L'astuce qui permet à l'anti-terrorisme de consulter des centaines de messageries chiffrées

En attendant les contentieux...

7 • 0

DROIT 19 MIN

Par Jean-Marc Manach
Le vendredi 11 juin 2021 à 16:46

Signaler une erreur Offrir

Auditionné à l'Assemblée, Gérald Darmanin a révélé un « truc » – ou « hack », au sens de détournement créatif d'une fonctionnalité non prévue à cet effet. Il permet aux autorités d'accéder aux messageries chiffrées de personnes radicalisées, mais également d'éclairer la surveillance « algorithmique » des « URL ».

Adoptées en 2017 à l'occasion de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT), les Mesures individuelles de contrôle administratif et de surveillance (**MICAS**) visent « *toute personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics* ».

Soit parce qu'elle « *entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme* », soit parce qu'elle « *soutient, diffuse ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* ».

Les MICAS permettent depuis au ministère de l'Intérieur d'interdire aux personnes visées de :

- se déplacer à l'extérieur d'un périmètre géographique déterminé, « *qui ne peut être inférieur au territoire de la commune* »,
- se présenter périodiquement aux services de police ou aux unités de gendarmerie, « *dans la limite d'une fois par jour* »,
- paraître dans un lieu déterminé,
- se trouver en relation directe ou indirecte avec certaines personnes, « *nommément désignées* »,

La loi SILT avait également prévu, pour les mêmes raisons, de **permettre** au juge des libertés et de la détention (JLD) du tribunal judiciaire de Paris, par une ordonnance écrite et motivée et après avis du procureur de la République antiterroriste, d'autoriser « *la visite d'un lieu ainsi que la saisie des documents et données qui s'y trouvent* […] *lorsqu'il existe des raisons sérieuses de penser qu'il est fréquenté par une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics* ».

La loi précise cela dit que ne peuvent être concernés les « *lieux affectés à l'exercice d'un mandat parlementaire ou à l'activité professionnelle des avocats, des magistrats ou des journalistes et les domiciles des personnes concernées* ».

Le texte prévoit en outre que, et « *aux seules fins de prévenir la commission d'actes de terrorisme* », si la perquisition (rebaptisée « *visite domiciliaire* ») révèle l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, « *il peut être procédé à leur saisie ainsi qu'à celle des données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite* ».

+1 100 % de visites domiciliaires et saisies de données

Lors de son **audition** par la commission des lois au sujet du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, le 17 mai dernier, Gérald Darmanin avait précisément été interrogé par le député (LFI) Ugo Bernalicis au sujet de ces MICAS :

> « *Bien évidemment, je partage l'objectif que vous avez tous rappelé : prévenir la commission d'actes terroristes. Nous devons faire tout notre possible pour l'atteindre, avec discernement et équilibre. […] Déjà, lors de l'examen de la loi SILT, nous nous étions opposés aux MICAS. Notre position n'a pas varié. Nous continuons à nous demander pourquoi la procédure n'est pas judiciaire. Vous avez parlé des visites domiciliaires qui auraient permis de déjouer des attentats : si l'attentat était imminent, pourquoi la procédure n'a-t-elle pas été judiciarisée ?* »

En réponse, le ministre de l'Intérieur explique que, pour ce qui est de la judiciarisation, « *les visites domiciliaires, qui sont extrêmement efficaces et utiles, sont toujours autorisées par le juge des libertés. Le ministre de l'Intérieur ne peut pas décider des perquisitions en s'affranchissant des règles* » :

> « *Lorsque nous pensons avoir identifié une personne dangereuse, nous adressons un dossier au juge ; s'il estime que ce dossier n'est pas assez solide, il ne donne pas son autorisation et il n'y a pas de visite domiciliaire. En France, le ministre de l'Intérieur ne peut pas décider seul d'entrer chez les gens, quand bien même ils seraient soupçonnés de préparer un acte terroriste.* »

C'est ainsi qu'au lendemain de la mort de Samuel Paty, le 16 octobre 2020, « *j'ai pris la décision, à la demande du Président de la République, d'organiser plus de 200 visites domiciliaires* », explique le ministre.

En comparant le **décompte** des mesures de police administrative prises dans le cadre de la loi SILT, tel qu'affiché sur le site web de l'assemblée nationale, avec les sauvegardes qu'en avait fait archive.org, on découvre effectivement une véritable explosion du nombre de visites et saisies effectuées sous couvert de MICAS.

