veiligheid van de staat
sûreté de l'état
VSSE

OBJET :

Préparation de l'audition du 28/04 en Commission de l'Économie de la Chambre des Représentants – Résolution 1182 relative aux applications de traçage des contacts.

Monsieur le Président,
Chers membres de la Commission,

Je tiens tout d'abord à vous remercier de m'avoir offert la possibilité de m'exprimer au sujet du développement des applications dites de « traçage des contacts ». Le fait que mon service soit de plus en plus souvent convié à ce genre de débat - j'ai d'ailleurs déjà été invité à prendre part à cette commission par le passé dans le cadre de la problématique de la 5G - constitue selon moi un signe de la confiance grandissante accordée par les parlementaires au professionnalisme des avis que nous mettons à disposition en tant que service.

Votre invitation à venir vous exposer notre vision concernant les applications de traçage des contacts ne m'est parvenue que vendredi dernier. Étant donné que des réponses concrètes n'ont pu être immédiatement apportées aux questions éventuelles, j'ai décidé de vous présenter un bref aperçu de trois aspects en rapport avec la thématique examinée aujourd'hui, que nous considérons comme essentiels en tant que service de renseignement :

1. Tout d'abord, j'aborderai la question du cadre juridique, et plus spécifiquement des mécanismes de contrôle.

2. Ensuite, nous examinerons les risques potentiels inhérents à l'introduction d'une application de traçage des contacts pour la survenue de menaces que mon service est légalement tenu de suivre.

3. Sur le plan des aspects techniques, enfin, nous passerons en revue une série d'éléments à ne pas négliger avant d'autoriser une application de traçage des contacts dans un contexte belge.

veiligheid van de staat
sûreté de l'état
VSSE

1. CONTEXTE JURIDIQUE

Penchons-nous dans un premier temps sur le **contexte juridique** des applications de traçage des contacts.

La Sûreté de l'État a pour mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté de la Belgique. Dans le cadre de cette mission, la VSSE a la possibilité de recourir aux méthodes de renseignement, telles que la collecte de données de communication électronique. Toutefois, la VSSE ne peut pas agir comme bon lui semble. Tant la conservation de ce type de données par des opérateurs de communication électronique que l'accès de la VSSE à ces données sont strictement réglementés.

La loi du 13 juin 2005 relative aux communications électroniques régit la conservation des données de communication électronique. Cette loi définit les catégories de données à conserver par les opérateurs, les conditions dans lesquelles ces données doivent être conservées, et détermine quelles autorités ont accès à ces données et à quelles fins celles-ci peuvent être utilisées. La loi prévoit notamment que les opérateurs sont tenus de conserver les données de trafic et de localisation - des données en rapport avec la communication - et que les services de renseignement et de sécurité peuvent réquisitionner ces données dans le cadre de leur mission de renseignement.

Un AR portant exécution de la loi relative aux communications électroniques spécifie par ailleurs les catégories de données à conserver par les opérateurs : données personnelles de l'utilisateur final, date et heure du début et de la fin d'un appel, données de localisation...

Lorsque, dans le cadre de sa mission de renseignement, la Sûreté de l'État veut avoir accès à ces données conservées par des opérateurs, une série de conditions doivent être remplies. La loi du 30 novembre 1998 organique des services de renseignement et de sécurité régit l'accès à ces données.

Tout d'abord, il convient de respecter les principes de subsidiarité et de proportionnalité. Les données de localisation et de trafic peuvent **uniquement** être réquisitionnées si des méthodes moins intrusives pour la vie privée se révèlent insuffisantes afin de collecter les informations nécessaires pour mener à bien la mission de renseignement. En outre, la

réquisition de ces données doit être proportionnelle à la gravité de la menace potentielle au sujet de laquelle la Sûreté de l'État mène l'enquête.

