Messageries fédérées : des « résistances numériques » par l'architecture ?

Par **Ksenia Ermoshina** et **Francesca Musiani**

Les technologies de chiffrement, « invisibles » pour la plupart des internautes, ont des implications fondamentales pour nos libertés individuelles et notre présence collective sur Internet. Alors que certains outils numériques très populaires, comme WhatsApp, utilisent le chiffrement dit « de bout en bout » (voir le Glossaire à la suite de l'article), de nombreuses tentatives de régulation nationale et supranationale appellent aujourd'hui à neutraliser ces technologies. Le chiffrement des outils de communication à la disposition des internautes est devenu l'un des principaux champs de bataille (DeNardis, 2014) de la gouvernance de l'Internet. Cette « bataille » a lieu entre plusieurs acteurs, des organisations internationales de standardisation qui forgent et normalisent les protocoles de chiffrement aux grandes entreprises du numérique (« GAFAM »), en passant par les institutions, les universitaires et développeurs, et des communautés d'enthousiastes venus de l'univers du logiciel libre, prônant la « re-décentralisation » d'Internet.

En contribuant à éclairer ce mouvement vers la re-décentralisation, notre article présente l'état actuel du développement de projets qui font le choix de « fédérer » les réseaux de communication, à l'opposition des applications dites « centralisées » comme Signal ou Whatsapp. Ces dernières, tout en proposant un chiffrement de bout en bout de haute qualité, dépendent d'un point central où les données des usagers sont traitées (et parfois stockées), ou collaborent avec les GAFAM (en partageant, par exemple, des méta-données des utilisateurs). Les auteurs des applications fédérées proposent une autre vision des libertés numériques selon laquelle il n'est pas suffisant de chiffrer le contenu des messages échangés, mais il est crucial de repenser l'architecture même de nos réseaux, revendiquer la propriété de nos données, en garantir la portabilité. L'article montre comment, entre développement technique et revendications idéologiques, ces messageries structurent des formes de « résistance numérique » autour de ce qu'on a appelé les « 4 C » de la fédération : communauté, compatibilité, customisation et *care*.

Les architectures techniques des services Internet sont désormais au cœur des débats liés au numérique, notamment avec la critique des GAFAM et de leur modèle d'affaires basé sur l'extraction des données des usagers. En quête d'une plus grande autonomie informationnelle et d'un plus ample contrôle sur leurs données, certains internautes cherchent des alternatives aux plateformes centralisées et optent pour des solutions décentralisées, auto-hébergées ou maintenues par des collectifs d'hébergeurs indépendants qui tiennent à la transparence algorithmique et à la protection des données de leurs utilisateurs. La « bataille » se déroule à deux niveaux : la couche *infrastructurelle*, avec le développement

et la multiplication des instances fédérées (connues sous le nom de « Fediverse ») et la couche *protocole* permettant des échanges chiffrés entre ces nouveaux îlots communicationnels (serveurs ou instances). Le protocole peut être saisi comme langage utilisé par les serveurs pour se comprendre ; s'il est « interopérable », des serveurs à configuration différente seront capables de le déchiffrer. Les protocoles sont essentiels pour le fonctionnement de l'internet, fournissant son modèle conceptuel et l'ensemble des spécifications qui expliquent comment les données doivent être regroupées en paquets, adressées, acheminées et reçues ; la sélection et l'adoption de protocoles spécifiques ont d'importantes implications politiques et économiques, ainsi que techniques (DeNardis, 2009).

Les révélations d'Edward Snowden en 2013 ont été un événement marquant dans le développement du domaine des communications sécurisées (voir Snowden, 2019). Le chiffrement des communications à grande échelle et de manière plus facilement utilisable est devenu un sujet d'intérêt politique et public, avec l'apparition d'un nouvel imaginaire cryptographique, qui considère le chiffrement comme une condition préalable nécessaire à la formation de publics en réseau (Myers West, 2018). Les révélations ont également catalysé des débats de longue date dans le domaine des protocoles de communication sécurisée. La communauté du chiffrement (en particulier les collectifs universitaires et du logiciel libre) a renouvelé ses efforts pour créer des protocoles de messagerie sécurisée de nouvelle génération afin de surmonter les limites des protocoles existants, tels que PGP (Pretty Good Privacy) et OTR (Off-the-Record Messaging).

