veiligheid van de staat
sûreté de l'état
VSSE

ONDERWERP:

Voorbereiding hoorzitting kamercommissie Economie 28/4 – Resolutie 1182 in verband met contact tracing applicaties.

Mijnheer de voorzitter,
Geachte leden van de commissie,

Allereerst hartelijk dank om me de gelegenheid te geven me uit te spreken over de ontwikkeling van zogenaamde contact tracing apps. Het gegeven dat mijn dienst steeds vaker gevraagd wordt in dit soort discussies – ik was in deze commissie eerder al te gast in de context van de 5G problematiek – wijst voor mij op het groeiend vertrouwen dat parlementsleden stellen in de professionaliteit van de adviezen die we als dienst ter beschikking stellen.

Ik werd pas afgelopen vrijdag gevraagd u te komen inlichten over onze kijk op de contact tracing apps en ik kreeg niet onmiddellijk concrete duiding bij eventuele vragen. Ik heb er dan ook voor gekozen om u een korte toelichting te geven bij de drie aspecten van het thema dat ons vandaag bezig houdt, die voor ons als inlichtingendienst het meest belangrijk zijn:

1. Vooreerst ga ik graag in op het juridische kader en meer specifiek op de controlemechanismen.

2. Vervolgens ga ik dieper in op de mogelijke risico's die het introduceren van een contact tracing app biedt voor het tot stand komen van dreigingen die mijn dienst wettelijk geacht wordt op te volgen.

3. Ten slotte hoop ik u voor wat betreft de technische aspecten een aantal elementen mee te geven die van belang zijn alvorens een contact tracing app toe te laten binnen een Belgische context.

veiligheid van de staat
sûreté de l'état
VSSE

1. JURIDISCHE ACHTERGROND

In eerste instantie ga ik dus graag in op de **juridische achtergrond** van contact tracing apps.

De Veiligheid van de Staat heeft als opdracht het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de veiligheid van België bedreigt of zou kunnen bedreigen. In het kader van deze opdracht heeft de VSSE de mogelijkheid om inlichtingenmethoden in te zetten, zoals het verzamelen van elektronische communicatiegegevens. De VSSE kan dit echter niet zomaar doen, zowel de bewaring van deze gegevens door operatoren van elektronische communicatie als de toegang tot deze gegevens door de VSSE is strikt wettelijk geregeld.

De bewaring van elektronische communicatiegegevens wordt geregeld in de wet van 13 juni 2005 betreffende de elektronische communicatie. In deze wet wordt bepaald welke gegevens door de operatoren moeten worden bijgehouden, onder welke voorwaarden deze gegevens moeten worden bewaard, welke overheden toegang hebben tot deze gegevens en voor welke doeleinden deze gegevens kunnen worden gebruikt. Zo wordt onder meer bepaald dat operatoren verkeers- en lokalisatiegegevens – dit zijn de gegevens over de communicatie – dienen bij te houden en dat de inlichtingen- en veiligheidsdiensten deze gegevens kunnen vorderen in het kader van hun inlichtingenopdracht.

In een KB tot uitvoering van de wet op de elektronische communicatie wordt dan weer gespecifieerd welke categorieën van gegevens de operatoren dienen te bewaren, zoals de persoonsgegevens van de eindgebruiker, datum en tijdstip van aanvang en einde van een oproep, locatiegegevens, ...

Indien de Veiligheid de Staat – in het kader van haar inlichtingenopdracht – toegang wil tot deze gegevens die worden bewaard door operatoren, moet er voldaan worden aan een hele reeks voorwaarden. De toegang tot deze gegevens wordt geregeld door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Vooreerst moeten de principes van subsidiariteit en proportionaliteit worden nageleefd. De lokalisatie- en verkeersgegevens kunnen enkel worden gevorderd indien minder privacy-intrusieve methoden ontoereikend zijn om de informatie te verzamelen die noodzakelijk is om de inlichtingenopdracht te volbrengen. Bovendien moet de vordering van deze

gegevens in evenwicht zijn met de ernst van de potentiële dreiging waarnaar de Veiligheid van de Staat onderzoek voert.

