Bruxelles obéit à Macron : l’UE vote la fin du secret des messageries cryptées, whattsapp, proton…

écrit par Christine Tasin | 31 janvier 2021

Usés, les maires ruraux démissionnent en masse avant la fin de leur ...
https://francais.rt.com/france/53142-uses-les-maires-ruraux-demissionnent-... Mode Anonyme
1 août 2018 ... Selon un calcul de l'AFP réalisé à partir du répertoire national des élus en tenant compte de l'effet du non-cumul des mandats, le nombre de ...

De plus en plus de maires français démissionnent depuis dix ans
https://www.lemonde.fr/les-decodeurs/article/2018/08/30/de-plus-en-plus-de... Mode Anonyme
30 août 2018 ... En proie à des difficultés financières toujours plus importantes, les maires français sont de plus en plus nombreux à rendre leur écharpe ...

Ces maires qui démissionnent en série - Le Monde
https://www.lemonde.fr/politique/article/2018/08/25/ces-maires-qui-demissio... Mode Anonyme
25 août 2018 ... A deux ans des élections municipales, les défections d'édiles n'ont jamais été aussi nombreuses.

Pourquoi les maires démissionnent-ils ? - France Inter
https://www.franceinter.fr/emissions/le-telephone-sonne/le-telephone-sonne... Mode Anonyme
21 août 2018 ... Les démissions de maires en France ont augmenté de 55% par rapport à la précédente mandature. Pourquoi les petites communes ne s'en ...

Démissions en série chez les maires de France - L'Express
https://www.lexpress.fr/actualite/politique/demissions-en-serie-chez-les-mair... Mode Anonyme
10 août 2018 ... À moins de deux ans de la fin de leur mandat, de plus en plus de maires démissionnent de leurs fonctions, comme le montrent des chiffres ...

Usés par leur fonction, de plus en plus de maires démissionnent
www.lefigaro.fr/politique/2018/08/01/01002-20180801ARTFIG00317-uses-p... Mode Anonyme
1 août 2018 ... Un calcul réalisé à partir du répertoire national des élus indique que depuis 2014 , le nombre de maires démissionnaires est en hausse de 55% ...

« Je crains pour ma santé » : quand les maires préfèrent démissionner
https://www.ouest-france.fr/politique/je-crains-pour-ma-sante-quand-les-mai... Mode Anonyme
13 août 2018 ... Manque de moyens, surcharge de travail, fatigue… Le nombre de maires à démissionner en cours de mandat a augmenté de 55 % par rapport ...

Les maires français démissionnent de plus en plus – Politique | L ...
https://www.lopinion.fr/edition/politique/maires-francais-demissionnent-plus-... Mode Anonyme
10 août 2018 ... Charge de travail, restrictions budgétaires... accablés par les conditions de leur fonction, certains maires de France prennent la tangente.

Occitanie : le blues des maires qui démissionnent en série - 11/09 ...
https://www.ladepeche.fr/article/2018/09/11/2866507-occitanie-les-maires-r... Mode Anonyme
11 sept. 2018 ... De plus en plus, les maires jettent l'éponge avant la fin de leur mandat. Baisse globale des dotations de l'État, suppression de la taxe ...

C’est une mesure liberticide s’il en est qui s’est tramée dans notre dos. Une de plus. Une fois de plus. Avec, évidemment, le prétexte de pouvoir lutter contre le terrorisme. Le terrorisme, comme le Covid, sont utilisés pour rogner nos libertés fondamentales et les autorités se

gardent bien de faire ce qu'il faudrait pour y mettre vraiment fin. Et que l'initiative en ait été prise par Johnson et Macron qui font vivre une dictature Covid abominable en dit long sur leurs objectifs.

.

Tout commence quand Johnson et Macron, main dans la main, interpellent Bruxelles pour la sommer de voter l'obligation pour les messageries cryptées, Telegram, Signal, Whattsap, Protonmail… de permettre aux autorités compétentes d'avoir accès aux communications.

La France pousse l'UE à affaiblir le chiffrement des messageries

Le chiffrement des données sera-t-il bientôt sous contrôle en Europe ? Après les récents attentats survenus dans divers pays dont la France, le conseil des ministres de l'Union européenne serait sur le point d'adopter cette mesure.

Alors que les événements en France ont de nouveau soulevé l'épineux débat sur la liberté d'expression, le pays serait en bonne voie de convaincre les membres de l'Union européenne de mettre en place des dispositifs de contrôle pour surveiller les communications chiffrées.