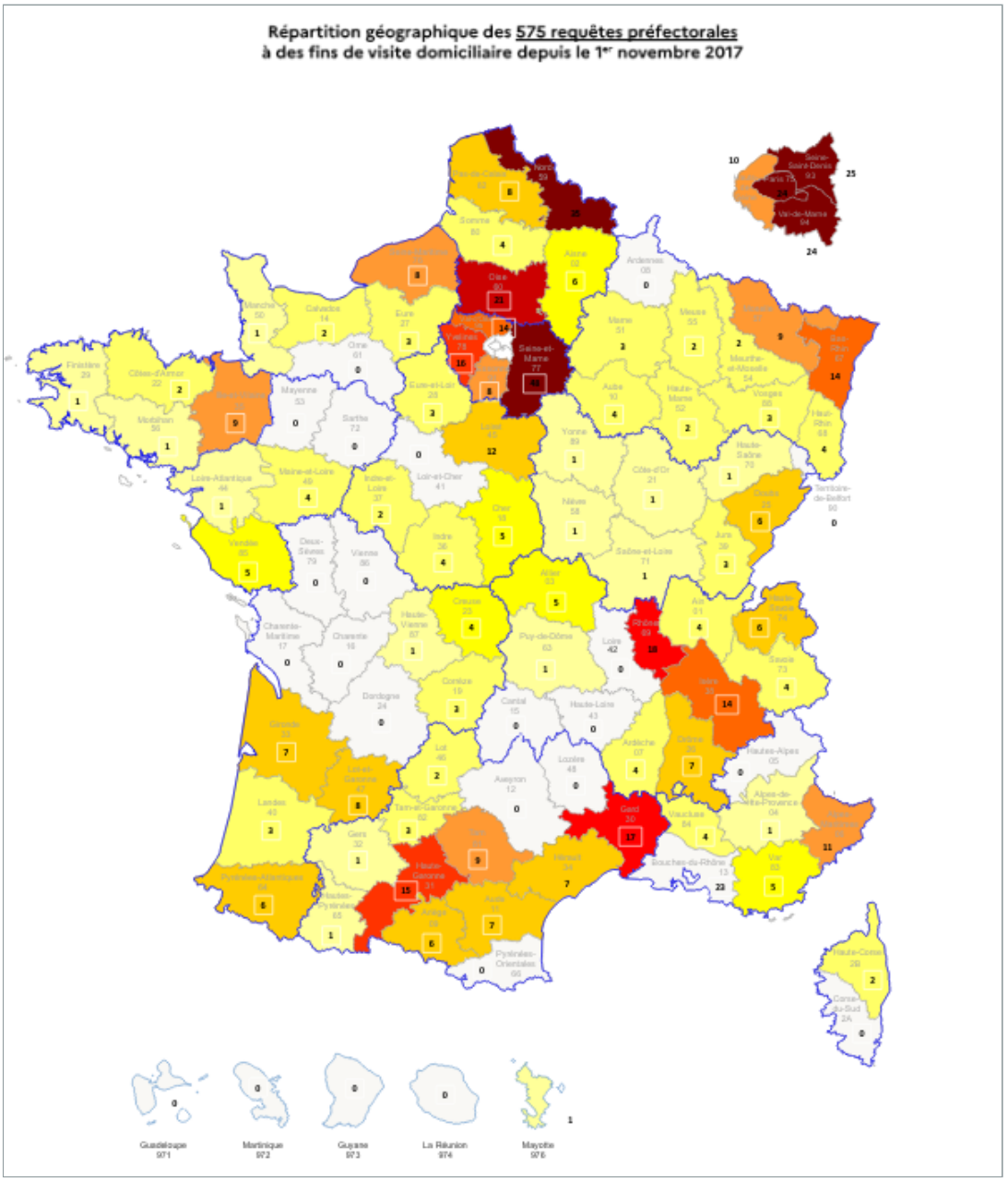
Au 2 octobre 2020, elle **recensait** en effet 231 requêtes préfectorales de visites domiciliaires et saisies cumulées depuis 2017, dont 188 « *données* » et 41 « *refusées* » par ordonnances du JLD, 174 visites et 98 saisies effectuées, 94 autorisations d'exploitation de données autorisées et 4 refusées, avec 1 seul contentieux recensé.

