DOC 55 **1182/005**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

14 mai 2020

PROPOSITION DE RÉSOLUTION

relative au développement potentiel d'une application mobile pour lutter contre le coronavirus (COVID-19) et à la nécessité de respecter les droits humains, en particulier le droit au respect de la vie privée

RAPPORT

FAIT AU NOM DE LA COMMISSION
DE L'ÉCONOMIE,
DE LA PROTECTION DES CONSOMMATEURS
ET DE L'AGENDA NUMÉRIQUE
PAR
M. **Michael FREILICH**

SOMMAIRE Pages

I. Procédure 3
II. Discussion générale 3
III. Discussion des considérants et des demandes et votes 14

Annexes
— rapport des auditions 25
— avis de la commission de la Justice 96

Voir:

Doc 55 **1182/ (2019/2020)**:
001: Proposition de résolution de Mme Soors, MM. Lachaert, Vanden Burre, Aouasti, Verduyckt et Mahdi et Mmes Van der Straeten, Fonck et Rohonyi.
002 à 004: Amendements.

Voir aussi:
006: Texte adopté par la commission.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

14 mei 2020

VOORSTEL VAN RESOLUTIE

betreffende de mogelijke ontwikkeling van een app ter bestrijding van het coronavirus COVID-19, en de noodzaak om de mensenrechten, en in het bijzonder het recht op privacy, te respecteren

VERSLAG

NAMENS DE COMMISSIE
VOOR ECONOMIE,
CONSUMENTENBESCHERMING
EN DIGITALE AGENDA
UITGEBRACHT DOOR
DE HEER **Michael FREILICH**

INHOUD Blz.

I. Procedure 3
II. Algemene bespreking 3
III. Bespreking van de consideransen en de verzoeken en stemmingen 14

Bijlagen
— verslag van de hoorzittingen 25
— advies van de commissie voor Justitie 96

Zie:

Doc 55 **1182/ (2019/2020)**:
001: Voorstel van resolutie van mevrouw Soors, de heren Lachaert, Vanden Burre, Aouasti, Verduyckt en Mahdi en de dames Van der Straeten, Fonck en Rohonyi.
002 tot 004: Amendementen.

Zie ook:
006: Tekst aangenomen door de commissie.

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Stefaan Van Hecke

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Michael Freilich, Katrien Houtmeyers, Anneleen Van Bossuyt	Peter De Roover, Joy Donné, Frieda Gijbels, Wouter Raskin
Ecolo-Groen	Tinne Van der Straeten, Stefaan Van Hecke, Gilles Vanden Burre	Julie Chanson, Laurence Hennuy, Dieter Vanbesien, Albert Vicaire
PS	Christophe Lacroix, Patrick Prévot, Philippe Tison	Malik Ben Achour, Ludivine Dedonder, Ahmed Laaouej, Eliane Tillieux
VB	Erik Gilissen, Reccino Van Lommel	Katleen Bury, Wouter Vermeersch, Hans Verreyt
MR	Benoît Friart, Florence Reuter	Magali Dock, Isabelle Galant, Caroline Taquin
CD&V	Leen Dierick	Jef Van den Bergh
PVDA-PTB	Roberto D'Amico	Maria Vindevoghel, Thierry Warmoes
Open Vld	Kathleen Verhelst	Robby De Caluwé, Tania De Jonge
sp.a	Melissa Depraetere	Anja Vanrobaeys, Kris Verduyckt

C. — Membre sans voix délibérative / Niet-stemgerechtigd lid:

DéFI	Sophie Rohonyi

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

MESDAMES, MESSIEURS,

Votre commission a examiné cette proposition de résolution, qui a obtenu l'urgence lors de la séance plénière de la Chambre du 23 avril 2020, au cours de ses réunions des 22 avril, 28 avril et 6 mai 2020.

I. — **PROCÉDURE**

Au cours de sa réunion du 22 avril 2020, la commission a décidé, en application de l'article 28.1 du Règlement de la Chambre, d'organiser une audition sur la proposition de résolution. Au cours de cette audition, qui s'est tenue le 28 avril 2020 et à laquelle les membres de la commission de la Justice ont été invités, les personnes suivantes ont été entendues:

— M. David Stevens, président de l'Autorité de protection des données (APD);

— le professeur Bart Preneel, KUL;

— Mme Olivia Venet, présidente de la Ligue des Droits Humains, et Mme Kati Verstrepen, présidente de la *Liga voor Mensenrechten*;

— M. Jaak Raes, administrateur général de la Sûreté de l'État;

— la professeure Élise Degrave, UNamur.

Le rapport de l'audition est annexé au présent rapport.

Au cours de sa réunion du 22 avril 2020, la Conférence des présidents a chargé la commission de la Justice de rendre à votre commission un avis sur les aspects de la proposition de résolution touchant au respect de la vie privée. La commission de la Justice a discuté de cet avis au cours de sa réunion du 29 avril 2020. Le rapport de M. Christoph D'Haese est annexé au présent rapport.

II. — **DISCUSSION GÉNÉRALE**

Mme Jessika Soors (Ecolo-Groen) souligne que la proposition de résolution ne préconise pas l'utilisation d'une application mais bien la fixation d'un maximum de conditions au cas où il serait décidé de recourir à une application.

DAMES EN HEREN,

Uw commissie heeft dit voorstel van resolutie, dat urgentie heeft verworven tijdens de plenaire vergadering van de Kamer van 23 april 2020, besproken tijdens haar vergaderingen van 22 april, 28 april en 6 mei 2020.

I. — **PROCEDURE**

Tijdens de vergadering van 22 april 2020 heeft de commissie beslist, met toepassing van artikel 28.1 van het Kamerreglement, een hoorzitting te houden over het voorstel van resolutie. Tijdens deze hoorzitting, die heeft plaatsgevonden op 28 april 2020 en waarop de leden van de commissie voor Justitie waren uitgenodigd, werden gehoord:

— de heer David Stevens, voorzitter van de Gegevensbeschermingsautoriteit (GBA);

— professor Bart Preneel, KUL;

— mevrouw Olivia Venet, voorzitster van de *Ligue des Droits Humains*, en mevrouw Kati Verstrepen, voorzitster van de Liga voor Mensenrechten;

— de heer Jaak Raes, administrateur-generaal van de Staatsveiligheid;

— professor Élise Degrave, UNamur.

Het verslag van de hoorzitting gaat in bijlage bij onderhavig verslag.

De Conferentie van voorzitters heeft tijdens haar vergadering van 22 april 2020 de commissie voor Justitie gelast om over de aspecten van het voorstel van resolutie die de privacy betreffen een advies te geven aan uw commissie. De commissie voor Justitie heeft tijdens haar vergadering van 29 april 2020 over dit advies vergaderd. Het verslag van de heer Christoph D'Haese gaat in bijlage bij onderhavig verslag.

II. — **ALGEMENE BESPREKING**

Mevrouw Jessika Soors (Ecolo-Groen) benadrukt dat de resolutie als zodanig geen pleidooi inhoudt voor het gebruik van een app, maar enkel pleit voor het instellen van een maximaal aantal voorwaarden wanneer men zou besluiten tot het gebruik van een app.

L'intervenante indique ensuite que tous les avis rendus au sujet de la proposition de résolution à l'examen, ainsi que les auditions organisées à ce sujet, sont positifs. L'exposé que vient de faire le ministre De Backer va également dans ce sens.

La proposition de résolution pourrait en outre servir de base légale à la poursuite des travaux concernant le développement d'une application éventuelle, ainsi qu'à l'adoption de propositions de loi ou d'autres initiatives législatives éventuelles.

Mme Barbara Pas (VB) fait observer que lorsqu'il a répondu aux questions orales, le ministre De Backer n'a pas répondu clairement à la question de savoir si une application de ce type était vraiment nécessaire.

L'intervenante estime, elle aussi, qu'il est indispensable de fixer des conditions, compte tenu des risques manifestes qu'un système de ce type présente à l'égard du respect de la vie privée. Elle craint toutefois que le remède soit pire que le mal.

Ainsi qu'il a été indiqué plus haut, l'article 22 de la Constitution exige la tenue d'un débat parlementaire à ce sujet.

La proposition de résolution soumet l'utilisation de l'application à trois conditions au moins: l'application devra être installée par un maximum de citoyens; les citoyens devront avoir confiance en cette application; et il faudra que la capacité de dépistage soit suffisante. L'intervenante craint qu'aucune de ces conditions ne soit remplie (elle renvoie notamment, à cet égard, à l'enquête évoquée par la Ligue des Droits Humains, qui visait à déterminer le pourcentage de citoyens disposés à installer une application de ce type).

Le ministre De Backer lui-même a déclaré qu'au moins 60 % des citoyens devaient installer l'application pour que son utilisation ait du sens et soit utile. Or, même en Autriche, seuls 3 à 4 % des citoyens l'ont installée en pratique malgré l'appel enthousiaste lancé en la matière par la Croix-Rouge; du reste, tout le monde ne dispose pas d'un smartphone.

Ensuite, il faut être attentif, ainsi que l'a indiqué le chef de la sûreté de l'État, à la vulnérabilité d'une telle application en termes de piratage (*hacking)* et d'espionnage.

La fiabilité d'une éventuelle application est également discutable à tout le moins au regard de l'échec manifeste du contrôle exercé par l'autorité publique sur les entreprises fabriquant des masques buccaux.

Zij stelt verder dat alle gevraagde adviezen en hoorzittingen over het voorstel van resolutie van positief waren; dit was eveneens het geval voor de presentatie van minister De Backer daarnet.

Bovendien vormt het voorstel van resolutie een wettelijke basis voor het verder vervolg van de werkzaamheden rond een eventuele app, evenals voor eventuele wetsvoorstellen of andere wetgevende initiatieven.

Mevrouw Barbara Pas (VB) wijst erop dat minister De Backer tijdens de mondelinge vragensessie geen eenduidig antwoord heeft gegeven op de vraag of een dergelijke app wel noodzakelijk is.

De spreekster is het er volledig mee eens dat een aantal voorwaarden moeten worden gesteld wegens de manifeste risico's voor de privacy, maar ze vreest dat de remedie erger zou kunnen zijn dan de kwaal.

Zoals reeds gezegd vereist artikel 22 van de Grondwet dat hieromtrent een parlementair debat wordt gevoerd.

Volgens de resolutie moeten minstens drie voorwaarden worden vervuld voor het gebruik van de app: een maximum aantal burgers moet de app installeren, de burgers moeten vertrouwen hebben in de app en er moet voldoende testcapaciteit aanwezig zijn. Welnu, de spreekster vreest dat geen enkele van de drie voorwaarden vervuld is (zij verwijst onder meer naar de door de Liga voor Mensenrechten aangehaalde enquête met betrekking tot het percentage burgers dat bereid zou zijn om een dergelijke app te installeren).

Minister De Backer heeft zelf gezegd dat minstens 60 % van de bevolking de app moet installeren opdat het gebruik ervan zinvol en nuttig zou zijn. Zelfs in Oostenrijk bleek maar 3 à 4 % van de bevolking in de praktijk de app te hebben geïnstalleerd, ondanks de warme oproep ter zake van het Rode Kruis; bovendien beschikt niet iedere burger over een smartphone.

Vervolgens dient men oog te hebben, zoals het hoofd van de staatsveiligheid hier heeft aangegeven, voor de kwetsbaarheid van een dergelijke applicatie voor hacking en spionage.

De betrouwbaarheid van een eventuele app is eveneens op zijn minst twijfelachtig, in het licht van de manifeste mislukking van de controle door de overheid op de bedrijven die mondmaskers vervaardigen.

L'intervenante conclut que si elle peut marquer son accord sur une série de conditions posées dans la proposition de résolution et plusieurs amendements, elle désapprouve le principe: les conditions de réussite ne sont pas remplies et le remède pourrait s'avérer pire que le mal lui-même.

Monsieur Christophe Lacroix (PS) souligne que ce sujet suscite beaucoup d'inquiétudes au sein de la population, à juste titre. Au-delà des données de santé, celles liées aux déplacements d'une personne sont extrêmement révélatrices de sa vie privée. L'anonymisation n'est pas une évidence. Si on sait où une personne habite et où elle travaille, on sait immédiatement mettre un nom derrière un signal téléphonique. On saura ensuite si elle se rend à la gay pride, un centre de planning familial, une clinique spécialisée, une manifestation, au siège d'un syndicat, dans une église, une mosquée, une synagogue ou chez un amant ou une maîtresse. Autant d'informations particulièrement sensibles. Or, c'est bien là le fondement de la protection de la vie privée: assurer à chacun le droit de mener librement la vie qu'il se choisit, sans craindre de devoir rendre des comptes.

La position du PS peut être résumée en trois points, Il faut:

— que l'application soit une nécessité par manque d'alternative;

— en minimiser le risque et donc reconnaître ce risque;

— une transparence totale à l'égard de la population.

Mais avant même d'établir la nécessité d'une application, il faut appliquer les recommandations de l'OMS au premier rang desquels le *testing* massif de la population. Une application ne sera pas une solution miracle.

Sur la nécessité

Quant à la nécessité elle-même, celle-ci semble de plus en plus faire défaut. Surtout maintenant que le suivi de la population se fait de façon "manuelle", via call center. L'application apparaît moins comme une nécessité puisqu'il existe au moins une alternative. D'ailleurs le ministre De Backer l'a reconnu lui-même: pour le moment, une application n'est pas la priorité pour organiser le déconfinement.

Si une application devait malgré tout être nécessaire, ceux qui la défendent devront d'abord démontrer sa

De spreekster besluit dat ze kan instemmen met een aantal voorwaarden die in de resolutie worden gesteld en eveneens met bepaalde amendementen, maar ten gronde is zij het oneens met het principe: de voorwaarden voor succes zijn niet voldaan en de remedie riskeert erger te zijn dan de kwaal.

De heer Christophe Lacroix (PS) onderstreept dat dit onderwerp de bevolking veel zorgen baart, en terecht. Niet alleen iemands gezondheidsgegevens, maar ook gegevens over diens verplaatsingen onthullen enorm veel over het privéleven van de betrokkene. Anonimisering is niet vanzelfsprekend. Indien men weet waar iemand woont en werkt, kan meteen een naam aan een telefoonsignaal worden gekoppeld. Daarna is geweten of die persoon naar de *gay pride* gaat, of naar een centrum voor gezinsplanning, een gespecialiseerd ziekenhuis, een betoging, een vakbondskantoor, een kerk, een moskee, een synagoge of nog een minnaar/minnares thuis bezoekt. Het betreft telkens bijzonder gevoelige informatie. Laat net dat de kern zijn van de bescherming van de persoonlijke levenssfeer: waarborgen dat iedereen het recht heeft te leven zoals hij/zij wil, zonder vrees om daar rekenschap voor te moeten afleggen.

Het PS-standpunt laat zich in drie punten vatten:

— de app moet noodzakelijk zijn omdat er geen alternatief voorhanden is;

— het risico moet tot een minimum worden beperkt en dat risico moet dus worden erkend;

— er moet volledige transparantie zijn ten aanzien van de bevolking.

Nog vóór de noodzaak van een app vaststaat, moeten echter de aanbevelingen van de Wereldgezondheidsorganisatie worden toegepast, in de eerste plaats het massaal testen van de bevolking. In deze crisis zal een app zal geen wondermiddel zijn.

De noodzaak

De noodzaak zelf lijkt er steeds nadrukkelijker níet te zijn, zeker omdat het contactonderzoek van de bevolking thans manueel gebeurt, via callcenters. Derhalve is een app kennelijk minder noodzakelijk, daar er minstens één alternatief is. Voorts erkende minister De Backer het zelf: vooralsnog wordt geen prioriteit gegeven aan de uitwerking van een app om de afbouw van de lockdown in goede banen te leiden.

Mocht een app toch nodig blijken, dan zullen de voorstanders van die methode eerst de noodzaak ervan

nécessité en fonction d'objectifs clairs et prédéfinis qui s'inscrivent dans le cadre d'une politique globale de santé publique.

Cette absence de nécessité démontrée est d'ailleurs la première remarque de l'APD:

— "L'Autorité constate que si le projet d'arrêté royal, la note au gouvernement et le Rapport au Roi démontrent en quoi l'utilisation d'applications numériques de dépistage de contacts est moins intrusive que le système existant faisant un usage exclusif de call-centers (et utilisé dans le cadre de la lutte contre d'autres épidémies), ils ne démontrent pas de manière suffisante l'efficacité et donc la nécessité et la proportionnalité de cette utilisation."

— "l'efficacité des applications numériques de dépistage de contacts ne peut pas être pensée en isolation de la politique globale de santé publique visant à lutter contre la propagation du coronavirus COVID-19 parmi la population."

Sur le risque

Quel que soit le type d'application choisie, celle-ci traitera des données à caractère personnel. Or, il faut partir du principe qu'aucun système n'est sûr à 100 %. Toute l'attention doit donc être portée sur la minimisation des risques. Cela concerne le nombre de données différentes traitées, ceux qui y ont accès, la durée d'existence de la donnée, la difficulté à réidentifier et les risques en cas de *hacking* des données.

Les services de renseignement l'ont rappelé pendant les auditions: il faut protéger les données face aux risques d'intrusion dont seraient capables des entités étatiques aux moyens humains et financiers considérables. On ne parle donc pas ici d'un *hacking* par un ado depuis sa chambre. Dans le même ordre d'idée, la technologie privilégiée par les spécialistes universitaires, serait celle du Bluetooth plutôt que la localisation GPS. Mais là aussi, les services de renseignement mettent en garde: le Bluetooth n'est pas une technologie suffisamment sécurisée et son efficacité n'est pas certaine puisqu'il risque d'y avoir beaucoup de faux signalements dus à une précision insuffisante.

Par ailleurs, il faut veiller à ne pas avoir une confiance aveugle dans le résultat de traitements automatisés de données (algorithmes). Il est établi de façon constante que ceux-ci ont une fâcheuse tendance à refléter les discriminations préexistantes au sein d'une société. Par exemple, une application pour smartphone ne concernerait

moeten aantonen, aan de hand van duidelijke en vooraf bepaalde doelstellingen die onderdeel zijn van een alomvattend volksgezondheidsbeleid.

De eerste opmerking van de GBA betreft overigens het feit dat die aangetoonde noodzaak er niet is:

— "De Autoriteit stelt vast dat het ontwerp van koninklijk besluit, de nota aan de regering en het Verslag aan de Koning weliswaar aantonen dat het gebruik van digitale contactopsporingsapplicaties minder ingrijpend is dan het bestaande systeem dat uitsluitend gebruik maakt van callcenters (en dat wordt gebruikt in de strijd tegen andere epidemieën), maar dat zij de doeltreffendheid en dus de noodzaak en de proportionaliteit van een dergelijk gebruik niet voldoende aantonen.";

— "de doeltreffendheid van de digitale contactopsporingsapplicaties [kan] niet los worden gezien van het algemene volksgezondheidsbeleid dat erop gericht is de verspreiding van het coronavirus COVID-19 onder de bevolking onder controle te houden.".

Het risico

Wat voor app er ook wordt gekozen, met dat systeem zullen persoonsgegevens worden verwerkt. Men dient evenwel uit te gaan van het principe dat geen enkel systeem volledig veilig is. Er moet dus veel aandacht gaan naar maximale risicobeperking. Daarbij gaat het om het aantal verschillende soorten verwerkte gegevens, de personen die er toegang toe hebben, de levensduur van het gegeven, de moeilijkheid van heridentificatie en tot slot de risico's bij hacking van de gegevens.

De inlichtingendiensten hebben tijdens de hoorzittingen in herinnering gebracht dat de gegevens moeten worden beschermd tegen de inmengingsrisico's waartoe staatsentiteiten met grote personele en financiële slagkracht in staat zouden zijn; het gaat hier dus niet over een tiener die vanuit zijn kamer een hacking opzet. In diezelfde gedachtegang geven de academische deskundigen de voorkeur aan bluetooth boven gps-plaatsbepaling. Maar ook op dat punt waarschuwen de inlichtingendiensten dat de bluetooth-technologie momenteel onvoldoende beveiligd is én dat de doeltreffendheid ervan niet vaststaat, aangezien ontoereikende precisie tot veel foute meldingen dreigt te leiden.

Voorts moet men zich hoeden voor blind vertrouwen in de resultaten van geautomatiseerde gegevensverwerking (algoritmen). Voortdurend wordt aangetoond dat die algoritmen de kwalijke eigenschap hebben bestaande maatschappelijke ongelijkheden te weerspiegelen; zo zal een smartphone-app alleen van nut zijn voor wie

pas ceux qui n'en ont pas. Or, ce sont souvent des personnes âgées qui sont pourtant les plus exposées aux risques du COVID-19.

Un autre risque qui est bien identifié par la résolution: que des employeurs exigent l'utilisation d'une application pour pouvoir se rendre sur le lieu de travail. Ce n'est uniquement un risque hypothétique. Un article publié le 5mai 2020 dans le journal "La libre Belgique" se concluait ainsi: "Le patron d'Inforius nous indique que de grandes entreprises privées songent sérieusement à promouvoir de telles applications au sein de leurs structures "par précaution" pour protéger leurs salariés et éviter tant que possible un arrêt de l'outil de travail.".

Sur la transparence

Il y a un double consensus sur une éventuelle application: elle doit être utilisée de façon volontaire (non imposées), et il faut que au moins 60 % de la population l'utilise. À titre de comparaison, l'application développée dans la très connectée Singapour connait un succès plutôt faible puisque seule une personne sur 5 l'utilise.

Lors des auditions, le professeur Preneel qui développe une application et qui est membre de l'APD, estime qu'un pourcentage de 15 % d'utilisateurs serait suffisant pour avoir une efficacité. Mais il n'a pas été en mesure d'expliquer comment il avait abouti à ce chiffre.

Partant, si on maintient une volonté de développer une application, il est fondamental que le citoyen ait confiance dans la sécurité des données, que les autorités soient les plus transparentes possible. Chaque coin d'ombre serait une raison de plus pour un citoyen de ne pas installer l'application.

Or, à cet égard, on ne peut pas dire que le gouvernement soit exemplaire. Il a mis en place une task force "*data against corona*" chargée d'utiliser/de développer les outils numériques pour lutter contre le coronavirus. Mais ni les missions, ni la composition, ni les travaux, ni les avis externes rendus sur ces missions ont été officiellement publics.

Lors des auditions, la professeure Elise Degrave a expliqué avoir elle-même essayé d'obtenir plus d'informations sur cette *task force*, ce qui lui avait été refusé.

een smartphone heeft, maar vaak lopen net senioren in deze COVID-19-crisis het meest gevaar.

Dit voorstel van resolutie wijst tevens op een ander risico, met name dat werkgevers hun werknemers ertoe verplichten een dergelijke app te gebruiken, zo niet mogen ze de werkvloer niet betreden. Dat risico bestaat wel degelijk, getuige een artikel dat op 5 mei 2020 verscheen in *La Libre Belgique*: "*Le patron d'Inforius nous indique que de grandes entreprises privées songent sérieusement à promouvoir de telles applications au sein de leurs structures "par précaution" pour protéger leurs salariés et éviter tant que possible un arrêt de l'outil de travail.".*

Transparantie

Met betrekking tot een mogelijke app is men het erover eens dat die moet worden gebruikt op vrijwillige basis (het gebruik ervan mag dus niet worden opgelegd), alsook dat minstens 60 % van de bevolking die app moet gebruiken. Ter vergelijking kan erop worden gewezen dat de app in Singapore, met zijn toch wel hoge internetpenetratiegraad, slechts een matig succes kent, aangezien slechts 1 op 5 mensen die app gebruikt.

Professor Bart Preneel, die een app heeft ontwikkeld en lid is van de Gegevensbeschermingsautoriteit, heeft tijdens de hoorzittingen aangegeven dat een app volgens hem al efficiënt is wanneer slechts 15 % van de bevolking die app gebruikt. Hij kon evenwel niet uitleggen hoe hij tot dat cijfer is gekomen.

Gesteld dat men nog steeds een app zou willen ontwikkelen, dan is het dus van fundamenteel belang dat de burger erop vertrouwt dat zijn gegevens veilig zijn en dat de overheden zoveel mogelijk transparantie aan de dag leggen. De burger zou elk verdoken aspect aangrijpen als bijkomend argument om de app niet te installeren.

In dat opzicht wordt echter vastgesteld dat de regering niet bepaald voorbeeldig heeft gehandeld. Ze heeft een *data against corona*-taskforce opgericht, die de digitale instrumenten ter bestrijding van het coronavirus moet ontwikkelen en gebruiken. Er kwam echter geen officiële bekendmaking van de taken, de samenstelling en de werkzaamheden van die groep, noch van de externe adviezen die over die taken werden uitgebracht.

Tijdens de hoorzittingen heeft professor Elise Degrave aangegeven dat zij zelf heeft geprobeerd meer over die taskforce te weten te komen, maar dat die informatie haar werd ontzegd.

C'est dans cette optique que M. Lacroix a déposé un amendement pour que le cadre éventuel de l'application fasse l'objet d'un projet de loi débattu au Parlement et non d'un simple arrêté royal.

M. Michael Freilich (N-VA) fait observer qu'il semble que le traçage des contacts soit un instrument indispensable pour nous permettre de reprendre à court terme le cours d'une vie la plus normale possible. Il est à espérer qu'il sera également un instrument efficace pour éviter une nouvelle menace de surcharge de notre système de santé, ou du moins, pour la différer le plus longtemps possible. Car si nous présentons une résilience suffisante à l'heure actuelle, un deuxième, un troisième voire un quatrième confinement pourraient avoir des conséquences désastreuses pour notre économie, notre prospérité, notre bien-être et notre moral.

Ce suivi des contacts se situe ainsi aux confins de la vie privée, de l'économie et de la santé et du bien-être. Aucune de ces trois préoccupations ne semble pouvoir être préservée totalement dans un avenir proche, mais il faut que nous veillions tous ensemble à devoir faire le minimum de concessions dans ces trois domaines.

Mardi dernier, une audition commune a eu lieu avec la commission de la Justice, laquelle s'est avérée très utile afin de clarifier davantage un grand nombre de questions dans ce dossier. L'intervenant signale toutefois qu'une multitude de préoccupations et d'interrogations subsistent pourtant chez nombre de collègues au sujet de la protection de la vie privée et de l'efficacité du suivi des contacts et d'une éventuelle application déployée à cet effet.

L'intervenant lui-même par exemple se demande déjà depuis plusieurs semaines pourquoi consacrer autant d'énergie et de moyens au suivi des contacts s'il devait s'avérer prochainement que certains concitoyens qui se voient conseiller d'effectuer un test ou de rester en quarantaine ne respectent pas cette demande.

Il se rend toutefois également compte qu'il est difficile, dans un État de droit démocratique, de soumettre des personnes contre leur volonté à un examen médical ou qu'il est impossible de prendre les citoyens en filature pour contrôler s'ils respectent réellement une quarantaine imposée. Les débats à cet égard seront sans doute encore très nombreux à l'avenir.

Il demeure quoi qu'il en soit beaucoup d'incertitudes concernant l'efficacité d'une éventuelle application de suivi des contacts. L'intervenant a appris au cours des auditions qu'une application pourrait certes déjà produire

Om die reden heeft de heer Lacroix een amendement ingediend om het eventuele raamwerk omtrent de app te doen vastleggen in een wetsontwerp dat aan het Parlement ter bespreking wordt voorgelegd, veeleer dan bij louter koninklijk besluit te werken.

De heer Michael Freilich (N-VA) wijst erop dat *contact tracing* een onmisbaar instrument lijkt om ons op korte termijn opnieuw een zo normaal mogelijk leven te bieden. Hopelijk zal het ook een nuttig instrument blijken om een nieuwe dreiging van overbelasting van ons gezondheidssysteem te vermijden of ten minste zo lang mogelijk uit te stellen. Want nu hebben we nog voldoende veerkracht, maar een nieuwe tweede of derde of vierde lockdown zou desastreuze gevolgen kunnen hebben voor onze economie, onze welvaart, ons welzijn, onze moraal.

Die *contact tracing* balanceert dan ook op het snijvlak van Privacy, Economie, en Gezondheid en welzijn. We lijken de eerstkomende tijd géén van die 3 kostbaarheden volstrekt gaaf te kunnen houden, maar we moeten er samen voor zorgen dat we op die 3 terreinen zo min mogelijk moeten inboeten.

Vorige week dinsdag was er een gemeenschappelijke hoorzitting met de commissie Justitie die zeer nuttig bleek voor het verder uitklaren van een flink aantal vraagtekens in dit dossier. Maar de spreker merkt dat veel collega's toch nog met flink wat bezorgdheden en vragen zitten rond privacy en effectiviteit van *contact tracing* en een mogelijke app in dat verband.

Hijzelf stelt zich bijvoorbeeld al een aantal weken de vraag wat voor zin het heeft om zoveel energie en middelen in die *contact tracing* te steken, als binnenkort zou blijken dat bepaalde medeburgers die aangeraden worden om zich te laten testen of om in quarantaine te gaan, zulk verzoek volstrekt naast zich neerleggen.

Hij beseft ook wel dat we in een democratische rechtsstaat mensen moeilijk tegen hun wil aan een medische test kunnen onderwerpen of onmogelijk mensen gaan schaduwen om na te gaan of men zich werkelijk aan een opgelegde quarantaine houdt. Hierover zal er wellicht nog heel wat debat zijn in de toekomst.

Er blijft sowieso ook nog veel mist hangen rond de effectiviteit van een mogelijke contact *tracing app.* De spreker heeft tijdens de hoorzittingen vernomen dat een app inderdaad al vanaf 15 % gebruikers significante

des effets significatifs à partir de 15 % d'utilisateurs mais qu'elle ne serait effectivement pleinement efficace qu'à partir de 60 % d'utilisateurs.

Or, il va sans dire qu'il appartient aux Régions de décider si une application est déployée ou non. Le débat de fond concernant l'efficacité devrait dès lors peut-être être mené à ce niveau.

Par ailleurs, il se pourrait que l'ouverture des frontières terrestres en perspective des vacances d'été soit liée d'une manière ou d'une autre au niveau européen à l'utilisation d'un échange de données entre applications de suivi des contacts. Ne rejetons dès lors pas d'avance une telle application. Si nous n'en tirons aucun avantage, elle ne nous nuira pas non plus, comme le dit un dicton flamand.

Or, le parlement doit faire son travail et veiller à ce que la barre soit placée le plus haut possible dans le domaine de la protection de la vie privée. Le groupe de l'intervenant approuvera la proposition de résolution à l'examen dans cette optique.

Mme Catherine Fonck (cdH) souligne au préalable que toute une série de mesures sont nécessaires pour endiguer l'épidémie. Le suivi numérique des contacts ne doit pas être considéré en soi et de manière isolée mais doit être envisagé conjointement avec toutes ces mesures, parmi lesquelles notamment l'isolement des cas positifs.

La première question qui se pose en ce qui concerne l'application est de savoir si elle est nécessaire. Sur ce point, l'intervenante observe une différence fondamentale avec d'autres systèmes de suivi sanitaire, tel que c'est par exemple le cas depuis des années pour la tuberculose. Le COVID-19 est en effet beaucoup plus contagieux et touche énormément d'individus. Alors que pour la tuberculose, on est confronté à environ 1 000 cas par an, les 1 000 voire 1 500 cas par jour risquent d'être atteints (après le confinement) pour ce virus. Si les contacts des jours précédents sont tracés pour chacune des personnes concernées, on arrive en quelques semaines à des milliers, voire des dizaines de milliers de contacts à tracer. En tout état de cause, le suivi manuel des contacts pose des problèmes en termes d'efficacité et d'efficience par rapport, par exemple, au suivi de la tuberculose.

Contrairement à ce qui est le cas pour d'autres épidémies, nombreuses sont les personnes qui ne présentent aucun symptôme mais qui sont tout de même contagieuses. En outre, un test peut être négatif un jour donné et positif le lendemain. Dès lors qu'il est impossible

effecten zou kunnen sorteren, maar dat die app inderdaad pas ten volle efficiënt zou zijn vanaf 60 %.

Al is het natuurlijk inderdaad wel aan de Gewesten om te beslissen of er een app wordt uitgerold of niet. Misschien moet het debat rond effectiviteit dan wel eerder daar ten gronde worden gevoerd.

Anderzijds zou het wel eens goed kunnen dat men op het Europees niveau het openstellen van de landsgrenzen met het oog op de zomervakantie binnenkort op de een of de andere manier zal koppelen aan het gebruik van en de gegevensuitwisseling tussen *contact tracing apps*. Laat ons zo'n app dus hier niet bij voorbaat afwijzen. Baat het niet, dan schaadt het niet, is een Vlaams gezegde.

Maar het Parlement moet zijn werk doen, en ervoor zorgen dat de lat op vlak van privacy zo hoog mogelijk wordt gelegd. Zijn fractie zal het voorliggend voorstel van resolutie in dat licht mee goedkeuren.

Mevrouw Catherine Fonck (cdH) benadrukt vooraf dat er een heel pallet aan maatregelen nodig is om de epidemie in te dijken: digitale tracering mag niet op zichzelf en geïsoleerd worden bekeken maar moet samen worden gezien met al deze maatregelen, waaronder onder meer de isolatie van positieve gevallen.

De eerste vraag die zich stelt met betrekking tot de applicatie is of ze noodzakelijk is. Op dit punt stelt de spreekster een fundamenteel verschil vast met andere systemen van sanitaire opvolging zoals bijvoorbeeld al jaren gebeurt voor tbc: COVID-19 is immers veel besmettelijker en treft enorm veel individuen: waar men voor tbc te maken heeft met ongeveer 1 000 gevallen per jaar, riskeert men voor dit virus te komen aan 1 000 en 1 500 gevallen per dag (na de *lockdown*). Indien men voor elk van de betrokkenen de contacten van de voorgaande dagen gaat terug traceren komt men op enkele weken tijd alsnog tot duizenden of zelfs tienduizenden contacten die moeten worden getraceerd. In elk geval stelt de manuele tracering hier problemen inzake effectiviteit en doeltreffendheid in vergelijking met bijvoorbeeld opvolging van tbc.

Een tweede fundamenteel verschil met andere epidemieën is het feit dat vele mensen geen symptomen vertonen maar toch besmettelijk zijn; bovendien kan een test vandaag negatief zijn maar morgen positief. Het is onmogelijk om de 11 miljoen Belgen dagelijks

de tester quotidiennement 11 millions de Belges, il est nécessaire de briser la chaîne de transmission selon d'autres modalités.

L'intervenante revient ensuite sur l'affirmation selon laquelle un taux de 60 % d'utilisateurs serait nécessaire pour assurer l'efficacité de l'application: dans quelle mesure cette affirmation est-elle corroborée par des preuves scientifiques? Il existe, en tout et pour tout, une seule étude scientifique à ce sujet, réalisée par l'Université d'Oxford (Fraser et consorts), dont l'intervenante cite l'une des conclusions: "Nos modèles indiquent que nous pouvons arrêter l'épidémie si environ 60 % de la population utilise l'application et, même avec un nombre inférieur d'utilisateurs de l'application, nous prévoyons toujours une réduction du nombre de cas de coronavirus".

Cette étude indique en outre que chaque utilisateur de l'application peut éviter qu'une à deux personnes deviennent porteuses du virus. Elle montre qu'un taux de 60 % d'utilisateurs permet de stopper l'épidémie alors que le traçage manuel ne permettra jamais d'assurer une surveillance de 60 % de la population. De plus, cette étude indique qu'un effet est déjà perceptible à partir de 15 % d'utilisateurs de l'application.

Comme il a été indiqué, toute application de ce type doit évidemment compléter un ensemble d'autres mesures. L'intervenante souligne en outre l'importance de prévoir, dans la résolution, une série de garanties en matière de protection de la vie privée, ainsi que d'autres conditions essentielles, comme le caractère décentralisé, le caractère volontaire, l'utilisation du Bluetooth, la destruction des données *a posteriori*, etc.

Il ne faut pas être naïf: le traçage manuel a également un impact important sur le respect de la vie privée dès lors qu'il utilise une banque de données dans laquelle les données ne sont pas anonymisées mais pseudonymisées: la membre attend avec beaucoup d'intérêt l'avis du Conseil d'État à ce sujet.

En outre, le but est également d'éviter un nouveau confinement et un confinement éventuellement plus strict. L'intervenante préfère l'isolement temporaire de certains individus à un confinement général et collectif.

Enfin, les mesures prises en Belgique sont très différentes du système appliqué en Asie, où les données sont centralisées, si bien que l'État exerce un contrôle pour que les gens restent chez eux: il va de soi que ce système n'est pas défendable du point de vue du respect de la vie privée.

M. Kris Verduyckt (sp.a) estime que la proposition de résolution a été une bonne initiative, sans être lui-même

te testen en dus zijn er andere manieren nodig om de transmissieketens te breken.

De spreekster gaat vervolgens in op de bewering dat 60 % gebruikers van de app noodzakelijk zou zijn voor doeltreffendheid: welke wetenschappelijke evidentie bestaat er voor deze bewering? Er is hier welgeteld sprake van één wetenschappelijke studie, namelijk van de Oxford-universiteit (Fraser cs) en de spreekster citeert vervolgens één conclusie van deze studie: "*our models show we can stop the epidemic if approximately 60 % of the population use the app and even with lower numbers of app users we still estimate a reduction in the number of coronavirus cases"*

De studie stelt verder dat elke gebruiker van de app kan vermijden dat een à twee personen drager worden van het virus. De studie toont aan dat je de epidemie kan stoppen met 60 %, maar manuele tracering zal nooit 60 % surveillance geven op het niveau van de bevolking. Bovendien toont de studie dat er reeds een effect is vanaf 15 % gebruikers van de app.