Daarnaast wordt er voorzien in een ruime controle. Als diensthoofd van de Veiligheid van de Staat neem ik een schriftelijke en met redenen omklede beslissing tot uitvoering van de inlichtingenmethode. Deze beslissing dient eerst ter kennis worden gebracht van een specifieke Commissie van drie magistraten, de BIM-commissie, voordat de inlichtingenmethode mag worden uitgevoerd. Het Vast Comité I, het controleorgaan op de werking van mijn dienst, is eveneens bevoegd om een controle uit te voeren op de inlichtingenmethode.

De Veiligheid van de Staat moet de inlichtingenmethode beëindigen zodra de potentiële dreiging is weggevallen, de methode niet langer nuttig is of wanneer er een onwettigheid wordt vastgesteld. De BIM-Commissie en het Vast Comité I kunnen eveneens de inlichtingenmethode schorsen en/of stopzetten wanneer niet langer wordt voldaan aan de wettelijke voorwaarden of wanneer er een onrechtmatigheid wordt vastgesteld. Er kan ook beslist worden tot vernietiging van de reeds verzamelde gegevens.

Tot slot wordt bepaald dat de gegevens verzameld door de Veiligheid van de Staat niet langer mogen worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze werden opgeslagen.

Als gevolg van deze controle kunnen belangrijke methoden in sommige gevallen omwille van procedurele redenen te laat of niet aangewend worden. We zijn als dienst echter overtuigd van het algemeen belang van deze controles, die de democratisch rechten en vrijheden – die we als dienst nota bene zelf geacht worden te beschermen – dienen.

Indien er dus beslist wordt tot ontwikkeling van een app ter bestrijding van het coronavirus COVID-19, stelt de Veiligheid van de Staat voor om een wettelijk kader te ontwikkelen dat voorziet in gelijkaardige waarborgen als deze in de wet op de elektronische communicatie en de wet op de inlichtingen- en veiligheidsdiensten. Zo dient duidelijk geregeld te worden welke gegevens mogen worden bewaard, onder welke voorwaarden de gegevens moeten worden bewaard, wie – onder welke voorwaarden – toegang mag hebben tot deze gegevens, waarvoor de gegevens mogen worden gebruikt en tot slot voorzien in een ruime controle op de verwerking van deze gegevens.

Later in deze toelichting zal blijken dat bepaalde apps claimen geen gegevens te bewaren en eventuele identificatiegegevens te anonimiseren. Zoals in het technische luik omschreven, moet dit steeds nog hard gemaakt kunnen worden. Vanuit veiligheidsperspectief dient er controle te zijn op die apps en moet dus ook gecontroleerd kunnen worden of de claims waarheidsgetrouw zijn, waar de kruising juist gebeurt, of bepaalde gegevens ook niet in een andere (commerciële) context kan worden gebruikt, …

Het is een kwestie van voorzichtigheid en goed bestuur om zeer behoedzaam met deze apps om te gaan.

2. RISICO'S VAN DE INTRODUCTIE VAN EEN CONTACT TRACING APP

Ik wil het in dit kader hebben over de risico's die verbonden zijn aan deze applicaties. Een risico wordt bepaald door de dreiging enerzijds, en de kwetsbaarheid anderzijds.

Wanneer we naar het **aspect dreiging** kijken op het vlak van spionage of inmenging door buitenlandse inlichtingendiensten, moeten we oog hebben voor hun capaciteit en hun eventuele intentie om ons land te schaden. Zo mogen we er niet blind voor zijn dat bepaalde landen beschikken over een offensief beleid dat hen in staat stelt om op grote schaal aan technische spionage te doen in binnen- en buitenland.

Cyberaanvallen zijn een realiteit. Het valt dan ook geenszins uit te sluiten dat derden *(lees: minder bevriende naties)* misbruik zullen trachten te maken van de kwetsbaarheden die inherent zijn aan dit soort apps. Dit is in het bijzonder het geval wanneer deze breed worden uitgerold in de maatschappij, inclusief onder personen met toegang tot gevoelige informatie.