En outre, un contrôle étendu est prévu. En tant que dirigeant du service de la Sûreté de l'État, je suis tenu de prendre une décision motivée par écrit afin de permettre la mise en œuvre de la méthode de renseignement. Cette décision doit, au préalable, être portée à la connaissance d'une commission spécifique composée de trois magistrats, la Commission BIM, pour que la méthode de renseignement puisse être mise en œuvre. Le Comité permanent R, l'organe de contrôle du fonctionnement de mon service, est également compétent pour contrôler la méthode de renseignement.

La Sûreté de l'État doit mettre fin à la méthode dès que la menace potentielle a disparu, lorsque la méthode n'est plus utile à la finalité ou en cas de constat d'une illégalité. La Commission BIM et le Comité permanent R peuvent également suspendre et/ou mettre fin à la méthode en cas de non-respect des conditions légales ou de constat d'une illégalité. Il peut aussi être décidé de détruire les données déjà collectées.

Enfin, la loi prévoit que les données recueillies par la Sûreté de l'État ne peuvent être conservées plus longtemps que nécessaire aux fins pour lesquelles celles-ci ont été stockées.

À la suite de ces contrôles, il arrive que des méthodes d'importance cruciale soient mises en œuvre trop tardivement ou ne soient pas utilisées. En tant que service, nous restons néanmoins convaincus de l'intérêt général des contrôles, qui servent les droits et libertés démocratiques que notre service est d'ailleurs censé protéger.

Si la décision est dès lors prise de développer une application pour lutter contre le COVID-19, la Sûreté de l'État propose de mettre en place un cadre réglementaire qui devra prévoir des garanties semblables à celles reprises dans la loi relative aux communications électroniques et la loi organique des services de renseignement et de sécurité. Ainsi, il conviendra de définir clairement quelles catégories de données pourront être conservées, dans quelles conditions les données devront être conservées et comment - et donc à nouveau dans quelles conditions - autoriser l'accès à ces données, à quelles fins les données pourront être utilisées et, enfin, de prévoir un contrôle étendu en ce qui concerne le traitement des données.

Lors de cette présentation, nous verrons également que certaines applications se targuent de ne pas conserver de données et d'anonymiser les données d'identification éventuelles. Comme précisé dans la partie technique, cela reste à confirmer. Pour des raisons de sécurité, ces applications doivent faire l'objet de contrôles et il importe aussi de vérifier si de tels arguments sont fiables, où le croisement intervient, si certaines données ne peuvent pas être également utilisées dans un autre contexte (commercial)…

Gérer avec ces applications une extrême précaution est une question de prudence et de bonne administration.

2. RISQUES INHÉRENTS À L'INTRODUCTION D'UNE APPLICATION DE TRAÇAGE DES DONNÉES DE CONTACT

Je voudrais aborder à présent la question des risques liés à ces applications. Un risque se définit en termes de menace, d'une part, et de vulnérabilité, d'autre part.

Si nous considérons l'espionnage ou l'ingérence par des services de renseignement étrangers **sous l'angle de la menace,** il y a lieu de prêter attention à leurs capacités et à leur éventuelle intention de porter atteinte à notre pays. Ainsi, nous devons garder à l'esprit que certains pays ont développé une stratégie offensive leur permettant de se livrer à de l'espionnage technique à grande échelle, tant sur leur territoire qu'à l'étranger.

Les cyberattaques sont une réalité. En aucun cas nous ne pouvons exclure que des tiers *(lire : des nations moins « amies »)* tentent à l'avenir de tirer parti des vulnérabilités inhérentes à ce type d'applications. Et en particulier lorsque ces dernières sont utilisées à grande échelle, y compris par des personnes qui ont accès à des informations sensibles.

S'il devait être fait usage d'une application, nombre d'acteurs, parmi lesquels mon service, plaident en faveur de son développement par une entreprise belge. Mais qu'entend-on par « entreprise belge » ? Les parties prenantes doivent-elles être toutes belges ? La reprise d'une telle entreprise n'est-elle dès lors pas permise ? Les membres de la direction ou les développeurs peuvent-ils être d'une autre nationalité ?