Or, les chiffres à jour au 5 mars 2021 **cumulaient** 575 requêtes préfectorales de visites et saisies, dont 504 « *données* » et 63 « *refusées* » par ordonnances du JLD, 451 visites et 239 saisies effectuées, 206 autorisations d'exploitation de données autorisées et 11 refusées, avec 31 contentieux recensés…

alors que la seconde période est prêt de deux fois plus courte, le nombre de visites est passé de 23 à 277 (soit +1 108 %), celui des saisies effectuées de 14 à 141 (+ 1 007 %), et les demandes d'autorisation d'exploitation de données accordées de 14 à 112 (+800 %). Et ce, alors même que l'on ne dénombrait plus que 64 mesures individuelles de contrôle administratif et de surveillance « *en vigueur* ».

+ 3 400 % de contentieux

La répartition territoriale **montre (.pdf)** par ailleurs de (très) grandes disparités en fonction des régions et des départements, la Seine-et-Marne, le Nord et l'Île de France étant largement surreprésentés.



Le Gouvernement **indique** que « *57 visites domiciliaires ont donné lieu à des poursuites pénales dont 30 pour des faits de terrorisme* » :

> « *Si 14 visites domiciliaires ont ensuite donné lieu au prononcé de MICAS, 39 ont ciblé des individus faisant l'objet d'une MICAS. Dans le contexte de l'assassinat de Samuel Paty, le rapport d'application de la loi SILT relève que 272 requêtes préfectorales de visites domiciliaires ont été adressées au JLD entre le 18 octobre et le 23 novembre 2020, soit davantage qu'au cours des trois premières années d'application de la loi SILT.* »

> « *Leur objet était de consulter, sur des tablettes, des ordinateurs et des téléphones tenus cachés, les messages qui ne pouvaient pas être écoutés à distance, parce qu'ils avaient été échangés sur les nouveaux types de messagerie que j'ai évoqués tous à l'heure.* »

En l'espèce, ces visites auraient « *permis d'ouvrir nombre de procédures judiciaires* », mais sans que le ministre ne précise pour autant combien l'auraient été suite à la découverte de « *messages qui ne pouvaient pas être écoutés à distance* ».

Le ministre ne précise pas non plus combien de suspects auraient refusé de déverouiller leurs téléphones et/ou messageries, combien de demandes d'autorisation d'exploitation de données auraient été couronnées de succès ou, a contrario, auraient résisté au Centre technique d'assistance (CTA), l'unité de la DGSI chargée de décrypter les données chiffrées.

Il n'en reste pas moins que plus de la moitié des visites domiciliaires ont entraîné une saisie de données, qu'elles ont quasiment toutes fait l'objet de demandes d'autorisation d'exploitation de ces données – signe que le suspect avait potentiellement refusé de déverouiller un ou plusieurs comptes ou terminaux –, et que seules 11 d'entre elles ont été refusées par le JLD.

4. Visites et saisies (articles L. 229-1 à L. 229-3 du code de la sécurité intérieure)

	Requêtes préfectorales	Ordonnances du JLD		Visites effectuées	Saisies effectuées	Demandes d'autorisation d'exploitation de données	Autorisations d'exploitation		Contentieux (cumul)
		Donnée	Refusée				Donnée	Refusée	
Au 14 mai 2021	591	518	65	463	244	226	210	11	34

Le fait que le dernier décompte, en date du 14 mai dernier, ne **dénombre** que 16 requêtes préfectorales, 12 visites et 5 saisies effectuées, ainsi que 4 autorisations d'exploitation de données accordées depuis le 5 mars, montre par ailleurs qu'il s'agissait probablement de mesures opportunistes prises suite au meurtre de Samuel Paty.

Pour autant, et d'un point de vue judiciaire, il n'est pas anodin de constater que le ministère de l'Intérieur n'avait enregistré en octobre 2020 qu'un seul et unique contentieux depuis 2017 à la rubrique visites et saisies, alors que le total cumulé du décompte en date du 5 mars dernier en totalisait 31 (soit +3 100 %), et 34 au 14 mai (+3 400 %).

Il sera dès lors intéressant de découvrir ce qu'en dira la jurisprudence, mais également ce qui motiverait cette explosion de recours.

En attendant, le **projet de loi Renseignement** « *prévoit, à titre dérogatoire, la possibilité de prolonger à deux ans la durée cumulée de la mise en œuvre des MICAS* », contre un an auparavant. Le gouvernement précise au demeurant qu'« *environ 75 % des personnes faisant l'objet de MICAS sont des sortants de prison* ».

Il propose également de « *permettre la saisie de supports informatiques au cours de visites domiciliaires en cas d'opposition de la personne concernée* » et « *dès lors que l'occupant du domicile fait obstacle à l'accès aux données contenues dans ces supports* ».

