuard prétend ne rien collecter, mais sans preuve. Telegram et surtout WhatsApp en collectent une quantité significative, ce qui constitue leur principal risque pour la vie privée.
- **Anonymat** : Session et Olvid offrent le plus haut niveau d'anonymat en ne requérant aucun identifiant personnel. TeleGuard suit avec son ID spécifique. Signal s'est grandement amélioré avec les noms d'utilisateur masquant le numéro de téléphone. Telegram et WhatsApp, exigeant un numéro de téléphone, offrent le moins d'anonymat.
- **Architecture** : La décentralisation de Session et le modèle sans confiance d'Olvid offrent une meilleure résilience à la censure et aux pannes, et renforcent la protection des métadonnées par rapport aux architectures centralisées de Signal, WhatsApp, Telegram et TeleGuard. Cependant, la centralisation peut permettre une meilleure performance et une synchronisation plus simple.
- **Transparence** : Signal est le champion de la transparence (tout open source, audits réguliers, finances publiques). Olvid (client open source, certifications) et Session (open source, audit) sont également très bons. Telegram est moyen (client ouvert, serveur fermé, audits limités). WhatsApp et TeleGuard sont les moins transparents (code fermé, pas d'audits publics). La transparence est essentielle pour bâtir la confiance en matière de sécurité.
- **Structure et Financement** : Le modèle à but non lucratif de Signal est idéalement aligné avec la protection de la vie privée. Le modèle freemium d'Olvid et celui de Session (fondation/crypto) sont également bien positionnés. Le modèle de Telegram (premium/pub limitée) est acceptable mais moins transparent. Le modèle de WhatsApp est intrinsèquement conflictuel en raison de son appartenance à Meta. Celui de TeleGuard est lié à une entreprise privée dont les motivations exactes restent floues.

5. Évaluation pour les Utilisateurs Novices : Forces et Faiblesses

Pour un utilisateur débutant, voici un résumé simple des avantages et inconvénients de chaque application :

- **TeleGuard**

    - *Forces (promises)* : Permet de discuter sans donner son numéro de téléphone. Basé en Suisse, pays réputé pour la protection des données.
    - *Faiblesses (réelles)* : Aucune preuve de sécurité (code secret, pas de tests indépendants connus). On ne peut pas vérifier si les promesses sont tenues. Fiabilité douteuse.
- **Olvid**
    - *Forces* : Sécurité maximale prouvée (chiffre même "qui parle à qui", certifié par l'État français). Très anonyme (pas besoin de numéro ou d'email).
    - *Faiblesses* : Moins connu (vos amis ne l'utilisent peut-être pas). Ajouter des contacts demande une étape manuelle (scanner un code). Certaines fonctions (appels de groupe) sont payantes.
- **Session**
    - *Forces* : Très anonyme (pas besoin de numéro ou d'email). Protège très bien les informations sur "qui parle à qui" grâce à son réseau spécial.
    - *Faiblesses* : Peut être un peu plus lent que d'autres applications. Les appels sont moins anonymes que les messages. Il faut bien garder sa "phrase de récupération" pour ne pas perdre son compte.
- **Telegram**
    - *Forces* : Très populaire, beaucoup de fonctions amusantes (stickers, grands groupes, chaînes d'info). Rapide et facile à utiliser.
    - *Faiblesses* : **Pas sécurisé par défaut**. La plupart des discussions peuvent être lues par Telegram. Il faut penser à activer les "Secret Chats" (qui ne marchent pas pour les groupes). Collecte des informations sur votre utilisation.
- **Signal**
    - *Forces* : Très sécurisé par défaut (tous les messages et appels sont protégés). Très transparent (code vérifiable, tests indépendants). Géré par une fondation sans but lucratif. De plus en plus populaire. Permet maintenant de cacher son numéro.
    - *Faiblesses* : Demandait un numéro de téléphone (moins un problème maintenant). Peut-être un peu moins de "gadgets" que Telegram.
- **WhatsApp**
    - *Forces* : Utilisé par presque tout le monde, très facile pour rester en contact. Messages et appels personnels bien protégés par défaut.
    - *Faiblesses* : Appartient à Facebook (Meta), qui collecte beaucoup d'informations sur vous (qui vous contactez, quand, etc.) pour ses autres services et la publicité. Les sauvegardes des messages ne sont pas protégées par défaut. Code secret.