Uiteraard moet de app zoals gezegd complementair zijn aan een geheel van andere maatregelen. De spreekster benadrukt verder het belang van een aantal waarborgen voor de bescherming van de privacy in de resolutie, evenals een aantal andere essentiële voorwaarden zoals het decentrale karakter, de vrijwilligheid, het gebruik van bluetooth, de vernietiging van de gegevens achteraf enzovoort.

Men mag niet naïef zijn: manuele tracering heeft eveneens een diepgaande impact op de privacy want er wordt gebruik door die gemaakt van een gegevensbank, waarin de gegevens niet geanonimiseerd zijn maar gepseudonimiseerd: zij kijkt met veel belangstelling uit naar het advies van de Raad van State hieromtrent.

Verder is het ook de bedoeling dat morgen een nieuwe en eventueel strengere l*ockdown* kan worden vermeden. De spreekster verkiest een tijdelijke isolering van individuen boven een algemene en collectieve *lockdown.*

Ten slotte zijn de maatregelen die in België worden genomen zeer verschillend van hetgeen in Azië gebeurt waar de gegevens worden gecentraliseerd, zodat de staat controle uitoefent opdat de mensen thuis zouden blijven: uiteraard is dit niet verdedigbaar vanuit een privacy-oogpunt.

De heer Kris Verduyckt (sp.a) is van mening dat het voorstel van resolutie een goed initiatief is geweest zonder

très favorable à une éventuelle application: il s'agit de fixer un cadre pour rendre une certaine technologie acceptable. En effet, aujourd'hui, on dispose de certaines technologies qui permettent de faire beaucoup de choses qui peuvent être très invasives au niveau de la vie privée: la question se pose de savoir si on va les utiliser ou non.

En tout cas, la protection de la vie privée est un combat dans lequel le législateur est toujours en retard: à cet égard, l'intervenant renvoie aux problèmes récents en matière de protection de la vie privée liés à l'application ZOOM, qui est beaucoup utilisée, ainsi que le débat qui s'est engagé récemment en Flandre sur une certaine application TIKTOK.

Le Vlaams Belang souligne qu'une majorité des citoyens interrogés affirment qu'ils n'utiliseront pas une éventuelle application. L'intervenant souhaite répliquer que le comportement humain est difficilement prévisible: qui aurait pu prévoir, il y a quelques années, que les sites de rencontres comme Tinder connaîtraient un tel succès? L'intervenant plaide donc pour que l'on adopte l'approche inverse et que l'on ait confiance dans l'avenir. En outre, le raisonnement du Vlaams Belang n'est pas correct: en votant en faveur de cette résolution, on fera en sorte qu'une éventuelle application fonctionne, à l'avenir, de la manière dont le législateur le souhaite.

Enfin, il faut bien admettre qu'une série de problèmes pratiques se posent, comme le taux de participation de 60 % qui est en principe exigé et le fait que Bluetooth n'est pas protégé à 100 % contre le *hacking* (même s'il s'agit d'une information codée). En tout cas, son groupe soutiendra la proposition de résolution.

Mme Nathalie Gilson (MR) souligne que le traçage par l'application est très important, comme l'a déjà expliqué Mme Fonck. En revanche, le traçage manuel est très invasif au niveau de la vie privée: ainsi, les participants doivent donner les coordonnées de toutes les personnes avec lesquelles ils ont eu des contacts au cours des cinq derniers jours; il faut en outre également tenir compte de la réaction de ces personnes qui devront être appelées par téléphone: peut-être ne souhaitent-elles pas du tout être contactées.

En tout cas, l'application devra nous permettre de retrouver au plus vite nos libertés constitutionnelles, qui sont actuellement restreintes.

Par ailleurs, la *toolbox* développée par la Commission européenne, de même qu'une série d'autres garanties, peuvent sans doute accroître la confiance des citoyens par rapport au contrôle des risques que présenteraient une application quant au respect de la vie privée.

daarbij zelf een grote fan te zijn van een eventuele applicatie: het gaat erom een kader vast te leggen om een bepaalde technologie aanvaardbaar te maken. Immers, vandaag zijn technologieën beschikbaar die heel veel zaken toelaten die met name heel privacy-invasief kunnen zijn: de vraag is of we deze gaan inschakelen of niet?

In elk geval is de bescherming van de privacy een strijd waarbij de wetgever steeds achteraanloopt: in dit verband verwijst de spreker naar de recente privacyproblemen van de veelgebruikte applicatie ZOOM, evenals de recente discussie rond een bepaalde TIKTOK-app in Vlaanderen.

Vlaams Belang wijst erop dat een meerderheid van de ondervraagde burgers verklaart een eventuele app niet te zullen gebruiken. De spreker wenst daar tegenover te stellen dat het menselijk gedrag moeilijk te voorspellen is: wie had enkele jaren geleden kunnen voorspellen dat dating sites zoals Tinder een dergelijk succes zouden kennen. De spreker pleit er dus voor om dit om te draaien en daarentegen vertrouwen te hebben in de toekomst. Bovendien is de redenering van het Vlaams Belang onjuist: door deze resolutie te stemmen zal een eventuele app in de toekomst werken zoals de wetgever dat wenst.

Ten slotte moet men wel toegeven dat er zich een aantal praktische problemen stellen zoals de in principe vereiste participatiegraad van 60 % en het feit dat bluetooth niet 100 % bestand is tegen hacking (hoewel het wel om gecodeerde informatie gaat). In elk geval zal zijn fractie het voorstel van resolutie steunen.

Mevrouw Nathalie Gilson (MR) benadrukt dat de tracering door de applicatie zeer belangrijk is zoals ook mevrouw Fonck reeds heeft uiteengezet. Daartegenover staat dat de manuele tracering zeer privacy-invasief is: zo dienen de deelnemers de coördinaten van alle personen waarmee ze de voorbije vijf dagen contact hebben gehad door te geven; bovendien moet men ook rekening houden met de reactie van deze betrokkenen die moeten worden opgebeld: misschien wensen zij helemaal niet gecontacteerd te worden.

In elk geval zal de app ons moeten toelaten om zo snel mogelijk onze grondwettelijke vrijheden, die momenteel ingeperkt, zijn terug op te nemen.

Daarnaast kunnen de door de Europese Commissie ontwikkelde *toolbox* evenals een reeks andere waarborgen de burgers wellicht meer vertrouwen geven wat het beheersen van de privacyrisico's van een applicatie betreft.

Vu que le traçage manuel est plus invasif, l'intervenante a déposé une série d'amendements en vue de renforcer la protection de la vie privée, d'autant que plus de 2 000 personnes seront mobilisées pour le traçage manuel.

L'intervenante a appris que l'arrêté royal prévoyant une série de règles relatives au respect de la vie privée dans le cadre du traçage manuel a été publié et qu'il pourrait y avoir très rapidement un autre instrument législatif. Sur ce point, elle préfère une proposition de loi à un projet de loi, car cela permet au parlement de se saisir de ce problème dans son ensemble. Ses amendements sur le traçage manuel sont donc retirés puisqu'un autre instrument législatif en traitera. Ceux sur le traçage digital sont maintenus.

M. Egbert Lachaert (Open Vld) souligne que son groupe a soutenu et cosigné la proposition de résolution, car son groupe est demandeur d'un débat parlementaire et d'un cadre législatif autour du respect de la vie privée, sans être forcément favorable à une application.

Nous savons aujourd'hui que l'autorité fédérale est uniquement compétente pour le cadre légal et que ce seront les communautés qui décideront s'il y aura ou non une application.

Quoi qu'il en soit, une loi est nécessaire; son groupe n'a pas tranché quant à savoir s'il doit s'agir d'une proposition de loi ou d'un projet de loi. En tout cas, après le vote de la résolution, un débat parlementaire sera encore nécessaire.

M. Nabil Boukili (PVDA-PTB) souligne qu'il est essentiel que l'on utilise tous les moyens pour endiguer l'épidémie et pour trouver des solutions. Cela étant, une série de problèmes fondamentaux se posent tout de même en ce qui concerne le respect de la vie privée, tant pour ce qui est d'une éventuelle application que pour le traçage physique. L'utilité des instruments utilisés peut aussi être remise en question.

L'intervenant peut également souscrire à certaines observations formulées par les intervenants précédents. Il présentera en tout cas plusieurs amendements afin que la résolution offre davantage de garanties en matière de respect de la vie privée. Son groupe soutiendra la résolution mais souhaite que de solides garanties soient prévues à l'égard de la protection de la vie privée et de l'efficacité de la réponse en matière de santé publique.

Vermits manuele tracering meer invasief is, heeft de spreekster een aantal amendementen ingediend, temeer daar men meer dan 2 000 mensen gaat inzetten voor manuele tracering.

De spreekster heeft vernomen dat het koninklijk besluit is gepubliceerd dat een aantal privacyregels stelt voor de manuele tracering en dat er heel snel een ander wetgevend instrument zou kunnen komen. Op dit punt geeft zij de voorkeur aan een wetsvoorstel boven een wetsontwerp, want op die manier kan het parlement de zaak voor 100 % naar zich toe trekken. Haar amendementen over de manuele tracering worden dus ingetrokken vermits een ander wetgevend instrument daarover zal handelen. De amendementen over de tracering via de app blijven behouden.

De heer Egbert Lachaert (Open Vld) benadrukt dat zijn fractie het voorstel van resolutie heeft gesteund en medeondertekend, omdat zijn fractie vragende partij is voor een parlementair debat en voor een wetgevend kader rond privacy zonder daarbij per se een voorstander te zijn van een app.

Ondertussen weten we dat de federale overheid enkel bevoegd is voor het wettelijk kader en dat het de gemeenschappen zijn die zullen beslissen of er al dan niet een app zal komen.

In elk geval is er een wet nodig; voor zijn fractie is het niet uitgemaakt of het moet gaan om een wetsvoorstel op een wetsontwerp. In elk geval echter is na het stemmen van de resolutie nog een parlementair debat nodig.

De heer Nabil Boukili (PVDA-PTB) benadrukt dat het essentieel is dat alle middelen worden ingezet om de epidemie in te dijken en om oplossingen te vinden. Dit gezegd zijnde, stellen zich toch een aantal fundamentele problemen inzake de bescherming van de privacy zowel met betrekking tot een eventuele app als voor de fysieke tracering. Ook de nuttigheid van de gebruikte instrumenten kan in vraag worden gesteld.

De spreker kan zich verder aansluiten bij een aantal opmerkingen die door de vorige sprekers werden gemaakt. In elk geval zal hij een aantal amendementen indienen teneinde in de resolutie meer waarborgen in te voegen met betrekking tot de bescherming van de privacy. Zijn fractie zal de resolutie steunen maar wenst solide waarborgen inzake de bescherming van de privacy en de doeltreffendheid van de respons inzake volksgezondheid.

M. Sammy Mahdi (CD&V) fait observer que cette problématique a déjà été examinée en détail au cours de trois réunions différentes de la commission ainsi qu'en commission de la Justice. Il ajoute qu'à la question de savoir si une application mobile est nécessaire, il répondrait pas la négative. Telle n'est toutefois pas la question à laquelle la réunion de ce jour doit répondre. Il s'agit plutôt de la question du cadre juridique qu'il convient de mettre en place pour que les développeurs d'une application mobile de ce type ne puissent pas dérober les données personnelles de nos concitoyens.

Un élément important est ressorti des auditions, à savoir qu'une capacité de dépistage de 15 à 20 % répartie sur tout le territoire serait plus efficace que l'installation de la l'application mobile par 60 % de nos concitoyens.

Enfin, en ce qui concerne la préférence accordée à un projet ou à une proposition de loi, l'intervenant adhère à la position de M. Lachaert: ce qui importe le plus, c'est que l'on établisse un cadre juridique.

M. Gilles Vanden Burre (Ecolo-Groen) souligne que c'est l'importance d'avoir un débat parlementaire qui a principalement motivé son groupe à cosigner la proposition de résolution à l'examen. L'intervenant souligne que le Parlement s'est montré prompt à agir dans ce dossier: il renvoie notamment aux auditions qui ont eu lieu au sein de cette commission la semaine dernière, ainsi qu'à l'avis remis par la commission de la Justice.

En outre, cette commission vient d'avoir un entretien détaillé et intéressant avec le ministre en charge de l'agenda numérique: l'intervenant a été agréablement surpris par l'état d'esprit du ministre, qui plaide explicitement en faveur d'une approche respectueuse de la primauté du respect de la vie privée.

Ce débat doit en tout cas s'inscrire dans le cadre plus large de l'assouplissement progressif du confinement, qui s'étalera peut-être encore sur plusieurs semaines, voire sur plusieurs mois. Il concerne notamment le dépistage et le traçage et, à titre complémentaire, une réflexion sur les applications numériques offrant des garanties strictes en matière de protection de la vie privée.

L'intervenant conclut en indiquant que son groupe estime, lui aussi, qu'un texte de loi s'impose.

M. Christophe Lacroix (PS) clarifie les arguments de l'étude d'Oxford. Selon cette étude, 80 % des utilisateurs de téléphones mobiles doivent participer au système. Cela représenterait quelque 56 % de la population du Royaume-Uni.

De heer Sammy Mahdi (CD&V) merkt op dat deze problematiek reeds uitgebreid werd besproken op drie verschillende vergaderingen in deze commissie en in de commissie voor Justitie. Hij voegt eraan toe dat zijn antwoord op de vraag of een app noodzakelijk is, negatief zou zijn, maar dit is niet de vraag die deze vergadering moet beantwoorden. Het gaat daarentegen om de vraag welk juridisch kader moet worden geschapen opdat de ontwikkelaars van een dergelijke app niet aan de haal zouden gaan met de privégegevens van onze burgers.

Een belangrijk element uit de hoorzittingen is verder dat 15-20 % testcapaciteit verspreid over het hele grondgebied efficiënter zou zijn dan dat 60 % van onze burgers de app zouden installeren.

Wat ten slotte de voorkeur voor een wetsontwerp of een wetsvoorstel aangaat kan de spreker zich aansluiten bij het standpunt van de heer Lachaert: het belangrijkste is dat een juridisch kader wordt gecreëerd.

De heer Gilles Vanden Burre (Ecolo-Groen) benadrukt dat het belangrijkste motief om dit voorstel van resolutie te ondertekenen voor zijn fractie het belang is van een parlementair debat. De spreker benadrukt dat het parlement in dit dossier snel is opgetreden: hij verwijst onder meer naar de hoorzittingen die vorige week hebben plaatsgevonden in deze commissie evenals het advies dat door de commissie voor Justitie werd gegeven.

Bovendien heeft deze commissie daarnet een uitgebreid en interessant onderhoud gehad met de minister bevoegd voor digitale agenda: de spreker was aangenaam verrast door de instelling van de minister die uitdrukkelijk pleit voor een "*privacy first"* -benadering".

Dit debat dient in elk geval te worden gesitueerd in het grotere kader van het geleidelijk loslaten van de *lockdown.* Dit zal nog weken en misschien wel maanden aanslepen; het gaat onder meer over testen en tracering en complementair een reflectie over digitale applicaties met strenge waarborgen voor de privacy.

De spreker besluit dat voor zijn fractie eveneens een wettekst noodzakelijk is.

De heer Christophe Lacroix (PS) verduidelijkt de argumenten in de Oxford-studie: volgens deze studie moet 80 % van de gebruikers van mobiele telefoons in het systeem stappen. Dit zou neerkomen op ongeveer 56 % van de bevolking van het Verenigd Koninkrijk.

Quant au choix entre un projet et une proposition de loi, le projet de loi offre l'avantage de requérir obligatoirement l'avis du Conseil d'État et de l'Autorité de protection des données. En outre, un projet de loi s'intègre plus facilement dans le cadre de la politique globale de la santé publique.

III. — **DISCUSSION DES CONSIDÉRANTS ET DES DEMANDES ET VOTES**

Intitulé

L'amendement n° 2 de Mme Gilson (DOC 1182/002) est retiré.

A. **Considérants**

Considérants A à Z

Ces considérants ne donnent lieu à aucune observation.

Ils sont adoptés à l'unanimité.

Considérant Z1 *(nouveau)*

L'amendement n° 3 de Mme Gilson (DOC 1182/002) est retiré.

Considérant Z2 *(nouveau)*

L'amendement n° 4 de Mme Gilson (DOC 1182/002) est retiré.

Considérant Z3 *(nouveau)*

Mme Nathalie Gilson (MR) présente *l'amendement n° 5* (DOC 1182/002) qui renvoie à l'obligation pour les tiers de respecter les règles en matière de secret professionnel (article 458 du Code pénal) et les dispositions du règlement général sur la protection des données.

L'amendement n° 5 est adopté par 15 voix et une abstention.

Considérant Z4 *(nouveau)*

Mme Nathalie Gilson (MR) présente *l'amendement n° 6* (DOC 1182/002) qui renvoie aux lignes directrices 03/2020 du Comité européen de la protection des

Wat de keuze voor een wetsontwerp of een wetsvoorstel betreft, biedt een wetsontwerp het voordeel van een verplicht advies van de Raad van State en van de Gegevensbeschermingsautoriteit. Bovendien is een wetsontwerp gemakkelijker te kaderen in het globale beleid inzake volksgezondheid.

III. — **BESPREKING VAN DE CONSIDERANSEN EN DE VERZOEKEN EN STEMMINGEN**

Opschrift

Amendement nr. 2 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken.

A. **Consideransen**

Consideransen A tot Z

Over deze consideransen worden geen opmerkingen gemaakt.

Ze worden eenparig aangenomen.

Considerans Z1 *(nieuw)*

Amendement nr. 3 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken.

Considerans Z2 *(nieuw)*

Amendement nr. 4 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken.

Considerans Z3 *(nieuw)*

Mevrouw Nathalie Gilson (MR) dient *amendement nr. 5* (DOC 1182/002) in. Dit verwijst naar de verplichting voor derden om de bepalingen inzake beroepsgeheim (artikel 458 van het Strafwetboek) en van de algemene verordening gegevensbescherming in acht te nemen.

Amendement nr. 5 wordt aangenomen met 15 stemmen en 1 onthouding.

Considerans Z4 *(nieuw)*

Mevrouw Nathalie Gilson (MR) dient *amendement nr. 6* (DOC 1182/002) in. Hierin wordt verwezen naar de richtlijnen 03/2020 van het Europees comité voor

données relatives au traitement des données de santé à des fins de recherche scientifique dans le contexte de l'épidémie de COVID-19. Elle renvoie à la justification des amendements.

L'amendement n° 6 est adopté par 15 voix et une abstention.

Considérant Z5 *(nouveau)*

Mme Sophie Rohonyi (DéFI) présente *l'amendement n° 12* (DOC 1182/003), qui précise que les données relatives à l'état de santé d'une personne sont des données sensibles, dont le traitement ne peut se justifier que dans des circonstances exceptionnelles bien déterminées et sous un contrôle très strict.

L'amendement n° 12 est adopté à l'unanimité.

Considérant Z6 *(nouveau)*

M. Nabil Boukili (PVDA-PTB) présente *l'amendement n° 13* (DOC 1182/003) qui indique que l'anonymisation des données de localisation est, dans de nombreux cas, problématique, si bien que le consentement des intéressés est requis avant de pouvoir traiter ces données. L'intervenant renvoie à la justification de l'amendement.

L'amendement n° 13 est rejeté par 5 voix contre 4 et 8 abstentions.

Considérant Z7 *(nouveau)*

M. Boukili (PVDA-PTB) présente *l'amendement n° 14* (DOC 1182/003) qui fait référence aux déclarations du ministre De Backer le 23 avril 2020, par lesquelles ce dernier affirmait qu'aucune application n'était nécessaire pour le suivi des contacts, qu'au moins 60 % de la population devraient utiliser l'application avant qu'elle ait un effet et, enfin, qu'on ne constatait qu'une adhésion limitée à l'étranger (3 à 4 % en Autriche). L'intervenante renvoie à la justification de l'amendement.

L'amendement n° 14 est rejeté par 10 voix contre 6.

B. **Demandes**

Demande n° 1a

Cette demande ne donne lieu à aucune observation.

gegevensbescherming, inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in de context van de COVID-19 epidemie. Zij verwijst naar de toelichting.

Amendement nr. 6 wordt aangenomen met 15 stemmen en 1 onthouding.

Considerans Z5 *(nieuw)*

Mevrouw Sophie Rohonyi (DéFI) dient *amendement nr. 12* (DOC 1182/003) in, waarin wordt gesteld dat gegevens betreffende de gezondheidstoestand van een persoon gevoelige gegevens zijn, waarvan de verwerking enkel kan gebeuren in uitzonderlijke en welbepaalde omstandigheden en onder zeer strikte controle.

Amendement nr. 12 wordt eenparig aangenomen.

Considerans Z6 *(nieuw)*

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 13* (DOC 1182/003) in. Hierin wordt gesteld dat de anonimisering van lokalisatiegegevens in veel gevallen problematisch is en dus de instemming vereist van de betrokkenen vooraleer deze gegevens mogen worden verwerkt. De indiener verwijst naar de toelichting bij het amendement.

Amendement nr. 13 wordt verworpen met 5 tegen 4 stemmen en 8 onthoudingen.

Considerans Z7 *(nieuw)*

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 14* (DOC 1182/003) in. Dit behelst een verwijzing naar de verklaringen van minister De Backer op 23 april 2020, waarbij hij stelde dat geen enkele applicatie noodzakelijk is voor de opvolging van contacten, dat minstens 60 % van de bevolking de applicatie zou moeten gebruiken vooraleer er een effect is en ten slotte dat in het buitenland slechts een beperkte adhesie werd vastgesteld (3 à 4 % in Oostenrijk). De indiener verwijst naar de toelichting bij het amendement.

Amendement nr. 14 wordt verworpen met 10 tegen 6 stemmen.

B. **Verzoeken**

Verzoek 1a

Bij dit verzoek worden geen opmerkingen gemaakt.

Elle est adoptée à l'unanimité.

Demande n° 1b

M. Nabil Boukili (PVDA-PTB) présente *l'amendement n° 5* (DOC 1182/003). Il tend à remplacer la demande 1b par une demande visant l'institution d'un comité de contrôle entièrement indépendant, composé de pirates éthiques et d'experts dans les domaines de la protection de la vie privée, des droits humains et de la cryptographie, et l'octroi de moyens suffisants à ce comité pour qu'il puisse mener à bien sa mission. Pour le surplus, l'intervenant renvoie à la justification écrite de son amendement.

L'amendement n° 15 est adopté à l'unanimité.

Demande n° 1c

M. Nabil Boukili (PVDA-PTB) présente l'*amendement n° 16* (DOC 1182/003), qui vise à compléter la demande en précisant que la lutte contre le coronavirus devrait être coordonnée au niveau fédéral.

L'amendement n° 16 est rejeté par 12 voix contre une et 2 abstentions.

La demande 1c est ensuite adoptée à l'unanimité.

Demande n° 1d

Cette demande ne donne lieu à aucune observation.

Elle est adoptée à l'unanimité.

Demande n° 1e

M. Nabil Boukili (PVDA-PTB) présente l'*amendement n° 17* (DOC 1182/003), qui vise à compléter la demande en précisant que le logiciel concerné devrait être développé en toute indépendance et de manière générique. Pour le reste, l'auteur renvoie à la justification de l'amendement.

L'amendement n° 17 est rejeté par 11 voix contre une et une abstention.

La demande 1e est ensuite adoptée à l'unanimité.

Het wordt eenparig aangenomen.

Verzoek 1b

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 15* (DOC 1182/003) *in.* Dit strekt ertoe verzoek 1b te vervangen door de instelling van een volledig onafhankelijk toezichtscomité, bestaande uit ethische hackers en experten inzake bescherming van het privéleven, mensenrechten en cryptografie, en dit comité voldoende middelen te geven om zijn controletaken goed te kunnen uitvoeren. De indiener verwijst verder naar de toelichting bij het amendement.

Amendement nr. 15 wordt eenparig aangenomen.

Verzoek 1c

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 16* (DOC 1182/003) in. Dit strekt ertoe het verzoek aan te vullen met de vraag om de strijd tegen het coronavirus te coördineren op federaal niveau.

Amendement nr. 16 wordt verworpen met 12 tegen 1 stem en 2 onthoudingen.

Verzoek 1c wordt vervolgens eenparig aangenomen.

Verzoek 1d

Bij dit verzoek worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Verzoek 1e

De heer Nabil Boukili (PVDA-PTB) dient amendement nr. 17 (DOC 1182/003) in. Dit strekt ertoe het verzoek aan te vullen opdat de betrokken software volledig onafhankelijk en generisch zou worden ontwikkeld. De indiener verwijst verder naar de toelichting bij het amendement

Amendement nr. 17 wordt verworpen met 11 tegen 1 stem en 1 onthouding.

Verzoek 1e wordt vervolgens eenparig aangenomen

Demande n° 1f

Cette demande ne donne lieu à aucune observation.

Elle est adoptée à l'unanimité.

Demande n° 1g

M. Michael Freilich (N-VA) présente l'*amendement n° 23* (DOC 1182/003) qui vise à compléter la demande en précisant que les données générées par l'application ne peuvent d'une quelconque manière être réutilisées ou couplées à d'autres données que dans la mesure où cela s'avère nécessaire à la lutte contre l'épidémie et, éventuellement, à des fins de recherche scientifique dans ce domaine. L'auteur renvoie à la justification de l'amendement.

Dans l'amendement 23, il est précisé que les données générées ne doivent pas être mélangées avec d'autres données. *Mme Barbara Pas (VB)* rappelle toutefois qu'au cours des auditions, la professeure Elise Degrave avait déclaré qu'elle ne croyait absolument pas qu'une telle base de données serait réellement indépendante. L'intervenante indique que personne ne pourra la convaincre du contraire.

L'amendement n° 23 est ensuite adopté par 10 voix et 6 abstentions. La demande 1g, ainsi modifiée, est ensuite adoptée par 15 voix et 2 abstentions.

Demande n° 1h

Cette demande ne donne lieu à aucune observation.

Elle est adoptée à l'unanimité.

Demande n° 1i

M. Michael Freilich (N-VA) présente l'*amendement n° 24* (DOC 1182/003), qui vise à permettre une identification individuelle minimale (par exemple un numéro de téléphone) dans le seul but de permettre la prise de contact nécessaire dans le cadre du suivi des contacts et de demander aux intéressés de se faire tester ou de se mettre en quarantaine. L'auteur renvoie à la justification de son amendement.

L'amendement n° 24 est rejeté par 9 voix contre 5 et une abstention.

La demande 1i est ensuite adoptée à l'unanimité.

Verzoek 1f

Bij dit verzoek worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Verzoek 1g

De heer Michael Freilich (N-VA) dient *amendement nr. 23* (DOC 1182/003) in. Dit strekt ertoe het verzoek aan te vullen om te garanderen dat de door de app gegenereerde gegevens op geen enkele manier mogen worden hergebruikt of aan andere gegevens worden gekoppeld dan nodig blijkt voor de doeleinden van bestrijding van de epidemie en van eventueel wetenschappelijk onderzoek daarrond. De indiener verwijst naar de toelichting bij het amendement.

Wat amendement nr. 23 betreft, wordt gesteld dat de gegenereerde gegevens niet mogen worden vermengd met andere data maar *mevrouw Barbara Pas (VB)* verwijst naar professor Elise Degrave die tijdens de hoorzittingen heeft verklaard dat ze er geen enkel vertrouwen in had dat een dergelijke databank echt onafhankelijk zou zijn; niemand kan de spreekster overtuigen van het tegendeel.

Amendement nr. 23 wordt vervolgens aangenomen met 10 stemmen en 6 onthoudingen. Het aldus gewijzigde verzoek 1g wordt vervolgens aangenomen met 15 stemmen en 2 onthoudingen.

Verzoek 1h

Bij dit verzoek worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Verzoek 1i

De heer Michael Freilich (N-VA) dient *amendement nr. 24* (DOC 1182/003) in. Dit strekt er toe een minimale individuele identificatie (bijvoorbeeld een telefoonnummer) toe te laten voor loutere doeleinden van contactname, die nodig blijkt in het kader van *contact tracing* en verzoeken in dat kader om zich te laten testen of in quarantaine te gaan. De indiener verwijst naar de toelichting bij het amendement.

Amendement nr. 24 wordt verworpen met 9 tegen 5 stemmen en 1 onthouding.

Verzoek 1i wordt vervolgens eenparig aangenomen

Demandes nos 1j et 1k

Ces demandes ne donnent lieu à aucune observation.

Elles sont adoptées à l'unanimité.

Demande n° 1l

M. Michael Freilich (N-VA) présente *l'amendement n° 25* (DOC 1182/003) tendant à disposer que le gouvernement devra tout mettre en œuvre pour limiter le risque de manipulation des données autant et aussi fermement que possible. Il vise donc une obligation de moyens. L'intervenant renvoie à la justification de son amendement.

L'amendement n° 25 est rejeté par 10 voix contre 4 et 3 abstentions.

La demande n° 1l est ensuite adoptée à l'unanimité.

Demandes nos 1m et 1n

Ces demandes ne donnent lieu à aucune observation.

Elles sont adoptées à l'unanimité.

Demande n° 1o

M. Michael Freilich (N-VA) présente *l'amendement n° 26* (DOC 1182/003) tendant à inscrire le traçage manuel des contacts dans la politique globale de lutte contre l'épidémie, ce traçage étant essentiel. L'intervenant renvoie à la justification de son amendement.

L'amendement n° 26 est ensuite adopté par 14 voix et 3 abstentions. La demande n° 1o, ainsi modifiée, est adoptée à l'unanimité.

Demandes nos 1p, 1q et 1r

Ces demandes ne donnent lieu à aucune observation.

Elles sont adoptées à l'unanimité.

Verzoeken 1j en 1k

Bij deze verzoeken worden geen opmerkingen gemaakt.

Ze worden eenparig aangenomen.

Verzoek 1l

De heer Michael Freilich (N-VA) dient *amendement nr. 25* (DOC 1182/003) in. Dit strekt ertoe te bepalen dat de regering alles in het werk moet stellen om het risico op de manipulatie van gegevens zoveel en zo sterk mogelijk te beperken; het gaat dus om een inspanningsverbintenis. De indiener verwijst naar de toelichting.

Amendement nr. 25 wordt verworpen met 10 tegen 4 stemmen en 3 onthoudingen.

Verzoek 1l wordt vervolgens eenparig aangenomen

Verzoeken 1m en 1n

Bij deze verzoeken worden geen opmerkingen gemaakt.

Ze worden eenparig aangenomen.

Verzoek 1o

De heer Michael Freilich (N-VA) dient *amendement nr. 26* (DOC 1182/003) in. Dit strekt ertoe in de beschrijving van het omvattend beleid tegen de epidemie de manuele contact *tracing* op te nemen, vermits deze essentieel is. De indiener verwijst naar de toelichting.

Amendement nr. 26 wordt vervolgens aangenomen met 14 stemmen en 3 onthoudingen. Het aldus gewijzigde verzoek 1o wordt vervolgens eenparig aangenomen.

Verzoeken 1p, 1q en 1r

Bij deze verzoeken worden geen opmerkingen gemaakt.

Ze worden eenparig aangenomen.

Demande n° 1s

M. Michael Freilich (N-VA) présente *l'amendement n° 27* (DOC 1182/003) tendant à ce que, dans le contexte européen, le gouvernement privilégie la collaboration au sujet des applications avec les pays voisins qui offrent les mêmes garanties en matière de sécurité des données que celles qui sont poursuivies dans la résolution à l'examen.

L'amendement n° 27 est ensuite adopté par 9 voix contre 6. La demande n° 1s, ainsi modifiée, est adoptée par 15 voix contre 2.

Demande n° 1t

M. Michael Freilich (N-VA) présente *l'amendement n° 28* (DOC 1182/003) tendant à remplacer les mots "avec une date fixe de fin d'utilisation de l'application mobile" par les mots "avec une date de fin d'utilisation de l'application déterminée préalablement ou suffisamment déterminable". L'intervenant renvoie à la justification de son amendement.

L'amendement n° 28 est ensuite adopté par 12 voix et 5 abstentions. La demande 1t, ainsi modifiée, est adoptée à l'unanimité.

Demande n° 1u

Mme Nathalie Gilson (MR) présente *l'amendement n° 11* (DOC 1182/002) tendant à supprimer le traitement de plaintes de la liste des exceptions possibles à la suppression définitive des données. L'auteure renvoie à la justification de son amendement.

L'amendement n° 11 est ensuite adopté par 10 voix contre 2 et 4 abstentions. La demande n° 1u, ainsi modifiée, est adoptée à l'unanimité.

Demande n° 1v

M. Michael Freilich (N-VA) présente *l'amendement n° 29* (DOC 1182/003), qui tend à prévoir que l'audit sollicité dans la demande ne peut avoir lieu que s'il existe des preuves ou des indications suffisantes de problèmes relatifs à de graves atteintes à la protection de la vie privée. L'intervenant renvoie à la justification.

Verzoek 1s

De heer Michael Freilich (N-VA) dient *amendement nr. 27* (DOC 1182/003) in. Dit amendement wil ervoor zorgen dat de regering in Europees verband prioriteit geeft aan samenwerking met de buurlanden rond apps die dezelfde garanties bieden inzake dataveiligheid dan deze die worden nagestreefd in deze resolutie.

Amendement nr. 27 wordt vervolgens aangenomen met 9 tegen 6 stemmen. Het aldus gewijzigde verzoek 1s wordt vervolgens aangenomen met 15 stemmen tegen 2 stemmen.

Verzoek 1t

De heer Michael Freilich (N-VA) dient *amendement nr. 28* (DOC 1182/003) in. Dit strekt ertoe de woorden "vaststaande einddatum" voor het exit-scenario te vervangen door de woorden "vooraf bepaalde of voldoende bepaalbare einddatum". De indiener verwijst naar toelichting bij het amendement.

Amendement nr. 28 wordt vervolgens aangenomen met 12 stemmen en 5 onthoudingen. Het aldus gewijzigde verzoek 1t wordt vervolgens eenparig aangenomen.

Verzoek 1u

Mevrouw Nathalie Gilson (MR) dient *amendement nr. 11* (DOC 1182/002) in. Dit strekt ertoe de klachtbehandeling als mogelijke uitzondering op de onherroepelijke vernietiging van de data te schrappen. De indienster verwijst naar toelichting bij het amendement.

Amendement nr. 11 wordt vervolgens aangenomen met 10 tegen 2 stemmen en 4 onthoudingen. Het aldus gewijzigde verzoek 1u wordt vervolgens eenparig aangenomen.

Verzoek 1v

De heer Michael Freilich (N-VA) dient *amendement nr. 29* (DOC 1182/003) in. Dit strekt ertoe de in het verzoek gevraagde audit enkel te laten doorgaan indien er voldoende bewijzen of aanwijzingen zijn van problemen met betrekking tot grove schendingen op het vlak van privacy. De indiener verwijst naar de toelichting.

L'amendement n° 29 est ensuite rejeté par 13 voix contre 4. La demande 1v, ainsi modifiée, est ensuite adoptée à l'unanimité.

Demande n° 1w *(nouvelle)*

M. Nabil Boukili (PVDA-PTB) présente *l'amendement n° 18* (DOC 1182/003), qui tend à insérer une demande 1w aux termes de laquelle les analyses d'impact relatives à la protection des données des différentes applications examinées sont rendues publiques. L'intervenant renvoie à la justification de l'amendement.

L'amendement n° 18 est ensuite adopté par 14 voix et 3 abstentions.

Demande n° 1x (*nouvelle*)

M. Nabil Boukili (PVDA-PTB) présente *l'amendement n° 19* (DOC 1182/003), qui tend à insérer une demande 1x aux termes de laquelle on part toujours des besoins du secteur des soins de santé pour développer d'éventuelles applications et que ces applications ne seront activées que lorsque tous les moyens humains de détection des contacts (tests, traçage et isolement) auront été mis en œuvre. L'intervenant renvoie à la justification.

L'amendement n° 19 est ensuite rejeté par 11 voix contre 3 et 2 abstentions.

Demande n° 1y (*nouvelle*)

M. Nabil Boukili (PVDA-PTB) présente *l'amendement n° 20* (DOC 1182/003), qui tend à insérer une demande 1y aux termes de laquelle il est explicitement interdit de combiner des données collectées dans le cadre d'une applications avec d'autres données à caractère personnel ou avec d'autres bases de données.

L'amendement n° 20 est ensuite adopté par 11 voix contre 6.

Demande n° 1z (*nouvelle*)

Mme Nathalie Gilson (MR) présente *l'amendement n° 30* (DOC 1182/003), qui tend à insérer une demande 1z aux termes de laquelle les collaborateurs de tiers qui auraient accès à des données recueillies ou enregistrées dans le cadre de l'application sont soumis au secret professionnel comme le prévoit l'article 458 du

Amendement nr. 29 wordt vervolgens verworpen met 13 tegen 4 stemmen. Het aldus gewijzigde verzoek 1v wordt vervolgens eenparig aangenomen

Verzoek 1w *(nieuw)*

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 18* (DOC 1182/003) in. Dit strekt ertoe een nieuw verzoek 1w toe te voegen, luidens hetwelk de gegevensimpactanalyses van de verschillende onderzochte applicaties publiek worden gemaakt. De indiener verwijst naar de toelichting bij het amendement.