En l'état, la saisie de documents et données précitées ne pouvait en effet être mise en œuvre qu'« *à condition qu'un lien avec la menace alléguée soit établi* ». Or, souligne le projet de loi, « *certaines données stockées dans des supports informatiques peuvent être inaccessibles, en raison de mots de passe que l'occupant du domicile visité refuse de communiquer à l'autorité administrative, ce qui empêche en conséquence de procéder à leur saisie* ».

L'absence de méta-données téléphoniques rend suspect

Le ministre tient tout d'abord à préciser que « *les dispositions que nous vous proposons n'ont pas pour objet de viser toutes les informations de l'internet français, comme vous le craignez, mais bien de cibler les personnes* », notamment en matière de trafic de drogue et de grande criminalité. Il cite à ce sujet **l'opération** de la gendarmerie ayant permis d'arrêter des centaines d'utilisateurs du cryptophone Encrochat.

Il fait ensuite la distinction « *entre les réseaux sociaux qui ont un système de messagerie, d'une part, et les messageries cryptées, d'autre part* », tout en précisant que « *l'utilisation des messageries des réseaux sociaux par des terroristes est très inquiétante* ». Sans rentrer dans le détail d'affaires « *couvertes par le secret de l'enquête ou par le confidentiel défense* », il en évoque quand même deux, rendues publiques dans la presse.

Le terroriste de la basilique de Nice avait ainsi circulé pendant plusieurs semaines sur le territoire européen avant d'arriver en France, sans jamais utiliser sa ligne téléphonique ni envoyer de SMS : « *il n'est passé que par la messagerie de Facebook, à laquelle nous n'avons pas accès. Qu'il n'ait pas utilisé son téléphone pour téléphoner devrait attirer notre attention !* »

D'autre part, l'homme qui a tué Samuel Paty avait quant à lui « *manifestement communiqué avec des personnes qui se trouvaient sur le théâtre irako-syrien à travers la messagerie d'Instagram* ». Dès lors « *des écoutes téléphoniques classiques ne nous auraient donc rien appris* ».

Profiter du fait que les messageries chiffrées passent par Internet

Gérald Darmanin revient ensuite sur les « *messageries cryptées [sic], comme Telegram, WhatsApp ou Signal, [qui] ont précisément bâti leur modèle économique sur la garantie de ne pas pouvoir être écouté* » :

> « *Que les choses soient claires : il ne s'agit pas d'écouter les conversations téléphoniques qui se font sur ces applications mais de profiter du fait qu'elles passent par des connexions internet. Pour les cibles les plus dangereuses, et sous le contrôle de la CNCTR, le recueil des données informatiques permettra d'accéder au terminal informatique de la personne qui utilise ces messageries pour recueillir les données qui sont stockées dans ces messageries. Il ne s'agit donc pas d'écoutes classiques, vous l'aurez compris.* »

Lui aussi interrogé à ce sujet, Jean-Michel Jacques, rapporteur pour avis, explique pour sa part qu'« *elles représentent un problème technique majeur* » :

> « *Nos services de renseignement disposent de laboratoires de recherche et de développement, et améliorent continuellement leurs techniques d'investigation, de façon à se mettre au niveau de l'utilisation que des terroristes peuvent faire de ces messageries. À ce stade, cela n'appelle pas de réponse sur le plan juridique. La question est cependant d'actualité : nos services travaillent sur le sujet.* »

Lors des débats précédent l'adoption du projet de loi à l'Assemblée, la principale innovation du texte – l'extension de l'usage des algorithmes aux URL –, a été « *évacuée en moins de quarante-cinq minutes* », **déplore** Le Monde, le député (LFI) Ugo Bernalicis ayant été celui qui a posé le plus de questions :

> « *Pourrez-vous collecter et exploiter les adresses en https et, le cas échéant, comment ? Comment ferez-vous pour ceux qui utilisent des VPN – réseaux privés virtuels –, c'est-à-dire des voies détournées pour passer par d'autres serveurs ? Allez-vous obliger les opérateurs de messagerie cryptée à installer des portes dérobées, sous peine de les retirer de l'App Store ou de Google Play ? Concrètement, comment cela va-t-il fonctionner ? Enfin, pour le traitement automatisé des données, allez-vous avoir recours aux services de l'entreprise Palantir ?* »

Des questions restées sans réponses, la ministre des Armées tout comme le rapporteur, Loïc Kervran, se drapant derrière des « *impératifs de sécurité* ». La première n'en a pas moins répondu que « *non, nous n'imposons pas l'installation de pièges et que nous n'utilisons pas Palantir pour les algorithmes* ». Le second, par ailleurs membre de la délégation parlementaire au renseignement (DPR), que le dispositif pourrait profiter de certaines « *erreurs* » commises par les personnes aux comportements suspects :