La « *mess of messengers* » des communications chiffrées

En réponse à la compréhension de plus en plus répandue de la sécurité des communications en ligne comme une question sociale et politique importante, la messagerie chiffrée est un domaine dynamique, et en devenir. Malgré la naissance de plusieurs projets novateurs, les développeurs sont toujours en pleine évolution quant à la manière de mettre en œuvre les propriétés de sécurité et de confidentialité, ou les normes de gestion du chiffrement au sein des conversations de groupe, car il n'existe pas de norme claire à adopter pour ces propriétés. En termes de vie privée, le travail est encore immature ; même les applications de messagerie sécurisée les plus populaires, telles que Signal, exposent les métadonnées des utilisateurs via l'obligation d'associer les utilisateurs à leur numéro de téléphone.

Pour toutes ces raisons, la nouvelle génération de messageries sécurisées est encore non-standardisée et fragmentée, ce qui conduit les utilisateurs de ces outils à exister dans des dizaines de « silos » incapables d'interagir les uns avec les autres (Sparrow & Halpin, 2015). Le *silo effect*, c'est-à-dire l'impossibilité d'interagir entre des outils de messagerie différents ou de migrer d'une application vers une autre, a été considéré comme l'un des obstacles les plus importants à l'adoption d'applications de messagerie sécurisée. Or, les protocoles dits « fédérés » proposent une solution possible au problème des silos en permettant une communication entre une multitude d'instances ou de serveurs différents, sans forcer les utilisateurs à converger vers un serveur unique. Par exemple, l'*email* est un système de communication fédéré qui s'appuie sur des « protocoles de transport » qui sont universels pour la quasi-

totalité des fournisseurs de services *email* dans le monde et nous permettent de communiquer sans nécessairement utiliser le même service *mail*.

Plusieurs projets proposent d'utiliser des solutions fédérées en y intégrant le chiffrement et les caractéristiques de sécurité les plus récentes, pour ainsi garantir non seulement la protection du contenu des messages, mais aussi la liberté de choix des serveurs, la résistance aux éventuels blocages, la meilleure protection de l'anonymat et des métadonnées. Or, ces applications souffrent encore d'un certain nombre de limitations liées à la facilité d'usage et au passage à l'échelle.

Notre méthode

Fondée sur la littérature dérivée des *science and technology studies* (STS), notre approche peut être décrite comme une ethnographie multi-sites. Nous avons entrepris des recherches dans et entre plusieurs lieux, en ligne et hors ligne, et nous avons explicitement considéré des protocoles et systèmes techniques spécifiques comme « faisant partie d'un contexte plus large qui dépasse les limites du site de terrain » (Muir, 2011). Nous visons à donner un sens aux systèmes émergents et aux communautés de pratique par le biais de « descriptions analytiques détaillées » (*analytical thick descriptions*; pour un traitement récent du concept, introduit pour la première fois par l'anthropologue Clifford Geertz, voir Ponterotto, 2006) d'événements, d'artefacts et d'organisations. En particulier, nous prêtons attention aux moments de crise, de débat, de controverse, pour essayer de comprendre la vie d'un artefact technique, de sa création à son appropriation et à ses reconfigurations par les utilisateurs, jusqu'à ce qu'il devienne un sujet de débat public, de gouvernance, de *lobbying*. La principale méthodologie pour atteindre cet objectif a consisté à observer des groupes, des événements ou des communautés, tout en menant des entretiens avec leurs membres et en lisant des documents tels que des notes de publication, des listes de diffusion et des comptes rendus des séances de travail.

Fédération : entre compromis technique et choix idéologique

Les architectures fédérées connaissent actuellement une phase de développement et d'utilisation accrue. Elles sont présentées comme des alternatives, d'une part, aux applications centralisées qui introduisent un « point de défaillance unique » dans le système et manquent par ailleurs d'interopérabilité, et d'autre part, aux applications complètement décentralisées, de type pair-à-pair (P2P) (comme le système BitTorrent, ou l'application FireChat) qui nécessitent des niveaux plus élevés d'engagement, d'expertise et de responsabilité de la part de l'utilisateur (et de son équipement informatique). La fédération est parfois décrite comme un projet techno-politique ambitieux; les architectures fédérées ouvrent le « noyau dur » des concepteurs de protocoles et impliquent un nouveau type d'acteur, l'administrateur système, responsable de la maintenance de l'ensemble de serveurs nécessaire au fonctionnement des réseaux fédérés. La fédération est censée contribuer à atténuer le très haut degré de responsabilité personnelle détenu par un fournisseur de services centralisés, tout en répartissant cette responsabilité et les moyens de calcul – les ressources matérielles et logistiques nécessaires au

système – avec différents degrés d'engagement possibles, en favorisant la liberté des utilisateurs de choisir entre différentes solutions et différents serveurs.