Amendement nr. 18 wordt vervolgens aangenomen met 14 stemmen en 3 onthoudingen.

Verzoek 1x *(nieuw)*

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 19* (DOC 1182/003) in. Dit strekt ertoe een nieuw verzoek 1x in te voegen, luidens hetwelk steeds wordt vertrokken vanuit de behoeften van de gezondheidssector bij de ontwikkeling van eventuele apps en die apps slechts mogen worden ingezet nadat alle menselijke middelen voor contactopsporing (testen, traceren en isoleren) werden aangewend. De indiener verwijst naar de toelichting.

Amendement nr. 19 wordt vervolgens verworpen met 11 tegen 3 stemmen en 2 onthoudingen.

Verzoek 1y *(nieuw)*

De heer Nabil Boukili (PVDA-PTB) dient *amendement nr. 20* (DOC 1182/003) in. Dit strekt ertoe een nieuw verzoek 1y toe te voegen, luidens hetwelk expliciet wordt verboden dat gegevens verzameld in het kader van een app worden gecombineerd met andere persoonsgegevens of met andere gegevensbanken.

Amendement nr. 20 wordt vervolgens aangenomen met 11 tegen 6 stemmen.

Verzoek 1z *(nieuw)*

Mevrouw Nathalie Gilson (MR) dient *amendement nr. 30* (DOC 1182/003) in. Dit strekt ertoe een nieuw verzoek 1z toe te voegen, luidens hetwelk de medewerkers van derden, die toegang zouden hebben tot gegevens verzameld of geregistreerd in het kader van de app, worden onderworpen aan het beroepsgeheim

Code pénal et au Règlement général sur la protection des données.

L'auteure renvoie à la justification de l'amendement.

L'amendement n° 30 est ensuite adopté par 9 voix contre 4 et 4 abstentions.

Demande n° 2

Cette demande ne donne lieu à aucune observation.

Elle est adoptée à l'unanimité.

Demande n° 3 (*nouvelle*)

MM. Khalil Aouasti et Christophe Lacroix (PS) présentent *l'amendement n° 1* (DOC 1182/002), qui tend à insérer une demande 3 qui prévoit que s'il estime nécessaire de mettre en œuvre une telle application mobile de suivi, le gouvernement soumet à la Chambre un projet de loi qui encadrerait cette mise en œuvre. Les auteurs renvoient à la justification de l'amendement.

L'amendement n° 1 est rejeté par 9 voix contre 6 et 2 abstentions.

Demande n° 4 (*nouvelle*)

L'amendement n° 7 présenté par Mme Gilson (DOC 1182/002) est retiré.

Demande n° 5 (*nouvelle*)

L'amendement n° 8 présenté par Mme Gilson (DOC 1182/002) est retiré.

Demande n° 6 (*nouvelle*)

L'amendement n° 9 présenté par Mme Gilson (DOC 1182/002) est retiré.

Demande n° 7 (*nouvelle*)

Mme Nathalie Gilson (MR) présente l'*amendement n° 10* (DOC 1182/002), tendant à insérer une demande 6 qui prône un modèle de récolte et de transmission des données assurant une compatibilité et une interopérabilité

zoals voorzien bij artikel 458 van het Strafwetboek en aan de algemene verordening gegevensbescherming.

De indienster verwijst naar de toelichting bij het amendement.

Amendement nr. 30 wordt vervolgens aangenomen met 9 tegen 4 stemmen en 4 onthoudingen.

Verzoek 2

Bij dit verzoek worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Verzoek 3 *(nieuw)*

De heren Khalil Aouasti en Christophe Lacroix (PS) dienen *amendement nr.* 1 (DOC 1182/002) in. Dit amendement voegt een nieuw verzoek 3 in dat bepaalt dat indien de regering de invoering van een *contact tracing app* noodzakelijk acht, zij bij de Kamer van volksvertegenwoordigers een wetsontwerp indient dat de krijtlijnen omtrent de invoering ervan bepaalt. De indieners verwijzen naar de toelichting bij het amendement.

Amendement nr. 1 wordt verworpen met 9 tegen 6 stemmen en 2 onthoudingen.

Verzoek 4 *(nieuw)*

Amendement nr. 7 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken.

Verzoek 5 *(nieuw)*

Amendement nr. 8 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken

Verzoek 6 *(nieuw)*

Amendement nr. 9 van mevrouw Gilson (DOC 1182/002) wordt ingetrokken.

Verzoek 7 *(nieuw)*

Mevrouw Nathalie Gilson (MR) dient *amendement nr. 10* (DOC 1182/002) in. Dit voegt een nieuw verzoek 6 in, waarin wordt gepleit voor een op Europees niveau compatibel en interoperabel model voor dataverzameling

mutuelle au niveau européen afin de restaurer la liberté de circulation au sein de l'Union européenne. L'auteur renvoie à la justification de l'amendement.

L'amendement n° 10 est ensuite adopté par 10 voix et 7 abstentions.

Demande n° 8 (*nouvelle*)

M. Michael Freilich (N-VA) présente l'amendement n° 21 (DOC 1182/003), tendant à insérer une demande au gouvernement fédéral visant à ce que celui-ci dépose à la Chambre des représentants un projet de loi fixant les contours du déploiement d'une telle application mobile de suivi des contacts, s'il juge que sa mise en place est utile. L'auteur renvoie au développement de l'amendement.

L'amendement n° 21 est rejeté par 11 voix contre 6.

Demande n° 9 (*nouvelle*)

M. Michael Freilich (N-VA) présente l'*amendement n° 22* (DOC 1182/003), tendant à insérer une demande visant à veiller à ce que soient désignés des développeurs et des *datacenters* de préférence européens et prioritairement belges lors d'une éventuelle sélection de prestataires de services en vue d'élaborer le suivi des contacts. L'auteur renvoie à la justification de l'amendement.

Mme Barbara Pas (VB) signale que la question-clé dans tous les amendements est de savoir quelles seront les modalités de contrôle et de mise en pratique.

Par ailleurs, si l'on affirme déjà aujourd'hui qu'une application n'est en réalité pas nécessaire ou qu'elle est inutile, il n'est pas nécessaire non plus de créer un cadre juridique.

S'agissant de l'amendement n° 23, l'intervenante indique que les données générées ne peuvent pas être mélangées avec d'autres données. Or, le professeur Elise Degrave a affirmé lors des auditions qu'elle n'avait nullement confiance en une véritable indépendance d'une telle banque de données. Personne n'est en mesure de convaincre l'intervenante du contraire.

Concernant l'amendement n° 22, l'intervenante demande ce que l'on entend par "une entreprise belge": s'agit-il d'une entreprise dont les actionnaires sont établis en Belgique? Ou le siège doit-il se trouver en Belgique?

en -communicatie om aldus de vrijheid van verkeer binnen de Europese Unie te herstellen. De indienster verwijst naar de toelichting bij het amendement.

Amendement nr. 10 wordt vervolgens aangenomen met 10 stemmen en 7 onthoudingen.

Verzoek 8 *(nieuw)*

De heer Michael Freilich (N-VA) dient *amendement nr. 21* (DOC 1182/003) in. Dit voegt een nieuw verzoek in waarin de regering wordt gevraagd om, indien zij de uitvoering van een dergelijke *contact tracing app* nuttig acht, in de Kamer van volksvertegenwoordigers een wetsontwerp in te dienen dat de krijtlijnen omtrent die invoering bepaalt. De indiener verwijst naar toelichting bij het amendement.

Amendement nr. 21 wordt verworpen met 11 tegen 6 stemmen.

Verzoek 9 *(nieuw)*

De heer Michael Freilich (N-VA) dient *amendement nr. 22* (DOC 1182/003) in. Dit voegt een nieuw verzoek in waarbij wordt gevraagd erop toe te zien dat bij een gebeurlijke selectie van dienstverleners voor de uitwerking van de *contact tracing* bij voorkeur Europese, en dan prioritair Belgische, ontwikkelaars en datacenters worden aangeduid. De indiener verwijst naar de toelichting bij het amendement.

Mevrouw Barbara Pas (VB) merkt op dat de hamvraag voor alle amendementen is hoe men dit gaat controleren en in de praktijk brengen.

Verder, als men vandaag al verklaart dat een app eigenlijk niet nodig of niet nuttig is, dan is het ook niet nodig om een juridisch kader te creëren.

Wat amendement nr. 23 betreft, wordt gesteld dat de gegenereerde gegevens niet mogen worden vermengd met andere data maar professor Elise Degrave heeft in de hoorzittingen verklaard dat ze er geen enkel vertrouwen in had dat een dergelijke databank echt onafhankelijk zou zijn; niemand kan de spreekster overtuigen van het tegendeel.

Wat amendement 22 betreft, vraagt zij wat wordt bedoeld met "een Belgisch bedrijf": gaat het om een bedrijf waarvan de aandeelhouders in België zijn gevestigd? Of moet de hoofdzetel zich in België bevinden?

M. Michael Freilich (N-VA) renvoie aux réponses que M. Raes, administrateur général de la Sûreté de l'État, a données lors des auditions. Il ne doit pas absolument s'agir de développeurs flamands: on trouve également des développeurs de qualité ailleurs. On entend que celui qui développe le logiciel habite et travaille en Belgique de manière à ce que la communication soit facile. Il s'agit en réalité d'une entreprise qui est inscrite dans notre pays.

Mme Jessika Soors (Ecolo) fait remarquer qu'il s'agit en fait, en l'occurrence, d'un débat marginal, car ce sont les entités fédérées qui décideront s'il y aura une application et si oui, laquelle.

M. Kris Verduyckt (sp.a) fait remarquer que M. Raes s'est prononcé sur la sécurité des applications concernées: il est évident que la Belgique peut exercer moins de surveillance, par exemple, sur des applications chinoises. Pour le reste, la résolution à l'examen contient de nombreux éléments concrets et contraignants qui correspondent aux avis des experts, comme le caractère volontaire et décentralisé, Bluetooth, le caractère temporaire du stockage des données, le contrôle par l'APD, etc. Par ailleurs, il reste cependant quelques points plus difficiles ou plus vagues.

Mme Barbara Pas (VB) admet que certaines choses sont bel et bien contrôlables, mais les points concernant le respect de la vie privée sont difficilement contrôlables ou ne le sont pas.

L'amendement n° 22 est ensuite adopté par 10 voix contre 3 et 4 abstentions.

*
* *

L'ensemble de la proposition de résolution, telle qu'elle a été modifiée, est ensuite adopté par 12 voix contre 2 et 3 abstentions.

Le résultat du vote nominatif est le suivant:

Ont voté pour:

Ecolo - Groen: Stefaan Van Hecke, Gilles Vanden Burre, Jessika Soors

PS: Christophe Lacroix, Patrick Prévot et Philippe Tison

MR: Benoît Friart, Nathalie Gilson

CD&V: Sammy Mahdi

Open Vld: Kathleen Verhelst

De heer Michael Freilich (N-VA) verwijst naar de antwoorden die het hoofd van de staatsveiligheid, de heer Raes, gegeven heeft tijdens de hoorzittingen. Het hoeft niet per se te gaan om Vlaamse ontwikkelaars: ook elders zijn er goede te vinden. Er wordt bedoeld dat diegene die de software ontwikkelt in België woont en werkt zodat communicatie gemakkelijk is. Eigenlijk gaat het om een bedrijf dat hier is ingeschreven.

Mevrouw Jessika Soors (Ecolo) merkt op dat het hier eigenlijk gaat om een marginaal debat want de deelstaten zullen beslissen of er een app komt en zo ja welke.

De heer Kris Verduyckt (sp.a) merkt op dat de heer Raes zich heeft uitgesproken over de veiligheid van de betrokken apps: het is evident dat België minder toezicht kan uitoefenen op bijvoorbeeld Chinese apps. Deze resolutie bevat verder vele concrete en afdwingbare zaken die overeenstemmen met de adviezen van de experten zoals het vrijwillige en decentrale karakter, bluetooth, het tijdelijk karakter van de gegevensopslag, het toezicht door de GBA enzovoort. Daarnaast zijn er wel enkele moeilijkere of vagere punten.

Mevrouw Barbara Pas (VB) beaamt dat bepaalde zaken wel controleerbaar zijn maar de punten inzake privacy zijn moeilijk of niet te controleren.

Amendement nr. 22 wordt vervolgens aangenomen met 10 tegen 3 stemmen en 4 onthoudingen.

*
* *

Het gehele, aldus gewijzigde voorstel van resolutie, wordt vervolgens aangenomen met 12 tegen 2 stemmen en 3 onthoudingen.

De naamstemming is als volgt:

Hebben voorgestemd:

Ecolo - Groen: Stefaan Van Hecke, Gilles Vanden Burre, Jessika Soors

PS: Christophe Lacroix, Patrick Prévot en Philippe Tison

MR: Benoît Friart, Nathalie Gilson

CD&V: Sammy Mahdi

Open Vld: Kathleen Verhelst

PVDA-PTB: Nabil Boukili

sp.a: Kris Verduyckt

Ont voté contre:

VB: Barbara Pas et Reccino Van Lommel

Se sont abstenus:

N-VA: Anneleen Van Bossuyt, Katrien Houtmeyers et Michael Freilich

Le rapporteur, *Le président,*

Michael FREILICH Stefaan VAN HECKE

PVDA-PTB: Nabil Boukili

sp.a: Kris Verduyckt

Hebben tegengestemd:

VB: Barbara Pas en Reccino Van Lommel

Hebben zich onthouden:

N-VA: Anneleen Van Bossuyt, Katrien Houtmeyers en Michael Freilich

De rapporteur, *De voorzitter,*

Michael FREILICH Stefaan VAN HECKE

ANNEXE: RAPPORT DES AUDITIONS

I. — PROCÉDURE

M. Stefaan Van Hecke, président, donne lecture de l'article 28, 2*bis*, du Règlement de la Chambre[1] et invite les orateurs à entamer leur exposé en répondant aux questions figurant dans cette disposition.

II. — EXPOSÉS INTRODUCTIFS

A. Exposé introductif de M. David Stevens, président de l'Autorité de protection des données (APD)

M. David Stevens (APD) indique qu'il préside l'Autorité de protection des données, laquelle devra rendre un avis sur un éventuel futur arrêté royal (AR) ou loi concernant cette matière. À un stade ultérieur, l'avis de l'APD pourra également être sollicité au sujet de toute analyse d'impact relative à la protection des données effectuée par les autorités publiques. M. Stevens est membre du Comité européen de la protection des données (CEPD). Depuis quelques semaines, l'orateur a également rejoint la *Taskforce* "Data & Technology against Corona", créée par les ministres De Backer et De Block. Abstraction faite de sa rémunération ordinaire, il souligne qu'il n'a pas été rémunéré pour participer à la présente audition.

L'orateur articulera son exposé autour de méprises que l'on entend fréquemment et qu'il souhaite épingler et rectifier.

Une première méprise concerne la confusion de finalités. Pour lutter contre le coronavirus, on peut être appelé à poursuivre différents objectifs: le premier est le traçage, c'est-à-dire le suivi de la localisation de personnes ou d'appareils mobiles afin d'en tirer des connaissances. En Belgique, le traçage sur une durée plus longue n'a encore jamais eu lieu. Le traçage des contacts, c'est-à-dire la cartographie des contacts d'une personne (infectée par le COVID-19 en l'occurrence) afin de repérer des contaminations potentielles, n'a pas davantage encore été mené. Un troisième objectif,

[1] "En cas d'auditions (…), il est demandé aux orateurs de préciser explicitement au début de l'audition:
1° s'ils sont ou ont été associés à quelque autre titre que ce soit à des initiatives relatives à la législation à l'examen, et
2° s'ils sont rémunérés pour leur contribution à l'audition, et le cas échéant, par quelle instance.".

BIJLAGE: VERSLAG VAN DE HOORZITTINGEN

I. — PROCEDURE

De heer Stefaan Van Hecke, voorzitter, geeft lezing van artikel 28, 2*bis*, van het Kamerreglement[1] en nodigt de sprekers uit om hun uiteenzetting aan te vangen met het beantwoorden van de in deze bepaling opgenomen vragen.

II. — INLEIDENDE UITEENZETTINGEN

A. Inleidende uiteenzetting van de heer David Stevens, voorzitter van de Gegevensbeschermingsautoriteit (GBA)

De heer David Stevens (GBA) geeft aan dat hij voorzitter is van de GBA, die een advies zal moeten uitbrengen over een mogelijke toekomstige wet of koninklijk besluit (KB) omtrent deze materie. De GBA kan in een later stadium ook om advies verzocht worden omtrent een eventuele door de overheid uitgevoerde gegevensbeschermingseffectbeoordeling. De heer Stevens is lid van het Europees Comité voor Gegevensbescherming (*European Data Protection Board* of EDPB). Sinds enkele weken is de spreker ook lid van de taskforce "*Data & Technology against Corona*", opgericht door de ministers De Backer en De Block. Afgezien van zijn gewone remuneratie wordt hij niet bezoldigd voor zijn deelname aan deze hoorzitting.

De spreker zal zijn inleidende uiteenzetting benaderen aan de hand van een reeks regelmatig gehoorde misvattingen, die hij wenst te duiden en recht te zetten.

Een eerste misvatting heeft te maken met het vermengen van doelstellingen. Bij de bestrijding van het coronavirus kunnen verschillende doelen worden nagestreefd: een eerste is *tracking*, namelijk het opvolgen van de locatie van personen of mobiele toestellen teneinde daar kennis uit te puren. Tracking over een langere periode is in België nog niet gebeurd. *Contact tracing*, dat is het in kaart brengen van de contacten van een (*in casu* met COVID-19 besmette) persoon teneinde mogelijke besmettingen op te sporen, is evenmin al toegepast. Een derde doelstelling, het genereren van

[1] "Bij hoorzittingen (…) wordt sprekers gevraagd om bij het begin van de hoorzitting duidelijk te vermelden of ze:
1° in een andere hoedanigheid betrokken zijn of geweest zijn bij initiatieven betreffende de voorliggende wetgeving, en
2° betaald worden voor de bijdrage aan de hoorzitting en in voorkomend geval door welke instantie.".

recueillir des informations stratégiques a, quant à lui, été mis en œuvre depuis le début de la crise du coronavirus; ce sont plus particulièrement les données télécom qui sont utilisées pour dresser un profil de mobilité de la population. Sur la base de ces données, des rapports agrégés anonymes sont rédigés, qui permettent de savoir combien d'appareils mobiles ont circulé combien de temps dans une localité dont le code postal diffère de celui de l'utilisateur. Dans le débat public, ces trois objectifs sont souvent confondus, alors qu'ils sont fondamentalement différents.

Parallèlement, la *Taskforce* a encore évalué d'autres éléments parmi lesquels: les informations à la population; l'(auto)triage (outils en ligne permettant à l'utilisateur d'obtenir une indication de la contamination sur la base de symptômes ressentis subjectivement); la téléconsultation (consultation médicale à distance); et enfin, des accessoires connectés (tels que des bracelets qui émettent un signal dès que l'on s'approche trop près d'un autre appareil).

Pour atteindre ces différents objectifs, différents types de technologies sont pertinents (GPS, Bluetooth, données télécoms). Celles-ci sont aussi souvent confondues à tort, et c'est d'emblée la deuxième méprise: la confusion des technologies. Pour tracer des personnes, le GPS est sans doute la technologie la plus adéquate et ce, parce qu'elle permet une localisation beaucoup plus précise que les données télécom (dans des cas d'urgence, la connexion au moyen de trois antennes permet certes une localisation assez précise, mais elle ne peut pas être utilisée à grande échelle). D'un autre côté, les données télécom présentent le grand avantage d'être toujours disponibles pour tous les utilisateurs mobiles. À cela s'ajoute le fait qu'elles ne nécessitent aucune installation au préalable. Dans ces conditions, les données télécom constituent sans doute l'instrument le plus adéquat pour générer anonymement des informations stratégiques déterminées (en matière de mobilité par exemple). La technologie Bluetooth, enfin, a une précision jusqu'à quelques mètres et permet d'enregistrer assez précisément les contacts entre téléphones portables. L'inconvénient, ou la limitation, car suivant l'objectif, il peut également s'agir d'un avantage – est que le Bluetooth n'enregistre que le contact local entre appareils, et non pas le lieu où le contact s'est produit. Si cette dernière information est jugée nécessaire, il faut l'obtenir d'une autre manière (GPS).

La troisième méprise que M. Stevens veut balayer définitivement est que l'application de traçage des contacts serait le remède miracle dans la lutte contre le coronavirus. Il est essentiel de bien cerner la stratégie de sortie et la place qu'occuperait l'application dans ce cadre. Une telle stratégie comprend différentes étapes: tester

beleidsinformatie, wordt wel al geïmplementeerd sinds het begin van de coronacrisis; in het bijzonder worden telecomgegevens gebruikt om een indicator te genereren van het mobiliteitsgedrag van de bevolking. Op basis van telecomgegevens worden anonieme geaggregeerde rapporten opgesteld, die een inzicht geven in hoeveel mobiele toestellen hoelang in een andere postcode zijn geweest. De drie voormelde doelstellingen worden in het publieke debat frequent door elkaar gehaspeld, doch zijn fundamenteel verschillend.

Daarnaast heeft de taskforce nog andere zaken geevalueerd, waaronder: informatie aan de bevolking; (zelf) triage (online tools die de gebruiker toelaten om op basis van subjectief ervaren symptomen een besmettingsindicatie te verkrijgen); *teleconsult* (dokterconsultatie op afstand); en tot *slot wearables* (bijvoorbeeld armbandjes die een signaal geven wanneer men te dicht bij een ander toestel komt).

Voor die verschillende doelstellingen zijn verschillende types van technologieën (gps, bluetooth, telecomgegevens) relevant. Ook die worden, en dat is de tweede misvatting, vaak ten onrechte vermengd. Om mensen te *tracken*, is gps wellicht de meest geschikte technologie, en wel omdat het een veel nauwkeurigere lokalisatie mogelijk maakt dan telecomgegevens (in noodgevallen is via de connectie met drie antennes weliswaar ook een redelijk nauwkeurige lokalisatie mogelijk, doch dit kan niet op grote schaal worden gebruikt). Anderzijds bieden telecomdata het grote voordeel dat ze altijd en voor alle mobiele gebruikers beschikbaar zijn. Daarbij komt dat geen enkele installatie vooraf noodzakelijk is. Gelet op die omstandigheden zijn telecomgegevens wellicht het meest geschikte instrument om anoniem bepaalde beleidsinformatie (bijvoorbeeld inzake mobiliteit) te genereren. bluetooth ten slotte is tot op enkele meters precies en kan vrij accuraat contacten tussen mobiele telefoons registreren. Het nadeel – of de beperking, want afhankelijk van de doelstelling kan dit ook een voordeel zijn – is dat bluetooth enkel lokaal contact tussen toestellen registreert, niet de locatie waar dit plaatsvond. Als die laatste informatie noodzakelijk wordt geacht, moet ze op een andere manier (gps) worden verkregen.

De derde misvatting die de heer Stevens uit de wereld wil helpen is dat de *contact tracing*-app het wondermiddel zou zijn in de strijd tegen het coronavirus. Het is essentieel dat we goed weten wat de exitstrategie is en welke plaats de app daarin zou innemen. Een dergelijke strategie omvat verschillende stappen: het testen

des personnes et rendre compte des contaminations; cartographier les contacts des personnes infectées et les tester; identifier et contacter les personnes infectées; et enfin, conseiller et suivre les contacts. La technologie peut déjà soutenir toutes ces étapes: il est important de délimiter clairement quelle(s) étape(s) l'application doit prendre en charge précisément.

La quatrième méprise est de croire que le PEPP-PT et le DP-3T sont pareils. Le premier (*Pan-European Privacy-Preserving Proximity Tracing*) désigne la variante centralisée, où une seule instance (en l'espèce l'autorité publique) décide de conserver tous les *identifiants* temporaires d'appareils dans une seule base de données centrale. Le DP-3T renvoie à la variante décentralisée, où les informations sont stockées de manière la plus décentralisée possible sur les appareils locaux des utilisateurs finals. Il est évident que sous l'angle de la protection de la vie privée, une base de données centrale comporte beaucoup plus de risques (abus, détournement d'usage ou *function creep*, recyclage) que la variante décentralisée, où les données sont réparties entre des millions d'appareils et ne sont centralisées qu'en cas de nécessité (en l'espèce en cas de contamination). Même les auteurs de la proposition de résolution ne semblent pas tout à fait échapper à cette méprise puisqu'ils préconisent la variante décentralisée, dans la proposition, tout en renvoyant, dans une note, au système PEPP-PT.

La cinquième méprise consiste à prendre le caractère volontaire de l'application pour un consentement. Pour l'APD, il est crucial que la base juridique de l'application ne se fonde pas uniquement sur le consentement. Si tel était le cas, chaque instance ou entreprise s'efforcerait, après la crise, d'obtenir un tel consentement pour proposer un service similaire. Or, ce consentement pourrait ne pas être valable, ce qui pousserait l'APD à intervenir. Une option nettement plus sûre consiste, en revanche, à soutenir le fondement juridique de l'application dans l'intérêt public et donc, à le doter d'une base légale. Cette option est également cohérente avec le fait que l'application, théoriquement du moins, constitue une sérieuse ingérence dans la vie privée.

Il serait erroné de penser – sixième méprise – que l'application de traçage des contacts est une compétence purement fédérale. La proposition de résolution a clairement mis en avant que ce n'est pas le cas. Selon l'orateur, le ministre fédéral compétent n'a jamais eu l'intention de développer l'application seul. La protection de la vie privée constitue incontestablement une compétence fédérale que l'APD est chargée de contrôler.

van mensen en het rapporteren van besmettingen; het in kaart brengen van contacten van besmette personen en het testen van die mensen; het identificeren en contacteren van besmette personen; en ten slotte het adviseren en opvolgen van contacten. De technologie kan al deze stappen ondersteunen; van belang is dat duidelijk wordt afgebakend welke stap(pen) de app precies moet ondersteunen.

Het is een misvatting – de vierde – om te denken dat PEPP-PT hetzelfde is als DP-3T. Het eerste acroniem duidt op de centrale variant, waarbij één instantie (in dit geval de overheid) beslist dat alle tijdelijke *identifiers* van toestellen worden bijgehouden in één centrale databank. DP-3T verwijst naar de decentrale variant, waar de informatie zo veel mogelijk decentraal, op de lokale toestellen van de eindgebruikers, wordt opgeslagen. Het is evident dat, vanuit privacy-oogpunt, een centrale databank veel meer risico's inhoudt (op misbruik, *function creep*, recyclage) dan de decentrale variant, waarbij de data verspreid zitten over miljoenen toestellen en enkel gecentraliseerd worden wanneer dat nodig is (*in casu* bij besmetting). Ook de auteurs van het voorstel van resolutie lijken niet helemaal immuun voor deze misvatting; in het voorstel wordt gepleit voor de decentrale variant, maar wordt tezelfdertijd in een voetnoot verwezen naar PEPP-PT.

De vijfde misvatting houdt in dat het vrijwillig karakter van de app wordt verward met de toestemming. Voor de GBA is het cruciaal dat de juridische basis van de app niet louter gestoeld is op toestemming. Mocht dat het geval zijn, dan zou na de crisis elke instantie of elk bedrijf proberen een dergelijke toestemming te verkrijgen om een gelijkaardige dienst te gaan aanbieden. Die toestemming zal misschien niet geldig zijn, waardoor de GBA daartegen kan optreden. Maar een veel veiliger optie is om de juridische grondslag van de app te schragen in het openbaar belang en dus te voorzien in een wettelijke basis. Dit strookt ook met het feit dat de app, althans theoretisch, een serieuze inmenging in het privéleven vormt.

Het zou fout zijn – misvatting nr. 6 – om te denken dat de *contact tracing*-app een louter federale bevoegdheid is. Uit het voorstel van resolutie komt duidelijk naar voren dat dat niet het geval is. Het is volgens de spreker ook nooit de bedoeling van de bevoegde federale minister geweest om de app alleen uit te bouwen. Privacy is wel ontegensprekelijk een federale bevoegdheid, waarop de GBA toezicht houdt.

Enfin, la dernière méprise est que Google et Apple seraient également en train de développer une application de traçage des contacts. C'est faux; ce qu'elles développent, ce sont des *interfaces de programmation d'application* (API), de manière à ce que les appareils Androïd puissent communiquer avec les appareils Apple et *vice versa*.

M. Stevens évoque ensuite brièvement les activités exercées par l'APD dans le cadre de la crise du nouveau coronavirus. L'APD a publié, dès le 13 mars 2020, une communication relative au traitement des données à caractère personnel sur le lieu de travail. Elle a également élaboré des directives sur l'utilisation des applications concernant la santé et assure la mise à jour d'un dossier thématique concernant le COVID-19 sur son site web.

L'APD a toujours fait preuve de transparence au sujet de son implication dans la *task force* "*Data & Technology against Corona*". Ce groupe de travail est composé de représentants des cabinets des ministres De Backer et De Block et de représentants de la plateforme *eHealth*, de Sciensano, du SPF Santé publique et de l'APD. L'objectif principal poursuivi par l'APD au sein de la *task force* est de tenter d'éviter la commercialisation des applications et des appareils qui portent le plus atteinte à la vie privée. L'APD ne fait rien, à cet égard, qui soit contraire au rôle formel qui lui est assigné; elle rend parfois un avis *a posteriori* ou pointe directement les failles des applications.

L'Union européenne s'est exprimée clairement, dans de nombreux documents et au travers de différentes instances, en faveur d'une application de traçage des contacts fondée sur la technologie Bluetooth et fonctionnant de façon décentralisée sur une base volontaire. La Commission européenne a développé une boîte à outils à cet effet. L'EDPB a quant à lui élaboré des directives qui privilégient également cette piste, tout comme le Contrôleur européen de la protection des données. L'orateur estime d'ailleurs qu'il ne faut pas s'attendre à ce qu'une application unique soit déployée dans toute l'Europe.

B. **Exposé introductif du professeur Bart Preneel, KUL**

Le professeur Bart Preneel est membre du consortium DP3-T, qui est association de coopération informelle entre une dizaine d'universités européennes qui s'efforcent de trouver une solution décentralisée sous la forme d'une recherche de contacts décentralisée dans le cadre de la crise actuelle. Il s'agit d'une coopération volontaire, non rémunérée, informelle et ouverte. Tous les documents, codes, contacts, etc. sont publiquement accessibles; ils sont ouverts aux commentaires qui peuvent être mis

De laatste misvatting tot slot is dat Google en Apple ook een *contact tracing*-app aan het ontwikkelen zijn. Dit is niet zo; wel bouwen zij *application programming interfaces* (API's), om ervoor te zorgen dat Android-toestellen ook met Apple-toestellen zouden kunnen communiceren en *vice versa*.

Vervolgens gaat de heer Stevens kort in op de activiteiten van de GBA met betrekking tot het nieuwe coronavirus. Al op 13 maart 2020 publiceerde de GBA een mededeling over de verwerking van persoonsgegevens op de werkvloer. De Autoriteit heeft voorts richtsnoeren uitgewerkt over het gebruik van gezondheidsapps en houdt ook een themadossier over COVID-19 bij op haar website.

De GBA is steeds transparant geweest over haar betrokkenheid bij de taskforce "*Data & Technology against Corona*". De taskforce is samengesteld uit vertegenwoordigers van de kabinetten van ministers De Backer en De Block, het *eHealth*-platform, Sciensano, de FOD Volksgezondheid en de GBA. De belangrijkste rol van de GBA binnen de taskforce is om te trachten vermijden dat de meest privacy-invasieve apps en toestellen op de markt zouden komen. De GBA doet daar niets wat in strijd is met haar formele rol; soms geeft zij achteraf advies of stelt zij apps rechtstreeks in gebreke.

De EU heeft in tal van documenten en via allerlei instanties een duidelijke voorkeur uitgesproken voor een *contact tracing*-app die gebaseerd is op bluetooth-technologie, decentraal werkt en vrijwillig is. De Europese Commissie heeft een *toolbox* in die zin ontwikkeld. De EDPB van zijn kant heeft richtsnoeren uitgewerkt die ook die voorkeur uitspreken, en de Europese Toezichthouder voor Gegevensbescherming heeft hetzelfde gedaan. De spreker verwacht overigens niet dat er één app zal komen die in heel Europa zal worden uitgerold.

B. **Inleidende uiteenzetting van professor Bart Preneel, KUL**

Professor Bart Preneel is lid van het DP3-T-consortium, een los samenwerkingsverband tussen een tiental Europese universiteiten, die proberen een decentrale oplossing te vinden onder de vorm van decentrale contactopsporing in het kader van de huidige crisis. Het gaat om een vrijwillige, niet vergoede, informele en open samenwerking en alle documenten, codes, contacten en dergelijke zijn publiek toegankelijk; ze zijn opengesteld voor feedback die kan worden opgeladen

en ligne sur le site web[2]. Des discussions transparentes sont menées à ce sujet, également sur le point de savoir si une application est nécessaire ou pas.

La proposition développée par le consortium a été soumise à la *task force*. Plusieurs réunions ont réuni à ce sujet le professeur Preneel et la *task force*.

Le professeur Preneel est également membre du Centre de connaissances de l'APD, mais il est clair qu'il ne sera pas associé aux avis éventuels de l'APD sur le DP-3T. L'orateur précise par ailleurs qu'il est uniquement rémunéré par la KUL.

Introduction

Le suivi des contacts joue un rôle important dans le cadre de l'épidémie actuelle, car les personnes infectées sont contagieuses avant de présenter des symptômes. Il suffit normalement d'isoler les personnes symptomatiques, mais cette solution est inefficace, dans l'épidémie actuelle, car les personnes infectées ont déjà contaminé d'autres personnes avant de développer des symptômes, ce qui explique la courbe exponentielle à laquelle nous sommes confrontés. Les personnes infectées doivent être isolées avant qu'elles soient symptomatiques.

Rechercher les contacts revient à déterminer avec qui une personne contaminée a été en contact: pour que ce système fonctionne, il faut que le nombre d'infections ne soit pas trop élevé et il faut disposer de suffisamment de tests, ainsi que d'une capacité suffisante (par le biais de l'application ou de traceurs de contact en ligne).

La solution actuellement appliquée est le traçage manuel, qui consiste à téléphoner aux personnes et à leur demander avec qui elles ont été en contact. Il s'agit d'une démarche très invasive à l'égard de la vie privée (questions personnelles et intimes), dont le succès dépend en outre de la mémoire de chaque personne interrogées. Par ailleurs, il est parfois impossible de communiquer des informations sur les personnes avec qui on a eu des contacts (il est par exemple impossible de fournir des informations (nom ou autres données) sur les personnes à côté de qui on est assis dans le train ou dans le bus; le traçage manuel est voué à l'échec dans ce cas).

D'où l'intérêt d'un traçage numérique: le projet DP-3T se fonde sur le principe "*privacy by design*" (prise en compte du respect de la vie privée lors de la conception). Il est bien plus rapide que le traçage manuel: la précision du gps (civil, les applications militaires étant beaucoup plus précises) se situe entre trois et six mètres, mais le

[2] *https//github.com/DP-3T/documents*.

op de website[2]. Hierover worden transparante discussies gevoerd, zelfs over het feit of men al dan niet een app nodig heeft.

Het voorstel dat het consortium heeft ontwikkeld werd aangemeld bij de taskforce en professor Preneel heeft hierover enkele keren vergaderd met de taskforce.

Professor Preneel is eveneens lid van het Kenniscentrum van de GBA maar het is duidelijk dat hij niet zal betrokken zijn bij eventuele adviezen van de GBA over DP-3T. Verder wordt hij enkel betaald door de KUL.

Inleiding

Contact tracing is belangrijk in deze epidemie omdat mensen besmettelijk zijn voordat ze symptomen vertonen. Normaal dient men enkel mensen met symptomen te isoleren, maar hiermee komt men in deze epidemie steeds te laat, omdat besmette personen al mensen besmetten vooraleer ze zelf symptomen hebben, waardoor ment tot de gekende exponentiële curve komt. Mensen dienen te worden geïsoleerd vooraleer ze symptomen hebben.

Contactopsporing betekent nagaan met wie een besmet persoon in contact is geweest: om haalbaar te zijn mogen er niet teveel infecties zijn, moet men voldoende testen hebben en moet er voldoende capaciteit zijn in het systeem (via de app of met *online tracers*).

De huidige oplossing is manueel tracen, dit wil zeggen mensen opbellen en vragen met wie ze in contact zijn geweest. Dit is zeer privacy-invasief (persoonlijke en intieme vragen) en beperkt door het geheugen van de ondervraagde en bovendien zijn er een aantal contacten waarover men geen informatie kan geven (als men naast iemand op de trein of bus gezeten heeft kent men niet de naam of andere gegevens van de betrokkene en zal manuele tracing falen).