> *personnellement, tout comme nos services. Je ne suis assuré, y compris sur des cas réels, que, comme le disait Mme la ministre, cet algorithme présente un intérêt, notamment à cause des erreurs que font les cibles qui nous intéressent. C'est une technique pertinente et les URL représentent pour l'algorithme une information non négligeable.* »

Une analyse confirmée par Florence Parly : « *Oui, les apprentis terroristes commettent parfois des erreurs, et ne comptez pas sur moi pour vous dire lesquelles. Heureusement qu'ils font des erreurs et que nous les exploitons. Mais il ne m'appartient pas de vous dire, dans l'hémicycle, quelles sont les erreurs commises* ».

Le rapporteur a en outre justifié l'algorithme au motif qu'« *il fonctionne avec les données téléphoniques, et nous voulons que ce soit également le cas avec les données URL. Pourquoi ? Parce qu'une grande partie des communications n'utilisent pas un protocole téléphonique, mais un protocole internet* [...] *cela permettra de capter des communications qui pourraient éventuellement nous intéresser, grâce à un algorithme bien paramétré pour les détecter* ».

Comment les services s'attaquent au chiffrement

Les services de renseignement, comme nous l'avons **déjà relevé**, ont depuis des années développé des « *capacités techniques interministérielles* ». Ces CTIM « *regroupent autant les besoins d'interceptions (câbles sous-marins, etc.) que le Pôle national de cryptanalyse et de décryptement (PNCD)* », à savoir le super-calculateur de décryptage des communications chiffrées créé en 1999 en contrepartie de la libéralisation de l'usage de la cryptographie par les entreprises et le grand public.

- **Décryptage de capacités « secret défense » de la DGSE**

En septembre 2020, la commission des finances de l'Assemblée nationale **indiquait** pour sa part que « *les besoins liés aux CTIM concernent principalement la cryptanalyse et le décryptement, les projets d'acquisition de moyens matériels et logiciels d'un programme de big data ainsi que les travaux de modernisation du dispositif de surveillance internationale* ».

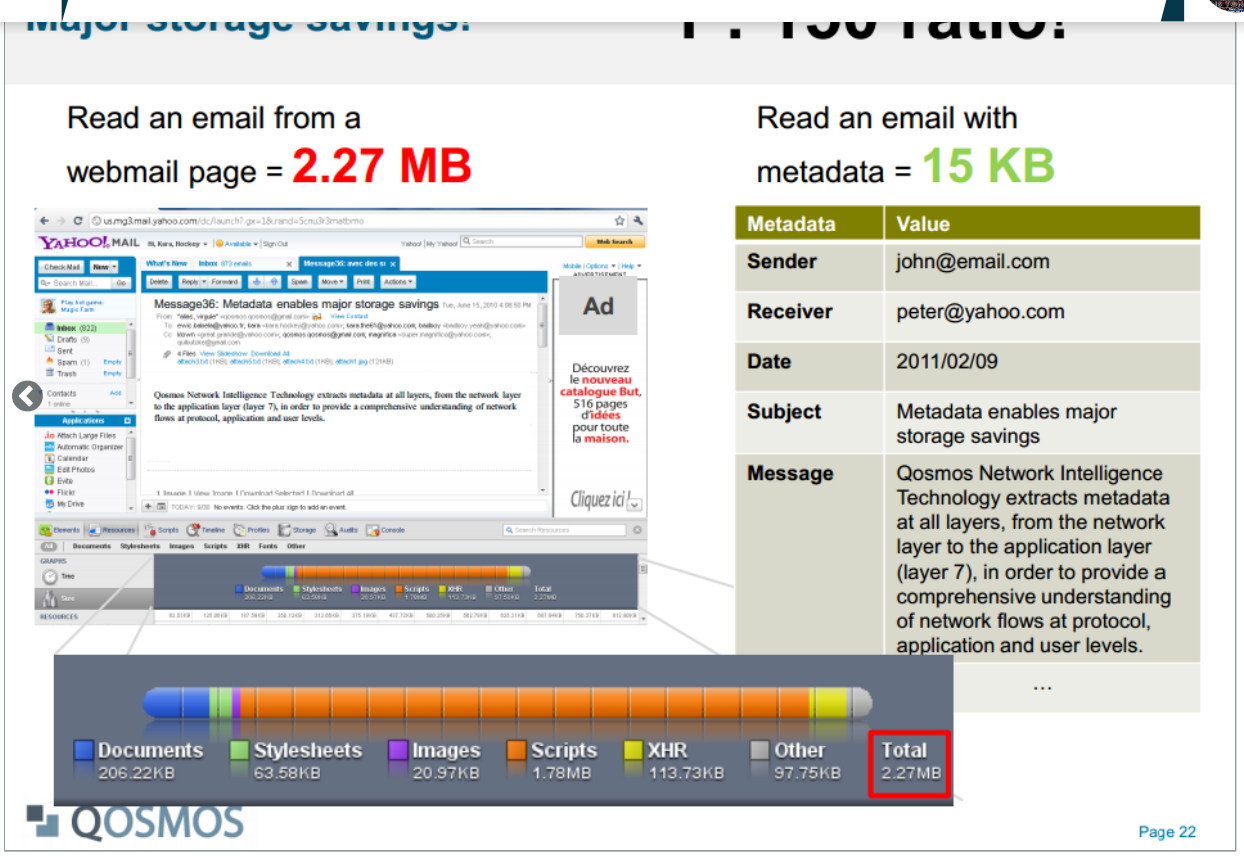
Reste donc encore à savoir si ce programme de « *big data* » porterait en tout ou partie sur la surveillance algorithmique des méta-données téléphoniques, tel qu'adopté par la loi Renseignement en 2015, et celle des « *adresses complètes de ressources utilisées sur internet* » (pour reprendre la formulation ésotérique du gouvernement) et étrangement assimilée aux seules URL, quand bien même personne ne **parvient** à comprendre comment elle pourrait fonctionner, ni même si elle pourrait fonctionner.