Le choix éventuel d'un développeur belge doit dès lors s'opérer sur la base de critères stricts préalablement établis, auxquels ce développeur devra répondre. Nous plaidons

d'ores et déjà en faveur de la sélection, le cas échéant, d'un développeur belge qui travaille avec un système totalement ancré sur l'infrastructure existante en Belgique (serveurs, centres de données, réseaux…). Dans le cas contraire, il nous faudrait d'office faire face à des risques de sécurité plus importants.

Les puissances étrangères ne sont bien sûr pas les seules susceptibles de s'intéresser aux applications de traçage de contacts en raison de leurs données et des possibilités d'ingérence qu'elles offrent. À cet égard, nous devons également tenir compte de la menace émanant des **acteurs non étatiques,** aux motivations différentes.

Ainsi, certains groupements qui entendent commettre des délits profiteront volontiers de la présence de GSM à proximité du lieu visé. Cette technologie offre des possibilités insoupçonnées aux acteurs non étatiques entrés aujourd'hui dans l'ère du hacking : ils peuvent ainsi suivre des entreprises ou des personnes privées, les mettre sous pression, leur faire du chantage, etc.

Dans ce contexte, outre les intentions délictueuses déjà évoquées, n'oublions pas que des organisations aux objectifs extrémistes ou autres sont susceptibles de faire usage de cette technologie en vue de surveiller leurs partisans ou de garder leurs adversaires à distance. Un groupement extrémiste ou une secte peut habilement utiliser une telle technologie pour limiter les mouvements de ses adeptes dans un certain périmètre et en écarter effectivement ses opposants.

Afin de contrer les menaces, en particulier celles qui émanent des puissances étrangères, il convient d'adopter une stratégie de sécurité offensive qui vise à diminuer les capacités des services de sécurité étrangers. À l'heure actuelle, la Belgique ne dispose pas des mêmes possibilités que celles des puissances étrangères ou des acteurs non étatiques. Il nous faut dès lors et avant tout veiller à maintenir notre vulnérabilité à son plus bas niveau.

Ces **vulnérabilités** présentent un lien avec la technologie et je ne peux donc que difficilement me prononcer au sujet de ces applications. En effet, mon service n'a pas été en mesure d'en étudier tous les éléments dans un délai aussi court. De manière générale, nous constatons que ces vulnérabilités sont comparables à celles d'autres applications, comme celles permettant la vidéoconférence, par exemple. Ainsi, une application peut présenter des **vulnérabilités techniques** au niveau de sa programmation.

veiligheid van de staat
sûreté de l'état
VSSE

> *À cet égard, je pense notamment à ladite « zero day attack ». Il s'agit d'une menace qui tente de mettre à profit les failles d'un programme qui, au moment de l'attaque, n'ont pas encore été détectées par d'autres personnes ou par les développeurs. La dénomination de l'attaque fait référence au moment de sa survenue. Ainsi, une « zero day attack » débute avant le jour même (jour 1) où le développeur se rend compte de la faille de sécurité. Cela signifie que celui-ci n'a, à ce moment, aucune chance de partager un correctif du programme avec ses utilisateurs.*

L'infrastructure est aussi susceptible de présenter des vulnérabilités. L'ensemble des données générées par ces applications de traçage doivent en effet transiter par des lignes de communication avant d'être enregistrées sur des serveurs centraux. Est-il possible de sécuriser cette transmission ? Qu'en est-il si l'entreprise qui a développé l'application fait tout à coup l'objet d'un rachat par un entreprise étrangère (étatique ou non) ? Qui est le propriétaire des données envoyées par une application sur des serveurs étrangers ?