Vandaar het belang van een digitale tracering: het DP-3T-ontwerp is gebaseerd op *privacy by design* en gaat veel sneller; de nauwkeurigheid van (civiele) gps (militaire applicaties gaan veel verder) bedraagt drie à zes meter, maar gps werkt niet in gebouwen, in tegenstelling tot bluetooth: als men de radio's zou kunnen

[2] *https//github.com/DP-3T/documents*.

gps ne fonctionne pas à l'intérieur des bâtiments, contrairement au Bluetooth: si l'on parviendrait à adapter les radios, le Bluetooth peut offrir une précision de 30 cm. Les applications actuelles ne vont pas aussi loin (on ne peut pas demander à tous les citoyens de modifier la radio Bluetooth dans leur *smartphone*). Elles offrent une précision située entre 50 cm et 1 m, ce qui devrait être suffisant, car la contamination nécessite un contact de 5 à 10-15 minutes. Cette solution n'est bien entendu pas parfaite dès lors que la propagation dépend également des flux d'air et d'autres éléments (un écran de protection en plexiglas empêche par exemple la propagation). Des progrès ont toutefois été réalisés et les experts estiment que le système proposé pourra être suffisamment fiable.

Les deux approches sont complémentaires, notamment parce que certaines personnes ne possèdent pas de smartphone. Elles devront donc être utilisées conjointement pour sortir de la crise.

L'application vise à résoudre un problème très spécifique: avertir les personnes qui se trouvaient à proximité d'une personne infectée et les exhorter à se mettre en quarantaine ou à se faire tester (à titre facultatif, des informations peuvent également être communiquées en vue de promouvoir la recherche épidémiologique).

L'application est fondée sur le principe de la prise en compte du respect de la vie privée lors de la conception: aucune banque de données centrale n'est donc créée. C'est grâce au téléphone que l'on détermine, sur la base des données qu'il contient, si une personne s'est trouvée à proximité d'une personne contaminée, et un minimum d'informations sont centralisées. Cela signifie qu'il n'y a pas non plus de service central susceptible de reconstruire le "graphe social" (qui a été en contact avec qui), les décisions étant prises au niveau local.

Les données ne seront utilisées que pour déterminer qui se trouvait à proximité de la personne infectée. Ce système ne pourra pas être appliqué à d'autres fins car il n'y a pas de données centralisées. Il ne sera pas possible, par exemple, d'identifier les personnes qui ont violé les règles de la quarantaine en se rendant dans leur résidence secondaire.

Le système protège entièrement les identités: on ne sait pas qui a été en contact avec qui, ni où et quand. On sait uniquement qu'il y a eu un risque: c'est ce qu'on appelle la minimisation des données. Par ailleurs, le droit à l'oubli est inhérent au système: des informations sont téléchargées dans une banque de données, mais elles deviennent obsolètes et disparaissent automatiquement après deux à trois semaines ("extinction"). Dès qu'il n'y

aanpassen kan men bij bluetooth tot 30 cm gaan. De huidige applicaties gaan echter niet zover (men kan immers niet iedereen vragen om de bluetooth-radio in zijn smartphone aan te passen) en zitten op een nauwkeurigheid van 50 cm tot 1 meter, wat voldoende zou moeten zijn, omdat voor een overdracht een contact nodig is van 5 tot 10 à 15 minuten. Dit is natuurlijk niet perfect want de propagatie hangt ook af van de luchtstroom en van andere elementen (een plexischerm bijvoorbeeld verhindert propagatie). Er is wel vooruitgang geboekt en de experten denken dat het voldoende betrouwbaar kan worden gemaakt.

Beide aanpakken zijn complementair onder andere omdat sommige mensen geen smartphone hebben; beide zullen samen nodig zijn om uit de crisis te geraken.

De app wil dus een heel specifiek probleem oplossen: mensen die in de nabijheid zijn geweest van een besmet persoon waarschuwen en aanmoedigen om in quarantaine te gaan of zich te laten testen (facultatief kan ook informatie worden aangeboden voor epidemiologisch onderzoek).

De applicatie is gebaseerd op het principe van *privacy by design*: er wordt dus geen centrale database opgebouwd. De beslissing of men in de buurt van een besmet persoon is geweest wordt genomen op zijn telefoon, op basis van gegevens op die telefoon en er is minimale centrale informatie. Dat betekent dat er ook geen centrale dienst is die de "sociale graaf" (wie met wie in contact is geweest) kan reconstrueren. Beslissingen worden lokaal genomen.

Data worden enkel gebruikt om nabijheid te detecteren; men kan dit systeem niet gebruiken voor andere doeleinden want er zijn geen centrale data, men kan dus bijvoorbeeld niet nagaan wie de quarantaineregels heeft verbroken en naar zijn tweede verblijf is gegaan.

Het systeem beschermt volledig de identiteiten: men weet niet met wie men in contact is geweest, noch waar en wanneer, enkel dat er een risico is geweest: dit noemt men dataminimalisatie. Daarnaast is het "recht om vergeten te worden" inherent geïmplementeerd: er wordt informatie opgeladen in een database maar na twee à drie weken is deze informatie verouderd en verdwijnt ze automatisch ("dooft uit"). Zodra er geen nieuwe besmettingen meer

aura plus de nouvelles contaminations, plus aucune nouvelle information ne sera enregistrée et le système s'éteindra de lui-même.

En ce qui concerne la sécurité du système, l'orateur précise qu'il permet d'éviter les signalements faux ou incorrects (il n'est donc pas possible de signaler soi-même une contamination). Ce système ne pourra être activé que sous contrôle médical ou après la réalisation d'un test.

La précision joue également un rôle fondamental car il faut éliminer les faux négatifs et les faux positifs: croiser une personne dans la rue ne peut pas être considéré comme un contact; le système doit pouvoir être appliqué à plus de 10 millions voire à plus de 100 millions d'utilisateurs (à l'échelle européenne) et déployé d'ici quelques semaines (après six semaines de recherche; il n'est pas nécessaire de développer de nouvelles technologies ou de distribuer de nouveaux appareils). Ce système fonctionnera en outre sur une base volontaire et l'orateur espère qu'il sera interopérable au niveau européen.

Comment le système fonctionne-t-il? (Exposé simplifié)

L'utilisateur doit d'abord installer l'application (il doit s'agir de l'application correcte, ce qui est garanti par *Google Play* ou par l'*App Store*). Cette application va créer une clé uniquement connue dans le cadre de l'application. Cette clé va générer des codes (plusieurs centaines) aléatoires qui seront envoyés sans nom ni identification. L'application ne sait pas qui est l'utilisateur et elle ne dispose d'aucun renseignement à son sujet.

Le processus se déroule ensuite comme suit: lorsque l'individu sort avec son téléphone, l'application envoie ces codes en Bluetooth. Le même code est envoyé chaque seconde pendant environ 15 minutes. Il est ensuite modifié. Il est donc impossible de suivre une personne sur la base de ces codes, puisqu'ils sont modifiés toutes les 15 minutes.

L'application reçoit également des codes d'autres utilisateurs proches qui sont conservés dans l'application, ainsi qu'un créneau horaire (approximatif) concernant une partie de la journée ou une journée donnée.

Si une personne présente des symptômes, elle consultera, en principe, un médecin. Il y aura alors une interaction avec Sciensano: dès lors, un lien sera établi avec le système médical: le numéro NISS sera utilisé à cette fin et le numéro de téléphone sera également saisi pour pouvoir contacter la personne ultérieurement. S'il est établi que le test est positif et que la personne est effectivement contaminée, elle recevra un code dans son application et ce code sera utilisé pour télécharger sa clé

zijn, wordt geen nieuwe informatie meer opgeladen en het systeem zal uit zichzelf uitsterven.

Qua veiligheidseigenschappen wordt valse of incorrecte rapportering van besmettingen vermeden (zelf-rapportering is dus niet mogelijk). Enkel met medisch toezicht of na een test kan het systeem worden geactiveerd.

Nauwkeurigheid is ook heel belangrijk om valse negatieve of valse positieven te verwijderen: elkaar kruisen in de straat mag niet beschouwd worden als een contact; het systeem moet schaalbaar zijn naar meer dan 10 of zelfs meer dan 100 miljoen gebruikers (Europese schaal), en kan worden uitgerold binnen een paar weken vanaf nu (na zes weken onderzoek, er moeten geen nieuwe technologieën worden ontwikkeld of nieuwe toestellen worden verdeeld). Bovendien is het een vrijwillig systeem en hopelijk interoperabel op Europees niveau.

Hoe werkt het systeem? (Vereenvoudigde uitleg)

Men gaat eerst als gebruiker de app installeren (de juiste app, wat wordt gegarandeerd door *Google Play* of de *App Store*). Deze app zal dan een sleutel aanmaken die enkel binnen deze app bekend is. Met deze sleutel worden codes gegenereerd (enkele honderden); dit zijn willekeurige codes die worden uitgestuurd, zonder naam of identificatie. De app weet niet wie de gebruiker is en heeft geen gegevens over hem.

Wat er dan gebeurt, is het volgende: als men buiten komt met zijn telefoon zal die app die codes in bluetooth uitsturen. Dezelfde code blijft elke seconde gedurende ongeveer 15 minuten uitgestuurd worden en dan verandert de code. Op basis van deze codes kan men mensen dus niet volgen want ze worden elke 15 minuten aangepast.

Wat de app ook doet is codes ontvangen van andere gebruikers in de buurt die worden bijgehouden in de app, evenals een (ruw) tijdslot, in de orde van een dagdeel of een dag.

Stel dat iemand symptomen krijgt, dan zal die in principe een arts bezoeken; dan komt er een interactie met Sciensano: op dat moment wordt er een link gelegd met het medisch systeem: hiervoor wordt het INSZ-nummer gebruikt en ook het telefoonnummer wordt ingegeven om de persoon achteraf te kunnen contacteren. Als er vastgesteld wordt dat de test positief is en de persoon inderdaad besmet is, dan krijgt hij een code in zijn app en zal hij met die code zijn geheime sleutel in de centrale

secrète dans la base de données centrale. Cela signifie que ce code qui était secret deviendra soudainement public, mais aucun nom n'y sera associé, seulement une date (celle de la contamination). Dès lors, l'application créera une nouvelle clé et la clé précédente ne sera plus utilisée pour créer de nouveaux codes. Cela signifie que l'application ne pourra plus être utilisée pour ensuite vérifier si une personne contagieuse continue néanmoins de se déplacer. Ce n'est pas l'objectif poursuivi par l'application et d'autres méthodes sont nécessaires à cette fin.

Dernière étape: toutes les autres applications vont se connecter à la base de données et télécharger la clé dans l'application. Il s'agit donc du code d'une personne infectée dont on ne connait pas l'identité: elle va alors déterminer si la clé de la personne infectée correspond à l'un des codes que l'on a reçus. Une analyse sera ensuite effectuée par l'application – entièrement localement – afin de déterminer si l'utilisateur court un risque (d'autres éléments étant également pris en compte, tels que la distance et la durée du contact). En cas de risque, l'utilisateur recevra une indication et les étapes suivantes dépendront de ce que la *Taskforce* ou Sciensano décidera. Par exemple, la personne pourra être invitée à rester chez elle, à appeler un certain numéro, à se faire tester ou à entrer son numéro au *contact tracing center*. Cela ne relève pas du champ d'application du protocole DP-3T et pourra varier d'un pays à l'autre et d'une phase à l'autre de l'épidémie.

En ce qui concerne l'interaction avec le médecin, celui-ci recevra le numéro NISS (indispensable pour être soigné en Belgique) et le numéro de téléphone, et une interaction sera établie au moyen d'un code sur l'écran du médecin et d'un code sur l'écran de l'application. Ensuite, les tests seront effectués: s'ils sont positifs, l'application sera contactée; l'utilisateur recevra un code par sms et pourra ainsi télécharger la clé dans la banque de données centrale (ce qui empêchera de télécharger de fausses notifications).

Une autre composante est aussi entièrement optionnelle: l'utilisateur peut décider de collaborer à des enquêtes épidémiologiques, auquel cas des informations codées sont envoyées, une fois par jour, à une banque de données qui conserve les données suivantes: infection éventuelle de l'individu, contacts infectés rencontrés (sans mention des noms, seule une clé étant enregistrée: pseudonyme, l'identité de la personne n'est pas connue), durée des contacts et chronologie par rapport au moment de la contamination. Ces informations permettent aux épidémiologistes de déterminer comment l'épidémie se propage mais sans disposer de données de localisation

database opladen. Dit betekent dat de code die geheim was nu plots publiek wordt, maar daar staat geen naam bij, enkel een datum (van de besmetting). Op dat moment zal de app een nieuwe sleutel aanmaken en wordt de huidige sleutel niet meer gebruikt om nieuwe codes aan te maken. Dat betekent dat de app niet meer kan gebruikt worden om achteraf na te gaan of iemand die besmettelijk is toch nog rondloopt. Dat is niet het doel van de app en daarvoor zijn andere methoden nodig.

De laatste stap: alle andere apps gaan met de database connecteren en gaan die sleutel in de app downloaden. Het gaat dus om de code van een besmet persoon maar men weet niet wie het is: men gaat dan kijken of de sleutel van de besmette persoon past op één van de codes die men ontvangen heeft. In de app gebeurt dan – volledig lokaal – een analyse of de gebruiker een risico loopt (waarbij ook andere elementen meespelen, zoals afstand en duurtijd van het contact). Als er een risico is krijgt de gebruiker een indicatie en de volgende stappen hangen dan af van wat de taskforce of Sciensano hierover beslist. De persoon kan bijvoorbeeld worden gevraagd om thuis te blijven of om een bepaald nummer te bellen of om zich te laten testen of nog om zijn nummer in te geven bij het *contact tracing center*. Dit valt buiten het bereik van DP-3T en kan per land en ook per fase van de epidemie verschillen.

Wat de interactie met de arts aangaat, deze krijgt het INSZ-nummer (anders krijgt men geen behandeling in België) en het telefoonnummer en er wordt een interactie gerund waarbij gekeken wordt met een code op het scherm van de arts en een code op het scherm van de app. Dan gebeuren de testen: als deze positief zijn, zal contact worden genomen met de app; de gebruiker krijgt een code via sms en daarmee kan de gebruiker de sleutel opladen in de centrale database (zo kan men geen valse meldingen opladen).

Er is ook nog een andere volledig optionele component: men kan als gebruiker beslissen om mee te werken aan epidemiologisch onderzoek waarbij één keer per dag gecodeerde informatie wordt verstuurd aan een database, die bijhoudt of men besmet is of niet, welke besmette contacten men heeft gezien (zonder vermelding van namen, enkel een sleutel: dit is een pseudoniem, men weet niet wie dit is;) wat de duur is van de contacten en het tijdstip ten opzichte van het moment van de besmetting. Deze informatie laat epidemiologen toe na te gaan hoe de epidemie zich voortplant, maar zonder lokalisatiegegevens (bijvoorbeeld die school of

(par exemple dans telle école ou tel supermarché). Les pays peuvent choisir de proposer cette option ou non. Il en va de même pour les utilisateurs.

Il y a donc trois banques de données dans le système: premièrement la banque de données DP-3T qui ne contient que les clés et les données chronologiques: elle est anonyme et n'est pas soumise à la réglementation médicale (selon les experts juridiques). Cette banque de données peut également servir pour l'interopérabilité. En d'autres termes, elle peut dialoguer avec d'autres banques de données d'autres pays: actuellement, de nombreux pays européens adoptent cette solution et peuvent échanger ces clés: par exemple, lorsqu'un utilisateur de l'application suisse se rend en Autriche (ces deux pays appliquant cette solution), cet utilisateur peut ensuite télécharger les clés autrichiennes sur son application. Il ne s'agit pas de données sensibles car ces clés ne contiennent aucune information sur les personnes ou les lieux. Cela ne représente pas non plus beaucoup de données: on estime qu'il s'agit de quelques mégaoctets par pays et par jour.

Il existe par ailleurs une banque de données Sciensano (infrastructure distincte) qui conserve – temporairement – un numéro de GSM. Dès que la personne a été prévenue, ce numéro peut être effacé rapidement. Le numéro n'est pas lié à une clé et Sciensano ne dispose donc jamais de cette clé. Il est important que ces deux banques de données fassent l'objet d'une gestion distincte.

La troisième et dernière banque de données est, comme indiqué antérieurement, la banque de données épidémiologiques.

Points supplémentaires

Pour que l'application soit efficace, certains estiment que sa pénétration doit atteindre 60 % avant sa mise en service. La réponse scientifique est que nous n'en savons rien. L'orateur pense qu'elle peut fonctionner à partir d'un taux de pénétration de 15 à 20 % (si, par exemple, 80 % des étudiants utilisent l'application, bien qu'il soit évidemment souhaitable d'augmenter ce taux). Beaucoup de choses dépendent des modèles, qui donnent tous des résultats différents.

Le professeur Preneel pense que le système est suffisamment précis. Il fonctionne au niveau international et bénéficie du soutien de Google et d'Apple.

Il est vrai qu'en principe, aucune de ces applications fonctionne convenablement via le Bluetooth sur les iPhones car, pour des raisons de respect de la vie privée, les iPhones interdisent l'envoi d'informations en utilisant le Bluetooth en arrière-plan, si l'application n'est pas

die supermarkt). Landen kunnen kiezen om dit al dan niet te implementeren; hetzelfde geldt voor gebruikers.

Er zijn dus drie databases in het systeem: ten eerste is er de DP-3T-database die gewoon de sleutels en tijdstippen bevat: deze is anoniem en niet onderworpen aan medische regulering (aldus de juridische experten). Deze databank kan ook werken voor interoperabiliteit, met andere woorden ze kan praten met databases in andere landen: momenteel wordt in heel wat Europese landen deze oplossing gekozen en men kan dan deze sleutels uitwisselen: als bijvoorbeeld een gebruiker van de Zwitserse app naar Oostenrijk gaat (deze beide landen zijn dit aan het implementeren), kan die achteraf de sleutels van Oostenrijk op zijn app downloaden. Dit is niet gevoelig want deze sleutels bevatten geen informatie over personen of locaties. Het gaat ook niet over veel data: naar schatting gaat het over enkele megabytes per land en per dag.

Daarnaast is er een database Sciensano (gescheiden infrastructuur): daarin wordt – tijdelijk – een gsm-nummer opgeslagen. Nadat de persoon gewaarschuwd is kan dat nummer snel worden vernietigd. Het nummer is niet gekoppeld aan een sleutel en Sciensano krijgt zulke sleutel dus nooit te zien. Het is belangrijk dat de twee voormelde databases onder afzonderlijk beheer staan.

De derde en laatste database is zoals vermeld de epidemiologische.

Bijkomende punten

Voor effectiviteit is volgens sommigen 60 % penetratie van de app nodig vooraleer hij zou werken: het wetenschappelijk antwoord is dat we het niet weten: de spreker denkt dat het kan werken vanaf 15 tot 20 % (als bijvoorbeeld 80 % van de studenten de app zou gebruiken, hoewel meer uiteraard wenselijk is). Veel hangt af van de modellen die alle verschillende resultaten geven.

Professor Preneel denkt dat het systeem voldoende nauwkeurig is, het werkt internationaal, en er is steun van Google en Apple.

Het is wel zo dat in principe geen enkele van deze apps via bluetooth naar behoren werkt op iPhones, omdat om privacyredenen iPhones verbieden dat men informatie zou sturen over bluetooth "*in the background*", als de app niet aanstaat. Het werkt dus enkel als de app

ouverte. Cela ne fonctionne donc que si l'application est à l'avant-plan et tant que le téléphone n'est pas verrouillé. Se promener constamment avec un iPhone ainsi paramétré n'est cependant pas sans danger et vide rapidement la batterie. Apple a proposé de résoudre ce problème et Google coopère également pour améliorer l'interface avec le Bluetooth. Ils proposent une solution et la DP-3T se concerte étroitement avec leurs équipes de développement. Ils refusent d'ailleurs de soutenir toute solution non décentralisée. Une discussion est actuellement en cours entre la France, l'Allemagne et le Royaume-Uni, qui ont tous des solutions centralisées, l'Allemagne étant toutefois passée à une solution décentralisée le week-end dernier.

Ce n'est pas un système parfait, mais sa conception offre des garanties maximales de respect de la vie privée et une protection maximale contre l'utilisation abusive d'une base de données centrale.

C. **Exposé introductif de M. Jaak Raes, administrateur général de la Sûreté de l'État (VSSE)**

M. Jaak Raes (VSSE) répond par la négative aux questions énoncées à l'article 28, 2*bis*, du Règlement de la Chambre.

Contexte juridique

L'orateur entend commencer par aborder le cadre juridique, en particulier la question des mécanismes de contrôle, pour ce qui concerne les applications de traçage des contacts.

La mission de la VSSE est de collecter, d'analyser et de traiter les renseignements relatifs à toute activité qui menace ou pourrait menacer la sûreté de la Belgique. Dans le cadre de cette mission, la VSSE peut utiliser des méthodes de renseignement, telles que la collecte de données de communications électroniques. La VSSE ne peut toutefois pas procéder comme bon lui semble. Tant la conservation de ces données par les opérateurs de communications électroniques que l'accès à ces données par la VSSE sont strictement réglementés par la loi.

La conservation des données de communications électroniques est réglée par la loi du 13 juin 2005 relative aux communications électroniques. Cette loi détermine quelles données doivent être conservées par les opérateurs, les conditions de conservation de ces données, quelles autorités ont accès à ces données et à quelles fins ces données peuvent être utilisées. Cette loi dispose notamment que les opérateurs doivent conserver les données de trafic et de localisation – qui

"*in the foreground*" staat en de telefoon niet "gelocked" is. Het is echter heel onveilig en batterijslurpend om constant zo met zijn iPhone rond te lopen. Apple heeft aangeboden om dit probleem op te lossen en ook Google werkt mee om de interface met bluetooth te verbeteren. Zij stellen een oplossing voor en DP-3T staat in nauw overleg met hun ontwikkelteams; zij weigeren trouwens een oplossing te ondersteunen die niet decentraal is. Er is nu een discussie bezig tussen Frankrijk, Duitsland en het Verenigd Koninkrijk, die alle centrale oplossingen hebben; Duitsland is echter vorig weekend overstag gegaan naar een decentrale oplossing.

Dit is geen perfect systeem maar het ontwerp biedt maximale privacygaranties met maximale bescherming tegen het misbruik van een centrale database.

C. **Inleidende uiteenzetting van de heer Jaak Raes, administrateur-generaal van de Veiligheid van de Staat (VSSE)**

De heer Jaak Raes (VSSE) beantwoordt de in artikel 28, 2*bis*, van het Kamerreglement opgenomen vragen ontkennend.

Juridische achtergrond

De spreker gaat vooreerst in op het juridische kader, en meer specifiek op de controlemechanismen, inzake *contact tracing*-apps.

De VSSE 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

sont les données relatives à la communication – et que les services de renseignement et de sécurité peuvent demander ces données dans le cadre de leurs missions de renseignement.

Un arrêté royal pris en exécution de la loi relative aux communications électroniques précise à son tour les catégories de données que les opérateurs doivent conserver, comme les données personnelles de l'utilisateur final, la date et l'heure exacte du début et de la fin de l'appel, les données de localisation, etc.

Si la VSSE souhaite, dans le cadre de ses missions de renseignement, accéder à ces données conservées par les opérateurs, elle doit respecter toute une série de conditions. L'accès à ces données est réglé par la loi organique des services de renseignement et de sécurité du 30 novembre 1998 ainsi que par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (communément appelée loi MRD ou BIM).

D'abord, la VVSE doit respecter les principes de subsidiarité et de proportionnalité. Les données de localisation et de trafic ne peuvent être demandées que si des méthodes portant moins atteinte à la vie privée sont insuffisantes pour recueillir les informations nécessaires à l'accomplissement des missions de renseignement. Par ailleurs, la demande de ces données ne doit pas être disproportionnée au regard de la gravité de la menace potentielle sur laquelle la VVSE enquête.

La législation prévoit en outre un contrôle approfondi. En sa qualité d'administrateur général de la VVSE, M. Raes prend toujours des décisions écrites et motivées pour permettre l'application de la méthode de recueil d'informations. Ces décisions doivent d'abord être notifiées à une commission spécifique composée de trois magistrats, la commission BIM, avant que la méthode de recueil d'informations puisse être appliquée. La VSSE doit convaincre cette commission que les informations qu'elle souhaite obtenir ne peuvent pas être obtenues d'une autre manière et que la mesure est proportionnée au regard du risque potentiel.

La VVSE doit mettre fin à l'application de la méthode de recueil d'informations dès que la menace potentielle a disparu, que la méthode n'est plus utile ou qu'une illégalité est constatée. La commission BIM et le Comité permanent R peuvent également suspendre et/ou interrompre l'application de la méthode de recueil d'informations lorsque les conditions légales ne sont plus remplies ou qu'une illégalité est constatée. Il peut aussi être décidé de détruire les données déjà recueillies.

– 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 gespecificeerd 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, enzovoort.

Indien de VSSE – in het kader van haar inlichtingenopdracht – toegang wil tot deze gegevens die worden bewaard door operatoren, moet er worden voldaan 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 alsook door de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (gemeenzaam de BIM-wet genoemd).

Vooreerst moeten de principes van subsidiariteit en proportionaliteit worden nageleefd. De lokalisatie- en verkeersgegevens kunnen enkel worden gevorderd indien minder privacy-invasieve 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 VSSE onderzoek voert.

Daarnaast wordt er voorzien in een ruime controle. Als diensthoofd van de VSSE neemt de heer Raes 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. De VSSE zal deze commissie ervan moeten overtuigen dat de informatie die ze graag wenst te krijgen, op geen enkele andere manier kan worden verkregen, en dat de maatregel proportioneel is in het licht van het mogelijke risico.

De VSSE 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 al verzamelde gegevens.

Enfin, la législation dispose que les données recueillies par la VSSE ne peuvent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles ont été recueillies.

En raison de ce contrôle, il arrive dans certains cas que des méthodes importantes soient appliquées tardivement ou ne le soient pas du tout pour des raisons de procédure. Cependant, la VSSE est convaincue de l'importance fondamentale de ces contrôles, qui servent à protéger nos droits et libertés démocratiques.

Par conséquent, si l'on décide de développer une application pour lutter contre le COVID-19, la VSSE propose d'élaborer un cadre juridique offrant des garanties similaires à celles offertes par la loi relative aux communications électroniques et par la loi organique des services de renseignement et de sécurité. Ce cadre devra déterminer clairement quelles données pourront être conservées, dans quelles conditions elles devront l'être, qui pourra y accéder (et dans quelles conditions) et à quelles fins elles pourront être utilisées. Enfin, il conviendra de prévoir également un contrôle approfondi du traitement de ces données.

Risques liés à l'introduction d'une application de traçage des contacts

M. Raes examine ensuite les risques potentiels liés à l'introduction d'une application de traçage des contacts du point de vue d'un service de renseignement civil.

L'ampleur d'un risque est déterminée par la menace, d'une part, et la vulnérabilité, d'autre part. Le premier aspect concerne l'espionnage ou l'ingérence des services de renseignement étrangers. Il est important, à cet égard, de tenir compte de leur capacité et de leur éventuelle intention de nuire à notre pays. Force est par exemple de constater que certains pays mènent une politique offensive qui leur permet de s'adonner à l'espionnage technique à grande échelle sur leur territoire et à l'étranger.

Il n'est donc nullement exclu que des pays avec lesquels nous entretenons des liens d'amitié moins forts tenteront d'exploiter les faiblesses inhérentes aux applications de cette nature. Ce sera tout particulièrement le cas si ces applications sont déployées à grande échelle dans la société, y compris parmi des personnes disposant d'un accès à des informations sensibles.

Si l'objectif est d'utiliser une application de cette nature, de nombreux acteurs et la VSSE plaident pour que son développement soit confié à une entreprise

Tot slot wordt bepaald dat de gegevens verzameld door de VSSE 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. De VSSE is echter overtuigd van het algemeen belang van deze controles, die de democratisch rechten en vrijheden dienen.

Indien er dus beslist wordt tot ontwikkeling van een app ter bestrijding van het coronavirus COVID-19, stelt de VSSE 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 en waarvoor de gegevens mogen worden gebruikt. Tot slot dient ook voorzien in een ruime controle op de verwerking van deze gegevens.

Risico's van de introductie van een contact tracing-app

Vervolgens besteedt de heer Raes aandacht aan de mogelijke risico's die verbonden zijn aan het introduceren van een *contact tracing*-app, en dit vanuit het perspectief van een burgerlijke inlichtingendienst.

Een risico wordt bepaald door de dreiging enerzijds, en de kwetsbaarheid anderzijds. Het eerste aspect situeert zich op het vlak van spionage of inmenging door buitenlandse inlichtingendiensten. Daarbij moet men oog hebben voor hun capaciteit en hun eventuele intentie om ons land te schaden. Zo mag men er niet blind voor zijn dat bepaalde landen een offensief beleid voeren dat hen in staat stelt om op grote schaal aan technische spionage te doen in binnen- en buitenland.

Het valt dan ook geenszins uit te sluiten dat 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 de VSSE, pleiten ervoor om, indien men een app zou willen hanteren, te kiezen voor een Belgisch bedrijf. Maar wat is een Belgisch

belge. Mais qu'entend-t-on par "entreprise belge"? Les actionnaires devront-ils tous être belges? Cette entreprise ne pourra-t-elle donc pas être rachetée? Les dirigeants ou les développeurs de cette entreprise pourront-ils être d'une autre nationalité?

Le choix éventuel d'un développeur belge signifie également qu'il faudra encore définir des critères stricts que ce développeur devra respecter. Le cas échéant, la VSSE plaide d'ores et déjà pour que le choix se porte sur un développeur belge qui travaille avec un système fonctionnant entièrement sur l'infrastructure présente en Belgique (serveurs, centre de données, réseaux, …).

Des puissances étrangères ne seront évidemment pas les seules à s'intéresser aux données et aux possibilités d'interférence offertes par les applications de traçage des contacts. À cet égard, il faut également tenir compte de la menace émanant d'acteurs non étatiques animés par d'autres motivations. Par exemple, certains groupes qui souhaitent commettre des crimes ne seront que trop heureux de savoir si des téléphones portables sont à proximité de l'endroit où ils veulent frapper. Cette technologie offre aux acteurs non étatiques, qui recourent aujourd'hui déjà au piratage informatique, des possibilités inédites de suivre des entreprises et des particuliers, de les soumettre à des pressions et de les faire éventuellement chanter, etc.

Il ne faut pas oublier à cet égard qu'outre les groupes criminels, il existe aussi des organisations ayant un agenda extrémiste ou d'une autre nature qui peuvent également utiliser cette technologie pour surveiller leurs partisans ou pour tenir leurs opposants à distance.

Afin de contrer les menaces, en particulier celles émanant des puissances étrangères, il est nécessaire de disposer d'une politique de sécurité offensive, axée sur la réduction des capacités des services de sécurité étrangers. Toutefois, la Belgique ne dispose actuellement pas des mêmes capacités que des puissances étrangères ou des acteurs non étatiques. Notre principale préoccupation devra donc surtout être de réduire au maximum notre vulnérabilité.

Ces failles sont liées à la technologie et il est dès lors difficile de se prononcer au sujet des applications dont la VSSE n'a pas pu étudier tous les paramètres. On peut cependant affirmer à titre général que ces paramètres sont similaires à ceux d'autres applications, par exemple des applications qui permettent de réaliser des vidéoconférences. Le logiciel peut dès lors présenter des failles techniques.

Des failles peuvent également être présentes au niveau de l'infrastructure. Que se passera-t-il si l'entreprise qui

bedrijf? Moeten de aandeelhouders allemaal Belgisch zijn? Mag een dergelijk bedrijf dan niet overgenomen worden? Mogen directieleden of ontwikkelaars van een andere nationaliteit zijn?

Ook een eventuele keuze voor een Belgische ontwikkelaar betekent dat er nog steeds strikte criteria moeten worden uitgewerkt waaraan de ontwikkelaar dient te voldoen. De VSSE pleit 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, …).

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. In dit verband moet men ook rekening 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 mag men 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.

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 uitspraken te doen met betrekking tot de apps waarvan de VSSE niet alle informatie heeft kunnen bestuderen in een korte tijdsspanne. Algemeen kan wel gesteld worden dat deze gelijk lopen met die van andere applicaties, zoals degene waarmee aan videoconferenties wordt gedaan. Zo kunnen er technische kwetsbaarheden in de software zitten.

Kwetsbaarheden kunnen zich ook situeren in de infrastructuur. Wat indien het bedrijf achter de app plots

a développé l'application est soudainement rachetée par une entreprise étrangère (nationale ou non)? Qui est propriétaire des données stockées sur des serveurs situés à l'étranger par le biais d'une application?

S'agissant des solutions commerciales, il faut en tout cas tenir compte du cadre légal du pays d'origine de l'application de suivi des contacts. En effet, dans certains pays, la collaboration (obligatoire) entre les entreprises et les services nationaux de sécurité est envisageable.

Quelles formes de risques le déploiement d'applications de ce type peut-il présenter? Premièrement, elles présentent un risque d'espionnage, à savoir d'extraction de données (concernant par exemple l'identité, les déplacements et les contacts d'une personne ou d'un groupe de personnes). Une stratégie de sortie de la crise du COVID-19 qui dépendrait de ce type d'applications présenterait également un risque de sabotage ou d'intégrité du système. Dans un cadre plus large, des attaques menées par le biais de cette technologie pourraient être intégrées dans une attaque hybride plus vaste.

Notions techniques

Le troisième volet de l'exposé inclut quelques réserves techniques que M. Raes passe rapidement en revue eu égard à l'exposé introductif de l'orateur précédent.

L'orateur renvoie à un article très récent du Néerlandais Jaap Haartsen, qui inventa la technologie Bluetooth à la demande d'Ericsson dans les années 90. M. Haartsen a vivement critiqué l'approche néerlandaise de l'application de suivi des contacts qui, selon lui, avait les allures d'un cirque médiatique. L'orateur se réjouit dès lors qu'un appel à une certaine retenue ait été lancé dans la presse belge à cet égard et appelle à poursuivre, avec discrétion, les travaux concernant l'application de suivi des contacts dans le cadre de la crise du coronavirus. M. Haartsen estime d'ailleurs aussi que le Bluetooth ne permet pas de localiser avec suffisamment de précision et risque dès lors de générer beaucoup de faux positifs.

M. Raes conclut en constatant que les possibilités et les options sont nombreuses mais qu'il n'existe jusqu'à présent aucune application qui combine les différentes composantes nécessaires, une localisation précise, une identification unique par utilisateur, un recueil d'informations contextuelles et une couverture suffisante.

Il signale en outre que la VSSE s'emploie également à répertorier toutes sortes de tentatives de désinformation et la diffusion de nouvelles mensongères dans le cadre de la crise du coronavirus.

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 worden gehouden met het wettelijk kader in het land van oorsprong van de *contact tracing*-app. In bepaalde landen is er immers de mogelijkheid tot een (verplichte) samenwerking tussen bedrijven en hun nationale veiligheidsdiensten.

Welke soorten risico's kunnen zich zoal manifesteren bij het implementeren van dit soort applicaties? 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). 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. In een breder kader kunnen aanvallen via deze technologie geïntegreerd worden in een ruimere hybride aanval.

Technische noties

Het derde luik van de uiteenzetting omvat enkele technische bedenkingen, waar de heer Raes snel overgaat gelet op de inleidende uiteenzetting van de vorige spreker.

De spreker verwijst naar een zeer recent artikel van Jaap Haartsen, de Nederlander die in de jaren 90 in opdracht van Ericsson de bluetooth-technologie uitvond. De heer Haartsen hekelde de Nederlandse aanpak van de corona app, die volgens hem de allures had van een mediacircus. Het stemt de spreker dan ook tevreden dat in de Belgische pers is opgeroepen tot enige terughoudendheid ter zake, en hij roept op om de werkzaamheden met betrekking tot de corona app discreet verder te zetten. De heer Haartsen meent overigens ook dat bluetooth een onvoldoende nauwkeurige plaatsbepaling toelaat en als zodanig veel valse positieven dreigt te genereren.

De heer Raes besluit 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 combineert.

Hij merkt nog op dat de VSSE ook bezig is met het in kaart brengen van allerhande pogingen tot desinformatie en het verspreiden van *fake news* in het kader van de coronacrisis.

D. **Exposé introductif de Mmes Olivia Venet, présidente de la Ligue des Droits Humains, et Kati Verstrepen, présidente de la Liga voor Mensenrechten**[3]

Mme Olivia Venet (Ligue des Droits Humains) fait observer que la résolution visée a pointé les enjeux en termes de droits humains, et notamment du droit au respect de la vie privée, que pose le développement de solutions technologiques de *tracking*. Il convient toutefois de relever qu'aucun projet de texte de loi n'est effectivement soumis à l'analyse, laquelle ne se fait donc pas *in concreto* mais bien de manière purement théorique.

L'oratrice renvoie à une lettre ouverte de la Ligue datant du 17 avril et adressée aux responsables politiques: "Lutte contre le COVID-19 et développement de solutions technologiques de "*tracking*" – les droits humains ne doivent pas devenir des victimes collatérales"[4].

À cet égard, il ressort des dernières informations présentes dans la presse que les autorités publiques semblent choisir de s'orienter vers un système de call center plutôt que d'application mobile.