Le choix d'une messagerie sécurisée implique souvent de naviguer entre différents pôles : la **sécurité maximale** (qui peut demander plus d'efforts ou être moins répandue, comme Olvid ou Session), la **facilité d'utilisation et la popularité** (qui peuvent cacher des compromis sur la vie privée, comme WhatsApp ou Telegram), et un **équilibre** entre ces aspects (que Signal s'efforce d'atteindre). Il n'existe pas de "meilleure" application universelle, mais plutôt un choix qui dépend de ce qui est le plus important pour *vous*.

6. Compromis et Conclusion

Choisir une application de messagerie implique presque toujours de faire des compromis entre différents aspects.

6.1 Les Compromis Inévitables

- **Sécurité vs. Facilité d'utilisation** : Des mesures de sécurité renforcées, comme l'absence de sauvegarde automatique dans le cloud, la nécessité de vérifier manuellement les contacts ou de gérer une clé de récupération, peuvent rendre l'application un peu moins pratique au quotidien.
- **Confidentialité vs. Fonctionnalités** : Certaines fonctionnalités pratiques, comme la suggestion d'amis basée sur vos contacts ou l'intégration poussée avec d'autres services, reposent souvent sur la collecte de données (métadonnées) qui réduisent votre vie privée. Les très grands groupes ouverts ou les bots peuvent aussi être moins privés par nature.
- **Anonymat vs. Découverte des contacts** : Ne pas utiliser son numéro de téléphone renforce l'anonymat mais rend plus difficile de retrouver automatiquement ses amis qui utilisent déjà l'application.
- **Sécurité vs. "Effet Réseau"** : Une application ultra-sécurisée ne vous sera pas très utile si aucun de vos contacts ne l'utilise. Parfois, une application "suffisamment" sécurisée mais largement adoptée peut être plus pratique.

6.2 Tableau Récapitulatif des Compromis

Ce tableau résume les principaux avantages, inconvénients et compromis de chaque application du point de vue d'un utilisateur novice.

Application	Avantages Clés (Sécurité/Confidentialité)	Inconvénients Clés (Sécurité/Confidentialité)	Compromis M Facilité/Fonctionnal
TeleGuard	Anonymat revendiqué (pas de Tél.), Serveurs Suisse	Manque total de preuves (fermé, pas d'audits), Fiabilité incertaine	Promesses fortes ma vérifiables vs. Alterna transparentes
Olvid	Sécurité max prouvée (E2EE tout + métadonnées, ANSSI), Anonymat très élevé	Base utilisateurs plus faible, Ajout contact manuel, Fonctions avancées payantes	Sécurité/Confidentiali vérifiables vs. Moindr popularité/commodité
Session	Anonymat très élevé, Protection métadonnées excellente (décentralisé)	Lenteur potentielle, Appels moins anonymes (P2P), Gestion clé récupération	Anonymat/Confidenti métadonnées au top Performance/Simplici appels

Application	Avantages Clés (Sécurité/Confidentialité)	Inconvénients Clés (Sécurité/Confidentialité)	Compromis M Facilité/Fonctionnal
Telegram	Fonctionnalités riches, Populaire, Rapide	Sécurité par défaut faible (Pas E2EE), Protocole critiqué, Collecte métadonnées	Fonctionnalités/Popu Sécurité/Confidentiali faibles
Signal	Sécurité E2EE forte par défaut, Très transparent, Non-profit, Anonymat OK	Moins de "gadgets" que Telegram?	Excellent équilibre Sécurité/Confidentiali vs. Peut-être moins " Telegram
WhatsApp	Extrêmement populaire, Facile, E2EE perso par défaut	Collecte massive métadonnées (Meta), Backups non E2EE défaut,	Popularité/Facilité ext Confidentialité métad faible (Meta)

6.3 Conclusion et Recommandations Finales

Il n'y a pas d'application de messagerie parfaite qui coche toutes les cases pour tout le monde. Le choix dépend de vos priorités personnelles et de votre niveau de préoccupation concernant votre vie privée et la sécurité de vos communications.