Sauf à imaginer, **hypothèse** que nous avons déjà formulée, que les algorithmes cherchent en fait à analyser le trafic chiffré pour identifier certains patterns bien particuliers, à commencer par les utilisateurs de telles ou telles applications en particulier, dont l'utilisation aurait été avérée par des terroristes ou criminels en bande organisée, à l'image des **cryptophones** Encrochat et SKY ECC qui ont récemment défrayés la chronique, par exemple.

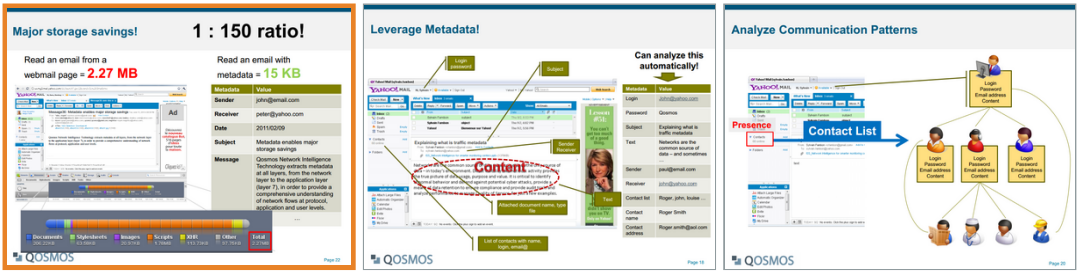
L'un des documents Snowden avait ainsi **révélé** que la DGSE avait mis en relation son « *principal partenaire industriel* » avec le GCHQ, en 2009, à mesure qu'il pouvait l'aider à relever « *ce qui était devenu le plus grand défi du GCHQ – continuer à effectuer une surveillance en masse, malgré la propagation du chiffrement en ligne commercial, en cassant ce chiffrement* » (des télécommunications -ndlr).

Les Français s'étaient alors déclaré « *clairement très désireux de fournir des présentations sur leur travail qui comprenait la détection de chiffrement dans les supports à grande vitesse* ». On a depuis eu confirmation que ce partenaire n'était autre que Qosmos, un des leaders de l'inspection des paquets en profondeur (DPI), et que c'était la DGSE qui lui avait **donné l'idée** de se lancer sur le juteux marché de l'interception légale.

Qosmos se **présentait** alors comme capable d'« *identifier les applications cachées derrière la majeure partie des flux chiffrés en utilisant des techniques avancées d'analyse statistique, de prédiction de session et d'inspection des certificats* », mais également de filtrer les flux de sorte de n'avoir qu'à analyser que les seules méta-données.