[…]
Selon le média autrichien ORF, face à ces récents événements, en cinq jours, le conseil des ministres de l'Union européenne s'est accordé sur de nouvelles mesures anti-terroristes. Plus précisément, un texte pour une proposition de loi vise à obliger les opérateurs de messageries sécurisées à mettre en place des backdoors. Ces portes dérobées permettraient aux services de renseignement d'accéder au contenu des conversations sécurisées.

La France serait particulièrement impliquée dans ce projet initié par la Grande-Bretagne. Le secrétaire d'État français à

l’Europe, Clément Beaune, s’est entretenu avec la ministre européenne Karoline Edtstadler, membre du parti populiste en Autriche.

.

Un accès exceptionnel imposé

Lors d’une conversation chiffrée, les échanges sont sécurisés entre les deux parties. Sur une messagerie mobile, le principe du chiffrement est simplifié mais bien en place. Les deux parties disposent chacune d’une clé publique et d’une clé privée. L’expéditeur d’un message utilise indirectement la clé publique de son destinataire pour crypter le contenu. Ce dernier est capable de déchiffrer le message avec sa propre clé privée.

Toutefois, les messages transitent le plus souvent via un serveur. Les autorités demandent à ce que les opérateurs mettent à disposition des jeux de clés supplémentaires et identiques afin de pouvoir déchiffrer les messages. Le processus repose sur la notion d’un « accès exceptionnel ». Cette proposition émane du centre national de cybersécurité britannique, une division des services des renseignements GCHQ.

Concrètement, WhatsApp ou Signal autoriseraient en quelque sorte des intrusions de type « *man-in-the-middle* ».

Ce dispositif de surveillance est possible lorsqu’il y a un serveur tiers. Ce n’est pas le cas avec Olvid, une jeune pousse française qui expliquait récemment avoir conçu la messagerie la plus sécurisée du monde.

[…]

Il est également expliqué que si les autorités sont légalement en mesure de récupérer des données, ces dernières ne sont pas

lisibles.

Le texte devra être adopté par le groupe de travail du Conseil sur la coopération dans le secteur de la sécurité nationale (COSI) le 19 novembre. La semaine suivante, il sera présenté au Conseil des représentants permanents des États membres de l'UE.

Début décembre, ce projet sera ensuite envoyé au parlement européen. Néanmoins, selon ORF : « *Compte tenu de l'apparente unanimité, il serait toutefois possible que le Conseil des ministres mette en œuvre le règlement envisagé dans son essence, même sans l'implication du Parlement.* »

Source : ORF via Google Translate

https://www.clubic.com/messagerie-instantanee/actualite-20557-la-france-pousse-l-ue-a-affaiblir-le-chiffrement-des-messageries.html

.

Cela se poursuit par l'accord de Bruxelles qui devrait faire voter cela incessamment cela au parlement. Or on n'en a pas entendu parler, ce qui signifie sans doute que, une fois de plus, la dictature bruxelloise piétine le Parlement qui ne sert que de chambre d'enregistrement des décisions de Der Leyen, et est son alibi démocratique.

Le texte bruxellois qui prouve que tout cela n'est pas « du complotisme » ni du délire de persécution :

https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf

Et sa traduction google ci-dessous. On voit en passant que Bruxelles ne se bat par pour les peuples d'Europe, ni pour

l’Europe mais pour « des règles mondiales » c’est écrit en toutes lettres. Et il y a encore des millions de traîtres prêts à voter pour des Européistes !!!!!

12143/1/20 REV 1
MP / dk
1
JAI.1
LIMITE
FR

Conseil de la Union européenne Bruxelles, le 6 novembre 2020 (OU. En) 12143/1/20
REV 1 LIMITE JAI 851 COSI 156 CHATS 73 ENFOPOL 256 COPEN 287 DATAPROTECT 106 CYBER 198 IXIM 107
REMARQUE

De:
Présidence
À:
Délégations
Matière:
Projet de résolution du Conseil sur le cryptage
– Sécurité par cryptage et sécurité malgré le cryptage

Les délégations trouveront en pièce jointe la version révisée **1** du projet de résolution du Conseil sur Chiffrement. Il reflète les commentaires reçus des États membres avant et pendant la réunion informelle VTC des conseillers JAI (cryptage) le 3 novembre 2020.