Il est fondamental que l'adoption d'un quelconque système de suivi fasse l'objet d'un véritable débat parlementaire, en toute transparence. À ce stade, cette absence de transparence peut être pointée du doigt et il conviendra de s'assurer de l'intervention effective du pouvoir législatif dans l'adoption du cadre légal dans lequel les mesures envisagées pourront être mises en œuvre. Il conviendra également de permettre aux autorités compétentes (Conseil d'État et APD notamment) d'émettre un avis circonstancié quant aux mesures envisagées, outre la consultation nécessaire d'experts.

Quoi qu'il en soit, tous les systèmes envisagés impliquent des atteintes manifestes à la vie privée, bien que de manière différente. Ces atteintes doivent dès lors être prévues par une loi, elles doivent poursuivre un but légitime et être proportionnelles à l'objectif poursuivi. Les données collectées ne peuvent être utilisées à d'autres fins.

[3] Les deux oratrices répondent négativement aux questions énoncées à l'article 28, 2*bis*, du Règlement de la Chambre.

[4] *http://www.liguedh.be/lettre-contre-le-covid-19-tracage-et-respect-de-la-vie-privee-la-ligue-des-droits-humains-la-federation-internationale-des-droits-humains-et-la-liga-voor-mensenrechten-adresse-une-lettre-au-gouver*.

D. **Inleidende uiteenzetting van de dames Olivia Venet, voorzitster van de *Ligue des Droits Humains*, en Kati Verstrepen, voorzitster van de Liga voor Mensenrechten**[3]

Mevrouw Olivia Venet (Ligue des Droits Humains) merkt op dat in de op stapel staande resolutie wordt gewezen op de uitdagingen op het vlak van de mensenrechten, in het bijzonder het recht op eerbiediging van het privéleven, als gevolg van de ontwikkeling van technologische *tracking*-oplossingen. Er moet echter op worden gewezen dat geen enkel ontwerp van wettekst daadwerkelijk wordt geanalyseerd. De analyse gebeurt dus niet concreet, maar slechts louter theoretisch.

De spreekster verwijst naar een aan de beleidsverantwoordelijken gerichte open brief van 17 april 2020 van de *Ligue des Droits Humains* met als titel *Lutte contre le COVID-19 et développement de solutions technologiques de* "*tracking*" *– les droits humains ne doivent pas devenir des victimes collatérales*[4].

Ter zake blijkt uit de recentste informatie in de pers dat de overheid meer lijkt te denken aan een systeem met een callcenter, veeleer dan met een mobiele app.

Het is van wezenlijk belang dat over de instelling van om het even welk systeem van opvolging een grondig en volstrekt transparant parlementair debat plaatsgrijpt. Momenteel kan dat gebrek aan transparantie aan de kaak worden gesteld. Men zal erop moeten toezien dat de wetgevende macht daadwerkelijk zijn rol kan spelen bij de aanneming van het wettelijk kader waarbinnen de geplande maatregelen ten uitvoer zullen kunnen worden gelegd. Voorts zullen ook de bevoegde instanties (onder meer de Raad van State en de GBA) de mogelijkheid moeten krijgen om een omstandig advies over de geplande maatregelen uit te brengen, naast de noodzakelijke raadpleging van deskundigen.

Hoe dan ook brengen alle overwogen systemen duidelijke inbreuken op de persoonlijke levenssfeer met zich, hoewel dat op verschillende wijzen geschiedt. Die inbreuken moeten dan ook in een wet worden geregeld, moeten een gerechtvaardigd doel nastreven en moeten met dat doel in verhouding staan. De ingezamelde gegevens mogen niet voor andere doeleinden worden gebruikt.

[3] Beide spreeksters beantwoorden de in artikel 28, 2*bis*, van het Kamerreglement opgenomen vragen ontkennend.

[4] *http://www.liguedh.be/lettre-contre-le-covid-19-tracage-et-respect-de-la-vie-privee-la-ligue-des-droits-humains-la-federation-internationale-des-droits-humains-et-la-liga-voor-mensenrechten-adresse-une-lettre-au-gouver*.

Il convient également de s'assurer que les procédés adoptés sont ceux qui, avec des résultats similaires, sont les moins invasifs pour la vie privée. Il s'ensuit que toutes les options possibles doivent être examinées et évaluées mais aussi que le procédé doit être partie intégrante d'une stratégie globale dans laquelle il s'inscrit.

Le consentement des personnes concernées doit être libre et éclairé par des informations précises. La collecte ne peut être effectuée que sur une base volontaire. La question de l'anonymisation des données est également essentielle, notamment dans la perspective d'un *call center* qui collecterait lesdites données.

Les mesures doivent être strictement limitées dans le temps. Le risque est en effet réel de voir se pérenniser les moyens de surveillance adoptés dans un contexte de crise, en l'absence de détermination d'un cadre légal strict et de finalités précises. La conservation limitée et l'effacement automatique des données doivent donc également être déterminés, en rapport direct avec l'objectif poursuivi.

Enfin, la mise en œuvre d'un système de suivi des personnes atteintes du coronavirus contient, en outre, des risques d'atteintes aux droits fondamentaux autres que celui du respect de la vie privée: liberté d'association, de réunion, d'expression, atteintes à la non-discrimination mais aussi risques d'atteintes aux droits économiques sociaux et culturels, lesquels doivent également être pris en considération.

Mme Kati Verstrepen (Liga voor Mensenrechten) indique que la *Liga voor Mensenrechten* se réjouit particulièrement de l'initiative visant à adopter une résolution prévoyant qu'une application ne sera déployée dans le cadre de la lutte contre le coronavirus que si de nombreuses conditions sont réunies.

La *Liga voor Mensenrechten* souscrit pleinement aux conditions énumérées dans le texte de la proposition de résolution.

La *Liga voor Mensenrechten* a déjà signalé, dans une communication précédente[5], l'utilité potentielle d'une application contre le coronavirus pour nous déconfiner

Er moet ook op worden toegezien dat men bij gelijkaardige resultaten kiest voor de werkwijzen die de kleinste weerslag op de persoonlijke levenssfeer hebben. Daaruit volgt dat alle mogelijke opties moeten worden onderzocht en geëvalueerd, maar ook dat de werkwijze integraal deel moet uitmaken van een alomvattende strategie die er het kader voor vormt.

De betrokkenen moeten op basis van nauwkeurige informatie vrije en geïnformeerde toestemming kunnen geven. De gegevensinzameling mag alleen op vrijwillige basis geschieden. Het anoniem maken van de gegevens is eveneens van wezenlijk belang, in het bijzonder wanneer men denkt aan een callcenter dat de betrokken gegevens zou inzamelen.

De maatregelen moet strikt worden beperkt in de tijd. Wanneer geen strikt wettelijk kader met nauwkeurige doelstellingen wordt vastgelegd, bestaat er immers een reëel risico dat de in een crisiscontext ingestelde toezichtmiddelen een permanente aard krijgen. In samenhang met het nagestreefde doel moet dus ook worden voorzien in de beperkte bewaring en in het automatisch wissen van de gegevens.

Tot slot houdt de instelling van een systeem van opvolging voor coronavirusdragers ook bedreigingen in met betrekking tot andere grondrechten dan de eerbiediging van de persoonlijke levenssfeer, namelijk de vrijheid van vereniging, de vrijheid van vergadering, de vrijheid van meningsuiting en het recht op non-discriminatie. Er moet ook rekening worden gehouden met het risico op inbreuken op de economische, sociale en culturele rechten.

Mevrouw Kati Verstrepen (Liga voor Mensenrechten) geeft aan dat de Liga bijzonder opgezet is met het initiatief om een resolutie aan te nemen waarin voorzien wordt dat een app alleen zal ingezet worden in de strijd tegen het coronavirus als tal van voorwaarden vervuld zijn.

De Liga voor Mensenrechten onderschrijft de voorwaarden zoals deze opgesomd worden in de tekst van het voorstel van resolutie volledig.

In eerdere communicatie[5] wees de Liga voor Mensenrechten al op het mogelijk nut van een coronaapp om ons sneller uit de *lockdown* te halen, maar

[5] Voir les publications suivantes: *https://www.knack.be/nieuws/belgie/een-app-in-de-strijd-tegen-corona-alleen-met-respect-voor-privacy/article-opinion-1584535.html* et *https://www.mo.be/opinie/kunnen-we-nu-eindelijk-de-corona-app-definitief-begraven*.

[5] Zie volgende publicaties: *https://www.knack.be/nieuws/belgie/een-app-in-de-strijd-tegen-corona-alleen-met-respect-voor-privacy/article-opinion-1584535.html* en *https://www.mo.be/opinie/kunnen-we-nu-eindelijk-de-corona-app-definitief-begraven*.

plus rapidement, mais elle a simultanément mis l'accent sur les nombreux dangers de l'installation rapide et irréfléchie d'un tel outil.

Après avoir appris que, selon une étude de l'Université d'Anvers, près de la moitié des personnes interrogées refuseraient d'installer une application, la *Liga voor Mensenrechten* a décidé de réaliser une étude supplémentaire.

Une série de questions ont été soumises aux personnes interrogées dans le cadre d'un sondage. Il leur a par exemple été demandé si elles étaient disposées à utiliser une application de traçage et de suivi des contacts dans le cadre d'une stratégie de sortie de crise.

Selon cette enquête, 6 % seulement des personnes interrogées ne voient pas d'inconvénient à utiliser une application de ce type. La moitié des personnes interrogées ont répondu qu'elles ne voulaient en aucun cas utiliser cette application et 44 % ont répondu qu'elles ne voulaient utiliser une application de ce type que si son utilisation était subordonnée à certaines conditions.

Ces conditions sont les suivantes:

— utilisation temporaire de l'application;

— certitude que les données ne sont pas conservées dans une banque de données centralisée;

— garantie que les données sont conservées de manière totalement anonyme et sécurisée.

Certains indiquent qu'ils utiliseront peut-être cette application:

— s'il est certain que l'application n'est utilisée que pour le suivi de l'épidémie;

— si un usage abusif des données est impossible et si celles-ci ne peuvent pas non plus être utilisées par d'autres autorités publiques;

— si une surveillance indépendante de l'utilisation de l'application est mise en place;

— si le code source est rendu public.

Lorsqu'on associe les résultats de ce sondage aux conclusions de nombreux scientifiques[6] selon lesquelles une application contre le coronavirus ne sera utile que

[6] Voir notamment: *https://simassocc.files.wordpress.com/2020/04/persbericht-16-4-2020-assocc1.pdf*.

tegelijk focuste ze op de talrijke gevaren van het snel en ondoordacht installeren van een dergelijke tool.

Nadat eerder uit een onderzoek van de Universiteit Antwerpen was gebleken dat zo goed als de helft van de ondervraagden zou weigeren om een app te installeren besloot de Liga voor Mensenrechten een verder onderzoek te doen.

Er werd een poll gelanceerd waarbij de respondenten een aantal vragen voorgelegd werden. Zo werd gevraagd naar de bereidheid voor het gebruik van een *tracking-and-tracing* -app in de exitstrategie.

Uit deze bevraging bleek dat slechts 6 % van de respondenten geen probleem ziet bij het gebruik van een dergelijke app. De helft van de ondervraagden geeft aan de app in geen enkel geval te willen gebruiken en 44 % geeft aan de app alleen te willen gebruiken als daar voorwaarden aan gekoppeld zijn.

Deze voorwaarden zijn:

— het tijdelijk gebruik van de app;

— de zekerheid dat de gegevens niet opgeslagen worden in een centrale databank;

— de garantie dat de gegevens volstrekt anoniem en vergrendeld opgeslagen worden.

Sommigen geven aan deze app mogelijk wel te gebruiken op voorwaarde dat:

— er zekerheid is dat de app alleen gebruikt wordt voor het opvolgen van de epidemie;

— er geen misbruik kan gemaakt worden van de gegevens en ze ook niet kunnen gebruikt worden door andere overheden;

— er onafhankelijk toezicht komt op het gebruik van de app;

— de broncode openbaar wordt gemaakt.

Als men de resultaten van deze bevraging koppelt aan de bevindingen van tal van wetenschappers[6] dat een corona-app alleen maar nuttig is als er voldoende

[6] Zie o.m. *https://simassocc.files.wordpress.com/2020/04/persbericht-16-4-2020-assocc1.pdf*.

si le nombre d'utilisateurs est suffisant, il apparaît clairement qu'il ne faut pas attendre de miracle de cet outil numérique.

Les préoccupations concernant l'inclusion sont frappantes dans ce sondage. Qu'adviendra-t-il des personnes handicapées ou âgées qui n'ont pas de smartphone ou qui ne savent pas s'en servir? Les personnes dont la situation financière est précaire peuvent-elles être équipées d'un smartphone doté de la technologie adéquate de manière à ce qu'elles puissent également bénéficier de la protection offerte par l'application?

On répond partiellement à cette préoccupation en plaçant le traçage et le suivi des contacts sociaux entre les mains de contrôleurs "humains", comme on le propose aujourd'hui.

La *Liga voor Mensenrechten* émet cependant également des réserves à cet égard. Comme à l'égard de l'application envisagée, l'inquiétude est grande à l'égard des effets considérables d'un tel contrôle de masse en matière de droits humains car la différence est mince entre l'information et le contrôle.

Une telle approche n'a d'utilité que s'il existe une capacité de test suffisante et que la population a suffisamment confiance. Les personnes devront partager des informations hautement confidentielles en coopérant à pareil système et elles ne le feront que s'il y a suffisamment de garanties que le respect de la vie privé est également assuré dans le cadre de ce système.

Les conditions figurant dans la proposition de résolution devront être reprises *mutatis mutandis* lors de la mise en place d'un système de contrôle "personnel".

Peu importe finalement que les données soient collectées par voie numérique ou par l'intervention humaine. À un moment donné, ces données sont rassemblées dans une banque de données et les citoyens doivent avoir suffisamment de garanties que les données sensibles qui sont conservées le sont en toute sécurité, qu'elles ne sont utilisées que dans le but auquel elles sont destinées et qu'elles ne sont pas conservées au-delà du délai nécessaire.

La *Liga voor Mensenrechten* insiste dès lors afin qu'un tel système fasse l'objet d'un véritable cadre juridique créé au niveau fédéral, en accord avec les entités fédérées. Ce cadre juridique doit être élaboré dans le respect de l'article 8 de la Convention européenne des droits de l'homme (CEDH), de l'article 7 de la Charte des droits fondamentaux de l'Union européenne, de l'article 22 de la Constitution, des règles prévues dans le Règlement

gebruikers zijn, dan is het meteen duidelijk dat er niet te veel heil moet worden verwacht van deze digitale tool.

Wat opvalt in de bevraging is de bezorgdheid rond de inclusiviteit. Wat met mensen die een functiebeperking hebben of ouderen die geen smartphone hebben of er niet mee kunnen omgaan? Kunnen mensen in financiële moeilijkheden voorzien worden van een smartphone met de juiste technologie, zodat ook zij kunnen genieten van de bescherming die de app kan bieden?

Aan deze bezorgdheid wordt voor een deel tegemoet gekomen als men de *tracking-and-tracing* in handen geeft van "menselijke" controleurs, zoals thans wordt voorgesteld.

Toch heeft de Liga voor Mensenrechten ook hier bedenkingen bij. Net als bij een app is er grote bezorgdheid over de ingrijpende effecten op mensenrechten bij een dergelijke massale *screening* omdat de grens tussen informatie en controle erg dun is.

Een dergelijke aanpak heeft enkel zin als er voldoende testcapaciteit is en als er voldoende vertrouwen is van de bevolking. Mensen zullen erg vertrouwelijke informatie moeten delen als ze hun medewerking aan een dergelijk systeem verlenen en zullen dat alleen maar doen als er voldoende waarborgen worden geboden dat ook in dit systeem de privacy verzekerd is.

De voorwaarden opgenomen in het voorstel van resolutie zullen dan ook *mutatis mutandis* moeten worden overgenomen bij de installatie van een systeem van "persoonlijke" controle.

Of data verzameld worden via digitale weg of via "*humane*" weg maakt uiteindelijk weinig uit. Op een bepaald ogenblik worden deze data verzameld in een databank en moeten de burgers voldoende garanties hebben dat de gevoelige data die worden opgeslagen veilig zijn, enkel gebruikt worden voor het doel waarvoor ze bestemd zijn en niet langer bijgehouden worden dan nodig is.

De Liga voor Mensenrechten dringt er dan ook op aan dat voor een dergelijk systeem een degelijk wettelijk kader wordt gecreëerd op federaal niveau, in samenspraak met de deelstaten. Bij de totstandkoming van dit wettelijk kader moet rekening worden gehouden met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), met artikel 7 van het Handvest van de Grondrechten van Europese Unie, met artikel 22 van de

général sur la protection des données (RGPD) et des recommandations formulées par les commissions, organes consultatifs et experts compétents. Il faudra en outre agir en tenant compte des dispositions prévues par la proposition de résolution à l'examen.

E. **Exposé introductif de la professeure Elise Degrave, UNamur**

La professeure Elise Degrave (UNamur) est professeure à faculté de droit et chercheuse en droit du numérique. Elle répond par la négative aux questions posées en application de l'article 28, 2*bis*, du Règlement de la Chambre.

En ce qui concerne la nature de la proposition de résolution, l'oratrice estime que le texte est un premier pas positif en vue d'entamer la réflexion sur la souveraineté numérique de l'État. Il s'agit d'un véritable socle offrant un certain nombre de garanties. Tout comme l'ont souligné les représentantes de la *Liga voor Mensenrechten* et de la Ligue des Droits Humains, il demeure néanmoins essentiel de rédiger une proposition de loi, ainsi que l'impose au demeurant l'article 22 de la Constitution:

"Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit."

Le risque existe en effet qu'à un moment donné, l'avancement technologique soit tel que tout débat démocratique devient impossible, dès lors qu'on en arriverait à une sorte de disposition toute faite qui serait approuvée dans l'urgence et majorité contre opposition sans réel débat démocratique de fond.

Sur le fond, la proposition de résolution offre une bonne synthèse d'un certain nombre de points pour lesquels la vigilance s'impose, en particulier en ce qui concerne la protection des données à caractère personnel. L'oratrice n'est pas encore en mesure d'adopter une position claire en la matière, en raison des nombreuses inconnues sur le plan technologique, telles que le taux de pénétration de l'application concernée, de trop nombreux points n'ayant pour l'instant pas encore été tranchés.

La professeure Degrave renvoie par ailleurs à l'article 8 de la CEDH, qui prescrit le droit au respect de la vie privée et familiale:

Grondwet, met de regels opgenomen in de Algemene Verordening Gegevensbescherming (AVG) en de aanbevelingen gedaan door de bevoegde commissies, adviesorganen en experten. Bovendien moet worden gehandeld naar de bepalingen opgenomen in het voorliggende voorstel van resolutie.

E. **Inleidende uiteenzetting van Professor Élise Degrave, UNamur**

Professor Élise Degrave (UNamur) is professor aan de faculteit rechten en onderzoekster in digitaal recht (*droit du numérique*). Zij beantwoordt de in artikel 28, 2*bis*, van het Kamerreglement opgenomen vragen ontkennend.

Wat de aard van het voorstel van resolutie betreft vindt de spreekster de tekst een goede eerste stap in de reflectie over de digitale soevereiniteit van de staat. Het gaat over een degelijke sokkel met een aantal waarborgen. Het blijft echter essentieel om, zoals de vertegenwoordigsters van de Liga voor Mensenrechten en de *Ligue des Droits Humains* al hebben aangehaald, een wetsvoorstel te redigeren, zoals trouwens ook opgelegd wordt door artikel 22 van de Grondwet:

"Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht."

Het risico bestaat immers dat men op een bepaald moment zo ver zal gevorderd zijn op technologisch vlak, dat een echt democratisch debat niet meer mogelijk zal zijn, omdat men zou komen tot een soort sleutel-op-de-deur-bepaling die dringend en meerderheid tegen oppositie zou worden goedgekeurd, zonder een echt democratisch en fundamenteel debat.

Inhoudelijk biedt het voorstel van resolutie een goede synthese van een aantal punten waarvoor waakzaamheid geboden is, voornamelijk met betrekking tot de bescherming van privégegevens. De spreekster is nog niet in staat om een duidelijk standpunt voor of tegen in te nemen, gelet op de vele technologische onbekenden, zoals de penetratiegraad van de betrokken applicatie, te veel zaken zijn op dit moment nog niet duidelijk getrancheerd.

Professor Degrave verwijst verder naar het artikel 8 van het EVRM, dat het recht op eerbiediging van privé, familie- en gezinsleven inhoudt:

"1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.".

Il apparaît donc que, d'une part, le respect de la vie privé ne peut être réduit au RGPD et que, d'autre part, la protection de la vie privée est une condition essentielle à l'exercice d'un certain nombre d'autres droits et libertés: par exemple, en ce qui concerne les données relatives à la santé et le risque de discrimination ou les données religieuses et le risque d'atteintes à la liberté de culte.

C'est ainsi qu'un texte aujourd'hui conforme au RGPD peut poser ultérieurement problème au regard d'autres libertés. Il existe une grande incertitude en la matière, dès lors qu'il est impossible de savoir aujourd'hui si une application est nécessaire, et ce, en raison du manque de clarté concernant les masques, les tests, etc. Dans ce contexte, l'oratrice voit un potentiel dans l'utilisation de bracelets, qui ne portent pas atteinte à la vie privée et qui permettent au citoyen de vérifier si la distance d'un mètre et demi est respectée.

Eu égard à la situation catastrophique à laquelle nous sommes confrontés, la tentation est grande de suivre n'importe quelle piste pour sortir de la crise. Il s'agit donc de réaliser un bilan des avantages et des risques de chaque application potentielle, car les choix technologiques d'aujourd'hui détermineront les choix de société de demain.

L'État dispose déjà aujourd'hui de très nombreuses données essentielles sur tous les citoyens. Il s'agit de données fiscales, familiales, cadastrales, sanitaires, etc. recueillies sans leur accord. L'État a jusqu'à présent su conserver la confiance des citoyens, mais sans cette confiance, toute l'administration numérique de l'État s'effondrerait. La professeure Degrave renvoie à cet égard à un arrêt du Conseil d'État du 26 avril 2005 (n° 143 683, *Van Merris*), qui sanctionne sévèrement l'utilisation abusive de données commise par un fonctionnaire.

La professeure Degrave pointe deux éléments qui menacent la confiance du citoyen.

"1. Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.".

Hieruit moge blijken dat enerzijds het respect voor het privéleven niet mag worden gereduceerd tot de AVG en anderzijds dat bescherming van de privacy een essentiële voorwaarde is voor de uitoefening van een aantal andere rechten en vrijheden: bijvoorbeeld wat gezondheidsgegevens betreft en het risico op discriminatie of nog religieuze gegevens en het risico voor inbreuken op de godsdienstvrijheid.

Op die manier kan een tekst die vandaag conform is aan de AVG later problemen geven met betrekking tot andere vrijheden. Er heerst ter zake een grote mate van onzekerheid omdat het vandaag onmogelijk is te weten of een app noodzakelijk is, wegens de onduidelijke stand van zaken met betrekking tot maskers, testen, enzovoort. In dit verband ziet de spreekster potentieel in het gebruik van armbanden, die niet privacy-invasief zijn en die de burger toegelaten om na te gaan of de afstand van anderhalve meter wordt gerespecteerd.

Gezien de catastrofale toestand bestaat het risico dat men om het even wat zou proberen om uit de crisis te geraken: het komt er dus op aan om voor elke mogelijke applicatie een balans te maken van de voordelen en de risico's, vermits een technologische keuze vandaag een maatschappijkeuze voor morgen impliceert.

Op dit moment beschikt de staat al over heel veel essentiële gegevens over alle burgers die zonder hun toestemming werden verkregen, met name fiscale, familiale, kadastrale, gezondheidsgegevens enzovoort. Tot nu toe heeft de staat het vertrouwen van de burgers behouden, maar zonder dit vertrouwen zou de gehele digitale administratie van de staat ineenstorten. Professor Degrave verwijst hier naar een arrest van de Raad van State van 26 april 2005 (nr. 143 683, *Van Merris*), waarbij misbruik van gegevens door een ambtenaar streng werd gesanctioneerd.

Volgens professor Degrave stellen er zich twee bedreigingen voor het vertrouwen van de burger.

L'oratrice cite d'abord le manque de transparence potentiel (ainsi que l'évoque également la proposition de résolution), en particulier la nécessité de rendre le code source disponible dans le format *open source*: le code pourra ainsi être examiné et amélioré par des programmateurs externes. L'oratrice se fait du souci à ce sujet car elle n'a elle-même pas obtenu l'accès aux travaux de la *task force*: lorsqu'elle s'est adressée au cabinet du ministre De Backer à cet effet, elle a reçu un lien vers le site internet de la plateforme *eHealth*, qui est gérée par le responsable de la Banque Carrefour de la Sécurité sociale (BCSS). Il s'agit des deux principales plateformes de traitement de données en Belgique et elles sont très efficaces. La professeure Degrave craint donc pour l'indépendance de la nouvelle plateforme.

Deuxième menace: les données recueillies dans le cadre du traçage en vue de la lutte contre le COVID-19 risquent d'être ensuite utilisées pour renforcer différentes formes de surveillance; en effet, les administrations fiscales et sociales utilisent déjà aujourd'hui des outils de profilage – basés sur l'intelligence artificielle – dont le fonctionnement est secret, dans le but de faire de l'exploration de données, à l'aide d'algorithmes antifraude, en exploitant toutes les informations dans les banques de données de l'État. Il est grand temps que le Parlement se penche sur ces différentes techniques d'intelligence artificielle (des techniques comparables ayant récemment été interdites aux Pays-Bas sur la base de l'article 8 de la CEDH). La Chambre doit donc aller au-delà de ce que prévoit le considérant J de la proposition de résolution car les données de traçage récoltées dans le cadre de la lutte contre le COVID risquent par exemple d'être utilisées pour renforcer le contrôle policier sur les citoyens.

La professeure Degrave explique que certaines données provenant du traçage réalisé au moyen de l'application pourraient être anonymisées (cela pourrait se faire en éliminant le lien entre la personne et la donnée). Cela signifie que ces données ne relèveraient plus du champ d'application de la protection des données, mais que d'autres caractéristiques comme le sexe, l'âge, etc. seraient conservées. On pourrait ensuite croiser ces données avec d'autres informations déjà détenues par la BCSS et donc identifier certains schémas – et constater par exemple que certaines personnes sont beaucoup plus souvent malades que la moyenne ou se rendent régulièrement dans des endroits connus pour des trafics de drogue. L'objectif (par exemple la lutte contre la consommation de drogue) peut être légitime, mais il faut se demander qui a décidé d'organiser cette surveillance. La réponse est la suivante: la personne qui a conçu l'algorithme. Cette situation n'est pas normale et le Parlement doit en être conscient.

Ten eerste gaat het over het risico op een gebrek aan transparantie, met name (dit staat ook in het voorstel van resolutie) de noodzaak tot het beschikbaar maken van de broncode onder het *opensource*-formaat: op die manier kan de code worden besproken en verbeterd door externe programmeurs. De spreekster maakt zich op dit punt zorgen omdat zij zelf geen toegang heeft gekregen tot de werkzaamheden van de taskforce: toen zij zich hierop wendde tot het kabinet van minister De Backer werd haar een link toegestuurd naar de internetsite van het *eHealth*-platform, dat wordt geleid door de verantwoordelijke van de Kruispuntbank voor de Sociale Zekerheid (KBSZ). Dit zijn de twee grootste platforms voor gegevensverwerking in België en ze zijn zeer efficiënt. Professor Degrave vreest dus voor de onafhankelijkheid van het nieuwe platform.

Een tweede bedreiging bestaat hierin dat de gegevens die worden verzameld in het kader van de tracering voor COVID-19 achteraf zullen worden gebruikt voor de versterking van allerlei vormen van toezicht ("*surveillance*"); immers, vandaag al gebruiken de fiscale en sociale administraties een aantal profileringshulpmiddelen – op basis van artificiële intelligentie – waarvan het functioneren geheim is, om aan de hand van antifraude-algoritmes aan *datamining* te doen en zulks op alle gegevens die in de gegevensbanken van de Staat zitten. Het is hoog tijd dat het Parlement zich buigt over deze verschillende technieken van artificiële intelligentie (in Nederland werden vergelijkbare technieken recent vernietigd op basis van artikel 8 van het EVRM). De Kamer moet dus verder gaan dan wat wordt aangegeven in considerans J van het voorstel van resolutie want de traceringsgegevens het kader van de COVID-bestrijding zouden bijvoorbeeld kunnen worden misbruikt voor het versterken van het politietoezicht op de burgers.

Professor Degrave legt uit dat bepaalde gegevens afkomstig uit de tracing via de app zouden kunnen worden geanonimiseerd (door de band te verbreken tussen de persoon en het gegeven) en bijgevolg vallen de betrokken gegevens niet meer onder de toepassing van de gegevensbescherming, maar blijven toch nog bepaalde andere karakteristieken bewaard zoals geslacht, leeftijd, enzovoort. Men zou deze gegevens dan kunnen kruisen met andere gegevens die men al bezit in de schoot van de KBSZ en zo kan men bepaalde patronen opsporen, bijvoorbeeld dat bepaalde mensen veel meer ziek zijn dan gemiddeld of nog dat ze regelmatig naar plaatsen gaan die gekend zijn voor drugstrafiek. De doelstelling (bijvoorbeeld bestrijding van druggebruik) kan legitiem zijn, maar de vraag is wie beslist heeft om aan dergelijke surveillance te doen; het antwoord is diegene die het algoritme heeft ontworpen. Welnu, dat is niet normaal en het Parlement moet zich hiervan bewust zijn.

Il convient donc de renforcer la proposition de résolution et de faire figurer dans son dispositif l'interdiction de réutiliser toute donnée quelconque provenant de l'application envisagée, sous quelque forme que ce soit. L'oratrice estime par ailleurs qu'il faut rompre le lien entre l'application et les administrations, c'est-à-dire les plateformes *eHealth* et BCSS. Ces dernières sont certes très efficaces et constituent un très beau modèle, mais on ne peut pas créer un État dans l'État. L'oratrice plaide dès lors pour une approche fondée sur le principe de la prise en compte du respect de la vie privée lors de la conception (*privacy by design*), également en ce qui concerne la gestion des données de sécurité sociale. Elle renvoie à cet égard à un exemple intéressant, celui de l'application autrichienne gérée par la Croix-Rouge autrichienne, dans laquelle les données sont uniquement enregistrées à l'échelon local, sur le téléphone de l'utilisateur. Ce système se fonde sur un code *open source* accessible au public. Cette application a été analysée par des ONG actives dans le domaine de la protection des données et peut être considérée comme un exemple de bonne pratique. Le citoyen ne fait confiance à certains outils que s'ils sont validés par des ONG.

La professeure Degrave se penche enfin sur le lien avec les GAFAM. Apple et Google ont déjà été salués aujourd'hui comme des modèles: Apple et Google disposent effectivement d'excellents chercheurs et d'une capacité de stockage de données considérable, et on peut douter que les autorités belges disposent de moyens comparables. D'aucuns – surtout les jeunes – estiment aujourd'hui qu'il n'y a aucun problème, car nous fournissons de toute façon déjà toutes les informations nous concernant à Google dans le cadre, par exemple, de *Google Maps* ou *Google Health*.

L'oratrice oppose à ce discours le fait qu'un citoyen peut très bien vivre sans Google (de plus en plus d'alternatives sont du reste disponibles), mais pas sans l'État: si l'État s'associe en l'espèce à Google, le citoyen sera contraint de transmettre son dossier de santé à Google. Et ce dernier n'hésitera pas à dominer l'État: il ne faut pas confier les clés de la gestion de la politique publique à Google; l'oratrice doute que les GAFAM soient guidées par des intentions philanthropiques. Pourquoi viennent-ils tout à coup nous aider? Parce que cela leur permet d'entraîner leurs algorithmes avec toutes ces données et qu'il sera ainsi ensuite possible d'organiser par exemple un traçage pour la grippe, le sida, etc. Sommes-nous prêts à prendre le risque de créer une société d'exclusion sociale?

Het voorstel van resolutie moet dus worden versterkt en dient ook te verzoeken een verbod op te leggen tot een hergebruik van elk gegeven afkomstig uit de applicatie, onder welke vorm dan ook. Daarnaast moet volgens de spreekster ook de band worden verbroken tussen applicatie en administratie, zijnde de *eHealth*- en KBSZ-platformen. Deze laatste zijn weliswaar zeer efficiënt en vormen een zeer mooi model, maar men mag geen staat in de staat creëren. De spreekster pleit bijgevolg voor de benadering van *privacy by design*, ook voor het beheer van de gegevens in de sociale zekerheid. Zij verwijst in deze context naar het interessante voorbeeld van de Oostenrijkse app, die wordt beheerd door het Oostenrijkse Rode Kruis en waarbij de gegevens enkel lokaal worden opgeslagen op de telefoon van de gebruiker; het gaat om een code in *opensource* die toegankelijk is voor het publiek. Deze app is geanalyseerd door ngo's die actief zijn in gegevensbescherming en kan als een goede praktijk worden beschouwd. De burger zal maar vertrouwen hebben in bepaalde middelen als ze gevalideerd zijn door ngo's.

Professor Degrave gaat ten slotte in op de band met de GAFAM. Apple en Google werden hier vandaag al toegejuicht als modelvoorbeelden: dit is uiteraard verleidelijk want Apple en Google hebben zeer goede onderzoekers en beschikken over een enorme opslagcapaciteit voor gegevens, waarvan men kan betwijfelen of de Belgische overheid over iets vergelijkbaars beschikt. Sommige, vooral jonge, mensen zeggen vandaag: "we geven toch al al onze gegevens aan Google in het kader van bijvoorbeeld *Google Maps of Google Health*, dus er is geen probleem".

De spreekster stelt daar tegenover dat een burger perfect kan leven zonder Google (er zijn trouwens ook steeds meer alternatieven beschikbaar), maar nooit zonder de staat: indien de staat Google hierin zou betrekken zal de burger verplicht zijn om zijn gezondheidsdossier aan Google te overhandigen. Welnu, Google zal niet aarzelen om de staat te domineren: men mag de sleutels voor het beheer van het openbaar beleid niet toevertrouwen aan Google; de spreekster heeft immers geen vertrouwen in de filantropie van de GAFAM. Waarom komen zij nu ineens ter hulp? Op die manier kunnen zij hun algoritmes trainen met al deze gegevens en wordt morgen het traceren mogelijk van bijvoorbeeld de griep, HIV, enzovoort. Zijn wij bereid om het risico te nemen om in een maatschappij van sociale uitsluiting terecht te komen?

III. — **QUESTIONS ET OBSERVATIONS DES MEMBRES**

M. Michael Freilich (N-VA) demande au professeur Preneel pourquoi il a récemment quitté le projet européen concernant une telle application mobile: ne savait-il pas que l'on y travaillait sur le stockage central de données? Que pense au demeurant le professeur de la direction dans laquelle s'engagent pour l'heure notamment la France et l'Allemagne dans ce domaine?

L'intervenant s'attarde ensuite sur la conservation de l'information dans une banque de données et non, par exemple, sur l'appareil d'une personne: les opérateurs télécoms font déjà quelque chose de similaire, notamment le stockage central des données de localisation: quelle est la différence?

En ce qui concerne le contrôle de l'application mobile, l'intervenant demande à M. Stevens comment il peut contrôler les applications mobiles provenant de l'étranger: existe-t-il en quelque sorte une obligation légale lorsque l'application mobile se trouve dans l'App Store?

L'APD dispose-t-elle de spécialistes dans des domaines techniques tels que le code source?

En ce qui concerne par ailleurs le traçage manuel, il s'agit d'une technique très invasive au niveau de la vie privée: où et comment seront par exemple stockées les données des *contact tracers*? Les autorités ne peuvent conserver elles-mêmes ces données: le *tracer* remettra-t-il alors une farde contenant tous ses contacts à l'intéressé?

Enfin, la législation relative à la protection de la vie privée offre-t-elle actuellement un cadre légal suffisant pour assurer une protection correcte ou faut-il légiférer davantage?

Enfin, dans le cadre des menaces d'espionnage et d'ingérence étrangère, l'intervenant demande à M. Raes si, sur certains appareils chinois, l'application mobile ne peut être piratée par le téléphone même.

Mme Jessika Soors (Ecolo-Groen) demande à M. Stevens si aujourd'hui l'APD rendrait un avis positif sur la proposition de résolution.

En ce qui concerne le calendrier, l'intervenante demande au professeur Preneel à quelle vitesse une application mobile pourrait être déployée dans la réalité, une fois que les ministres compétents ont donné leur approbation. Elle aimerait également en savoir plus sur la complémentarité entre l'application mobile et un éventuel traçage manuel. Enfin, selon les informations parues

III. — **VRAGEN EN OPMERKINGEN VAN DE LEDEN**

De heer Michael Freilich (N-VA) vraagt aan professor Preneel waarom hij recent is opgestapt uit het Europese project rond een dergelijke app: was het nieuw voor hem dat men daar werkt rond de centrale opslag van gegevens? Wat is trouwens de mening van de professor over de richting waarin met name Frankrijk en Duitsland zich momenteel begeven in deze aangelegenheid?

Vervolgens gaat de spreker in op het bijhouden van de informatie op een databank en dus bijvoorbeeld niet op het toestel van een persoon: vandaag doen de telecomoperatoren al iets dergelijks, met name de centrale opslag van lokalisatiegegevens: wat is dan het verschil?