Nogal wat actoren, en ook mijn dienst, pleiten ervoor om, indien men een app zou willen hanteren, te kiezen voor een Belgisch bedrijf. Maar wat is een Belgisch bedrijf? Moeten de aandeelhouders allemaal Belgisch zijn? Mag zo'n bedrijf dan niet overgenomen worden? Mogen directieleden of ontwikkelaars van een andere nationaliteit zijn?

Dus ook een eventuele keuze voor een Belgische ontwikkelaar betekent dat er nog steeds

strikte criteria moeten worden uitgewerkt waaraan de ontwikkelaar dient te voldoen. Wij pleiten er alvast voor om desgevallend te kiezen voor een Belgische ontwikkelaar die werkt met een systeem dat volledig draait op in België aanwezige infrastructuur (servers, datacenter, netwerken, …). Anders zijn er altijd grotere veiligheidsrisico's dan wanneer dit niet het geval is.

Het zijn natuurlijk niet enkel buitenlandse mogendheden die interesse zullen betonen in de data en in de mogelijkheden tot inmenging die de contact tracing apps bieden. We dienen in dit verband ook rekening te houden met de dreiging die uitgaat van **niet-statelijke actoren** met andere motivaties.

Zo zullen bepaalde groeperingen die misdrijven willen plegen maar al te graag zicht hebben op de aanwezigheid van gsm's in de buurt van de plaats waar men een slag wil slaan. Deze technologie biedt niet-statelijke actoren, die zich vandaag al inlaten met hacking, ongekende mogelijkheden om bedrijven en private personen te volgen, onder druk te zetten, eventueel af te persen en zo meer.

Daarbij mogen we niet vergeten dat naast het criminele oogmerk ook organisaties met een extremistische of een andere agenda gebruik kunnen maken van deze technologie om volgelingen in het oog te houden of om tegenstanders op afstand te houden. Een extremistische groepering of een sekte kan een dergelijke technologie handig gebruiken om de bewegingen van haar volgelingen te beperken tot bepaalde zones of buitenstaanders ook effectief buiten te houden.

Om dreigingen, zeker deze die uitgaan van buitenlandse mogendheden, tegen te gaan, is een offensief veiligheidsbeleid – gericht op het verminderen van de capaciteiten van de buitenlandse veiligheidsdiensten – nodig. Op dit moment beschikt België echter niet over dezelfde mogelijkheden als buitenlandse mogendheden of niet-statelijke actoren. Onze focus moet dus in eerste instantie vooral liggen op het minimaal houden van onze kwetsbaarheid.

Deze **kwetsbaarheden** zijn technologiegebonden en het is dus moeilijk om hier uitspraken over te doen met betrekking tot de apps waarvan mijn dienst niet alle informatie heeft kunnen bestuderen in deze korte tijdsspanne. Algemeen kan wel gesteld worden dat deze gelijk lopen met die van andere applicaties, zoals bijvoorbeeld degene waarmee

aan videoconferenties wordt gedaan. Zo kunnen er **technische kwetsbaarheden** in de software zitten.

> *In dit verband verwijs ik naar de zogenaamde zero-day-attack. Dat is een dreiging die probeert misbruik te maken van zwakke delen in software die op dat moment onbekend zijn voor anderen of de softwareontwikkelaar. De term is afgeleid van de leeftijd van de aanval. Een "zero-day"-aanval start op vóór de eerste dag dat de ontwikkelaar zich bewust is van het beveiligingslek, wat betekent dat de ontwikkelaar geen enkele kans heeft om een oplossing voor de software te verdelen naar gebruikers ervan.*

Kwetsbaarheden kunnen zich ook situeren in de infrastructuur. Al de data die deze contact tracing apps genereren moeten immers via communicatielijnen op centrale servers worden opgeslagen. Kan dat veilig gebeuren? En wat indien het bedrijf achter de app plots wordt overgekocht door een buitenlands (al dan niet staats-)bedrijf? Wie is eigenaar van de data die via een app op buitenlandse servers terecht komt?