À moins que les délégations n’envoient d’autres observations de fond, accompagnées d’un libellé concret suggestions, avant le 12 novembre 2020 midi, à paul.gaitzsch@diplo.de, COSI.DE2020@bmi.bund.de et cosi@consilium.europa.eu, la présidence a l’intention de présenter ce texte révisé pour approbation au COSI (VTC) le 19 novembre 2020, en vue d’une nouvelle soumission au COREPER (point I)
le 25 novembre 2020, suivie de l’adoption par le Conseil par procédure écrite.

Veuillez noter que la forme du document a été adaptée à une « résolution du Conseil », de sorte que le texte pourrait être traité pour adoption via une procédure écrite par le Conseil au cas où il aurait lieu au format VTC

12143/1/20 REV 1
MP / dk
1
JAI.1
LIMITE
FR

Conseil de laUnion européenne
Bruxelles, le 6 novembre 2020(OU. En)12143/1/20REV 1
LIMITE JAI 851 COSI 15 CHATS 73 ENFOPOL 256 COPEN 287DATAPROTECT 106 CYBER 198 IXIM 107
REMARQUE

De:
Présidence
À:
Délégations
Matière:
Projet de résolution du Conseil sur le cryptage
– Sécurité par cryptage et sécurité malgré le cryptage

Les délégations trouveront en pièce jointe la version révisée **1** du projet de résolution du Conseil sur Chiffrement. Il reflète les commentaires reçus des États membres avant et pendant la réunion informelle VTC des conseillers JAI (cryptage) le 3 novembre 2020.

À moins que les délégations n'envoient d'autres observations de fond, accompagnées d'un libellé concret suggestions, avant le 12 novembre 2020 midi, à paul.gaitzsch@diplo.de, COSI.DE2020@bmi.bund.de et cosi@consilium.europa.eu, la présidence a l'intention de présenter ce texte révisé pour approbation au COSI (VTC) le 19 novembre 2020, en vue d'une nouvelle soumission au COREPER (point I) le 25 novembre 2020, suivie de l'adoption par le Conseil par procédure écrite.

Veuillez noter que la forme du document a été adaptée à une « résolution du Conseil », de sorte que le texte pourrait être traité pour adoption via une procédure écrite par le Conseil au cas où il aurait lieu au format VTC.

1

Les modifications par rapport à la version précédente sont signalées en **gras, soulignées** et barrées

ANNEXE

Projet de résolution du Conseil sur le cryptage

Sécurité grâce au cryptage et à la sécurité malgré le cryptage

1. Préambule: Sécurité par cryptage et sécurité malgré le cryptage

L'Union européenne soutient pleinement le développement, la mise en œuvre et l'utilisation d'un cryptage fort.

Le cryptage est un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des gouvernements, industrie et société. Dans le même temps, l'Union européenne doit garantir la capacité des **autorités compétentes dans le domaine de la sécurité et de la justice pénale, par exemple le** droit autorités répressives et judiciaires, pour exercer leurs pouvoirs légaux, en ligne et hors ligne.

Selon les conclusions du Conseil européen des 1er et 2 octobre 2020 (EUCO 13/20), *l'UE tirer parti de ses outils et de ses pouvoirs réglementaires pour contribuer à façonner les règles et normes mondiales.* Il a été convenu que les fonds au titre du mécanisme de relèvement et de résilience seraient utilisés pour faire avancer des objectifs tels que *renforcer la capacité de l'UE à se protéger contre les cybermenaces, à assurer un environnement de communication, notamment grâce au cryptage quantique, et pour garantir l'accès aux données à des fins judiciaires et répressives.*

2. Utilisation actuelle / état du cryptage

Dans le monde d'aujourd'hui, la technologie de cryptage est de plus en plus utilisée dans tous les domaines de la vie publique et privée. Il est un moyen de protéger les gouvernements, **les infrastructures critiques,** la société civile, les citoyens et l'industrie en assurer la

confidentialité, la **confidentialité** et **l'intégrité** des **données** des communications et des données personnelles: il est Il est évident que toutes les parties bénéficient d'une technologie de cryptage haute performance. Le chiffrement a été identifié par les autorités de protection des données de l'UE comme un outil important contribuant par exemple à protection des données personnelles transférées en dehors de l'UE **mais sous réserve de l'exigence d'un niveau de protection essentiellement équivalent** , qui selon la Cour de justice est un
exigence pour les transferts de données **2** . Non seulement les appareils électroniques et les applications programmé pour crypter les données utilisateur stockées par défaut, mais de plus en plus de canaux de communication sont également sécurisé par un cryptage de bout en bout (E2E). Cela se traduit positivement par une réponse croissante par l'industrie de la communication et des applications, où la majorité des applications de messagerie instantanée et d'autres plates-formes en ligne ont également mis en œuvre un cryptage de bout en bout.