DPI Qosmos

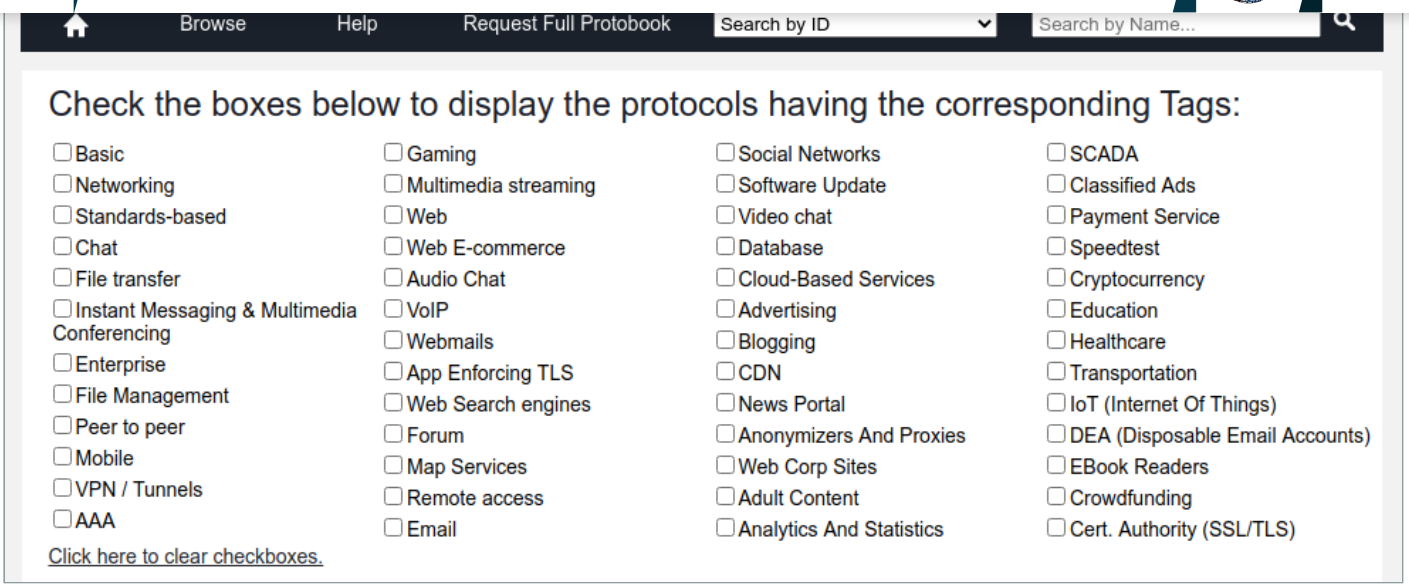


Qosmos se **targuait** également de pouvoir reconnaître plus de 1 300 protocoles différents, et d'être capable d'extraire plus de 6 000 types de métadonnées, tout en réduisant le poids des données à analyser par un ratio de 150.

Ce qui, vu qu'il est aussi question de **rerouter** les paquets de données sur les infrastructures centralisées du Groupement Interministériel de Contrôle (GIC), chargé de « *centraliser* » les techniques de renseignement pour le compte de la Commission nationale de contrôle des techniques de renseignement (CNCTR), représenterait un fort appréciable facteur d'économies financières et d'énergie.

Depuis, Qosmos explique pouvoir analyser le trafic (même et y compris « ***chiffré ou obscurci*** ») de données « *en temps réel et à grande vitesse lorsqu'il traverse les réseaux* », via la reconnaissance de **plus de 3500 protocoles**.

Il serait ainsi, et entre autres, capable d'identifier 8 différents types de protocoles chiffrés (dont SSH, SSL, TOR, I2P), mais également 13 protocoles liés à des crypto-monnaies (Bitcoin, Monero, Ripple et Ethereum), 24 anonymizers et proxies, 37 « *contenus pour adultes* », 90 VPN, 111 messageries instantanées (dont WhatsApp, Telegram et Signal), 150 jeux vidéo, 300 protocoles de streaming, etc.



On comprend mieux, dès lors, ce pourquoi ce que le projet de loi, dont l'étude d'impact évoquait des « *traitements automatisés tirant bénéfice des nouvelles possibilités offertes par les URL* » (quand bien même **cela serait impossible**, du fait que plus de 90 % du trafic étant chiffré) a préféré l'expression plus ésotérique d'« *adresses complètes de ressources utilisées sur internet* ».

De quoi nourrir notre **hypothèse** que ces nouveaux algorithmes, en analysant le trafic chiffré, chercheraient plutôt à identifier les utilisateurs de telles ou telles applications en particulier, permettre de deviner l'identité d'un anonyme diffusant des messages sur des réseaux sociaux, d'identifier la probabilité que deux individus communiquent entre-eux, ou encore d'établir le profil comportemental et les habitudes d'internautes anonymes.