En ce qui concerne les **solutions commerciales,** il convient également de tenir compte des conventions d'utilisation autorisant l'usage et l'éventuelle commercialisation des données. Il faut garder à l'esprit que l'utilisation d'applications de traçage d'origine étrangère s'inscrit dans un **cadre légal** en vigueur en dehors de la Belgique. Certains pays ont en effet instauré une possibilité (ou une obligation) de coopération entre leurs services de sécurité et les entreprises. Ces vulnérabilités offrent aux acteurs hostiles une opportunité d'accès aux données des applications, voire aux systèmes sur lesquels elles sont installées.

Quelles sortes de risques l'installation de ce genre d'applications est-elle susceptible d'engendrer ? À cet égard, il nous faut considérer tant la protection de la vie privée que les risques de sécurité au sens large.

Premièrement, il existe une possibilité **d'espionnage,** sous la forme d'extraction de données (d'identité, de déplacement, de contact d'une personne ou d'un groupe de personnes). Pouvez-vous imaginer la mine d'informations disponibles pour les services de renseignement étrangers si les travailleurs des entreprises privées et publiques, en ce compris les collaborateurs des partis politiques, par exemple, installaient une application de traçage des contacts sur leur GSM professionnel ?

Une **stratégie de sortie de la crise liée au COVID-19 reposant sur ce type d'applications** implique également un risque de sabotage du système ou un préjudice potentiel pour celui-ci. Des puissances étrangères pourraient ainsi tenter de **bloquer l'application ou de falsifier des données.** Ceci dans deux directions : en induisant des faux positifs ou des faux négatifs. Si, soudainement, un nombre important de faux « contaminés » venaient à être signalés, cette situation pourrait faire peser une pression considérable sur les hôpitaux et les laboratoires COVID-19. Par ailleurs, la confiance dans le système, voire dans l'autorité, pourrait se trouver ébranlée par ce genre d'atteinte à l'intégrité des données.

Dans un contexte plus large, cette technologie pourrait permettre d'associer différentes attaques en vue de perpétrer **une attaque hybride de plus grande ampleur.** Ceci pourrait se faire, par exemple, en combinaison avec d'autres actions, telles qu'une campagne de désinformation.

La **nécessité, pour notre pays, de conserver le contrôle** sur l'utilisation des données est un élément indispensable dans le cadre du déploiement de ce genre d'applications. Nous ignorons en effet tout de l'agenda de certaines entreprises commerciales ou de puissances étrangères, et nous ne savons pas davantage si l'intérêt de notre pays et de nos citoyens y figure en bonne place.

C'est pourquoi je tiens à rappeler un certain nombre de critères que j'ai présentés il y a quelques mois dans le cadre de la 5G :

1- L'éventuel caractère autoritaire du pays d'origine du fournisseur de l'application et/ou de l'infrastructure par laquelle les données transitent ;

2- La mesure dans laquelle un fournisseur peut se positionner en toute indépendance par rapport à son autorité nationale ;

3- L'existence et l'application d'une législation nationale qui permet à un État (non européen) d'avoir la mainmise sur des entreprises ;

4- L'indépendance du fonctionnement judiciaire du pays en question ;

5- L'ouverture en termes de gestion de l'entreprise et la mesure dans laquelle des facteurs tels que des aides d'État (déguisées), un manque de transparence dans la direction de l'entreprise ou encore l'actionnariat sont susceptibles de porter préjudice au fonctionnement normal du marché.

veiligheid van de staat
sûreté de l'état
VSSE

3. NOTIONS TECHNIQUES

Enfin, permettez-moi de vous présenter quelques **notions techniques** afin que nous ayons tous une même compréhension de la matière abordée. Il s'agit d'une question complexe, mais appréhender certains aspects techniques nous permettra de mieux comprendre le volet juridique et les dangers possibles dans le domaine de l'espionnage.

Pour exploiter au mieux le traçage des contacts, nous devons savoir qui est en contact avec qui, pendant combien de temps et où. Les données suivantes sont nécessaires à cette fin :

- Une localisation précise,
- Une identification unique par utilisateur,
- Une collecte d'informations contextuelles,
- Une couverture suffisamment grande.