Parmi les projets les plus populaires basés sur les architectures fédérées, on peut citer Mastodon, un équivalent open-source et libre de Twitter, un réseau de *microblogging* qui s'appuie sur le protocole ActivityPub (compatible avec d'autres plateformes du même type, comme Pleroma). Mastodon et Pleroma proposent une autre forme d'existence et de modération des communautés numériques : l'usager peut choisir une instance (ou serveur) selon ses goûts, valeurs ou intérêts. Le contact avec les modérateurs et administrateurs de l'instance est beaucoup plus direct (parfois même amical) et les usagers peuvent influencer le développement de l'interface de leur instance. Ces plateformes proposent également leurs façons de gérer les discours de haine, différentes de celles proposées par Twitter. Les administrateurs et les usagers des instances (hébergées par des bénévoles) ont la mainmise sur la circulation des contenus, à l'opposition de la modération corporative et centralisée proposée par les GAFAM. Avec les autres applications fédérées à code ouvert, comme Peertube (l'équivalent de YouTube), ou encore Pixelfed (l'équivalent d'Instagram), ces projets constituent ce qu'on appelle « Fediverse ».

La communauté des développeurs impliqués dans le domaine de la messagerie sécurisée mène des débats animés sur les limites et les opportunités des protocoles fédérés, qui vont de pair avec les débats sur les normes et les standards. Les partisans des solutions fédérées affirment que la réutilisation des protocoles standardisés existants ou le développement de nouvelles normes ouvertes peuvent améliorer l'interopérabilité et résoudre le problème des silos (Kent, 2019). En effet, les architectures fédérées semblent bien adaptées à la promotion de solutions plus locales et de solutions communautaires plus petites, dont le modèle économique ne dépend pas du simple nombre d'utilisateurs et de la disponibilité de leurs données pour la collecte et l'agrégation. D'autre part, selon les partisans des solutions centralisées, la fédération présente des problèmes de sécurité, car il est plus difficile de contrôler toutes les différentes implémentations d'un protocole fédéré et de s'assurer que tous les serveurs sont bien configurés. En effet, les solutions de messagerie fédérée ajoutent une couche de complexité dans la gouvernance des réseaux socio-techniques qu'elles structurent, car elles introduisent la nécessité d'une administration décentralisée des serveurs (ou « instances »).

Au travers des débats sur la fédération dans les messageries chiffrées, on a pu observer que la fédération se structure en tant qu'expérience, à la fois infrastructurelle et sociale, qui cherche un compromis entre la répartition des responsabilités sur un plus grand nombre d'acteurs, des niveaux de sécurité élevés et une meilleure ergonomie. La fédération est un projet politique et technique qui reconnaît les dangers inhérents aux solutions centralisées, mais qui cherche un « juste milieu » entre la centralisation et des solutions intégralement distribuées (comme les outils P2P, considérés comme nécessitant une courbe d'apprentissage plus élevée).

La fédération dans la messagerie sécurisée comporte notamment deux approches. Certains projets s'attachent à développer de nouveaux protocoles, tandis que l'autre approche dite « écologique »

consiste à recycler les anciens protocoles et les normes ouvertes existantes (par exemple Delta.Chat, un projet de *chat-over-email* qui adopte le protocole de transport « classique » SMTP). Ces deux approches ont par ailleurs en commun le souhait d'utiliser les infrastructures gérées par la communauté et des pratiques de « chiffrement social » afin de renforcer le niveau de sécurité au-delà de ce qui est rendu possible par les techniques de chiffrement elles-mêmes. La fédération est également explorée comme un moyen de rendre les applications de messagerie résistantes à la censure, un facteur qui joue un rôle de plus en plus important pour les utilisateurs vivant dans des contextes répressifs (voir le cas récent de blocage de Signal en Iran).