Bij **commerciële oplossingen** moet er hoe dan ook rekening gehouden worden met de gebruikers-overeenkomsten waarvoor de data gebruikt en eventueel gecommercialiseerd mogen worden. Vergeet ook niet dat er bij contact tracing apps van buitenlandse origine ook nog het in dat buitenland geldende **wettelijk kader** is. In bepaalde landen is er immers de mogelijkheid tot een (verplichte) samenwerking tussen bedrijven en hun nationale veiligheidsdiensten. Via deze kwetsbaarheden kunnen vijandige actoren zichzelf toegang verschaffen tot de applicatiegebonden data, of zelfs de systemen waarop deze geïnstalleerd zijn.

Welke soorten risico's kunnen zich dus zoal manifesteren bij het implementeren van dit soort applicaties? We moeten hierbij kijken naar zowel de privacy als naar de bredere security-risico's.

Ten eerste is er de mogelijkheid tot **spionage**, zijnde de extractie van data (zoals gegevens over de identiteit, de verplaatsingen en de contacten van een persoon of groep van mensen). Kan u zich voorstellen welke informatie beschikbaar wordt voor buitenlandse inlichtingendiensten indien werknemers van overheids- en privébedrijven, dus ook medewerkers van bv. politieke partijen, een contact tracing app dienen te installeren op hun werk-gsm?
Een **exitstrategie uit de COVID-19 crisis die afhankelijk is van dit soort applicaties**

maakt ook dat er een risico is op het vlak van sabotage of voor de integriteit van het systeem. Zo kunnen buitenlandse mogendheden trachten om de **applicatie te blokkeren of gegevens te vervalsen.** Dit kan in twee richtingen, via vals positieven of vals negatieven. Wanneer er opeens een grote groep valse 'besmetten' worden gesignaleerd, kan dit druk zetten op de ziekenhuizen en de COVID-19 labocapaciteit. Daarnaast zal dit soort data-integriteitsinbreuken het vertrouwen in het systeem, en mogelijks zelfs de overheid, ondermijnen.

In een breder kader kunnen aanvallen via deze technologie geïntegreerd worden **in een ruimere hybride aanval.** Dit kan bv. in combinatie met andere acties, zoals een gerichte desinformatiecampagne.

Essentieel voor de uitrol van dit soort applicaties is **dat ons land de controle houdt** op wat er gebeurt met de gegevens. We hebben immers geen zicht op wat de agenda is van commerciële bedrijven of buitenlandse mogendheden, en of deze in het belang is van ons land en onze burgers. Ik herhaal hier dan ook een aantal criteria die ik hier enkele maanden geleden gaf in het kader van 5G:

1- Het mogelijk autoritaire karakter van het land van herkomst van de leverancier van de app en/of infrastructuur waarover de data eventueel passeren.

2- De mate waarin een leverancier zich onafhankelijk kan opstellen ten opzichte van zijn nationale overheid

3- Het bestaan en de toepassing van nationale wetgeving die een (niet-EU) staat greep geeft op bedrijven

4- De onafhankelijkheid van de gerechtelijke werking in het land in kwestie

5- De openheid van bedrijfsvoering en de mate waarin factoren zoals (verdoken) staatssteun of niet-transparante bedrijfsleiding of aandeelhouderschap een normale marktwerking verstoren

veiligheid van de staat
sûreté de l'état
VSSE

3. TECHNISCHE NOTIES

Tot slot dus enkele **technische noties** zodat we allemaal een zelfde begrip hebben van datgene waarover we praten. Dit is voor ons allen een ingewikkelde materie, maar enig inzicht in de technische aspecten is nodig om het juridische luik en de mogelijke gevaren inzake spionage te begrijpen.

Om op een bruikbare manier aan contact tracing te doen, moeten we weten wie met wie in contact staat, hoelang en waar. Daartoe is nodig:

- Een accurate positiebepaling.
- Een unieke identificatie per gebruiker.
- Contextuele informatiewinning.
- Een voldoende grote dekking.

Wat betreft **positiebepaling** zijn er tal van oplossingen die gebruik maken van onder meer het GPS-signaal, de Bluetooth-functie, de ad-ID, wifi, ...