Wat de controle op de app betreft, vraagt de spreker aan de heer Stevens op welke manier hij apps uit het buitenland kan controleren: is hier sprake van een soort wettelijke verplichting wanneer de app zich bijvoorbeeld bevindt in de App Store?

Beschikt de GBA over specialisten wanneer het gaat om technische zaken als de broncode?

Wat verder de manuele tracering betreft gaat het om een zeer privacy-invasieve techniek: waar en hoe zullen bijvoorbeeld de gegevens van de *contact tracers* worden opgeslagen? De overheid mag deze gegevens niet zelf bijhouden: gaat de *tracer* dan bijvoorbeeld een mapje meegeven aan de betrokkene met al zijn contacten?

Biedt de privacywetgeving vandaag ten slotte een voldoende wettelijk kader voor een juiste bescherming of is er extra wetgeving nodig?

Tot slot vraagt de spreker aan de heer Raes, in het kader van de dreigingen van spionage en buitenlandse inmenging, of op bepaalde Chinese toestellen de app niet kan worden gehackt via de telefoon zelf.

Mevrouw Jessika Soors (Ecolo-Groen) vraagt de heer Stevens of de GBA vandaag een positief advies zou verlenen over het voorstel van resolutie.

Aan professor Preneel vraagt de spreekster, wat de timing betreft, hoe snel een app in de realiteit zou kunnen worden uitgerold, nadat de bevoegde ministers hun fiat zouden hebben gegeven. Daarnaast kreeg zij graag meer uitleg over de complementariteit tussen de app en eventuele manuele *tracing.* Ten slotte zou volgens persberichten minstens 60 % van de bevolking de app

dans la presse, au moins 60 % de la population devrait utiliser l'application mobile pour en assurer l'efficacité, alors que le professeur affirme que 10 à 15 % est en fait suffisant: cela signifie-t-il que l'application mobile ne serait pas moins efficace si le taux de pénétration était inférieur à 60 %?

Enfin, Mme Soors pose la question suivante à tous les orateurs: abstraction faite de la répartition des compétences entre l'autorité fédérale et les régions et dans la mesure où tous les cadres juridiques seraient en ordre, si les orateurs étaient les ministres compétents pour prendre une décision sur le suivi et la traçabilité, que feraient-ils aujourd'hui?

M. Khalil Aouasti (PS) constate que le professeur Preneel était membre du Centre de connaissances de l'APD: est-ce toujours le cas? S'il en est ainsi et que le centre de connaissances doit rendre un avis sur une éventuelle application mobile, n'y a-t-il pas un conflit d'intérêts? La personne concernée devrait en effet participer en tant qu'expert au développement de l'application et ensuite rendre un avis sur la même application au nom du centre de connaissances.

Un cadre juridique et une habilitation spécifique sont par ailleurs indispensables: alors qu'il s'avère que l'Allemagne dispose déjà d'une loi et que l'assemblée plénière de l'Assemblée nationale française se penche aujourd'hui sur un cadre juridique, après avis de la Commission nationale de l'informatique et des libertés (CNIL) du 24 avril 2020, la Belgique va-t-elle suivre la même voie et donc opter pour des dispositions légales?

L'intervenant demande ensuite à M. Stevens s'il est toujours membre du groupe paneuropéen de huit personnes et où on en est à cet égard.

L'APD a-t-elle par ailleurs été invitée à rendre un avis et, si tel est le cas, cet avis – critique à en croire la presse – peut-il être transmis aux membres de la commission?

À l'intention de M. Raes et du professeur Preneel, l'intervenant fait également observer que lors du débat précité tenu à l'Assemblée nationale sur l'algorithme Bluetooth, il s'est avéré qu'en termes de sécurité nationale, ce dernier serait dépassé et qu'il pourrait en outre être facilement piraté notamment par des puissances étrangères; en outre, cet algorithme serait en lice pour servir de norme européenne.

L'intervenant constate par ailleurs que la professeure Degrave n'est pas favorable à ce que la plateforme

moeten gebruiken opdat hij efficiënt zou zijn, terwijl de professor stelt dat 10 % tot 15 % eigenlijk voldoende is: betekent zulks dat de app niet minder efficiënt zou zijn indien de penetratiegraad lager dan 60 % zou zijn?

Ten slotte legt mevrouw Soors aan alle sprekers de volgende vraag voor: abstractie makend van de bevoegdheidsverdeling tussen de federale overheid en de gewesten en voor zover alle wettelijke kaders in orde zouden zijn, indien de sprekers de bevoegde ministers zouden zijn voor een beslissing omtrent *tracking-and-tracing*, wat zouden zij vandaag zouden doen?

De heer Khalil Aouasti (PS) stelt vast dat professor Preneel lid was van het Kenniscentrum van de GBA: is dit nog steeds het geval? Indien zulks het geval is en het Kenniscentrum een advies zou moeten geven over een eventuele app, zou er geen sprake zijn van een belangenconflict? Immers, de betrokkene zou als expert de app mee ontwikkelen en achteraf vanuit het Kenniscentrum advies moeten geven over dezelfde app.

Daarnaast zijn een wettelijk kader en een specifieke machtiging essentieel: nu blijkt dat Duitsland al een wet heeft en de plenaire vergadering van de Franse *Assemblée Nationale* vandaag vergadert over een wettelijk kader, na een advies van de *Commission nationale de l'informatique et des libertés* (CNIL) van 24 april 2020, zal België dezelfde weg opgaan en dus ook opteren voor een wettelijke regeling?

Vervolgens vraagt de spreker aan de heer Stevens of hij nog steeds lid is van de pan-Europese groep bestaande uit acht personen en hoever men in dat kader is gevorderd.

Werd verder de GBA om een advies gevraagd en indien zulks het geval is kan dit advies –dat volgens de pers kritisch is – aan de leden van deze commissie worden bezorgd?

Ter attentie van de heer Raes en professor Preneel merkt de spreker verder op dat het in het al vermelde debat van de *Assemblée Nationale* met betrekking tot het bluetooth-algoritme is gebleken dat dit laatste in termen van nationale veiligheid voorbijgestreefd zou zijn en bovendien gemakkelijk zou kunnen worden gehackt, onder andere door buitenlandse mogendheden; bovendien zou dit algoritme een kandidaat zijn voor de Europese standaard.

Verder stelt de spreker vast dat professor Degrave er geen voorstandster van is dat het *eHealth*-platform de

eHealth gère les données de l'application. Lui-même préférerait cependant que ces données soient gérées par une autorité publique: quels pourraient dans ce cas être les autres candidats?

En ce qui concerne la plateforme *eHealth*, l'intervenant a constaté sur le site internet de la plateforme qu'un certain nombre d'applications sont déjà proposées pour s'enregistrer: en termes de protection de la vie privée, un certain nombre de ces applications indiquent que les données sont confidentielles, mais qu'elles peuvent être transmises à un des partenaires du réseau eHealth: quel est l'avis de M. Stevens à ce propos?

M. Erik Gilissen (VB) souligne que le développement d'une application collectant des données anonymes par le biais du Bluetooth semble être une bonne solution. Un certain nombre de préoccupations subsistent toutefois en matière de respect de la vie privée. Un stockage décentralisé constitue une solution appropriée, mais il doit être associé au caractère volontaire à 100 % de l'application.

En outre, l'intervenant s'interroge sur le pourcentage minimal d'utilisateurs nécessaire pour que l'application soit efficace.

De plus, le code source doit être transparent et l'application ne doit pas pouvoir être utilisée à d'autres fins. L'utilisateur doit toujours conserver le contrôle des données: comment peut-on le garantir? Comment éviter que les données soient utilisées à d'autres fins? Comment répondre en outre à la préoccupation du citoyen concernant le respect de la vie privée et les fuites de données? On constate en effet que les citoyens ne sont pas suffisamment disposés à installer l'application et il apparaît donc que le cadre légal ne constitue qu'une partie du problème.

Mme Nathalie Gilson (MR) constate que la proposition de résolution ne vise que le traçage numérique. Elle apprend en outre que plus de 2 000 personnes seront recrutées pour assurer le traçage physique par l'intermédiaire de centres d'appel: l'intervenante demande à M. Stevens et à Mme Verstrepen comment cette collecte physique de données pourra se dérouler dans le respect de la vie privée.

Ensuite, la membre craint que le risque de manipulation (espionnage, piratage, fuites, etc.) n'augmente si l'on adopte une approche *open source*.

En outre, si les Régions sont effectivement compétentes pour le développement des applications, une interopérabilité est évidemment nécessaire au sein de la Belgique, voire au sein de l'Union européenne, qui

gegevens van de applicatie zou beheren. Nochtans geeft hij er de voorkeur aan dat deze gegevens zouden worden beheerd door een openbare overheid: wie zou in dit geval dan nog kandidaat kunnen zijn?

Wat het *eHealth*-platform betreft, heeft de spreker vastgesteld op de website van het platform dat daar al een aantal apps worden voorgesteld om jezelf te registreren: welnu, de privacytermen van een aantal van deze apps stellen dat je gegevens privé zijn maar dat ze wel kunnen worden overgedragen aan één van de partners in het *eHealth*-netwerk: wat is de mening van de heer Stevens hieromtrent?

De heer Erik Gilissen (VB) merkt op dat de ontwikkeling van een app met anonieme gegevens via bluetooth een goede oplossing lijkt. Wel blijven een aantal bezorgdheden bestaan omtrent privacy. Decentrale opslag is een goede oplossing maar moet worden gecombineerd met een 100 % vrijwillig karakter van de app.

Daarnaast vraagt de spreker welk percentage gebruikers minimaal noodzakelijk is opdat de app efficiënt zou zijn.

Verder dient de broncode transparant te zijn en mag de app niet bruikbaar zijn voor andere doeleinden. De gebruiker dient steeds de controle te behouden over de data: hoe kan dit worden verzekerd? Op welke manier kan worden voorkomen dat de data worden gebruikt voor andere doeleinden? Op welke manier kan verder de bezorgdheid van de burger omtrent privacy en datalekken worden aangepakt? Men stelt immers vast dat de burgers onvoldoende bereid zijn om de app te installeren en het blijkt dus dat het wettelijk kader maar een deel van het probleem vormt.

Mevrouw Nathalie Gilson (MR) stelt vast dat het voorstel van resolutie enkel de digitale tracering viseert. Zij verneemt verder dat meer dan 2 000 personen zullen worden aangeworven om aan fysieke tracering te doen via callcenters: de spreekster vraagt aan de heer Stevens en aan mevrouw Verstrepen op welke manier deze fysieke inzameling van gegevens zal kunnen verlopen met respect voor de privacy.

Vervolgens vreest het lid dat het risico voor manipulatie (spionage, hacking, lekken, enzovoort) groter zal zijn indien wordt gewerkt met een *opensource*-benadering.

Verder zijn de gewesten inderdaad bevoegd voor de ontwikkeling van de apps maar er is uiteraard interoperabiliteit nodig binnen België en zelfs in de schoot van de Europese Unie, die hieromtrent een *toolbox*

a développé une boîte à outils en la matière. De quelle manière une application pourra-t-elle contribuer à rétablir le plus rapidement possible la libre circulation au sein de l'espace européen?

Enfin, l'intervenante revient sur l'efficacité de l'application. Selon des articles de presse, il faut au moins 60 % d'utilisateurs pour que l'application soit efficace, mais l'enquête citée par Mme Verstrepen indique que seulement 6 % de la population est disposée à utiliser l'application. Est-ce la raison pour laquelle on a finalement opté pour le traçage physique? L'intervenante est d'ailleurs beaucoup plus préoccupée par ce traçage physique que par une application en ce qui concerne le respect des droits de l'homme et de la vie privée.

M. Sammy Mahdi (CD&V) s'étonne des observations du professeur Preneel selon lesquelles un taux de participation de 10 à 15 % serait suffisant pour assurer une utilisation efficace de l'application: comment peut-on le prouver? Des simulations réalisées en Suède et aux Pays-Bas ont montré que même un taux de participation de 60 % serait insuffisant s'il n'était pas suffisamment réparti sur l'ensemble du territoire: qu'en pense l'orateur?

En ce qui concerne le Bluetooth, l'intervenant se demande à quelle vitesse cette technologie va évoluer compte tenu des problèmes liés à la présence de plexiglas et de murs. Ces problèmes entraîneront en effet la détection de nombreux faux contacts positifs.

En outre, on peut s'interroger sur le nombre de personnes qui possèdent actuellement un smartphone approprié en Belgique. Les téléphones Apple équipés d'un système d'exploitation iOS ne peuvent actuellement pas être utilisés parce qu'ils doivent être actifs. En ce qui concerne les téléphones Android, la dernière mise à jour doit être installée pour pouvoir utiliser l'application. À la lumière de ces éléments, quel est, selon l'expert, le nombre de gsm appropriés actuellement en circulation? On constate d'ailleurs qu'en 2019, un senior sur quatre ne possédait pas de smartphone.

Le professeur Preneel pourrait-il en outre fournir une estimation du coût que représentent le développement et la maintenance de cette application?

Le débat public susmentionné qui a eu lieu aux Pays-Bas a effectivement peut-être été un cirque médiatique, mais il a tout de même montré que des pirates informatiques pouvaient s'introduire dans un gsm par le biais du Bluetooth, indépendamment de l'application, qui peut être sûre en elle-même: qu'en est-il selon l'expert?

À l'attention de M. Raes, l'intervenant souligne qu'il est apparu, aux Pays-Bas, qu'il est possible de renforcer la

heeft ontwikkeld: op welke manier zal een app kunnen bijdragen aan het zo snel mogelijk herstellen van het vrij verkeer binnen de Europese ruimte?

Ten slotte gaat de spreekster in op de doelmatigheid van de app: volgens persberichten waren hiervoor minstens 60 % gebruikers nodig, maar uit de door mevrouw Verstrepen aangehaalde enquête is gebleken dat slechts 6 % van de bevolking bereid zou zijn om de app te gebruiken: is het om reden dat uiteindelijk werd geopteerd voor de fysieke tracering? De spreekster maakt zich trouwens veel meer zorgen over deze fysieke tracering dan over een app, wat betreft het respect voor de mensenrechten en de privacy.

De heer Sammy Mahdi (CD&V) is verbaasd over de opmerkingen van professor Preneel dat een participatiegraad van 10 tot 15 % zou volstaan voor een efficiënt gebruik van de app: hoe kan dit worden gestaafd? Uit simulaties in Zweden en Nederland is gebleken dat zelfs 60 % onvoldoende zou zijn indien dit niet voldoende verspreid is over het hele grondgebied: wat is de mening van de expert hieromtrent?

Wat bluetooth betreft, vraagt de spreker hoe snel deze technologie zal evolueren gezien de problemen met onder meer plexiglas en muren: dit zal namelijk zorgen voor vele valse positieven.

Bovendien kan men zich afvragen hoeveel mensen vandaag in België een hiervoor geschikte smartphone bezitten? Wat Apple-telefoons betreft met een iOS-besturingssysteem, deze kunnen vandaag niet worden gebruikt omdat ze actief moeten zijn. Voor Android-telefoons is het nodig dat de laatste *update* is geïnstalleerd om de app te kunnen gebruiken. Hoeveel geschikte gsm's zijn er in het licht hiervan momenteel in omloop volgens de expert? Men stelt trouwens vast dat in 2019 een op de vier senioren geen smartphone bezat.

Kan professor Preneel verder een raming geven van de kostprijs voor de ontwikkeling en het onderhoud van deze app?

Het al vermelde openbare debat dat in Nederland heeft plaatsgevonden was inderdaad misschien eerder een mediacircus, maar toch is hieruit gebleken dat hackers zich via bluetooth toegang kunnen verschaffen tot een gsm, los van de app die op zichzelf veilig kan zijn: wat is hiervan aan volgens de expert?

Ter attentie van de heer Raes merkt de spreker op dat in Nederland is gebleken dat het mogelijk is om de

capacité du Bluetooth au moyen d'un dispositif. Cela générerait de nombreux faux contacts positifs et pourrait inquiéter de nombreuses personnes: quel est l'avis de l'expert à ce sujet?

L'intervenant demande ensuite à M. Stevens s'il estime que l'approche autrichienne est appropriée? Que pense-t-il en outre d'un code source ouvert ("*open source*")? M. Stevens considère-t-il la chasse aux bugs (en anglais "*bug bounties*", une méthode consistant à rétribuer les citoyens pour détecter des failles dans le système) comme une approche adéquate? Que pense l'expert du texte de la proposition de résolution? Serait-il lui-même partisan d'encore renforcer ce texte?

Enfin, l'intervenant demande aux représentants de la Ligue des Droits Humains s'ils sont préoccupés par l'utilisation de l'application par rapport aux activités quotidiennes des intéressés? Il va de soi que les non-utilisateurs ne peuvent pas être sanctionnés, mais ne serait-il pas souhaitable de récompenser, par exemple, l'utilisation de l'application?

M. Egbert Lachaert (Open Vld) comprend les préoccupations relatives au respect de la vie privée: son groupe a cosigné la proposition. Le texte actuel de la proposition de résolution est-il satisfaisant selon l'APD?

Étant donné que les conditions prévues dans la proposition de résolution sont très strictes, il sera très difficile de développer une application qui y sera conforme et de garantir qu'un nombre suffisant de citoyens l'utiliseront. L'alternative, c'est-à-dire le suivi des contacts physiques, ne rassure pas vraiment plus l'orateur à l'égard du respect de la vie privée: nous serons dès lors contactés téléphoniquement par différentes personnes physiques qui nous poseront toutes sortes de questions privées; ces informations seront conservées, etc. Quelle est la moins mauvaise de ces deux solutions?

M. Kris Verduyckt (sp.a.) constate que, selon M. Stevens, l'utilisation des données concernant les télécommunications est totalement anonyme alors que la professeure Degrave a fait référence aux travaux du professeur Yves-Alexandre de Montjoye, qui affirme que l'anonymat n'existe pas: qu'en est-il?

Procédera-t-on à un stockage centralisé des données? Qui, le cas échéant, possédera les données: les autorités publiques, les opérateurs de télécommunications ou une société tierce désignée à cette fin?

Quel est par ailleurs l'avis de M. Stevens à propos de la piste *open source* pour l'application?

capaciteit van bluetooth te versterken door middel van een bluetooth-versterker: zodoende zouden vele valse positieven worden gegenereerd en zouden vele mensen zich ongerust kunnen maken: wat is de mening van de expert hieromtrent?

Aan de heer Stevens vraagt de spreker vervolgens of hij van mening is dat de Oostenrijkse benadering goed is? Wat is verder zijn mening over een opensource-broncode? Vindt de heer Stevens de zogenaamde "*bug bounties*" (waarbij burgers financieel worden beloond om fouten in het systeem op te sporen) een goede benadering? Wat is de mening van de expert over de tekst van het voorstel van resolutie? Zou hij zelf de tekst van de resolutie nog verder versterken?

Ten slotte vraagt de spreker aan de vertegenwoordigers van de Liga voor Mensenrechten of zij zich geen zorgen maken omtrent het gebruik van de app ten opzichte van dagelijkse activiteiten van de betrokkenen? Uiteraard mogen niet-gebruikers niet bestraft worden maar zou het niet wenselijk zijn om bijvoorbeeld het gebruik van de app te belonen?

De heer Egbert Lachaert (Open Vld) begrijpt de bezorgdheden omtrent de privacy: zijn fractie heeft het voorstel mee ondertekend. Volstaat de huidige tekst van het voorstel van resolutie voor de GBA?

Aangezien de voorwaarden in het voorstel van resolutie heel strikt worden geformuleerd, is het heel moeilijk om een dergelijke app te ontwikkelen en ervoor te zorgen dat voldoende burgers de app ook gebruiken. Het alternatief, namelijk de fysieke *contact tracing*, stelt de spreker niet meteen meer gerust wat het privéleven betreft: we zullen worden opgebeld door verschillende fysieke personen die ons allerlei privévragen zullen stellen, deze informatie wordt opgeslagen enzovoort: wat is de minst slechte oplossing van de twee?

De heer Kris Verduyckt (sp.a) stelt vast dat volgens de heer Stevens het gebruik van telecomgegevens op een volledig anonieme manier gebeurt terwijl professor Degrave toch verwees naar het werk van professor Yves-Alexandre de Montjoye, die beweert dat anonimiteit niet bestaat. Wat is hiervan aan?

Zal worden voorzien in een centrale opslag van de gegevens? Wie zal eventueel de gegevens bezitten: de overheid, de telecomoperatoren of nog een aangestelde derde firma?

Wat is verder de mening van de heer Stevens omtrent een opensource-benadering voor de app?

S'agissant de la technologie Bluetooth, l'intervenant demande au professeur Preneel d'indiquer le temps (la durée) nécessaire pour obtenir un résultat? Est-ce possible, par exemple, lorsque des personnes en voiture attendent côte à côte à un feu rouge? On constate d'ailleurs que la fonction Bluetooth est souvent désactivée par de nombreux utilisateurs.

Il souhaite par ailleurs des précisions sur le pourcentage minimum d'utilisateurs pour qu'une telle application soit efficace. Enfin, n'est-il pas envisageable de procéder à l'actualisation d'applications des services publics existantes, comme "itsme", afin qu'elles disposent de plus de fonctionnalités; cela permettrait également de dépasser plus facilement la barre de 15 à 20 % d'utilisateurs.

Le membre demande à M. Raes si la technologie Bluetooth peut être facilement piratée? Il observe que, de plus, ce n'est pas vraiment une technologie stable, comme le savent tous ceux qui ont essayé de connecter un smartphone à une voiture par le Bluetooth.

L'intervenant attire l'attention de la Ligue des droits de l'Homme sur le fait qu'il y a, selon lui, un clivage entre les générations: les jeunes ont en effet déjà le sentiment que leurs données se trouvent un peu partout et adopteront dès lors plus facilement cette technologie. Par ailleurs, le membre craint qu'il s'agisse d'une obligation sociale, notamment de la part des employeurs.

Enfin, l'intervenant constate, comme le professeure Degrave, que les GAFAM ne sont effectivement pas des entreprises philanthropiques: comment sera-t-il possible de tenir ces entreprises à l'écart du processus? À moins que nous n'ayons besoin d'elles parce que la technologie s'appuie sur leurs systèmes …

Monsieur Nabil Boukili (PVDA-PTB) fait observer que dans un avis récent, l'autorité néerlandaise chargée des données personnelles (*Autoriteit Persoonsgegevens*, AP) indique que les données de localisation sont toujours des données personnelles. Ce qui implique que le consentement de la personne concernée doit donc être toujours demandé afin de pouvoir traiter ces informations. Toute personne qui sait où quelqu'un vit ou travaille et qui combine ces données avec les données de localisation "anonymisées" de nombreuses personnes peut utiliser cette combinaison pour déterminer à qui elles appartiennent. Il est important de souligner qu'il est impossible de rendre ce type de données anonymes, car elles ne sont jamais irréversibles. Quelle est la position de l'APD à ce sujet? Les données de localisation "anonymes" existent-elles?

L'article 35, 1, du RGPD stipule: "Lorsqu'un type de traitement, en particulier par le recours à de nouvelles

Aan professor Preneel vraagt de spreker, wat de bluetooth-technologie betreft, hoe lang (duurtijd) contact nodig is om een hit te verkrijgen? Is dit bijvoorbeeld mogelijk wanneer men naast elkaar staat te wachten in de wagen aan een rood licht? Men stelt trouwens vast dat de bluetooth-functie door veel gebruikers vaak wordt afgezet.

Daarnaast kreeg hij graag meer uitleg over het minimale gebruikerspercentage opdat een dergelijke app efficiënt zou zijn. Is het ten slotte niet denkbaar dat men overgaat tot een update van bestaande overheidsapps, zoals "itsme", zodat deze meer functionaliteiten hebben; zodoende zou men ook gemakkelijker boven de 15 tot 20 % gebruikers uitkomen.

Aan de heer Raes vraagt de spreker of de bluetooth-technologie gemakkelijk kan worden gehackt? Bovendien gaat het niet echt om stabiele technologie zoals iedereen weet die getracht heeft om zijn smartphone via bluetooth te connecteren met de wagen.

Ter attentie van de Liga voor Mensenrechten merkt de spreker op dat er volgens hem sprake is van een generatieverschil: jongeren hebben immers nu al het idee dat hun gegevens nu al overal verspreid zitten en zullen deze technologie dan ook gemakkelijker omarmen. Daarnaast vreest de spreker dat het zal gaan om een sociale verplichting, onder meer vanwege de werkgevers.

Ten slotte stelt de spreker samen met professor Degrave vast dat de GAFAM inderdaad geen filantropische instellingen zijn: op welke manier zal men deze bedrijven uit het proces kunnen weghouden? Tenzij we ze nodig hebben omdat de technologie immers draait op hun systemen…

De heer Nabil Boukili (PVDA-PTB) wijst erop dat de Nederlandse instantie die bevoegd is inzake persoonsgegevens (de Autoriteit Persoonsgegevens – AP) in een recent advies aangeeft dat locatiegegevens altijd persoonsgegevens zijn. Derhalve moet steeds de toestemming van de betrokkene worden gevraagd om die informatie te mogen verwerken. Om het even wie die weet waar iemand woont of werkt en die deze gegevens kruist met de van tal van mensen beschikbare "geanonimiseerde" locatiegegevens, kan bepalen om wiens gegevens het gaat. Het is belangrijk erop te wijzen dat dergelijke gegevens onmogelijk anoniem kunnen worden gemaakt omdat ze nooit onomkeerbaar zijn. Wat is het standpunt van de GBA daaromtrent? Bestaat er zoiets als "anonieme" locatiegegevens?

Artikel 35, 1, van de AVG luidt als volgt: "Wanneer een soort verwerking, in het bijzonder een verwerking

technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires."

Question à M Stevens: l'APD peut-elle garantir que, compte tenu de la grande importance sociale de cette discussion, ces analyses d'impact des différentes applications envisagées seront rendues publiques?

Le professeur Preneel, chef du groupe de recherche Cosic KUL, collabore au protocole DP-3T également cité dans la résolution. Le protocole DP-3T a été développé autour de l'idée d'utiliser le "BLE-RSSI" (Bluetooth *Low-Energy – Received Signal Strength Indicator)* pour déterminer à quel moment différentes personnes ont été à proximité les unes des autres sur une durée déterminée. Le principe est que la proximité d'un autre smartphone, qui utilise la même technologie, agit comme un proxy pour la transmission du coronavirus. Chaque fois que vous vous trouvez à proximité d'une personne compatible pendant un certain temps, celle-ci est stockée. Si un nombre suffisant de personnes utilisent une telle application tout au long de la journée, il serait possible de retrouver les personnes qui ont été en contact avec un patient positif au COVID-19 dans le cadre d'une stratégie de test et de suivi. La valeur ajoutée de l'application est que les personnes qui auraient été oubliées ou inconnues au patient pourraient être identifiées par cette méthode pour autant qu'elles utilisent également l'application.

M. Boukili a quelques questions fondamentales sur les prémisses sur lesquelles repose le fonctionnement du protocole et celles-ci concernent le taux d'adoption nécessaire, l'efficacité du protocole et la manière dont une large adoption d'une telle application peut changer notre société.

Pour ce qui concerne le taux d'adoption nécessaire, est-ce que le professeur Preneel peut indiquer quel est le pourcentage minimum de la population qui doit installer l'application?

Environ combien de smartphones en Belgique sont équipés du BLE, la variante spécifique du protocole Bluetooth utilisé dans ces appareils? Le site web Ars

waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Één beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.".

Vraag aan de heer Stevens: kan de GBA, in het licht van het grote maatschappelijke belang van deze discussie, waarborgen dat deze impactanalyses van de verschillende overwogen toepassingen openbaar zullen worden gemaakt?

Professor Preneel, hoofd van de onderzoeksgroep Cosic van de KUL, werkt mee aan het DP-3T protocol, dat eveneens in het voorstel van resolutie wordt vermeld. Het DP-3T protocol werd ontwikkeld rond het idee om de bluetooth *Low-Energy – Received Signal Strength Indicator* (afgekort BLE-RSSI) te gebruiken, met de bedoeling te bepalen op welk tijdstip verschillende mensen gedurende een bepaalde periode in mekaars nabijheid zijn geweest. Als principe geldt dat de nabijheid van een andere smartphone die van dezelfde technologie gebruik maakt, fungeert als een *proxy* voor de overdracht van het coronavirus. Telkens als iemand zich gedurende een bepaalde tijdspanne in de buurt van een compatibele persoon bevindt, wordt die persoon opgeslagen. Mochten voldoende mensen een dergelijke toepassing de hele dag door gebruiken dan zou het mogelijk zijn om na te gaan wie met een COVID-19-positieve patiënt in contact is gekomen als onderdeel van een test- en opvolgingsstrategie. De toegevoegde waarde van de applicatie bestaat erin dat mensen die zouden zijn vergeten of die onbekend zijn voor de patiënt, met die methode zouden kunnen worden geïdentificeerd op voorwaarde dat ook zij de applicatie gebruiken.

De heer Boukili heeft enkele fundamentele vragen omtrent de premissen waarop de werking van het protocol berust. Ze hebben betrekking op de noodzakelijke adoptiegraad, op de doeltreffendheid van het protocol en op de manier waarop een ruime aanwending van een dergelijke toepassing onze samenleving kan veranderen.

Kan professor Preneel in verband met de noodzakelijke adoptiegraad aangeven wat het minimumpercentage is van de bevolking dat de applicatie moet installeren?

Hoeveel smartphones ongeveer zijn in België uitgerust met BLE, de specifieke variant van het bij die toestellen gebruikte bluetooth-protocol? Op de webstek *Ars Technica*

Technica note que près de 60 % des smartphones dans le monde ne disposent pas de cette technologie et qu'il s'agit principalement des modèles les plus anciens et les moins chers.

L'efficacité dépend de la manière dont le BLE-RSSI peut estimer correctement les distances entre les personnes. Cette estimation est-elle précise et dépend-elle de facteurs externes tels que des obstacles peu élevés qui peuvent bloquer les signaux alors que la transmission du virus est possible, ou à l'inverse, des murs qui bloquent la transmission du virus mais qui ne sont pas remarqués dans le protocole. Combien de résultats faux positifs et faux négatifs le professeur attend-il?

Le 8 avril, le professeur Serge Vaudenay de l'EPFI à Lausanne, en Suisse, a publié une analyse du protocole DP-3T en préimpression dans laquelle il fait quelques remarques critiques sur la manière dont la technologie peut être utilisée de manière abusive. Le 21 avril, le "dépôt Github" du protocole DP-3T a publié une vue d'ensemble intitulée "Évaluation des risques en matière de confidentialité et de sécurité des systèmes de traçage numérique de proximité", dans laquelle différentes versions sont examinées. Il va sans dire qu'une analyse académique approfondie est nécessaire avant de demander à tout le monde dans la société de se promener avec une balise Bluetooth. La lecture de ces sources nous donne matière à réflexion. Est-ce que le professeur Preneel peut expliquer ce qui suit dans ce contexte?

Que signifie "*wardriving*" dans le deuxième document et est-ce que ce risque peut-être exclu dans le cadre d'un système de traçage basé sur le Bluetooth?

Peut-on exclure que les utilisateurs de toute forme de traçage Bluetooth puissent être suivis pendant un certain temps une fois qu'ils connaissent la "clé maîtresse" qui génère les "*Ephemeral IDs*"?

Est-il possible d'exclure la possibilité que les gouvernements utilisent les données de l'application, telles que le nombre de contacts sociaux que vous avez, pour vérifier si les personnes sont en quarantaine? Eventuellement après avoir donné un mandat d'accès?

Est-il possible d'exclure la possibilité que l'état de santé des personnes connues soit rendu accessible en les recherchant de manière ciblée?

Est-il possible d'exclure la possibilité que les pays ou régions où les différentes applications sont utilisées

wordt aangegeven dat wereldwijd bijna 60 % van de smartphones niet over die technologie beschikken en dat het daarbij vooral om de oudste en de goedkoopste modellen gaat.

De doeltreffendheid hangt af van de mate waarin de BLE-RSSI de afstand tussen de personen correct kan inschatten. Is die inschatting nauwkeurig en kan ze worden beïnvloed door externe factoren zoals lage obstakels die de signalen kunnen blokkeren terwijl het virus wel degelijk kan worden overgedragen? Of is het omgekeerd ook mogelijk dat muren die de overdracht van het virus tegengehouden, niet door het protocol worden opgemerkt? Hoeveel valse positieve en negatieve resultaten verwacht de professor?

Op 8 april 2020 heeft professor Serge Vaudenay van de *École polytechnique fédérale de Lausanne* in Zwitserland een voorpublicatie van een analyse van het DP-3T-protocol uitgebracht, waarbij hij enkele kritische kanttekeningen plaatst bij deze technologie, omdat ze namelijk kan worden misbruikt. Op 21 april werd op de website GitHub, waarop het DP-3T-protocol wordt gehost, een algemene beschouwing gepubliceerd, getiteld "*Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems*". Daarin werden verschillende versies onderzocht. Het spreekt voor zich dat een grondige academische analyse noodzakelijk is alvorens aan iedereen in de samenleving te vragen steeds een bluetooth-baken op zak te hebben. De lezing van die bronnen geeft stof tot nadenken. Kan professor Preneel in dat verband nadere toelichting geven bij de hierna volgende punten?

Wat betekent de term "*wardriving*" in het tweede document en kan dat risico in het raam van een op bluetooth gebaseerd traceringssysteem worden uitgesloten?

Kan worden uitgesloten dat de gebruikers van om het even welke vorm van bluetooth-tracering gedurende een bepaalde tijd kunnen worden gevolgd nadat ze de hoofdsleutel die "*Ephemeral IDs*" genereert, hebben weten te achterhalen?

Kan de mogelijkheid worden uitgesloten dat de regeringen de gegevens van de app (bijvoorbeeld het aantal sociale contacten) zullen gebruiken om te controleren of de personen in quarantaine zijn, eventueel nadat een toegangsmachtiging werd gegeven?

Kan de mogelijkheid worden uitgesloten dat de gezondheidstoestand van de personen die gekend zijn toegankelijk wordt gemaakt door ze gericht op te sporen?

Kan de mogelijkheid worden uitgesloten dat de landen en de regio's waar de verschillende apps worden gebruikt

soient également enregistrés dans l'application? Et, du point de vue de la protection de la vie privée et du principe de minimisation des informations, est-il préférable qu'une application soit développée au niveau fédéral ou au niveau des entités fédérées?

Ensuite, le ministre a déjà déclaré à plusieurs reprises que le déploiement d'une application appartient aux entités fédérées. Comme le coronavirus ne s'arrête pas à la frontière linguistique, cela signifie qu'un protocole doit être mis en place pour que les différentes applications puissent échanger des données entre elles.

Qu'est-ce que la Ligue des Droits Humains en pense? Le développement de différentes applications devant communiquer entre elles ne risque-t-il pas d'entraîner des risques supplémentaires pour leurs utilisateurs, notamment le risque de fuites dues à l'échange de données entre différentes applications?

Est-ce que la Ligue des Droits Humains craint que la crise actuelle soit utilisée pour mettre en place des mécanismes de contrôle à grande échelle qui ne seront pas supprimés progressivement après la crise?

On estime que 50 à 80 % de la population doit utiliser une telle application avant qu'elle fonctionne. L'orateur vient de demander au professeur Preneel quel devrait être ce pourcentage selon lui. En tout cas, ce pourcentage est très élevé. À titre de comparaison: 65 % des Belges ont un profil Facebook, moins de gens ont l'application Facebook sur leur portable. Le ministre De Backer lui-même a souligné qu'en Autriche, la Croix-Rouge a fait beaucoup de publicité pour une application COVID-19 et que seuls 3 à 4 % de la population utilisent efficacement l'application.

Outre le fait qu'une grande partie de la population pourrait ne pas vouloir utiliser une application corona, le membre souligne que tout le monde ne possède pas un smartphone. En particulier, les personnes âgées, les enfants ou les personnes en situation de pauvreté.

Qu'est-ce que la Ligue pense de l'accessibilité d'une application? Est-ce qu'il n'y a pas de risque d'effet Matthieu, laissant de côté précisément les personnes vulnérables qui en ont le plus besoin?

Finalement, l'orateur pose une question à M. Raes: les experts nous disent que la technologie Bluetooth est facile à pirater. Quelles sont les conditions requises pour qu'un système protège utilement son intégrité? Un smartphone commercial répond-il à ces exigences?

ook in de app worden geregistreerd? Uit het oogpunt van de bescherming van de persoonlijke levenssfeer en van het beginsel van gegevensminimalisatie rijst ten slotte de vraag of een app bij voorkeur op het federaal niveau dan wel op deelstaatniveau dient te worden ontwikkeld.

Voorts heeft de minister al meermaals verklaard dat de uitrol van een app een bevoegdheid van de deelstaten is. Aangezien het coronavirus niet stopt aan de taalgrens, betekent zulks dat een protocol moet worden ingesteld opdat de diverse apps onderling gegevens zouden kunnen uitwisselen.

Wat denkt de *Ligue des Droits Humains* daarvan? Dreigt de ontwikkeling van diverse apps die onderling moeten communiceren geen bijkomende risico's voor de gebruikers ervan met zich te brengen, in het bijzonder het risico op lekken ten gevolge van de gegevensuitwisseling tussen verschillende applicaties?