Voici quelques pistes pour vous guider :

- **Si votre priorité absolue est la sécurité maximale, prouvée et vérifiable, ainsi que l'anonymat**, et que vous êtes prêt à faire quelques efforts pour convaincre vos contacts ou pour une utilisation un peu moins immédiate : **Olvid** ou **Session** sont les meilleurs choix. Olvid offre des garanties techniques uniques (chiffrement métadonnées, pas de serveur de confiance) validées par des tiers. Session offre un anonymat robuste et une protection des métadonnées via la décentralisation.
- **Si vous recherchez le meilleur équilibre entre une sécurité forte et reconnue, une bonne protection de la vie privée (métadonnées), une grande transparence, une facilité d'utilisation et une base d'utilisateurs conséquente** : **Signal** est très probablement le choix le plus judicieux. Il est devenu la référence en matière de messagerie sécurisée fiable et accessible.
- **Si votre priorité est de pouvoir communiquer facilement avec le plus grand nombre de vos contacts existants**, et que vous acceptez que Meta (Facebook) collecte de nombreuses informations sur vos habitudes de communication (mais pas le contenu de vos messages personnels) : **WhatsApp** peut convenir, mais **pensez impérativement à activer l'option de chiffrement E2EE pour vos sauvegardes cloud**.
- **Si vous êtes attiré par les nombreuses fonctionnalités de Telegram (grands groupes, canaux, bots)**, et que vous êtes conscient que la sécurité par défaut est faible : utilisez

Telegram avec prudence. **Activez systématiquement les "Secret Chats"** pour toutes vos conversations sensibles (rappelez-vous qu'ils ne fonctionnent que pour les discussions à deux) et soyez conscient des risques liés à son protocole et à la collecte de métadonnées.

- **Concernant TeleGuard** : En l'absence de preuves tangibles (code source ouvert, audits indépendants) pour étayer ses fortes affirmations de sécurité, il est difficile de recommander **TeleGuard** sur la base de la confiance. Son utilisation comporte un risque lié à ce manque de transparence.

Enfin, demandez-vous : **"De quoi ou de qui est-ce que je veux protéger mes conversations?"**. La réponse à cette question (votre "modèle de menace") vous aidera à déterminer le niveau de sécurité et de confidentialité dont vous avez réellement besoin. N'oubliez pas non plus de toujours garder votre application de messagerie et le système d'exploitation de votre téléphone à jour, car les mises à jour corrigent souvent des failles de sécurité[43].

7. Glossaire Simplifié

- **Chiffrement de bout en bout (E2EE)** : Méthode de protection où seuls l'expéditeur et le destinataire peuvent lire le message. L'application elle-même ne le peut pas.
- **Métadonnées** : Informations sur la communication (qui parle à qui, quand, etc.), distinctes du contenu du message.
- **Code Source Ouvert (Open Source)** : Le "plan" de l'application est public, permettant à quiconque de vérifier sa sécurité.
- **Serveur Centralisé** : Toutes les communications passent par un point central géré par l'entreprise.
- **Serveur Décentralisé** : Les communications passent par un réseau de plusieurs serveurs indépendants.
- **Audit de Sécurité** : Examen approfondi de l'application par des experts externes pour trouver des failles.
- **Protocole de Chiffrement** : L'ensemble des règles et méthodes techniques utilisées pour sécuriser les messages (ex: Signal Protocol, MTProto).
- **Anonymat** : Possibilité d'utiliser l'application sans révéler son identité réelle (souvent liée au numéro de téléphone).
- **Fondation à but non lucratif (Non-profit)** : Organisation dont le but principal n'est pas de faire du profit, souvent financée par des dons (comme Signal).
- **Freemium** : Modèle où l'application de base est gratuite, mais des fonctionnalités avancées sont payantes (comme Olvid).