Reste encore à identifier comment et où les flux pourraient être dupliqués par le GIC, comme nous **le relevions** précédemment. Au vu du coût « *évalué à 20 millions d'euros pour l'achat et la mise en œuvre des dispositifs techniques et de 4 millions d'euros annuels pour leur maintien en condition opérationnelle* », le plus simple serait probablement d'utiliser les « *boîtes noires* » d'ores et déjà installées par la DGSE sur tout ou partie de la **vingtaine de points d'atterrissement** français des câbles sous-marins.

Cela reviendrait certes à priver le GIC et la DGSI des données ne transitant pas à l'international, mais les sites web et applications mobiles, quand bien même franco-français, et soumis au RGPD, reposant de plus en plus sur des « *services* » proposés par des entreprises américaines (**à commencer par Google**, notamment), il est loisible de penser que la surveillance du trafic Internet « *à l'international* » permettrait de surveiller une partie non négligeable de l'Internet « *franco-français* ».

Et ce, d'autant plus que la notion même de « *surveillance de masse* » et donc indifférenciée est devenue un horizon inatteignable, et que les services de renseignement technique sont contraints à devoir être « *plus ciblés et proportionnés* », comme **l'expliquait** la semaine passée Mike Burgess, le directeur de l'Australian Security Intelligence Organisation (ASIO, l'équivalent australien de la NSA) :

> « *Plus de données ont été créées au cours des 2 dernières années que dans le reste de l'histoire de l'humanité. Compte tenu du volume et de la complexité des données, nous ne cherchons pas une aiguille dans une botte de foin, nous recherchons une aiguille dans un champ de foin.* »

Pour me contacter de façon sécurisée (voire anonyme), **c'est par là**.

7 commentaires

Br31zh - 11/06/21 à 17:36:06 **#1**

Ahah, je me demande combien d'années de R&D il a fallu pour trouver qu'analyser le mail directement était plus rentable que d'analyser la page de webmail. Et que le chopper pendant qu'il transite en SMTP en clair ou peu sécurisé (ou directement sur les serveurs éventuellement) était plus facile que casser la sécurité du webmail...

Idiogène - 11/06/21 à 18:50:54 **#2**

On tire d'abord, on vire à babord ensuite !

C'est vraiment très intéressant.

Estya - 11/06/21 à 19:18:52 **#3**

ho, pas souvent que les jeux vidéos sont cités. je suis curieux de savoir comment sont filtrés les échanges sur les chat intégrés...

vivienfr - 11/06/21 à 21:29:14 **#4**

Je pense que le gros du trafic est identifié par le SNI qui est en clair dans les connexions HTTPS.

Quand il est absent le certificat doit suffit à trouver de qui il s'agit.

Col._Tatane - 11/06/21 à 23:51:50 **#5**

> **vivienfr a écrit :**
>
> Je pense que le gros du trafic est identifié par le SNI qui est en clair dans les connexions HTTPS.
>
> Quand il est absent le certificat doit suffit à trouver de qui il s'agit.

Dans ce cas ils vont être bien embêtés avec l'arrivée de TLS 1.3 et ESNI (qui chiffre le SNI) ainsi que la montée en puissance de DoH (DNS over HTTPS)

Chiuchu - 12/06/21 à 00:29:24 **#6**

Article d'excellente qualité. Merci pour ces éclairages.

Que sait-on de la législation sur la gestion de ces données ensuite ? (Où, combien de temps, qui a accès, etc.)

A-t-on déjà le nom ~~du barbouze~~, ~~de l'ex-interne,~~ de la fuite absolument non liée aux services qui revend les données à IKEA, Orange et compagnie ?

Est-ce que ces données font partie de celles qui seront transférées à **des entités étrangères** ?

Merci.

Chiuchu - 12/06/21 à 00:41:37 **#7**

pas à la solde du pouvoir !

Je me demande comment tu vis. J'ai une image très négative du journalisme français. Tu connais l'adage, soit chômeur, soit péripatéticienne…

Avec les Gilets Jaunes, les attentats islamistes expliqués très très rapidement, et la déferlante fasciste, on a pu voir que la presse est majoritairement un haut-parleur des pires positions idéologiques et complètement déconnectée du réel.

Voir des gens comme toi ça me redonne un peu de moral. J'espère en découvrir d'autres.

@+

Votre commentaire

Connecté en tant que TheBigBug

Commentaire…

Envoyer