Si la longueur et le format de cet article ne nous permettent pas de rendre pleinement compte de la pluralité de nos études de cas, nous présentons dans la section qui suit un aperçu du cas de Matrix.org, connu aujourd'hui sous le nom d'Element, comme cas emblématique des expérimentations en cours avec les modèles fédérés. Il s'agit d'une solution adoptée notamment par le gouvernement français, puis par le ministère de défense d'Allemagne comme application officielle de messagerie sécurisée.

Matrix : exemple d'une expérimentation en cours

Le projet Matrix.org a été lancé en 2014 par Matthew Hodgson et Amandine Le Pape, d'abord financé par l'entreprise Amdocs, puis par la fondation New Vector spécialement créée afin de garantir la durabilité économique du projet. À ce jour, il recense autour de 10 millions de comptes et plus de 20,000 serveurs. L'objectif principal du projet est de créer une architecture qui s'attaque aux problèmes d'interopérabilité de façon inédite et plus efficace par rapport à des projets précédents. Cette interopérabilité est censée devenir un avantage comparatif substantiel et un facteur d'adhésion pour les utilisateurs. L'équipe de Matrix n'adopte pas, par ailleurs, de position explicitement politique et ne vise pas à fournir des logiciels pour des publics spécifiques ayant un programme politique ou engagés dans des arènes politiques, comme les militants. Matthew Hodgson positionne son équipe comme « plutôt modérée, presque centriste » ; il identifie sa position comme une sorte de « pluralisme libéral », qui se reflète dans l'architecture même de son système ainsi que dans ses utilisateurs.

L'idée sous-jacente de Matrix est censée aller au-delà d'une application de messagerie instantanée ; elle est présentée par ses développeurs comme un écosystème entier qui pourrait être utilisé pour tout type de partage de données. Matthew Hodgson, ingénieur en chef de Matrix, a remarqué au cours de notre entretien avec lui : « Le modèle s'inspire fortement du réseau téléphonique [mais celui-ci] n'est pas ouvert, il est plutôt centralisé pour les opérateurs de télécommunications. Nous voulions donc créer un réseau complémentaire qui soit ouvert et décentralisé. »

Du point de vue de l'architecture, ce système fédéré relie une grande variété d'outils de messagerie différents (par exemple Slack, Mattermost, Skype, Telegram, Facebook Messenger et autres), laissant ainsi une certaine liberté aux utilisateurs, leur permettant de conserver leur interface habituelle, tout en se connectant avec d'autres. Matthew Hodgson souligne explicitement que Matrix tente de répondre aux

problèmes des silos, engendrés par le développement rapide et quelque peu « chaotique », d'après lui, de l'écosystème des messageries, en particulier sur les mobiles. Par ailleurs, l'équipe de Matrix propose sa propre application de messagerie appelée maintenant Element (auparavant connue comme Riot.im).

En termes de pluralisme des utilisateurs, Matrix dispose de plus de vingt mille serveurs et plus de deux millions de « salles » traitant de sujets très variés, allant de la cryptographie et de l'open-source, des monnaies virtuelles et de la décentralisation à de l'aide psychologique, en passant par des communautés de fans, des groupes de gauche et des salles de supporters intégristes de Donald Trump. Deux des principaux problèmes persistants pour Matrix sont la gestion du spam et le maintien d'un système de réputation décentralisé : deux questions qui, selon Matthew, sont encore ouvertes dans la recherche en informatique et doivent être soutenues par un positionnement « moralement neutre ».

En tant que projet fédéré, Matrix est déployé sur une multitude de serveurs (selon son développeur principal, plus de 20 000 en mars 2020) qui ne sont pas tous sous le contrôle de l'équipe. Chaque serveur peut avoir ses propres paramètres de confidentialité et ses propres politiques de collaboration (ou pas…) en matière d'interception légale. Ainsi, l'auto-hébergement des serveurs est promu par les développeurs comme un moyen d'augmenter la sécurité. De plus, en répondant au risque croissant de coupures d'Internet dans les régions politiquement instables, comme le Bélarus, Iran, Kyrgyzstan et autres, Matrix a récemment sorti une version alpha de Matrix P2P qui ne nécessite pas de connexion Internet.