2

Arrêt du 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner / Facebook Ireland Ltd,
Maximillian Schrems, ECLI: EU: C: 2020: 559:

---

3. Défis pour garantir la **sécurité** publique

La «vie numérique» et le cyberespace présentent non seulement de grandes opportunités, mais aussi des défis considérables: la numérisation des sociétés modernes comporte certaines vulnérabilités et le potentiel de **exploitation à des fins criminelles.** Ainsi, les criminels peuvent inclure facilement disponibles, prêts à l'emploi des solutions de cryptage conçues à des fins légitimes dans leur *modi operandi* **3** . Dans le même temps, les forces de l'ordre dépendent de plus en plus de l'accès aux preuves électroniques pour
lutter efficacement contre le terrorisme, le crime organisé, les abus sexuels sur les enfants (en particulier ses aspects

en ligne),
ainsi qu'une variété de crimes cybernétiques. **Pour les autorités compétentes, accès aux les preuves ne sont pas seulement essentielles pour mener à bien des enquêtes et ainsi** amener les criminels à la justice **, mais aussi pour protéger les victimes et contribuer à assurer la sécurité** . Cependant, il existe des cas où le chiffrement rend l'analyse du contenu des communications dans
le cadre d'accès aux preuves électroniques extrêmement difficile **ou pratiquement impossible malgré le fait que l'accès à ces données serait légal.** Indépendamment de la technologie environnement du jour, il est donc essentiel de préserver les pouvoirs des autorités **compétentes en le domaine de la sécurité et de la justice pénale** grâce à un accès légal pour mener à bien leurs tâches,
prescrite et autorisée par la loi. Ces lois prévoyant les pouvoirs d'exécution doivent toujours respecter pleinement la procédure régulière et les autres garanties, ainsi que les autres libertés et droits, en particulier droit au respect de la vie privée et des communications et droit à la protection des données personnelles.
4. Créer un **meilleur** équilibre
Le principe de sécurité par cryptage et de sécurité malgré le cryptage doit être respecté intégralité. L'Union européenne continue de soutenir un cryptage fort. Le chiffrement est un point d'ancrage de confiance dans la numérisation et **dans la protection des droits fondamentaux et** devrait être promue et développé.
Protéger la confidentialité et la sécurité des communications grâce au cryptage et en même temps confirmant la possibilité pour **les** autorités **compétentes dans le domaine de la sécurité et de la justice pénale** de accéder légalement des données pertinentes pour légitimes, à des fins clairement définies dans la lutte grave **et / ou les** crimes **organisés et le terrorisme** , y compris dans le monde numérique, sont extrêmement importants. Tout les mesures prises doivent soigneusement équilibrer ces intérêts

.

Que faire ?

Je n’ai quant à moi rien à cacher, je dis et j’écris sur ce site ce que je dis et écris via les messageries. Il n’empêche que l’idée même que, comme dans la défunte URSS des gens mal intentionnés, dans la dictature qui est en train de s’installer en France, mais pas seulement, puissent avoir accès à mes échanges privés. Surtout eu égard aux attaques que subissent la liberté d’expression et la liberté tout court. Il est évident que l’on va devoir, de plus en plus, faire de la Résistance et se cacher pour des choses aussi simples qu’un repas entre amis ! Alors il nous faut une messagerie sûre pour échanger entre amis, entre personnes de la même famille, entre adhérents et Résistants.

C’est pourquoi nous avons anticipé et acheté les droits d’une messagerie cryptée dans un pays échappant au totalitarisme européen, la Russie. On ne peut s’inscrire sur cette messagerie que si l’on est parrainé, ce qui en accroît la sécurité.

J’enverrai la semaine prochaine à tous nos adhérents les moyens d’avoir une adresse sur cette messagerie et je vais commencer à utiliser moi aussi cette messagerie, abandonnant peu à peu mes anciennes adresses.

Qui eût dit, il y a 70 ans, que c’est en Russie que l’on trouverait le monde libre ?