Vreest de *Ligue des Droits Humains* dat de huidige crisis zal worden aangewend om middelen voor grootschalige controle in te zetten die na de crisis niet geleidelijk zullen worden afgeschaft?

Opdat een dergelijke app zou werken, moet ze naar schatting door 50 tot 80 % van de bevolking worden gebruikt. De spreker heeft professor Preneel gevraagd hoe hoog dat percentage volgens hem moet zijn. Het is in elk geval heel hoog. Ter vergelijking: 65 % van de Belgen heeft een Facebookprofiel, maar het aantal gebruikers met de Facebook-app op hun gsm ligt lager. Minister De Backer heeft zelf benadrukt dat in Oostenrijk het Rode Kruis veel reclame voor een COVID-19-app heeft gemaakt, maar dat slechts 3 tot 4 % van de bevolking de app doeltreffend gebruikt.

Het lid benadrukt dat het niet alleen zou kunnen dat een groot deel van de bevolking de corona-app niet wenst te gebruiken, maar dat bovendien niet iedereen over een smartphone beschikt. De spreker denkt daarbij in het bijzonder aan de ouderen, aan de kinderen of aan de mensen in armoede.

Wat denkt de *Ligue des Droits Humains* over de toegankelijkheid van een app? Dreigt er geen Mattheuseffect te ontstaan, waarbij precies de kwetsbare personen die ze het meest nodig hebben uit de boot vallen?

Tot slot heeft de spreker een vraag voor de heer Raes. De deskundigen geven aan dat de bluetooth-technologie gemakkelijk gehackt kan worden. Welke voorwaarden moeten vervuld zijn zodat een systeem de integriteit ervan terdege beschermt? Voldoet een commerciële smartphone aan die vereisten?

Mme Catherine Fonck (cdH) aborde d'abord la question de la faisabilité de l'application: est-il possible de fournir un calendrier concernant la disponibilité d'une application de ce type en Belgique?

S'agissant de la question de l'efficacité, elle demande s'il est possible de fournir une projection de la capacité de dépistage nécessaire pour qu'une telle application puisse apporter toute sa plus-value.

En effet, il a été rapporté dans la presse qu'au moins 60 % de la population devrait installer l'application: quelle est la validité scientifique de ce chiffre et s'agit-il d'un pourcentage de la population générale ou des personnes qui présentent des symptômes? Ce pourcentage est-il un ordre de grandeur isolé ou doit-il être considéré en combinaison avec le *tracing* manuel?

Elle s'adresse ensuite aux membres de la *Task Force* "*Data & Technology Against Corona*": peuvent-ils indiquer si le gouvernement a déjà travaillé ou non à l'élaboration d'une base juridique pour ces applications?

Il existe certes déjà un cadre légal, notamment sur la protection de la vie privée et la prophylaxie des maladies transmissibles, qui s'inscrit dans un cadre sanitaire européen global. Mais n'est-il pas également nécessaire de prévoir une base légale pour la participation des 2 000 traceurs de contact, qui ne sont pas soumis au secret médical et qui présentent donc chacun des risques individuels en termes de respect de la vie privée des citoyens? L'intervenante donne l'exemple de fichiers Excel qui seraient accessibles à ces 2 000 participants: cela ne pose-t-il pas un risque d'atteinte à la vie privée au moins aussi grand que l'installation d'applications de suivi strictement réglementées?

La Commission nationale française de l'informatique et des libertés (CNIL), composée d'experts en matière de respect de la vie privée, a ouvert la porte à une application de ce type le week-end dernier: quelle est l'attitude des experts vis-à-vis de l'avis donné à ce sujet par la CNIL qui, en substance, ne voit pas d'ingérence dans la vie privée, dans l'application proposée, dès lors que son utilisation n'est pas imposée? (*https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid*).

Enfin, la membre se demande si les critiques très inquiétantes sur le rôle des GAFAM dans ce dossier sont toujours pertinentes dès lors que, techniquement, ils ne libèrent que le Bluetooth et donnent, de plus, pour la première fois, accès à leurs codes. En outre, Google ne créerait pas d'application mais remplirait seulement le rôle d'interface.

Mevrouw Catherine Fonck (cdH) gaat vooreerst in op de haalbaarheid van de operatie: is het mogelijk om een timing te verstrekken met betrekking tot de beschikbaarheid van een dergelijke app in België?

Wat daarnaast de efficiëntie betreft vraagt zij of het mogelijk is om een projectie te geven van de noodzakelijke testcapaciteit opdat een dergelijke app zijn volledige meerwaarde zou kunnen realiseren.

Men heeft inderdaad in de pers vernomen dat minstens 60 % van de bevolking de app zou moeten installeren: welke is de wetenschappelijke validiteit van dit cijfer en gaat het hier een percentage van de algemene bevolking of van diegenen die symptomen vertonen? Is deze 60 % een op zichzelf staande grootheid of moet dit percentage worden gezien in combinatie met manuele *tracing*?

Vervolgens richt zij zich tot de leden van de taskforce "*Data & Technology Against Corona*"*:* kunnen zij zeggen of de regering al heeft gewerkt rond een wettelijke basis voor deze apps of is zulks niet het geval?

Verder bestaat er uiteraard al een wettelijk kader, onder meer de wetgeving op de privacy en op de profylaxis van besmettelijke ziekten, die zich situeert in een globaal Europees sanitair kader. Is het niet nodig om daarnaast ook een wettelijke basis te voorzien voor de participatie van de 2 000 *contact tracers* die niet onderworpen zijn aan het medisch beroepsgeheim en die daardoor elk een individueel risico vormen voor de privacy van de burgers? De spreekster geeft het voorbeeld van Excelbestanden die toegankelijk zouden zijn voor deze 2 000 deelnemers: levert dit niet op zijn minst even grote risico's voor inbreuken op de privacy als de installatie van strikt gereglementeerde *tracing* apps?

De Franse CNIL, die bestaat uit experten inzake privacy, heeft het afgelopen weekend de deur geopend voor een dergelijke applicatie: wat is de houding van de experten ten opzichte van het advies dat de CNIL hieromtrent heeft verstrekt, dat ten gronde geen inbreuken op het privéleven ziet in de voorgestelde applicatie, aangezien het gebruik ervan niet wordt opgelegd? (*https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid*).

Ten slotte vraagt het lid zich af of de zeer verontrustende kritieken op de rol van de GAFAM in dit dossier nog wel pertinent zijn mits zij op technisch vlak enkel bluetooth zouden vrijgeven en bovendien voor het eerst ooit toegang geven tot hun codes; bovendien maakt Google zelf geen app maar vervult het enkel de rol van interface.

Mme Sophie Rohonyi (DéFI) souhaite tout d'abord poser quelques questions à MM. Stevens et Raes. On a appris que les centres d'appel auront besoin de 2 000 collaborateurs pour le suivi des contacts. Où en est le recrutement à cet égard? De qui s'agira-t-il? Quelles sont les exigences en matière de diplômes? Une formation spécifique est-elle prévue?

Il se murmure que les mutuelles vont pouvoir répondre à l'appel d'offres de l'autorité fédérale, compte tenu de leur expérience en matière de dossiers médicaux confidentiels. Est-ce exact et cela offre-t-il des garanties suffisantes en termes de respect de la vie privée?

En ce qui concerne le rôle des entités fédérées, en particulier des Régions, l'intervenante demande quelle Région sera compétente par example à l'égard d'une personne qui travaille à Bruxelles, qui y a ses contacts, mais qui est domiciliée en Flandre ou en Wallonie? Ou s'agira-t-il d'un centre d'appel unique cofinancé par les trois régions?

En ce qui concerne le rôle de l'Union européenne, la membre demande comment une harmonisation minimale entre les États membres peut être assurée dans le respect de la vie privée. Que pensent les experts des recommandations de l'Union européenne en la matière? Par l'intermédiaire de la KUL, 130 chercheurs participent à un projet européen visant à mettre au point une norme européenne permettant aux applications mobiles de fonctionner au-delà des frontières. Qu'en pensent les experts?

Le traçage doit par ailleurs aller de pair avec un dépistage massif, mais compte tenu des problèmes qui se sont posés dans les maisons de repos ainsi que dans les hôpitaux et auprès des personnes présentant des symptômes, on peut émettre certains doutes. Quid de la liberté du médecin de procéder à un test ou à la mise en quarantaine? Le médecin disposera-t-il encore d'une marge d'appréciation?

Qu'est-ce qui garantit que l'on pourra continuer à empêcher que l'intéressé puisse savoir qui l'a contaminé?

De quelle manière peut-on éviter que des données soient sauvegardées avant leur suppression automatique?

Compte tenu du caractère sensible des données médicales, tant le RGPD que la législation relative à la protection de la vie privée disposent que ces données ne peuvent être traitées que par des personnes soumises au secret médical. Ces opérations de traçage pourront-elles se dérouler sans le contrôle d'une personne soumise au secret médical?

Mevrouw Sophie Rohonyi (DéFI) wenst eerst enkele vragen te stellen aan de heren Stevens en Raes. Er werd vernomen dat de callcenters 2 000 medewerkers zouden nodig hebben voor contact tracing: hoe ver is men gevorderd met de aanwerving van de betrokkenen? Over wie gaat het? Welke zijn de diplomavereisten? Wordt een specifieke vorming voorzien?

Er wordt gefluisterd dat de mutualiteiten zouden ingaan op de offerteaanvraag van de federale overheid gezien hun ervaring met confidentiële medische dossiers: is dit correct en biedt dit voldoende garanties op het vlak van de bescherming van het privéleven?

Wat de rol van de gefedereerde entiteiten en met name de gewesten betreft vraagt de spreekster welk gewest bijvoorbeeld bevoegd zou zijn indien het gaat om een persoon die werkzaam is in Brussel en daar zijn contacten heeft maar gedomicilieerd is in Vlaanderen of in Wallonië? Of zou het gaan om één enkel callcenter dat door de drie gewesten samen wordt gefinancierd?

Wat de rol van de Europese Unie aangaat vraagt het lid hoe een minimale harmonisatie tussen de lidstaten kan worden voorzien met respect voor het privéleven? Wat is de mening van de experten over de aanbevelingen van de Europese Unie in deze materie? 130 onderzoekers nemen via de KUL deel aan een Europees project met het oog op het op punt stellen van een Europese standaard opdat de app over de grenzen heen zou werken: wat is de mening van de experten hieromtrent?

De tracering dient verder gepaard te gaan met massaal testen, maar gezien de problemen die zich hebben voorgedaan in de woonzorgcentra alsook in de ziekenhuizen en bij de mensen met symptomen kan men hierbij toch bedenkingen hebben: wat met de vrijheid van de arts om over te gaan tot een test of tot quarantaine: zal er morgen nog sprake zijn van een appreciatiemarge voor de betrokken arts?

Welke garantie bestaat er verder dat kan worden verhinderd dat de betrokkene kan zien wie hem of haar heeft besmet?

Op welke manier kan verder worden vermeden dat gegevens worden opgeslagen vooraleer ze "uitdoven"?

Gezien het gevoelig karakter van medische gegevens preciseren zowel de AVG als de privacywetgeving dat deze gegevens enkel kunnen worden gemanipuleerd door personen die onderworpen zijn aan een medisch beroepsgeheim: zullen deze traceringsoperaties kunnen verlopen zonder toezicht van een persoon die onder het medisch geheim valt?

L'intervenante, renvoyant au professeur Preneel, fait observer que les signaux Bluetooth peuvent avoir une force différente selon que l'appareil se trouve par exemple dans une poche ou dans la main de la personne. Cet élément n'entraîne-t-il pas un risque de faux positifs et de faux négatifs?

Renvoyant à la professeure Degrave, l'intervenante indique qu'elle comprend les réserves relatives aux GAFAM, mais quelle autre solution y a-t-il?

M. Gilles Vanden Burre (Ecolo-Groen) souligne, à l'intention de M. Stevens, que l'application mobile doit être considérée au regard de différents groupes cibles. La fracture numérique étant très importante en Belgique, l'utilisation de la technologie est beaucoup moins évidente – comme l'illustre l'accès aux smartphones et leur détention par les malades et les personnes âgées – dans les groupes marginalisés ou pour les enfants. Comment éviter de favoriser ainsi certaines catégories de citoyens?

L'intervenant demande par ailleurs des recommandations concrètes en ce qui concerne le traçage manuel. Des garanties spécifiques sont-elles nécessaires au sujet, par exemple, de la confidentialité ou de la durée de stockage maximale de certaines données?

Mme Kathleen Verhelst (Open Vld) s'enquiert de la probabilité que l'on parvienne effectivement à mettre au point une application mobile, compte tenu des considérations formulées en matière de participation, de respect de la vie privée, de coûts, de risques, etc.?

Est-il possible de fournir une estimation du coût total du déploiement de cette application? Le rendement global du projet a-t-il été évalué?

Sommes-nous soumis à des pressions internationales qui nous invitent à participer à une initiative européenne?

Qu'adviendra-t-il s'il apparait *a posteriori* que l'application n'est guère utile mais qu'entre-temps, beaucoup de protections ont été abandonnées en termes de respect de la vie privée?

Il est par ailleurs très positif de travailler à la fois sur les aspects technologiques, juridiques et de sécurité, mais nous sommes tellement concentrés sur la conception des dimensions technologiques et juridiques que nous risquons de définir d'ores et déjà la société de demain avant même d'avoir organisé d'avoir un débat social à ce sujet. Ne pourrions-nous pas attendre les résultats des autres pays, et organiser, dans l'intervalle, un débat de fond à ce sujet?

Ter attentie van professor Preneel merkt de spreekster op dat bluetooth-signalen een verschillende sterkte kunnen hebben naargelang bijvoorbeeld het toestel zich in de jaszak of een hand van de betrokkene bevindt: bestaat hierdoor niet het risico op valse positieven en valse negatieven?

Ter attentie van professor Degrave begrijpt de spreekster de reserves wat de GAFAM betreft, maar wat is het alternatief?

De heer Gilles Vanden Burre (Ecolo-Groen) merkt op, ter attentie van de heer Stevens, dat men de app dient te situeren ten opzichte van verschillende doelgroepen: aangezien de digitale kloof in België heel groot is, is dit heel wat minder vanzelfsprekend, wat blijkt uit de toegang tot en het bezit van smartphones bij zieken en bejaarden, in gemarginaliseerde groepen alsook voor kinderen: hoe zal men vermijden dat bepaalde categorieën van burgers hier worden bevoordeeld?

Daarnaast vraagt de spreker naar concrete aanbevelingen met betrekking tot de manuele tracering: zijn specifieke waarborgen nodig met betrekking tot bijvoorbeeld vertrouwelijkheid of maximum opslagduur van bepaalde gegevens?

Mevrouw Kathleen Verhelst (Open Vld) vraagt hoe groot de kans is dat men werkelijk tot een app komt, wanneer men rekening houdt met overwegingen inzake participatie, privacy, kosten, risico's, enzovoort?

Is het mogelijk om een inschatting te geven van de volledige kostprijs van de uitrol van een dergelijke app? Werd het rendement van dit hele opzet nader bekeken?

Is er sprake van internationale druk om mee te doen met een Europees initiatief?

Wat als achteraf zou blijken dat de app toch niet echt nuttig is maar ondertussen toch veel privacy zou zijn opgegeven?

Het is verder een zeer goede zaak dat men zowel op technologisch, juridisch als veiligheidsvlak tegelijk aan het werk is, maar men is zodanig bezig met het uitwerken van de technologische en juridische aspecten dat het risico bestaat dat we nu al de maatschappij van de toekomst gaan bepalen in plaats van vooraf een maatschappelijk debat te voeren. Zou men niet kunnen wachten op de resultaten van andere landen en ondertussen een grondig debat voeren?

Ne pourrait-on pas faire en sorte que cette application soit également mutuellement avantageuse pour le citoyen et bénéficie dès lors d'une plus large adhésion?

Mme Katleen Bury (VB) évoque le cadre légal. La Ligue des droits de l'Homme a parlé d'un conflit d'intérêts dans le cas où un membre de la *task force* émettrait également un avis par la suite. Qu'en est-il?

Comment la vie privée sera-t-elle préservée? Comment les données seront-elles rendues anonymes? Ne s'agira-t-il pas plutôt d'un pseudo-anonymat qui n'empêchera pas de retracer ultérieurement l'identité de la personne? La membre n'a en effet aucun mal à imaginer que les compagnies d'assurance, par exemple, seront très intéressées de savoir qui a été malade puisque cette maladie a un impact sur presque tous les organes humains.

IV. — **RÉPONSES DES ORATEURS**

M. Jaak Raes (VSSE) constate que beaucoup de questions ont trait à la technologie Bluetooth et en particulier au risque de voir celle-ci détournée dans le but de soustraire illégalement des données de sécurité aux détenteurs d'appareils Bluetooth.

L'orateur répète que le père spirituel de cette technologie a pris la plume cette semaine pour en expliquer les limites. Le Bluetooth suscite des attentes importantes. Bien que de nombreuses personnes disposent d'un smartphone équipé de cette technologie, il ne s'agit souvent pas de la version la plus récente pourvue d'une nouvelle radio qui permet d'évaluer les distances de façon très précise.

La Sûreté de l'État estime que la technologie Bluetooth actuellement utilisée par la plupart des appareils est susceptible d'être piratée et qu'elle n'offre donc pas une garantie de sécurité absolue. Les applications les plus modernes peuvent éventuellement être plus performantes à cet égard. On peut bien entendu réduire les risques en évitant de lier des données à caractère personnel aux radios Bluetooth, mais cela rendra le *tracing* individuel prévu dans la lutte contre le coronavirus impossible. Il convient donc de limiter autant que possible l'échange d'autres données à caractère personnel ou d'enregistrer celles-ci le cas échéant sur un autre serveur.

La Sûreté de l'État n'est pas compétente pour la désignation des *contact tracers*. Les citoyens doivent pouvoir être certains que les informations communiquées seront traitées correctement. L'orateur trace un parallèle avec les personnes qui travaillent au sein des services de renseignement et qui sont, elles aussi, potentiellement

Kan men er niet voor zorgen dat deze app ook andere *win-win*-aspecten oplevert voor de burger en op die manier ook meer gedragen zal zijn?

Mevrouw Katleen Bury (VB) gaat in op het wettelijk kader: de Liga voor Mensenrechten sprak van een belangenconflict indien een lid van de taskforce achteraf ook een advies uitbrengt: wat is hiervan aan?

Op welke manier zal de privacy worden gewaarborgd? Hoe zullen de gegevens worden geanonimiseerd? Gaat het niet eerder om een pseudo-anonimiteit waarbij men achteraf alsnog kan traceren over wie het gaat? Het lid kan zich immers perfect inbeelden dat bijvoorbeeld verzekeringsinstellingen zeker interesse zullen tonen om te weten wie ziek is geweest, aangezien de ziekte een impact heeft op nagenoeg alle menselijke organen.

IV. — **ANTWOORDEN VAN DE SPREKERS**

De heer Jaak Raes (VSSE) stelt vast dat vele vragen betrekking hebben op de bluetooth-technologie, in het bijzonder het risico dat deze zou worden misbruikt om op illegale wijze veiligheidsgegevens te ontfutselen aan de houder van een bluetooth-apparaat.

De spreker herhaalt dat de geestelijke vader van deze technologie eerder deze week in de pen klom om de grenzen ervan toe te lichten. De verwachtingen omtrent bluetooth zijn hooggespannen. Hoewel zeer veel mensen beschikken over een smartphone die is uitgerust met bluetooth-technologie, gaat het veelal niet om de modernste versie met een nieuwe radio die toelaat om zeer nauwkeurig afstanden in te schatten.

De Staatsveiligheid meent dat de bluetooth-technologie zoals die thans wordt gebruikt door de meeste toestellen, vatbaar is voor hacking en dus geen absolute veiligheidsgarantie biedt. De modernste applicaties kunnen eventueel meer veiligheidswaarborgen bieden. Men kan uiteraard op veilig spelen door de koppeling tussen persoonsgegevens en bluetooth-radio's te vermijden, maar op die manier maakt men ook de individuele tracing ter bestrijding van de coronacrisis onmogelijk. De aanbeveling is dus om zo weinig mogelijk andere persoonsgebonden informatie uit te wisselen of deze eventueel op te slaan op een server.

De Staatsveiligheid is niet bevoegd inzake de aanstelling van de *contact tracers*. Burgers moeten erop kunnen vertrouwen dat de meegedeelde informatie op een correcte wijze zal worden behandeld. De spreker trekt een parallel met mensen die werken binnen de inlichtingendiensten, die evenzeer potentieel kwetsbaar

vulnérables. Il faut pouvoir accorder sa confiance, mais il faut aussi pouvoir la retirer dès le premier signe d'abus. Eu égard à la présence d'un facteur humain, il n'est pas absolument exclu que des informations sensibles soient un jour utilisées de façon inappropriée dans le cadre du *contact tracing*. Mais ce risque peut être minimisé grâce à certaines mesures de sécurité, comme l'interdiction faite aux *contact tracers* d'emporter les informations recueillies en dehors de leur lieu de travail.

M. Freilich a évoqué le risque d'espionnage. L'orateur renvoie à cet égard à ce qu'il a expliqué devant cette commission au cours de l'audition relative au déploiement de la technologie 5G (DOC 55 0981/001, p. 12). Il avait indiqué à l'époque que dans ce domaine, les services de sécurité ont une approche géostratégique de l'analyse des risques, qui tient compte d'un certain nombre de caractéristiques du pays dont provient la technologie. Les critères appliqués en l'espèce sont les suivants: le caractère potentiellement autoritaire du pays d'origine du fournisseur; la mesure dans laquelle un fournisseur peut agir indépendamment de son autorité nationale (les opérations commerciales du fournisseur concerné sont-elles indépendantes des préoccupations et/ou des ingérences nationales?); l'existence et l'application d'une législation nationale qui donne à un État (non membre de l'UE) une emprise sur les entreprises et la mesure dans laquelle cette législation est compatible avec la législation de l'UE; l'indépendance de l'ordre judiciaire dans le pays en question (à défaut de quoi les services peuvent par exemple être contraints de commettre des infractions); la publicité des opérations commerciales et la mesure dans laquelle des facteurs tels que des aides d'État (cachées) ou une direction d'entreprise ou un actionnariat non transparents perturbent le fonctionnement normal du marché. M. Raes estime que ces critères s'appliquent *mutatis mutandis* à la technologie Bluetooth.

M. Raes indique en conclusion qu'il existe un risque de piratage et que pour réduire celui-ci au maximum, il s'indique d'échanger le moins possible de données à caractère personnel et surtout d'enregistrer celles-ci sur un serveur. La Sûreté de l'État n'est pas opposée au développement d'une application visant à lutter contre le coronavirus, à condition qu'il soit suffisamment tenu compte des aspects sécuritaires. Notre pays ne peut pas manquer ce rendez-vous, d'autant que nous serons sans doute confrontés dans le futur à une recrudescence du virus.

M. David Stevens (APD) estime qu'il est parfaitement possible de cumuler la qualité de membre de la *task force* et de président de l'APD sans qu'il soit question de confusion d'intérêts. L'orateur illustre son propos par

zijn. Men moet vertrouwen kunnen schenken, maar bij het eerste signaal van wangedrag moet dat vertrouwen ook kunnen worden ingetrokken. Er is een menselijke factor in het spel, dus het valt niet absoluut uit te sluiten dat er ooit ongepast gebruik zou worden gemaakt van gevoelige informatie in het kader van contact tracing. Maar dat risico kan worden geminimaliseerd door bepaalde veiligheidsmaatregelen, zoals het verbod voor *contact tracers* om de verkregen informatie mee te nemen buiten de werkplek.

De heer Freilich verwees naar de mogelijke dreiging van spionage. In dit verband herinnert de spreker aan de uiteenzetting die hij gaf in deze commissie tijdens de hoorzitting over de uitrol van 5G-technologie (DOC 55 0981/001, blz. 12). Hij legde toen uit dat de veiligheidsdiensten de risicoanalyse in dat verband geostrategisch benaderen, rekening houdend met een aantal karakteristieken van het land waaruit de technologie afkomstig is. Er worden daarbij met name de volgende criteria gehanteerd: het mogelijk autoritaire karakter van het land van afkomst van de leverancier; de mate waarin een leverancier zich onafhankelijk kan opstellen ten opzichte van zijn nationale overheid (staat de bedrijfsvoering van de betrokken leverancier los van nationale bekommeringen en/of inmenging?); het bestaan en de toepassing van nationale wetgeving die een (niet-EU-)Staat greep geeft op bedrijven, en de mate waarin die compatibel is met EU-wetgeving; de onafhankelijkheid van de gerechtelijke werking in het land in kwestie (bij gebreke waarvan diensten bijvoorbeeld kunnen verplicht worden inbreuken te plegen); en ten slotte de openheid van bedrijfsvoering en de mate waarin factoren zoals (verdoken) overheidssteun of niet-transparante bedrijfsleiding of aandeelhouderschap een normale marktwerking verstoren. De heer Raes is van mening dat deze criteria *mutatis mutandis* van toepassing zijn op bluetooth-technologie.

Tot besluit van zijn betoog stelt de heer Raes dat het risico op hacking bestaat en dat het, om dat risico maximaal te beperken, aanbeveling verdient zo weinig mogelijk persoonsgegevens uit te wisselen en deze vooral op te slaan op een server. De Veiligheid van de Staat is niet tegen de ontwikkeling van een app ter bestrijding van het coronavirus, gesteld dat er voldoende oog is voor de veiligheidsaspecten. Ons land mag deze boot missen, niet het minst omdat we in de toekomst wellicht zullen worden geconfronteerd met nieuwe opstoten.

De heer David Stevens (GBA) is van oordeel dat er geenszins sprake is van belangenvermenging bij het gelijktijdig uitoefenen van de functies van lid van de taskforce en voorzitter van de GBA. Hij illustreert dit

un exemple. Toutes les applications liées au coronavirus doivent être agréées par la *task force* avant d'être proposées sur *Google Play* ou sur l'*App Store*. Pour obtenir cet agrément – une sorte d'autorisation – l'application doit réussir un test préliminaire rapide réalisé par la *task force*. Des dizaines de tests ont ainsi déjà été effectués. L'orateur indique que ce contrôle est très performant. Les applications qui présentent des failles importantes en matière de vie privée sont écartées. Si l'APD ne faisait pas partie de la *task force*, des applications de ce type seraient commercialisées et l'APD exercerait son contrôle régulier, mais elle serait contrainte de le faire *a posteriori*. Le test préliminaire, qui n'entraîne pas d'approbation formelle, constitue une forme de *privacy by design.* M. Stevens est heureux de faire partie de la *task force*, au sein de laquelle il veille à garantir la protection de la vie privée. Il n'y a donc pas de confusion d'intérêts et il n'y en aura pas davantage si l'APD devait, dans une phase ultérieure, rendre un avis ou réaliser une analyse d'impact relative à la protection des données concernant une application précédemment soumise à un test.

L'APD peut bel et bien contrôler des applications à l'étranger, même si c'est plus compliqué que dans un contexte national. Le RGPD contient des règles à cet effet. La question pertinente est de savoir où se trouve le principal établissement de celui qui est responsable du traitement. Pour les applications axées sur la Belgique, l'APD peut être compétente et est en tout cas concernée, et elle prendra contact avec son homologue dans le pays où est localisé l'établissement principal de celui qui propose l'application. Dans le cadre de l'application "corona", cette question de compétence jouera sans doute un rôle moins important, vu que l'on créera un cadre légal dont la territorialité pourra faire partie.

L'orateur confirme qu'une expertise spécialisée suffisante est disponible au sein de l'APD. En interne, l'APD compte cinq ingénieurs ICT, qui sont associés activement à ce dossier. Par ailleurs, l'APD peut également s'appuyer sur douze experts externes, six au sein de la Chambre contentieuse et six au sein du Centre de connaissances, notamment le professeur Preneel et le professeur de Montjoye.

Faut-il se baser sur la même logique pour le traçage manuel que pour les applications de suivi des contacts? La réponse est nuancée. Les mêmes principes, à savoir ceux relatifs à la protection de la vie privée, sont pertinents, comme la transparence, la minimalisation, le *privacy by design,* etc. Une différence fondamentale est cependant que, dans la variante manuelle, une contamination a été constatée et on vise une relation de personne à personne (également avec les personnes avec lesquelles la personne contaminée a eu des contacts),

aan de hand van een voorbeeld. Alle apps die te maken hebben met het coronavirus hebben een toezegging nodig vanwege de taskforce alvorens ze op Google Play of de App Store mogen terechtkomen. Die toezegging, een soort machtiging, volgt op het succesvol ondergaan van een snelle, preliminaire test door de taskforce. Tientallen tests werden zo al uitgevoerd. Volgens de spreker is deze check een uitstekende zaak. Apps die ernstige privacy-gebruiken vertonen worden eruit gefilterd. Mocht de GBA geen deel uitmaken van de taskforce, zouden zulke apps op de markt komen en zou de GBA haar reguliere toezicht uitoefenen, doch men zou noodgedwongen achter de feiten aanhollen. De preliminaire test, die geen formele goedkeuring inhoudt, is in wezen een manifestatie van *privacy by design.* De heer Stevens is dan ook verheugd deel uit te maken van de taskforce, waar zijn enige bekommernis de bescherming van de privacy is. Van enige belangenvermenging is dus geen sprake, ook niet wanneer de GBA in een later fase een advies of een gegevensbeschermingseffectbeoordeling zou dienen uit te brengen over een app die eerder een test onderging.

De GBA kan wel degelijk toezicht uitoefenen op apps in het buitenland, zij het dat dit moeilijker is dan in een nationale context. De AVG bevat daaromtrent regels. De relevante vraag is waar de belangrijkste vestiging zich bevindt van degene die verantwoordelijk is voor de verwerking. Voor apps die zich op de België richten is de GBA mogelijk bevoegd en in ieder geval betrokken, en zal zij contact nemen met haar tegenhanger in het land waar de hoofdvestiging van de app-aanbieder gelokaliseerd is. In het kader van de corona-app zal die bevoegdheidskwestie wellicht minder spelen, nu hiervoor een wettelijk kader zal worden geschapen waarvan de territorialiteit deel kan uitmaken.

De spreker bevestigt dat er binnen de GBA voldoende gespecialiseerde expertise voorhanden is. Intern telt de GBA vijf ICT-ingenieurs in haar rangen, die actief worden betrokken bij dit dossier. Daarnaast kan de GBA ook bogen op twaalf externe experten, zes in de Geschillenkamer en zes in het Kenniscentrum, waaronder professor Preneel en professor de Montjoye.

Dient voor manuele tracing dezelfde logica te gelden als voor de tracing apps? Het antwoord is genuanceerd. Dezelfde principes, met name op het vlak van privacy, zijn relevant, zoals transparantie, minimalisatie, *privacy by design* enzovoort. Een fundamenteel verschil is echter dat er bij de manuele variant een besmetting werd vastgesteld en er een één-op-één-relatie wordt beoogd (ook met de personen met wie de besmette persoon in contact is geweest), daar waar het er bij de app om draait om op een zo anoniem mogelijke wijze contacten tussen

alors que, dans le cas de l'application, il s'agit d'enregistrer des contacts entre personnes d'une manière aussi anonyme que possible. Ce type d'application n'est pas la panacée. Il s'agit d'une tentative de soutenir le traçage manuel des contacts de manière judicieuse. Le traçage des contacts manuel et automatisé doit être considéré comme complémentaire, la répartition des compétences étant réglée en ce sens que la première forme doit être organisée au niveau régional.

M. Stevens répond à la question visant à savoir si le cadre légal est efficace que, conformément aux recommandations européennes, il faut viser un intérêt général, ce qui requiert une base légale. L'orateur ne se prononce pas quant à savoir s'il doit s'agir d'une loi ou d'un arrêté royal. On ne peut en aucun cas se contenter d'un simple consentement, ce qui permettrait à certaines grandes entreprises technologiques de lancer la même application.

L'orateur indique qu'il est en effet toujours associé au Comité européen de la protection des données (*European Data Protection Board* ou EDPB), qui rassemble les représentants des autorités nationales de protection des données de l'UE. L'APD a d'ailleurs collaboré très activement à l'élaboration des recommandations européennes.

Selon M. Stevens, on ne peut exclure que, sur le site internet de la Taskforce, certaines applications énumérées ne satisfassent pas entièrement aux obligation du RGPD. La Taskforce se limite en effet à un screening préliminaire des applications, qui n'est pas suivi d'une approbation formelle; il est impossible, en quelques semaines, de soumettre des dizaines d'applications à une analyse approfondie du respect des conditions liées à la protection de la vie privée. Cette mission limitée est d'ailleurs aussi explicitement mentionnée sur le site internet. Il est possible – et ce n'est absolument pas problématique d'un point de vue éthique ou déontologique – que la Chambre contentieuse doive se pencher, à un stade ultérieur, sur une application mentionnée sur le site internet.

Comme l'a fait remarquer à juste titre M. Gilissen, il règne chez les citoyens une certaine inquiétude concernant les fuites de données et les violations de la vie privée dans le cadre des applications de suivi des contacts. Selon M. Stevens, c'est normal et c'est même une bonne chose que cette question fasse l'objet d'un débat de société, y compris au sein de cette commission. Il se réjouit d'ailleurs que l'on ait tenu compte, dès le début de cette initiative, des préoccupations en matière de respect de la vie privée. L'ensemble des compétences du ministre concerné n'y est sans doute pas étranger.

personen te registreren. Zo'n app is geen wondermiddel. Het is een poging om de manuele contact tracing zinvol te ondersteunen. Manuele en geautomatiseerde contact tracing moeten als complementair worden beschouwd, waarbij de bevoegdheidsverdeling derwijze geregeld is dat die eerste vorm op gewestelijk niveau moet worden georganiseerd.

Op de vraag of het wettelijk kader afdoende is, antwoordt de heer Stevens dat, conform de Europese aanbevelingen, er een algemeen belang dient te worden nagestreefd, wat een wettelijke basis vereist. De spreker laat in het midden of dat een wet dan wel een genummerd KB dient te zijn. In geen geval mag worden volstaan met een loutere toestemming, wat bepaalde grote technologiebedrijven zou toelaten om dezelfde app te gaan lanceren.

De spreker geeft aan inderdaad nog steeds betrokken te zijn bij het Europees Comité voor Gegevensbescherming (*European Data Protection Board* of EDPB), waarin de vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten in de EU zijn vertegenwoordigd. De GBA heeft overigens zeer actief meegewerkt aan uitwerking van de Europese richtlijnen.

Volgens de heer Stevens valt het niet uit te sluiten dat op de website van de taskforce apps staan opgelijst die niet volledig beantwoorden aan de verplichtingen van de AVG. De taskforce beperkt zich immers tot een preliminaire *screening* van de apps, waarop geen formele goedkeuring volgt; het is niet mogelijk om binnen het tijdsbestek van enkele weken tientallen apps aan een grondige analyse van de privacyvoorwaarden te onderwerpen. Deze beperkte missie staat overigens ook expliciet vermeld op de website. Het is mogelijk – en vanuit ethisch of deontologisch oogpunt geenszins problematisch – dat de Geschillenkamer zich in een later stadium zou dienen te buigen over een op de website vermelde app.

Zoals de heer Gilissen terecht opmerkte, heerst er bij de burgers enige bezorgdheid over datalekken en schendingen van de privacy in het kader van de tracing apps. Volgens de heer Stevens is dit normaal en is het zelfs een goede zaak dat hieromtrent een maatschappelijk debat wordt gevoerd, inclusief in deze commissie. Het stemt hem trouwens tevreden dat de bekommernissen inzake privacy van bij het prille begin van dit initiatief zijn meegenomen. Wellicht is het takenpakket van de bevoegde minister daaraan niet vreemd.

Les fuites de données sont indissociablement liées à la réalité technologique et ne sont jamais à exclure. Cela ne signifie cependant pas qu'il ne faut pas s'en protéger.

M. Stevens est assez favorable aux logiciels à source ouverte. Le fait que le code source soit rendu public est un signe de transparence et laisse supposer que le développeur n'a rien à cacher. Cela indique que l'on travaille de façon décentralisée, ce qui est absolument préférable à une banque de données centrale de personnes contaminées et de contacts. Cependant, il faut bien sûr prendre en compte les risques liés aux applications à source ouverte, à savoir les risques sur le plan de la sécurité nationale.

Selon M. Stevens, l'approche autrichienne, dans le cadre de laquelle les aspects centraux de la contamination sont enregistrés par l'autorité de contrôle du respect de la vie privée, ne semble pas, à première vue, un exemple attrayant. Il s'agit d'un rôle opérationnel qui peut éventuellement être confié à un sous-traitant, moyennant un cadre contractuel correct. L'APD, qui est une autorité de contrôle et, en cette qualité, peut infliger des sanctions (même aux pouvoirs publics), ne devrait pas assumer un tel rôle; cela créerait une confusion d'intérêts.