De accuraatheid van GPS-lokalisatie is beperkt, zelfs de kruising van GPS met andere systemen geeft geen afdoende resolutie om op 1,5 meter nauwkeurig te bepalen waar iemand is geweest.

Bluetooth kan dan helpen. Maar Bluetooth continu openzetten zorgt dan weer voor veiligheidsrisico's. We compromitteren de toestellen van onze burgers als we verwachten dat ze continu de unieke identiteit van hun toestel via Bluetooth moeten uitzenden. Op die manier kan het gebruik van de gekozen contact tracing app ervoor zorgen dat andere apps – maar ook criminelen of buitenlandse mogendheden – hier misbruik van maken. Men verwijst in dit verband doorgaans naar zogenaamde leaky apps, letterlijk apps die op het vlak van veiligheid 'lek' zijn.

Positiebepaling is enkel relevant als je de positie van een specifiek toestel, gelinkt aan een specifieke persoon, kan bepalen. Om dat te bereiken moet elk toestel identificeerbaar zijn. Je hebt dus nood aan een vorm van **unieke identificatie.** Een aantal van de voorgestelde apps werken op basis van de ad-ID. Een ad-ID is een identiteit die klassiek wordt toegekend aan een advertentie ('ad') en die het dus voor bedrijven mogelijk maakt om op Facebook bij de juiste doelgroepen te adverteren.

Het gebruik van de ad-ID is verre van ideaal. Ook hier kan immers sprake zijn van lekken die kunnen toelaten om deze ad-ID te koppelen aan andere data van dezelfde persoon. Daarenboven kunnen gebruikers hun ad-ID nogal makkelijk wijzigen.

Bestaat er dan geen app die gebruik maakt van een ID los van persoon of toestel, die dus ook geen gebruik maakt van het telefoonnummer, het bluetooth adres, het ad-ID enzo-verder?

Er wordt momenteel door verschillende wereldspelers op het vlak van ICT gewerkt aan zo'n app die bovendien in staat is haar unieke identiteit regelmatig te veranderen. Ik bespaar u de details maar het zal een systeem worden dat gebaseerd is op meerdere sleutels die met elkaar in verband staan. Een van die sleutels kan dan continu uitgewisseld worden met de omgeving en door een soort van continue kruising kan dan op een relatief veilige wijze de sleutels van personen die besmet werden met COVID-19 gekruist worden met de sleutels van de bevolking waardoor duidelijk wordt wie met de zieke persoon in de buurt was zonder dat diens identiteit of exacte locatie bekend is voor de app. Deze oplossing is beloftevol.

In het voorstel voor resolutie dat vandaag voorwerp is van debat wordt verwezen naar DP-3T (*Decentralized Pivacy-Preserving-Proximity Tracing* – ook gekend onder de term PEPP-PT wat dan staat voor *Pan European Privacy Preserving Proximity Tracing*). Dat is een open source framework dat door wetenschappers is uitgewerkt om de privacy te beschermen bij dat soort toepassingen. Voor België zit de KU Leuven in die werkgroep (het team van professor Preneel). Oostenrijk en Zwitserland hebben dat framework ook gebruikt voor hun COVID-19-app. Het lijkt ons geen slecht idee om voor de Belgische (Vlaamse/Brusselse/Waalse) app ook het in dit kader uit te werken framework te gebruiken. Mogelijk kan er dan ook een beroep worden gedaan op de Oostenrijkse en Zwitserse ervaring.

Hoe dan ook: de voorgestelde oplossingen waaraan vandaag gewerkt wordt, hebben ook behoefte aan **contextuele informatie.** Mensen die in hetzelfde gebouw werken, zijn misschien met elkaar in contact, maar er kan ook een muur tussen hen zitten, waardoor er nooit sprake is geweest van een echt fysiek contact. We moeten vermijden dat één zieke een volledige dienst of bedrijf kan lamleggen omdat het systeem geen onderscheid kan maken tussen verdiepingen, belendende gebouwen etc.