1. What is Signal? 7 features that make it a go-to app for private ..., consulté le avril 27, 2025, https://www.zdnet.com/article/what-is-signal-7-features-that-make-it-a-go-to-app-for-private-secure-messaging/ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

2. Technology - Olvid, consulté le avril 27, 2025, https://olvid.io/technology/en ↩
3. olvid.io, consulté le avril 27, 2025, https://olvid.io/assets/brochures/Olvid_1-page-en.pdf ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩
4. Frequently Asked Questions - Session Private Messenger, consulté le avril 27, 2025, https://getsession.org/faq ↩
5. Is WhatsApp safe? The pros, cons, and hidden dangers, consulté le avril 27, 2025, https://us.norton.com/blog/privacy/is-whatsapp-safe ↩
6. Secure Encrypted Messaging - Defensive Computing Checklist, consulté le avril 27, 2025, https://defensivecomputingchecklist.com/SecureMessaging.php ↩ ↩ ↩ ↩ ↩ ↩
7. Is Telegram safe for the average user? - Norton Antivirus, consulté le avril 27, 2025, https://us.norton.com/blog/privacy/is-telegram-safe ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩
8. Telegram Encryption: An In-Depth Look at Security in 2024 - Insights For Success, consulté le avril 27, 2025, https://www.kiledjian.com/main/2024/8/30/telegram-encryption-an-in-depth-look-at-security-in-2024 ↩ ↩ ↩ ↩ ↩ ↩ ↩
9. TeleGuard on the App Store, consulté le avril 27, 2025, https://apps.apple.com/us/app/teleguard/id1505636751 ↩
10. Why not - free messenger, consulté le avril 27, 2025, https://www.freie-messenger.de/en/warumnicht/ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩
11. The Best Private Messaging Apps for 2025 | PCMag, consulté le avril 27, 2025, https://www.pcmag.com/picks/best-secure-messaging-apps ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩
12. Is Telegram really an encrypted messaging app? – A Few Thoughts on Cryptographic Engineering, consulté le avril 27, 2025, https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/ ↩ ↩
13. Salsa20 - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Salsa20 ↩ ↩
14. The Salsa20 Family of Stream Ciphers - SciSpace, consulté le avril 27, 2025, https://scispace.com/pdf/the-salsa20-family-of-stream-ciphers-4la86gmtaq.pdf ↩
15. TeleGuard app : r/privacy - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/1cbyhnd/teleguard_app/ ↩ ↩
16. Privacy Policy - TeleGuard, consulté le avril 27, 2025, https://teleguard.com/en/privacy ↩ ↩

17. SimpleX Chat - the first messaging platform that has no user identifiers - v2.2 of mobile apps with the new privacy and security features just released! - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/v4rhch/simplex_chat_the_first_messaging_platform_that/ ↩️ ↩️

18. TeleGuard - secure messenger from Switzerland, consulté le avril 27, 2025, https://teleguard.com/ ↩️ ↩️

19. Swisscows - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Swisscows ↩️ ↩️ ↩️

20. Olvid (software) - Wikipedia, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Olvid_(software) ↩️ ↩️ ↩️ ↩️ ↩️

21. Olvid 2025 Company Profile: Valuation, Funding & Investors ..., consulté le avril 27, 2025, https://pitchbook.com/profiles/company/339907-78 ↩️ ↩️

22. The Security of the Session Messenger – A Guide - Protectstar.com, consulté le avril 27, 2025, https://www.protectstar.com/en/blog/the-security-of-the-session-messenger-a-guide ↩️ ↩️ ↩️

23. Session | Send Messages, Not Metadata. | Private Messenger, consulté le avril 27, 2025, https://getsession.org/ ↩️ ↩️