En ce qui concerne la **localisation,** de nombreuses solutions utilisent notamment le signal GPS, la fonction Bluetooth, l'ad-ID, le wifi...

La précision de la localisation GPS a ses limites, et même l'association du GPS à d'autres systèmes n'offre pas une résolution suffisante pour déterminer avec précision à une distance de 1,5 mètre où une personne est allée.

La fonction Bluetooth peut être utile à cet effet. Toutefois, maintenir le Bluetooth activé en permanence entraîne des risques pour la sécurité. Nous compromettrions les appareils de nos concitoyens si nous envisagions qu'ils transmettent en continu l'identité unique de leur appareil via le Bluetooth. Ainsi, d'autres applications - mais également des criminels ou des puissances étrangères - risquent d'abuser de l'application de traçage des contacts lors de son utilisation. À cet égard, on parle généralement d'applications dites « leaky », donc littéralement des applications qui présentent des « fuites » en termes de sécurité.

La localisation n'est pertinente que s'il est possible de déterminer la position d'un appareil spécifique, lié à une personne spécifique. Pour ce faire, chaque dispositif doit être identifiable, et une forme **d'identification unique** est dès lors requise. Certaines des applications proposées fonctionnent sur la base de l'ad-ID ; il s'agit d'une identité classiquement attribuée à une publicité (« ad »), qui permet aux entreprises de faire de la publicité auprès des bons groupes cibles sur Facebook.

L'utilisation de l'ad-ID est loin d'être idéale. En effet, des fuites peuvent exister à ce niveau également, qui permettent de relier cette ad-ID à d'autres données de la même personne. En outre, les utilisateurs peuvent changer leur ad-ID assez facilement.

N'existe-t-il dès lors pas d'application qui utilise une identification indépendante d'une personne ou d'un appareil, et qui n'utilise donc pas non plus le numéro de téléphone, l'adresse Bluetooth, l'ad-ID, etc. ?

Plusieurs acteurs d'envergure mondiale dans le domaine ICT travaillent actuellement à la mise au point d'une telle application, permettant par ailleurs de modifier régulièrement son identité unique. Je vous en épargne les détails, mais il s'agira d'un système basé sur des clés multiples reliées entre elles. L'une de ces clés pourra donc être échangée en permanence avec l'environnement et, grâce à une forme de croisement continu, les clés des personnes contaminées par le COVID-19 pourront être croisées avec les clés de la population, ce qui permettra de déterminer clairement qui se trouvait à proximité de la personne malade, sans que son identité ou son emplacement exact ne soient connus par l'application. Cette solution est très prometteuse.

La proposition de résolution examinée aujourd'hui fait référence au DP-3T (*Decentralized Pivacy-Preserving Proximity Tracing* - également connu sous l'appellation « PEPP-PT », ou *Pan European Privacy Preserving Proximity Tracing*). Il s'agit d'un cadre « open source » développé par des scientifiques afin de protéger la vie privée dans ce type d'applications. La KU Leuven (l'équipe du Professeur Preneel) représente la Belgique dans ce groupe de travail. L'Autriche et la Suisse ont également utilisé ce cadre pour leur application COVID-19. Selon nous, recourir à ce cadre pour également développer l'application belge (wallonne/bruxelloise/flamande) constitue une bonne piste. Nous pourrions ainsi faire appel à l'expérience autrichienne et suisse.

En tout état de cause, les solutions proposées qui sont en cours de développement ont requièrent aussi **des informations contextuelles.** Les personnes qui travaillent dans le même bâtiment sont peut-être en contact les unes avec les autres, mais peuvent aussi être séparées par un mur, et donc n'avoir jamais réellement été en contact physique. Nous devons éviter une situation où une personne malade risque de paralyser tout un service ou une entreprise parce que le système ne peut pas établir de distinction entre les étages, les bâtiments voisins, etc.