Bovendien moet nagedacht worden over situaties als de diefstal van een toestel, de verkeerde link tussen apparaat en specifieke gebruiker, of het gebruik van een 'jammer' die de communicatie van het eigen apparaat verstoort. Op die manier kan een gebruiker al dan niet bewust vermijden om op een bepaald moment in quarantaine terecht te komen en werkt het hele systeem niet meer.

We hebben tot op heden geen apps gezien die ook die contextuele informatie meenemen. Daarvoor bestaat er tot nader orde maar één oplossing: de personen die ziek worden individueel bevragen.

Het succes van elke contact tracing app staat of valt ook met het aantal mensen dat hiervan gebruik maakt. De **dekkingsgraad** dus. Om bruikbaar te zijn, moet een app door minstens 60 % van de bevolking correct gebruikt worden. Dat is een bijzonder grote uitdaging.

Bovendien is de meest kwetsbare groep de bevolkingsgroep waarbij de smartphone het minst ingeburgerd is: de oudere generatie. Men zou hier vrij eenvoudig een oplossing voor kunnen vinden door goedkope single purpose toestelletjes te maken en deze quasi gratis ter beschikking te stellen. Wat is er nodig op een dergelijk toestel? Niet veel meer dan een bluetooth module, een USB poort om het toestel te kunnen opladen en een interface met andere toestellen. Zo'n toestel kan waarschijnlijk geproduceerd worden binnen een vormfactor niet veel groter dan die van een sleutelhanger. Ook voor de rest van de bevolking kan dit een meerwaarde bieden want dan maak je ineens komaf met de mogelijke veiligheidsproblemen door het constant moeten opzetten van bluetooth op je smartphone. Ook voor mensen die weigerachtig staan tegen het installeren van een app op hun smartphone kan dit een optie zijn.

Ik besluit dit technische hoofdstuk met de vaststelling dat er veel mogelijkheden en opties zijn, maar dat er tot op heden geen app bestaat die de verschillende benodigde bestanddelen, een accurate positiebepaling, een unieke identificatie per gebruiker, een contextuele informatiewinning en een voldoende grote dekking, in zich combineren.

veiligheid van de staat
sûreté de l'état
VSSE

4. BESLUIT

Ik wens mijn introductie hier af te ronden door nog even wat aandacht te besteden aan de rol die mijn dienst, de Veiligheid van de Staat, speelt in de strijd tegen COVID-19.

Mijn medewerkers zijn druk bezig met het in kaart brengen van allerhande pogingen tot desinformatie en het verspreiden van fake news. Met name daar waar extremistische organisaties of buitenlandse mogendheden in deze context opduiken, proberen we kort op de bal te spelen. Mijn dienst kon in dit verband al meerdere nota's met specifieke vaststellingen overmaken aan de federale en regionale overheden.

Voor de VSSE zien we niet direct een rol weggelegd voor wat betreft de praktische uitrol van een contact tracing app. We hebben onze rol als inlichtingendienst gespeeld door u hier vandaag onze bekommernissen kond te maken, meer bepaald door u een overzicht te bieden van de vragen die beantwoord dienen te worden wanneer een keuze dient te worden gemaakt m.b.t. specifieke apps en/of hun leverancier. De uiteindelijke keuze voor een dergelijke app is een politieke kwestie waarin de VSSE zich niet kan uitspreken. Wij hopen uiteraard dat met onze bezorgdheden rekening wordt gehouden en dat een keuze niet lichtzinnig wordt gemaakt.

De VSSE zal tijdens de COVID-19 crisis uiteraard haar verantwoordelijkheid blijven opnemen in de strijd tegen de bedreigingen als voorzien door de wet. Indien de optie van een contact tracing app weerhouden wordt, kunnen wij dan ook – binnen dit strikte wettelijke kader – een verdere opvolging voorzien van de dreigingen die hiermee gepaard gaan (en die ik eerder al heb vermeld).

Ik dank u voor de mogelijkheid om mij in deze kwestie uit te spreken en ik ben uiteraard bereid om te antwoorden op uw vragen hieromtrent.