24. About OPTF | Privacy is a fundamental right., consulté le avril 27, 2025, https://optf.ngo/about-optf ↩️

25. Introducing the Session Technology Foundation - Session Private Messenger, consulté le avril 27, 2025, https://getsession.org/introducing-the-session-technology-foundation ↩️ ↩️ ↩️ ↩️

26. The Digital Privacy Paradox: Encrypted Messaging App 'Session ..., consulté le avril 27, 2025, https://www.socpub.com/articles/digital-privacy-paradox-encrypted-messaging-app-session-solves-what-others-wont-18037 ↩️ ↩️

27. Best Secure and Encrypted Messaging Apps in 2025 - CyberInsider, consulté le avril 27, 2025, https://cyberinsider.com/secure-encrypted-messaging-apps/ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️

28. Is Telegram Safe? A Guide to the Secure Messaging App - Avast, consulté le avril 27, 2025, https://www.avast.com/c-is-telegram-safe ↩️ ↩️

29. Telegram Privacy Policy, consulté le avril 27, 2025, https://telegram.org/privacy?setln=fa ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️ ↩️

30. Signal vs Telegram: Security & Privacy Comparison - Cyber Citadel, consulté le avril 27, 2025, https://cybercitadel.com/signal-vs-telegram-a-detailed-comparison-of-security-and-privacy/ ↩️ ↩️

31. The best encrypted messaging apps in 2025 - Tom's Guide, consulté le avril 27, 2025, https://www.tomsguide.com/reference/best-encrypted-messaging-apps ↩

32. On the CCA (in)Security of MTProto - ResearchGate, consulté le avril 27, 2025, https://www.researchgate.net/publication/310823273_On_the_CCA_inSecurity_of_MTProto ↩

33. Telegram | Overview, History, & Facts | Britannica, consulté le avril 27, 2025, https://www.britannica.com/topic/Telegram-software ↩ ↩

34. Who Owns Telegram Messenger – CanvasBusinessModel.com, consulté le avril 27, 2025, https://canvasbusinessmodel.com/blogs/owners/telegram-messenger-who-owns ↩ ↩ ↩

35. Is Signal Safe? A Closer Look at the Privacy Messaging App, consulté le avril 27, 2025, https://www.cyberghostvpn.com/privacyhub/is-signal-safe/ ↩ ↩ ↩ ↩ ↩ ↩ ↩

36. Tightening up Text Message Security with Signal Private Messenger - Oklahoma Bar Association, consulté le avril 27, 2025, https://www.okbar.org/cm_articles/tightening-up-text-message-security-with-signal-private-messenger/ ↩ ↩ ↩ ↩ ↩ ↩ ↩

37. Which app for secure messaging : r/privacy - Reddit, consulté le avril 27, 2025, https://www.reddit.com/r/privacy/comments/1icijvv/which_app_for_secure_messaging/ ↩ ↩ ↩ ↩ ↩ ↩

38. en.wikipedia.org, consulté le avril 27, 2025, https://en.wikipedia.org/wiki/Signal_(software)#:~:text=Signal%20is%20now%20developed%20by,created%20by%20them%20in%202018. ↩ ↩ ↩ ↩

39. WhatsApp Privacy | Secure and Private Messaging - WhatsApp.com, consulté le avril 27, 2025, https://www.whatsapp.com/privacy ↩ ↩ ↩

40. Top 3 Companies Owned by Facebook (Meta) - Investopedia, consulté le avril 27, 2025, https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp ↩ ↩ ↩ ↩

41. Regular reminder that Telegram's encryption protocol, MTProto, is not secure, an... | Hacker News, consulté le avril 27, 2025, https://news.ycombinator.com/item?id=14375508 ↩ ↩ ↩

42. Olvid for Android - GitHub, consulté le avril 27, 2025, https://github.com/olvid-io/olvid-android ↩

43. Teleguard: Swiss Made Safe Messaging - Hacker News, consulté le avril 27, 2025, https://news.ycombinator.com/item?id=25882319 ↩