En outre, nous devons réfléchir à certaines situations comme le vol des appareils, le lien erroné qui peut exister entre un appareil et un utilisateur spécifique ou l'utilisation d'un brouilleur qui perturbe la communication de l'appareil proprement dit. Cela permettra d'éviter qu'un utilisateur soit ainsi placé en quarantaine, délibérément ou non, à un moment donné et que l'ensemble du système ne fonctionne plus.

À notre connaissance, il n'existe actuellement aucune application incluant de telles informations contextuelles. Jusqu'à nouvel ordre, une seule solution s'offre à nous : interroger individuellement les personnes qui tombent malades.

Le succès de toute application de traçage des contacts dépend par ailleurs du nombre de personnes qui l'utilisent, et donc du **taux de couverture.** Pour faire ses preuves, l'application doit être utilisée correctement par au moins 60 % de la population. Il s'agit là d'un défi de taille.

De plus, le groupe le plus vulnérable est précisément celui au sein duquel le smartphone est le moins répandu : les seniors. Une solution pourrait être rapidement trouvée à ce problème en développant des appareils à usage unique, peu coûteux et mis à disposition quasi gratuitement. Que faut-il installer sur un tel dispositif ? Rien d'autre qu'un module Bluetooth, un port USB pour pouvoir charger l'appareil et une interface avec d'autres appareils. Cet appareil peut être produit dans un format à peine plus grand que celui d'un porte-clés. Ce genre de solution peut également constituer une plus-value pour le reste de la population étant donné qu'elle écarte directement tout problème de sécurité éventuel occasionné par la nécessité d'activer en permanence le Bluetooth sur le smartphone. Il peut aussi s'agir d'une option pour les personnes qui hésitent à installer une application sur leur smartphone.

Je conclurai ce chapitre technique en soulignant que de nombreuses possibilités et options existent, mais pas encore d'application combinant les différents éléments nécessaires, une localisation précise, une identification unique par utilisateur, une collecte d'informations contextuelles et une couverture suffisamment étendue.

veiligheid van de staat
sûreté de l'état
VSSE

4. CONCLUSION

Permettez-moi de conclure mon introduction en insistant une nouvelle fois sur le rôle que mon service, la Sûreté de l'État, joue dans la lutte contre le COVID-19.

Mes collaborateurs travaillent d'arrache-pied à l'identification de toutes sortes de tentatives de désinformation et de diffusion de fake news. Nous nous efforçons en effet de réagir rapidement lorsque des organisations extrémistes ou des puissances étrangères interviennent dans ce contexte. Mon service a déjà transmis aux autorités fédérales et régionales plusieurs notes reprenant des observations spécifiques en la matière.

La VSSE ne joue pas un rôle direct en ce qui concerne le déploiement concret d'une application de traçage des contacts. Nous avons assumé notre mission de service de renseignement en vous faisant part de nos préoccupations aujourd'hui, en vous fournissant plus particulièrement un aperçu des questions qui méritent une réponse lorsqu'il s'agit de faire un choix concernant des applications spécifiques et/ou leur fournisseur. Le choix final d'une telle application relève de la sphère politique et la VSSE ne peut pas se prononcer à ce niveau. Nous espérons naturellement que nos préoccupations seront entendues et que le choix ne sera pas fait à la légère.

Tout au long de la crise du COVID-19, la VSSE continuera bien sûr à prendre ses responsabilités dans la lutte contre les menaces prévues par la loi. Par conséquent, si l'option d'une application de traçage des contacts est retenue, nous pourrons – dans ce cadre légal strict – assurer par la suite le suivi des menaces connexes (que j'ai déjà mentionnées précédemment).

Je vous remercie de m'avoir donné l'occasion de m'exprimer sur ce sujet et me tiens bien évidemment à votre disposition pour répondre à toutes vos questions en la matière.