Actuellement, Matrix s'efforce de réduire la diffusion de la désinformation, des discours de haine et du spam. En effet, alors que les GAFAM sont de plus en plus critiqués pour avoir permis la diffusion de ces contenus problématiques, des alternatives fédérées comme Mastodon ou Pleroma semblent offrir des moyens d'en minimiser la diffusion, par un mélange de modération sociale et technique par les administrateurs de serveurs ou d'instances. Or, cette ouverture du code et interopérabilité attirent des mouvances d'extrême droite, comme cela est le cas de Gab, solution elle-même basée sur Mastodon. Néanmoins, l'architecture de Mastodon et le principe d'interaction entre les instances ont permis d'exclure Gab du reste de la fédération, à la fois par le blocage de l'instance par les administrateurs des autres instances et par le refus d'inclure Gab dans la liste des instances qui respectent le code de bonne conduite publié sur le site de Mastodon. La controverse est quand même toujours en cours, car le code ouvert de Mastodon peut être réutilisé par tout un chacun pour déployer des instances, et le créateur de Mastodon Eugent Rochko reconnaît cet effet pervers de l'ouverture de son système. L'équipe de Matrix espère résoudre ce problème en déployant un système de réputation, et cherche un moyen pour les utilisateurs de filtrer le contenu en développant un système de filtres ouverts et modulables.

Les « quatre C » de la fédération : communauté, compatibilité, customisation et *care*

Les développeurs des dispositifs fédérés cherchent à trouver un compromis entre des niveaux de sécurité élevés et une meilleure ergonomie, et ce, par un dialogue constant entre des motivations

« idéologiques », telles que la répartition des responsabilités sur un plus grand nombre d'acteurs, et une proposition de définitions particulières de la liberté en ligne, comme le fait de donner aux utilisateurs le choix du niveau d'autonomie qu'ils souhaitent atteindre. Nous présentons en conclusion de cet article une tentative de systématisation et de conceptualisation de ce que le cas de Matrix et d'autres cas d'étude nous indiquent sur l'état actuel de la fédération et sa capacité à co-structurer des formes de « résistance numérique ». Nous mettons en avant les « quatre C de la fédération » : communauté, compatibilité, customisation et *care* (dans la lignée des travaux STS sur l'attention et le soin apporté-e-s aux technologies, voir, par exemple, Denis et Pontille, 2015).

L'(auto)-gouvernance et le développement des projets fédérés impliquent un important effort communautaire et dépendent de l'engagement de divers acteurs à accepter de nouveaux protocoles ouverts. La communication et le consensus entre les différents projets sont nécessaires pour pouvoir progresser dans un environnement fédéré. La transition vers les protocoles de chiffrement de prochaine génération au sein des écosystèmes fédérés sera probablement lente et difficile, cependant, nos recherches démontrent la montée en puissance d'une communauté diverse d'acteurs impliqués dans une coproduction d'éléments (protocoles, paquets, bibliothèques, etc.) nécessaires pour préparer les environnements fédérés à l'adoption du chiffrement par défaut. De nombreux projets, d'Autocrypt à Conversations, entreprennent d'importants efforts communautaires pour faire avancer l'écosystème de la messagerie sécurisée.

Le domaine des applications de messagerie instantanée chiffrée de bout en bout est très compétitif, avec des tensions importantes entre les développeurs de protocoles et d'applications, les acteurs responsables du fonctionnement technique, et les activistes de la communauté open-source. En raison de la nature même des messageries centralisées et non interopérables qui « enferment les utilisateurs » (selon les termes d'Elijah Sparrow, responsable du projet LEAP sur le chiffrement des communications) dans un outil doté d'interfaces et d'ensembles de fonctionnalités spécifiques, les messageries sont en concurrence pour les utilisateurs. La messagerie fédérée étant un écosystème ouvert, elle est structurée par un certain nombre d'efforts de collaboration et de coordination qui visent à augmenter et améliorer la compatibilité. Cependant, ces efforts ne sont pas exempts de tensions et de points de controverse ; outre la différence d'approche technique des différents projets, ces débats sont également dus à la nécessité d'« enrôler » un nombre important de développeurs afin de mettre en œuvre et de diffuser leur solution, et de pouvoir sécuriser les utilisateurs.

Les solutions de messagerie fédérée sont une forme de « résistance numérique par l'alternative », car elles tentent de répondre, par des choix d'architecture technique, à plusieurs problèmes importants rencontrés par les infrastructures de communication contemporaines. D'une part, la fragmentation du web et le manque d'interopérabilité, la concentration de la puissance et l'agrégation des données par des applications et des plateformes centralisées ; et d'autre part, la barrière socio-technique propre aux réseaux P2P qui appellent une plus grande expertise et responsabilité des utilisateurs et une meilleure performance de leurs appareils.

C'est là qu'intervient le troisième C – la customisation. Les modèles fédérés proposent aux utilisateurs de choisir parmi plusieurs fournisseurs de services et de migrer d'un serveur à un autre sans perdre leurs graphes sociaux. Le paradigme « le plus grand est le mieux » est donc remis en question par les messageries fédérées dont les modèles économiques ne dépendent pas du nombre d'utilisateurs ni de la collecte et de l'agrégation de leurs données. Dans les projets fédérés, les utilisateurs dépassent le rôle de « travailleurs de données », selon les termes de l'artiste et philosophe espagnol des médias Manuel Beltran ; les groupes d'utilisateurs plus petits semblent plus faciles à gérer, et les architectures fédérées facilitent la personnalisation et la localisation des technologies, en les adaptant aux besoins d'une communauté d'utilisateurs spécifique sans perdre la capacité d'interagir avec des réseaux plus vastes (en développant des ponts, des robots ou d'autres moyens de « brancher » les systèmes les uns aux autres). La fédération donne la possibilité aux petits projets de proliférer, posant par ailleurs un défi aux développeurs et chercheurs pour qui cela devient beaucoup plus difficile de documenter toutes les diverses implémentations d'un protocole donné.

En même temps, les implémentations d'un protocole fédéré sont plus difficiles à contrôler, ce qui peut créer des vulnérabilités dans différentes instances ou chez différents clients. Le développement réussi d'outils de communication fédérés nécessite donc de nouvelles formes d'organisation et de prise de décisions, ce qui est particulièrement difficile pour les réseaux décentralisés et peu structurés. Les formes fédérées de gouvernance de projet prennent forme par la variété des manières dont la documentation sur les protocoles est présentée et améliorée, les négociations constantes entre les acteurs impliqués, les rassemblements en présence (souvent informels), et les nouveaux efforts de standardisation. Les protocoles standardisés ou quasi-standardisés fonctionnent comme des instruments d'auto-gestion, de communication et de coordination entre les acteurs des réseaux fédérés, ce que Yochai Benkler a appelé la « coordination sans hiérarchie » (2006).

Cependant, la fédération ajoute une couche de complexité dans la gouvernance des messageries sécurisées en tant que réseaux socio-techniques, en introduisant de nouveaux acteurs clés, notamment les administrateurs système, responsables de la maintenance et de la croissance – le *care* (Denis & Pontille, 2015) – des infrastructures fédérées, notre quatrième et dernier C. La stabilité des écosystèmes fédérés dépend également de l'enrôlement réussi des acteurs responsables de leur maintenance, ce qui nécessite le développement d'une bonne documentation et de guides de « meilleures pratiques », ainsi que la diffusion de l'expertise technique par des événements pédagogiques hors ligne destinés aux présents et futurs administrateurs de systèmes.

Dans les systèmes fédérés, l'« attention à la plomberie » (Musiani, 2012) est particulièrement importante et acquiert une signification spécifique à l'architecture, car on ne peut pas compter sur une seule entité pour maintenir le système en état de fonctionnement, mais le besoin d'entretien et d'attention est réparti entre les multiples administrateurs de systèmes et les autres acteurs qui gèrent les différentes instances de l'espace fédéré (ainsi que les bibliothèques, les serveurs de clés et autres instances auxiliaires mais tout aussi importantes). La croissance des plateformes fédérées marque

un tournant vers des « espaces sûrs » gérés par la communauté, avec plus de pouvoirs délégués aux modérateurs humains (administrateurs de serveurs ou d'instances). Cela introduit de nouveaux risques de recentralisation du pouvoir au sein des réseaux fédérés (Raman et al., 2019), et appelle plus de recherches sur le rôle des responsables de la maintenance des infrastructures, des administrateurs et des modérateurs, en plus du noyau des concepteurs de protocoles.

Remerciements

Ce travail a été financé par le projet H2020 NEXTLEAP (H2020-ICT-2015 – Grant Agreement n° 688722, 2016-2018) et par le projet ANR ResisTIC (Agence Nationale de la Recherche française, ANR-17-CE26-0020, 2018-2022).

Biographies

Ksenia Ermoshina, docteure en socio-économie de l'innovation de MINES ParisTech (2016), est chargée de recherche au CNRS depuis 2019, et membre du Centre Internet et Société du CNRS. Elle est également chercheuse associée au Citizen Lab, Université de Toronto (Canada), et chercheuse/designeuse UX pour la messagerie Delta Chat. https://cis.cnrs.fr/ksenia-ermoshina/

Francesca Musiani, docteure en socio-économie de l'innovation de MINES ParisTech (2012), est chargée de recherche au CNRS depuis 2014, et directrice adjointe du Centre Internet et Société du CNRS qu'elle a cofondé en 2019. Elle est également chercheuse associée au Centre de Sociologie de l'Innovation (i3/MINES ParisTech) et Global Fellow auprès de l'Internet Governance Lab de l'American University à Washington, DC. https://cis.cnrs.fr/francesca-musiani/

Glossaire

Chiffrement de bout en bout : Modèle de chiffrement dans lequel seules les parties communicantes peuvent lire le message qui est chiffré lors du transit et sur les terminaux des utilisateurs.

PGP (Pretty Good Privacy) : https://fr.wikipedia.org/wiki/Pretty_Good_Privacy

OTR (Off-The-Record Messaging) : https://fr.wikipedia.org/wiki/Off-the-Record_Messaging

Métadonnées : Une métadonnée est la donnée fournissant des informations sur un ou plusieurs aspects de la donnée elle-même. Les métadonnées sont utilisées pour résumer les informations de base sur les données, ce qui peut faciliter le suivi des données spécifiques notamment afin de les retravailler.

SMTP : https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Références

DeNardis, Laura. 2009. Protocol Politics: The Globalization of Internet Governance. Cambridge: The MIT Press.

DeNardis, Laura. 2014. The Global War for Internet Governance. New Haven: Yale University Press.

Denis, Jérôme et David Pontille. 2015. « Material Ordering and the Care of Things », Science, Technology, & Human Values 40(3): 338-367.

Kent, Dominic. 2019. « Why is Having Multiple Messaging Platforms "Bad" in 2019 », Dispatch, https://dispatch.m.io/multiple-messaging-platforms-bad/

Muir, Stewart. 2011. "Multisited ethnography", dans: D. Southerton, D. (Dir.), Encyclopedia of Consumer Culture. London: Sage. http://dx.doi.org/10.4135/9781412994248.n375

Musiani, Francesca. 2012. « Caring About the Plumbing: On the Importance of Architectures in Social Studies of (Peer-to-Peer) Technology », Journal of Peer Production, 1. http://hal-ensmp.archives-ouvertes.fr/hal-00771863

Myers West, Sarah. 2018. « Cryptographic imaginaries and the networked public », Internet Policy Review 7(2). DOI: 10.14763/2018.2.792

Ponterotto, Joseph G. 2006. « Brief note on the origins, evolution, and meaning of the qualitative research concept thick description », The Qualitative Report 11(3): 538-549.

Raman, Aravindh, Sagar Joglekar, Emiliano De Cristofaro, Nishanth Sastry, and Gareth Tyson. 2019. « Challenges in the Decentralised Web: The Mastodon Case », dans: Proceedings of the Internet Measurement Conference, October 2019, pp. 217-229. Association for Computing Machinery.

Snowden, Edward. 2019. Permanent Record. New York: Henry Holt and Company.

Sparrow, Elijah, et Harry Halpin. 2015. « LEAP: The LEAP Encryption Access Project », dans: Reforming European Data Protection Law, pp. 367-383. Dordrecht: Springer.

Trienes, Jan, Andrés Torres Cano, et Djoerd Hiemstra. 2018. « Recommending Users: Whom to Follow on Federated Social Networks ». arXiv preprint arXiv:1811.09292