L'orateur est favorable à l'idée d'une implication citoyenne (qui passerait par exemple par des "chasses aux bugs" ou "*bug bounties*"). L'objectif central est de mettre en place un dispositif qui inspire confiance aux citoyens et qu'ils sont désireux de soutenir. Cette démarche s'inscrit également dans la philosophie du mouvement "numérique au service de l'intérêt général" ou "*data for good*", qui inspire également le niveau européen. L'orateur estime qu'à l'heure actuelle, la politique menée dans notre pays tient suffisamment compte de cette préoccupation. Ce n'est pas le cas partout: certains pays (par exemple la France) ont recours à des applications non décentralisées ou qui n'utilisent pas la technologie Bluetooth (Pologne). D'autres pays envisagent même d'imposer l'application.

Mme Soors a demandé si l'APD pourrait émettre un avis positif sur la proposition de résolution à l'examen. Abstraction faite du fait que l'APD n'a pas de compétence consultative formelle à l'égard des propositions de résolution, M. Stevens estime que le texte contient de nombreux éléments positifs: décentralisation, utilisation de la technologie Bluetooth et caractère volontaire de l'utilisation de l'application sont, à ses yeux, autant d'éléments essentiels pour apprécier la proportionnalité générale de la mesure envisagée. Quant à savoir si

Datalekken zijn onlosmakelijk verbonden met de technologische realiteit en vallen nooit uit te sluiten. Dit betekent uiteraard niet dat men zich daartegen niet hoeft te wapenen.

De heer Stevens staat eerder positief ten opzichte van opensource-*software*. Het publiek beschikbaar stellen van de broncode getuigt van transparantie en doet vermoeden dat de ontwikkelaar niets te verbergen heeft. Het duidt op een decentrale werking, wat absoluut te verkiezen valt boven een centrale gegevensbank van besmette personen en contacten. De risico's verbonden met opensource-apps, met name op het vlak van de nationale veiligheid, moeten uiteraard wel worden meegenomen.

De Oostenrijkse benadering, waarbij de centrale aspecten van de besmetting door de toezichthouder op het vlak van privacy zelf worden opgenomen, lijkt de heer Stevens op het eerste gezicht geen aantrekkelijk voorbeeld. Dit is een operationele rol die eventueel aan een onderaannemer kan worden toevertrouwd, middels een deftig contractueel kader. De GBA, die een toezichthouder is en in die hoedanigheid sancties kan opleggen (zelfs aan de overheid), zou een dergelijke rol niet moeten opnemen; dit zou neerkomen op een belangenvermenging.

De spreker is de idee van burgerbetrokkenheid (bijvoorbeeld via "*bug bounties*") genegen. De centrale doelstelling is om iets te bouwen waar de burgers vertrouwen in hebben en mee de schouders willen onderzetten. Dit strookt ook met de filosofie van "*data for good*" die ook het Europese niveau inspireert. De spreker meent dat het beleid in ons land momenteel voldoende rekening houdt met die bekommernis. Dit is niet overal het geval; in sommige landen wordt gewerkt aan apps die niet decentraal zijn (Frankrijk) of die niet werken met bluetooth-technologie (Polen). Er zijn ook landen die overwegen om de app te verplichten.

Mevrouw Soors vroeg of de GBA een positief advies zou verlenen omtrent het voorliggende voorstel van resolutie. Abstractie makend van het feit dat de GBA geen formele adviesbevoegdheid heeft inzake voorstellen van resolutie, meent de heer Stevens dat de tekst veel goede zaken bevat: decentralisatie, het gebruik van bluetooth-technologie en het vrijwillig karakter van de app zijn voor de spreker drie wezenlijke elementen in de beoordeling van de algemene proportionaliteit van de voorgenomen maatregel. Of de app effectief zal zijn

l'application envisagée se révélera efficace dans la lutte contre le coronavirus, rien ne permet malheureusement de l'affirmer avec certitude avant de l'avoir testée.

D'aucuns ont demandé comment la proposition de résolution pourrait être renforcée. L'orateur se félicite de (la qualité de) l'audition mais souligne qu'il reste des progrès à faire en termes de transparence du débat, en particulier en ce qui concerne la discussion relative à la base légale de l'application envisagée et le choix de l'instrument juridique (loi ou AR numéroté). L'orateur n'estime pas pour autant que nous devrions imiter nos voisins néerlandais, chez qui la sélection de l'application s'est opérée intégralement sur la place publique. Cette méthode ne fait que créer une illusion de transparence. L'AP, pendant néerlandais de l'APD, a été forcée de reconnaître, malgré toute son ouverture, qu'elle ne disposait pas de suffisamment d'informations pour porter un jugement pertinent sur les applications.

Différentes observations ont été formulées sur le couplage avec d'autres données et le rôle que la plateforme eHealth et la BCSS pourraient jouer à cet égard. M. Stevens n'a pas connaissance de ce couplage. Il suggère que la proposition de résolution pourrait être renforcée en insérant de manière plus explicite, dans le texte, l'interdiction de couplage avec d'autres données. De même, les rôles et les responsabilités des différents acteurs publics pourraient être précisés dans la proposition de résolution ou, mieux encore, dans la future loi ou le futur arrêté royal numéroté.

Enfin, compte tenu de la complémentarité entre le traçage de contacts manuel et le traçage numérique et les différents niveaux de pouvoirs où ils sont organisés, la proposition de résolution pourrait être renforcée en y renvoyant à la mise en place d'un consensus entre les différentes entités qui composent la Belgique.

M. Verduyckt a demandé des précisions sur l'anonymat des données télécoms utilisées par le groupe de travail pour cartographier la mobilité des citoyens. Le résultat final de ce traitement est un chiffre (public) indiquant combien d'appareils mobiles ont été utilisés pendant combien de temps dans une localité dont le code postal n'est pas le code postal propre de l'utilisateur. L'orateur cite l'exemple de son propre déplacement à Bruxelles en matinée: si son téléphone portable figurait déjà dans les données – ce qui supposerait l'arrivée d'au moins 29 autres téléphones à Bruxelles à partir du même code postal – il ne serait pas possible de déterminer l'itinéraire qu'il a emprunté. On peut débattre de la question de savoir si ces informations sont anonymes. En tout état de cause, l'anonymisation est suffisante à la lumière de l'objectif poursuivi. Comme cela a été indiqué

in de strijd tegen het coronavirus kunnen we helaas niet op voorhand met zekerheid weten.

De vraag werd gesteld hoe het voorstel van resolutie nog zou kunnen worden versterkt. De spreker is verheugd over de (kwaliteit van de) hoorzitting, maar meent dat er nog stappen kunnen worden gezet op het vlak van de transparantie van het debat. Dat is met name het geval voor de discussie over de wettelijke basis voor de app en de keuze van het juridische instrument (wet of genummerd KB). Daarmee wil de spreker niet gezegd hebben dat we moeten vervallen in de Nederlandse situatie, waar de selectie van een app integraal op het publieke forum plaatsvond. Hierdoor wordt slechts een illusie van transparantie gecreëerd. De Nederlandse tegenhanger van de GBA, de AP, moest spijts alle openheid toegeven dat ze over onvoldoende informatie beschikte om een zinvol oordeel te kunnen vellen over de apps.

Verschillende opmerkingen betroffen de koppeling met andere gegevens en de rol die het *eHealth*-platform en de KBSZ daarbij zouden opnemen. De heer Stevens heeft geen weet van zulke koppeling. Hij suggereert dat het voorstel van resolutie zou kunnen worden versterkt door het verbod op de koppeling met andere gegevens explicieter op te nemen in de tekst. Ook zouden de rollen en verantwoordelijkheden van de verschillende overheidsactoren kunnen worden verduidelijkt in het voorstel van resolutie of, beter nog, in de toekomstige wet of genummerd KB.

Gelet op de complementariteit tussen manuele en digitale contact tracing en de verschillende bevoegdheidsniveaus waarop zij worden georganiseerd, zou het voorstel van resolutie ten slotte kunnen worden versterkt door daarin een verwijzing op te nemen naar het creëren van draagvlak over de verschillende entiteiten van dit land heen.

De heer Verduyckt vroeg hoe het zat met de anonimiteit van telecomgegevens die worden aangewend door de taskforce om de mobiliteit van de burgers in kaart te brengen. Het eindresultaat van die verwerking is een (publiek) cijfer van hoeveel mobiele toestellen hoeveel tijd in een andere postcode dan hun eigen postcode hebben doorgebracht. De spreker geeft het voorbeeld van zijn eigen verplaatsing naar Brussel deze ochtend; als zijn mobiel toestel al in de cijfers zou voorkomen – wat veronderstelt dat minstens 29 andere toestellen vanuit dezelfde postcode naar Brussel zouden zijn gekomen – dan valt daar bijvoorbeeld niet uit af te leiden welk traject hij heeft gevolgd. Of dit anoniem is, is voer voor discussie. Het is alleszins voldoende geanonimiseerd in het licht van de nagestreefde doelstelling. Het eindresultaat is, zoals gezegd, een aantal, dat op zich volstrekt anoniem

précédemment, le résultat final est un nombre qui, en soi, est totalement anonyme bien qu'il ait été obtenu en traitant des données à caractère personnel. La loi sur les télécommunications prévoit d'ailleurs la possibilité d'un traitement anonymisé de ces données télécoms. Les trois opérateurs de téléphonie mobile rendent les données anonymes et les agrègent, après quoi un partenaire externe opérant dans un cadre contractuel strict les analyse et génère l'indicateur de mobilité.

En réponse à la question de M. Boukili, visant à savoir s'il existe, en définitive, des données de localisation anonymisées, M. Stevens indique que c'est le cas au travers de la conversion en chiffres.

Eu égard aux risques liés à l'utilisation des applications de traçage, il est logique que l'on évalue l'impact sur la protection des données. Ce point pourrait, du reste, également être intégré dans la proposition de résolution.

L'orateur n'a aucune idée du temps nécessaire pour développer une application de traçage. Ce calendrier relève d'une décision politique qui ne fait aucune différence dans la perspective de la protection des données.

M. Stevens ne dispose pas non plus d'informations sur les profils des personnes qui travailleront dans les centres d'appel. En tout état de cause, les aspects de cette question liés à la vie privée sont minimes. Mieux vaut adresser cette question aux ministres compétents.

La réponse à la question de M. Vanden Burre sur la manière d'empêcher l'exclusion de certains groupes tels que les enfants et les seniors réside dans la complémentarité. Outre le traçage automatisé, il existera de toute façon une variante manuelle. L'application de traçage doit venir en appui du traçage manuel, et garantir, en particulier, que ce dernier reste gérable.

M. Stevens peut difficilement évaluer dans quelle mesure il est probable que l'application devienne réalité. Il serait préférable que Mme Verhelst adresse cette question au ministre compétent. L'orateur confirme toutefois que si elle se concrétise, il s'agira d'une variante, protégeant suffisamment la vie privée des citoyens selon l'APD, ce qui implique qu'elle incorporera les trois caractéristiques décrites comme étant des garanties essentielles (Bluetooth, sur base volontaire, décentralisée). L'orateur souligne encore que certains pays, en Europe également, s'emploient à développer des systèmes dans lesquels ce n'est pas le cas.

L'orateur n'a pas subi de pressions internationales afin de participer à l'initiative européenne. Comme cela a déjà été mentionné, l'APD a collaboré très activement

is, zij het dat het wordt bereikt door een verwerking van persoonsgegevens. De telecomwet voorziet overigens in de mogelijkheid van een geanonimiseerde verwerking van die telecomgegevens. De drie mobiele operatoren anonimiseren en aggregeren de gegevens, waarna een binnen een strikt contractueel kader opererende externe partner de analyse doet en de mobiliteitsindicator genereert.

Op de vraag van de heer Boukili of geanonimiseerde lokalisatiegegevens überhaupt bestaan, antwoordt de heer Stevens bevestigend, namelijk door omzetting naar cijfers.

Gelet op de risico's verbonden met het gebruik van tracing apps, is het logisch dat er een gegevensbeschermingseffectbeoordeling zal worden uitgevoerd. Dit zou overigens eveneens kunnen worden toegevoegd in het voorstel van resolutie.

De spreker heeft geen zicht op de timing voor de tracing app. Dit is een beleidsbeslissing die vanuit het perspectief van de gegevensbescherming geen verschil maakt.

De heer Stevens heeft evenmin informatie omtrent de profielen van de personen die werkzaam zullen zijn in de callcenters. De privacyaspecten van die kwestie zijn alleszins minimaal. Deze vraag kan best worden gesteld aan de bevoegde ministers.

Het antwoord op de vraag van de heer Vanden Burre hoe kan worden vermeden dat bepaalde groepen zoals kinderen en ouderen worden uitgesloten, schuilt in de complementariteit; naast de geautomatiseerde tracing zal er in ieder geval een manuele variant zijn. De tracing app moet de manuele tracing ondersteunen, en er met name voor zorgen dat die laatste beheersbaar blijft.

De heer Stevens kan moeilijk inschatten hoe groot de kans is dat de app er werkelijk komt. Mevrouw Verhelst zou deze vraag best tot de bevoegde ministers richten. De spreker bevestigt wel dat als hij er komt, het in een variant zal zijn waarbij, naar de mening van de GBA, de privacy van de burgers voldoende beschermd zal zijn, wat impliceert dat hij de drie als essentiële waarborgen omschreven kenmerken (bluetooth, vrijwillig, decentraal) incorporeert. De spreker wijst er nogmaals op dat bepaalde, ook Europese landen, werken aan systemen waarin dit niet het geval is.

De spreker heeft geen internationale druk ervaren om te participeren in het Europese initiatief. De GBA heeft zoals al gezegd zeer actief meegewerkt aan de

aux directives du CEPD, dans lesquelles figurent les garanties précitées.

S'il devait apparaître que l'application n'est pas utile, il faudra mettre fin anticipativement à son utilisation. L'orateur estime qu'il est opportun que cette éventualité soit prévue dans la proposition de résolution. Cela s'inscrit également dans le cadre des principes en vigueur en matière de protection de la vie privée.

L'orateur ne considère pas qu'il est indiqué d'attendre que des résultats étrangers soient disponibles. Premièrement, il est assez urgent de déployer le suivi des contacts. En outre, l'orientation que suivront la plupart des pays est connue; les limites ont été exposées par le CEPD, lesquelles permettent de se mettre au travail. Il est d'ailleurs connu qu'il n'est pas possible de transposer tout simplement des exemples provenant d'autres pays dans un autre contexte national.

À la question de Mme Bury de savoir si les données collectées seront réellement anonymes et s'il ne sera pas possible à un stade ultérieur d'encore les associer à des personnes, M. Stevens répond que le caractère décentralisé de la banque de données offre des garanties suffisantes en la matière.

Le professeur Bart Preneel (KUL) donne davantage de précisions au sujet de la différence entre le PEPP-PT et le DP-3T. Début mars, la KUL a rejoint un grand consortium européen conduit par des acteurs allemands (PEPP-PT). Le but consistait à proposer une solution à la fois centralisée et décentralisée au sein de ce consortium. La structure de décision de ce consortium n'était toutefois guère transparente et, sous l'impulsion de l'Allemagne, le consortium continuait à défendre une solution centralisée auprès du monde extérieur. Finalement, le groupe d'étude de l'orateur a décidé de se retirer du consortium après à peine un mois. Le week-end passé, l'Allemagne a également signalé qu'elle privilégiait la solution décentralisée. La France est le seul grand pays qui travaille encore sur la solution centralisée au sein du PEPP-PT, avec son protocole ROBERT développé par l'Inria. Hier, des scientifiques français ont toutefois exprimé leur inquiétude à cet égard dans une lettre ouverte. Le Royaume-Uni est le dernier pays qui souhaite encore une solution centralisée indépendamment du PEPP-PT.

L'Europe souhaite une solution pour tous les pays mais tente de combler le retard qu'elle a en partie accumulé par rapport aux faits. Les États membres ont agi très vite et l'UE essaie d'aligner les différents pays par le biais de recommandations.

richtlijnen van de EDPB waarin voormelde garanties zijn opgenomen.

Mocht de app niet nuttig blijken, dan dient hij vroegtijdig worden stopgezet. De spreker vindt het een goede zaak dat deze eventualiteit voorzien is in het voorstel van resolutie. Een en ander strookt ook met de geldende principes inzake privacy.

De spreker meent niet dat het aangewezen is om te wachten tot er buitenlandse resultaten beschikbaar zijn. Vooreerst is er een zekere tijdsdruk om de contact tracing uit te rollen. Bovendien kennen we de richting die de meeste landen zullen uitgaan; de krijtlijnen werden uitgezet door de EDPB. Daarmee kunnen we nu aan de slag. Overigens is het bekend dat voorbeelden uit andere landen zich niet zomaar laten transponeren in een andere nationale context.

Op de vraag van mevrouw Bury of de verzamelde gegevens werkelijk anoniem zullen zijn en of niet het mogelijk zal zijn deze in een later stadium alsnog te linken aan personen, antwoordt de heer Stevens dat het decentrale karakter van de gegevensbank ter zake voldoende waarborgen biedt.

Professor Bart Preneel (KUL) geeft verdere toelichting over het verschil tussen PEPP-PT en DP-3T. Begin maart heeft de KUL zich aangesloten bij een groot Europees consortium geleid door Duitse spelers (PEPP-PT). De bedoeling was om binnen dat consortium zowel een centrale als een decentrale oplossing voor te stellen. De beslissingsstructuur van dat consortium was echter weinig transparant en op aansturen van Duitsland bleef het consortium naar de buitenwereld toe een centrale oplossing verdedigen. Uiteindelijk heeft de onderzoeksgroep van de spreker na een kleine maand besloten om uit het consortium te stappen. Afgelopen weekend heeft Duitsland aangegeven ook de voorkeur te geven aan een decentrale oplossing. Het enige grote land dat nog aan een centrale oplossing werkt binnen PEPP-PT is Frankrijk, met zijn door Inria ontwikkeld ROBERT-systeem. Gisteren echter hebben Franse wetenschappers in een open brief hun bezorgdheid hieromtrent geuit. Los van PEPP-PT is het Verenigd Koninkrijk het laatste land dat nog een centrale oplossing wil.

Europa wil één oplossing voor alle landen maar loopt voor een stuk achter de feiten aan. De lidstaten hebben zeer vlug gehandeld en de EU tracht de verschillende landen op één lijn te krijgen middels aanbevelingen.

L'interopérabilité limitée des différentes solutions constitue un problème de taille. Le fait de recueillir les informations concernant les chiffres aléatoires reçus dans une banque de données centralisée ou non centralisée relève d'une approche fondamentalement différente. Si une solution centralisée est associée à une solution décentralisée, le résultat est en quelque sorte le pire des deux mondes, à savoir la perte maximale de protection de la vie privée et l'efficience minimale. L'orateur s'attend à ce que des critiques acerbes soient formulées en Europe au cours des prochaines semaines au sujet de ce qu'il arriverait si un ressortissant d'un pays qui a opté pour une solution décentralisée voyageait à destination d'un pays qui a mis en œuvre une solution centralisée.

La principale raison pour laquelle l'orateur opte pour une solution décentralisée est que celle-ci présente moins de risques de piratage; la banque de données ne contient que des chiffres aléatoires qui ne sont pas réutilisables à d'autres fins. Le prix à payer pour ce risque inférieur de piratage est que les attaques locales, au moyen d'une antenne Bluetooth et d'une caméra, sont un peu plus aisées. De telles infractions sont toutefois également possibles sans application. Il s'agit essentiellement d'une mise en balance: est-on plus préoccupé par un abus centralisé ou par des attaques locales?

Des questions ont été posées au sujet du taux de pénétration exigé de l'application. Nul ne le sait en réalité; une étude indique que 60 % est le minimum requis, mais il se pourrait tout autant que ce taux soit supérieur ou inférieur. Les chiffres qui résultent des études dépendent dans une large mesure des hypothèses utilisées. Il ne fait toutefois pas de doute qu'une application ne fonctionnera pas si le taux de pénétration est inférieur à 10 %. Ce qui importe est de convaincre la population de l'utilité et de la sécurité de l'application afin d'obtenir un taux de pénétration aussi élevé que possible.

Qu'en est-il des personnes qui ne possèdent pas un smartphone approprié et quelle est la taille de ce groupe? Le professeur Preneel a posé cette dernière question aux opérateurs mais n'a pas encore pu obtenir de réponse. Les opérateurs disposent en tout état de cause de cette information; ils savent précisément de combien de personnes il s'agit. À l'étranger, une prospection a d'ailleurs déjà été réalisée au sujet de la possibilité de donner un Bluetooth-*token* aux personnes dépourvues de smartphone. De tels appareils existent déjà, seul le logiciel devrait être adapté, ce qui prendrait quelques semaines. Le coût d'un tel appareil est estimé à 5 à 10 euros. Il faut d'abord examiner si le système fonctionne correctement sur les smartphones, mais si tel est le cas, il sera possible d'envisager de déployer ces Bluetooth *tokens* sur une base volontaire.

Een groot probleem betreft de beperkte interoperabiliteit van de verschillende oplossingen. Of je informatie over ontvangen random getallen al of niet in een centrale gegevensbank verzamelt, is een fundamenteel verschillende benadering. Als je een centrale en een decentrale oplossing gaat koppelen, krijg je in zekere zin het slechtste van twee werelden: maximaal privacyverlies en minimale efficiëntie. De spreker verwacht dat er de komende weken in Europa nog een hartig woordje zal worden gepraat over wat er zou gebeuren als een burger vanuit een land dat voor een decentrale oplossing opteerde, naar een land dat een centrale oplossing implementeerde, zou reizen.

De hoofdreden waarom de spreker kiest voor een decentrale oplossing is dat het risico op *hacks* lager ligt; de gegevensbank bevat enkel random getallen, die niet herbruikbaar zijn voor andere doeleinden. De prijs die men betaalt voor dat lagere risico op *hacks* is dat lokale aanvallen, met een bluetooth-antenne en een camera, iets gemakkelijker zijn. Zulke overtredingen zijn echter ook mogelijk zonder een app. Het is in wezen een afweging: is men meer bezorgd over centraal misbruik of over lokale aanvallen?

Er werden vragen gesteld omtrent de vereiste penetratiegraad van de app. Eigenlijk weet men het niet; één studie zegt dat 60 % minimaal vereist is, maar het zou evengoed kunnen dat het meer of minder is. Uit studies voortvloeiende cijfers hangen in hoge mate af van de gebruikte veronderstellingen. Dat een app niet zal werken als de penetratie minder dan 10 % bedraagt, is echter een uitgemaakte zaak. Wat telt is de bevolking te overtuigen van het nut en de veiligheid van de app, om een zo hoog mogelijke penetratiegraad te verkrijgen.

Wat met mensen die geen geschikte smartphone hebben en hoe groot is die groep? Professor Preneel richtte deze laatste vraag aan de operatoren maar mocht nog geen antwoord krijgen. In ieder geval is het zo dat de operatoren over die informatie beschikken; zij weten precies over hoeveel mensen het gaat. In het buitenland werd overigens al verkennend onderzoek verricht naar de mogelijkheid om mensen zonder smartphone een bluetooth-token te geven. Zulke toestellen bestaan al, enkel de software zou dienen te worden aangepast, wat enkele weken zou kosten. De kost van zo'n toestel wordt geschat op 5 tot 10 euro. Eerst moet worden bekeken of het systeem goed werkt op smartphones, maar als dat het geval is kan eraan worden gedacht om zulke bluetooth-tokens op vrijwillige basis uit te rollen.

Le professeur Preneel conteste que son appartenance à la chambre contentieuse de l'APD puisse constituer un conflit d'intérêts.

L'application basée sur le protocole DP-3T est conçue de manière à ne pas pouvoir être utilisée à d'autres fins. Les situations gagnant-gagnant comportent des risques pour la vie privée et ne sont volontairement pas recherchées.

Plusieurs députés se sont inquiétés des faux positifs et des faux négatifs. Les citoyens peuvent contribuer eux-mêmes à éviter les faux positifs en désactivant la fonction Bluetooth de leur smartphone ou l'application dans certaines situations (par exemple à leur domicile). Le protocole DP-3T permet également à l'utilisateur de supprimer ultérieurement les données existantes des fichiers. On ne connaîtra le nombre de faux négatifs qu'une fois que le système aura été déployé à grande échelle. L'orateur pense qu'il est possible d'obtenir de bons résultats à cet égard.

La Suisse deviendra, à partir du 11 mai, le premier pays à déployer l'application (décentralisée). L'Autriche, l'Estonie et l'Espagne lui emboîteront le pas. Il se sera écoulé environ quatre semaines entre la décision du gouvernement suisse et le déploiement de l'application. Le code de cette application étant en accès libre, nous pourrons bénéficier des développements et des expériences des autres pays. Nous pourrons (ré)utiliser de nombreux éléments fondamentaux; il faudra uniquement adapter l'interface réservée aux autorités sanitaires et au monde médical à la situation belge. L'orateur estime donc que, si nous prenons un décision en ce sens, il devrait être possible de procéder au déploiement de l'application en Belgique une à deux semaines après son déploiement en Suisse.

Comment s'assurer que les versions de l'application installées sur les appareils des utilisateurs correspondent au code source qui sera publié? Il s'agit d'un problème bien connu. Il existe deux manières de vérifier que le code source et le code compilé (le code machine ou le code programme) correspondent. La première solution fonctionne toujours: il est possible de vérifier le code programme en détail et s'assurer qu'il correspond au code source. Cette méthode prend beaucoup de temps mais, pour la partie critique du code (comme les opérations cryptographiques), elle est certainement envisageable et offre de solides garanties. La deuxième solution consiste à utiliser une compilation déterministe (ou une compilation reproductible), ce qui permet de recompiler le code source pour une plateforme donnée et de vérifier si l'on obtient un résultat identique. Cette méthode n'est pas encore applicable à toutes les langues et à toutes les plateformes. Cette solution sera

Professor Preneel ontkent dat zijn lidmaatschap van de Geschillenkamer van de GBA een belangenconflict zou doen rijzen.

De app in het DP-3T protocol is zo ontworpen dat hij niet kan worden gebruikt voor andere doeleinden. Winwinsituaties leiden tot privacy-risico's en worden bewust niet opgezocht.

Verschillende vraagstellers waren bezorgd over valse positieven en valse negatieven. Die eerste kan de burger alvast zelf helpen vermijden, door zijn bluetooth-functie of de app in bepaalde situaties (bijvoorbeeld thuis) uit te schakelen. Het DP-3T protocol biedt ook de mogelijkheid voor de gebruiker om achteraf bestaande gegevens uit de bestanden te verwijderen. Het aantal valse negatieve meldingen zal moeten blijken uit de metingen, eens het systeem is uitgerold op grote schaal. De spreker denkt dat het haalbaar is om ter zake goede resultaten te boeken.

Zwitserland zal als eerste de (decentrale) app uitrollen, en wel vanaf 11 mei. Oostenrijk, Estland en Spanje zullen volgen. Er zullen ongeveer een viertal weken zitten tussen de Zwitserse beslissing en de uitrol. Gelet op het feit dat de code opensource is, zullen wij kunnen profiteren van de ontwikkelingen en ervaringen in andere landen. We zullen veel bouwstenen kunnen (her)gebruiken; enkel de interface met de gezondheidsautoriteiten en de medische wereld zal dienen te worden aangepast aan de Belgische situatie. De spreker schat dan ook dat, als we voortgang maken met de beslissing, een uitrol in België één à twee weken na de Zwitserse uitrol mogelijk moet zijn.

Hoe zal men kunnen garanderen dat de versies van de app die op de toestellen van gebruikers geïnstalleerd worden, overeenkomen met de broncode die vrijgegeven wordt? Het betreft een algemeen gekend probleem. Er zijn twee manieren om na te gaan of broncode en gecompileerde code (machinecode of programmacode) overeenkomen. De eerste werkt altijd: men kan de programmacode in detail nakijken en verifiëren of die overeenkomt met de broncode. Dat is heel tijdrovend, maar voor het kritische deel van de code (zoals de cryptografische operaties) is dat zeker haalbaar en geeft dat sterke waarborgen. Een tweede oplossing is gebruik maken van deterministische compilatie (*deterministic compilation* of *reproducible builds*). In dat geval kan men de broncode hercompileren voor een bepaald platform en nagaan of men identiek hetzelfde resultaat bekomt. Dit is nog niet mogelijk voor alle talen en platformen. Deze oplossing zal zeker gebruikt worden binnen DP-3T

certainement utilisée dans le cadre du protocole DP-3T si elle est envisageable, et elle l'est probablement pour une partie du code.

Mme Olivia Venet (Ligue des Droits Humains) indique que l'atteinte controversée à la vie privée doit être prévue par la loi et doit être nécessaire dans une société démocratique. L'oratrice fustige le manque de réflexion et d'analyse d'impact permettant d'évaluer cette nécessité. En effet, les autorités sont déjà en train de recruter des personnes qui seront chargées de tracer les contacts des personnes infectées, sans avoir décidé que cette méthode constitue réellement la meilleure solution à cet égard. Mme Venet rejoint la professeure Degrave lorsque celle-ci indique qu'il existe un risque réel que nous nous enfermions dans un processus que les organes législatifs n'ont pas réellement eu l'occasion d'analyser, d'examiner et à propos duquel ils n'ont pas pu se prononcer. L'oratrice estime que le cadre légal doit prendre la forme non pas d'un arrêté royal mais d'une loi, qui devra être soumise à l'avis de l'APD et du Conseil d'État.

L'oratrice ne souhaite absolument pas contester que la préoccupation première du président de l'APD est la protection de la vie privée, mais elle s'interroge toujours sur sa participation à la *task force*, au sein de laquelle les participants examineront des solutions, parviendront à un compromis et rédigeront un texte. Comment pourrait-on dès lors s'attendre à ce que l'APD, qui est présidée par un membre de cette même *task force*, rende un avis critique sur ce texte? Pour Mme Venet, il faut établir une distinction claire entre ces fonctions et il faudra, au besoin, que le président se retirer des délibérations.

L'oratrice s'inquiète des risques de dérives. Elle est convaincue que les applications doivent servir à renforcer les capacités des citoyens, et pas à les contrôler. Les institutions sont au service des citoyens. Ce n'est qu'avec eux que nous parviendrons à lutter effectivement contre le virus. Les institutions ne sont pas les ennemis des citoyens, et vice versa. C'est la philosophie qui doit présider à l'élaboration d'un cadre légal.

Il est certain que la garantie de l'anonymat est compromise au sein des *call centers*. Affirmer que des numéros de téléphone constituent des données anonymes ne tient pas debout. Un problème réel se pose à cet égard.

L'oratrice est opposée à l'octroi de récompenses dans le cadre de l'application. En effet, si des récompenses sont prévues, il ne peut plus être question d'une utilisation sur base volontaire, ce qui ouvre la porte à des discriminations et d'utilisation abusive des données.

als het haalbaar is; waarschijnlijk kan dat voor een deel van de code.

Mevrouw Olivia Venet (Ligue des Droits Humains) stelt dat de kwestieuze inbreuken op de bescherming van het privéleven bij wet moeten zijn voorzien en noodzakelijk moeten zijn in een democratische samenleving. De spreekster hekelt het feit dat er onvoldoende reflectie en impactanalyse is om die noodzakelijkheid te kunnen beoordelen. Men is thans al bezig met de rekrutering van de *contact tracers*, zonder dat beslist is dat dat werkelijk de beste oplossing is. Mevrouw Venet treedt professor Degrave bij wanneer zij stelt dat het risico reëel is dat we vastzitten in een proces waarbij de volksvertegenwoordiging niet terdege de kans heeft gekregen om de kwestie te onderzoeken, te bespreken en zich erover uit te spreken. De spreekster vindt dat het wettelijk kader de vorm moet aannemen van een wet – niet van een genummerd KB – na het advies te hebben ingewonnen van de GBA en de Raad van State.

De spreekster wil hoegenaamd niet ontkennen dat de voornaamste bekommering van de voorzitter van de GBA de privacybescherming is, maar blijft zich toch vragen stellen bij zijn deelname aan de taskforce. Binnen die schoot bespreekt men samen oplossingen, bereikt men een compromis, en werkt men een tekst uit. Hoe kan men dan verwachten dat de GBA, met aan het roer een lid van de taskforce, een kritisch advies uitbrengt over zo'n tekst? Volgens mevrouw Venet moet er een strikte functiescheiding zijn en moet de voorzitter zich desnoods terugtrekken uit de beraadslagingen.

De spreekster is beducht voor uitwassen. Het is haar overtuiging dat de apps moeten dienen om de burger toe te laten zijn capaciteiten te versterken, eerder dan om hem te controleren. De instellingen staan ten dienste van de burgers; enkel samen met hen zullen we erin slagen het virus effectief te bestrijden. De instellingen zijn niet de vijand van de burgers en omgekeerd. Het is die geestesgesteldheid die moet primeren bij het uitwerken van een wettelijk kader.

De anonimiteit staat wel degelijk onder druk bij de callcenters. Het gaat niet op om te beweren dat telefoonnummers anonieme gegevens zijn. Er is daar een reëel probleem.

De spreekster staat afkerig tegen het gebruik van beloning in het kader van de app. In dat geval is er immers geen sprake meer van gebruik op vrijwillige basis, wat de deur openzet voor discriminatie en misbruik van de gegevens. Het wettelijk kader moet hieraan paal en

Le cadre légal devra poser des balises en la matière et devra par ailleurs aussi régler des questions telles que la suppression et la conservation des données.

Mme Venet conclut en soulignant que des pays du monde entier ainsi que la Haut-Commissaire des Nations Unies aux droits de l'homme mettent en garde contre les risques de dérives et de restrictions illégales des libertés fondamentales. Les textes qui devront être rédigés par le Parlement devront protéger les citoyens contre ces risques, même en temps de crise.

Mme Kati Verstrepen (Liga voor Mensenrechten) indique qu'il faut se montrer vigilant à l'égard du suivi et du traçage physique. Dans le cadre du traçage manuel, le traitement anonyme des données est tout simplement impossible. Il faut par conséquent établir un cadre légal définissant très clairement les conditions dans lesquelles ce suivi et ce traçage physique peuvent avoir lieu. Il est inconcevable de procéder déjà au recrutement des personnes chargées du traçage des contacts alors qu'aucune réflexion sur un cadre légal n'a été menée jusqu'à présent.

En ce qui concerne les applications de traçage des contacts, l'oratrice redoute le phénomène de pression sociale, qui aura pour conséquence que l'accès aux services privés ou publics (par exemple l'horeca ou les transports en commun) ou même à l'emploi (par exemple le système des titres-services) sera subordonné à l'utilisation de l'application. Ce débat devra certainement être mené dans le cadre de celui sur le caractère volontaire de l'utilisation de l'application.

Un député a évoqué le fossé générationnel en indiquant que ce seront surtout les jeunes qui adopteront cette technologie et se poseront moins de questions sur la protection du respect de leur vie privée. Compte tenu de son caractère anonyme, l'enquête de la Ligue ne peut pas confirmer cette affirmation, mais le fait est que de très nombreux individus inquiets envoient des questions à la Ligue au sujet de la protection de la vie privée des jeunes.

Le danger que la crise actuelle serve à mettre en place des mécanismes de contrôle qui ne seront pas désactivés par la suite est réel. L'oratrice fait un parallèle avec la menace terroriste qui pesait il y a quelques années. Des mesures qui avaient été prises à cette époque, comme le doublement à 48 heures de la durée de détention prévue par la Constitution, semblent désormais acquises.

La professeure Élise Degrave (UNamur) affirme qu'il ne faut pas s'engager à la légère avec les GAFAM sans

perk stellen, en moet trouwens ook zaken regelen zoals de bewaring en het wissen van de gegevens.

Mevrouw Venet merkt ten slotte op dat overal ter wereld, ook door de vertegenwoordigster van het Hoog Commissariaat voor de Mensenrechten van de VN, wordt gewaarschuwd voor misbruiken en ongeoorloofde inperkingen van de fundamentele vrijheden. De teksten die door het Parlement worden opgesteld moeten de burgers daartegen in bescherming nemen, ook in tijden van crisis.

Mevrouw Kati Verstrepen (Liga voor Mensenrechten) stelt dat alertheid op zijn plaats is ten overstaan van de fysieke tracking-and-tracing. Bij de manuele variant is een geanonimiseerde verwerking van de gegevens simpelweg onmogelijk. Er moet dan ook een wettelijk kader komen dat zeer duidelijk omschrijft onder welke voorwaarden zulke fysieke *tracking-and-tracing* kan plaatsvinden. Het is onvoorstelbaar dat men *al contact tracers* aan het rekruteren is terwijl er nog niet eens is nagedacht over een wettelijk kader.

Wat de contact tracing apps betreft is de spreekster bevreesd voor sociale druk, waarbij toegang tot private of publieke diensten (bijvoorbeeld horeca, openbaar vervoer) of zelfs tewerkstelling (bijvoorbeeld het systeem van de dienstencheques) afhankelijk zullen worden gesteld van het gebruik van de app. Dit debat moet zeker worden gevoerd tegen de achtergrond van het vrijwillig karakter van de app.

Een vraagsteller refereerde aan het generatieverschil, waarbij vooral jongeren deze technologie zouden omarmen en zich minder vragen stellen wat de bescherming van hun privacy betreft. Uit de bevraging door de Liga zal het niet blijken, want die is anoniem, maar feit is dat de Liga erg veel bezorgde vragen omtrent privacy krijgt van jonge mensen.

Het gevaar dat de huidige crisis wordt aangewend om een aantal controlemechanismen te installeren die later niet worden teruggeschroefd, is reëel. De spreekster trekt een parallel met de terrorismedreiging enkele jaren geleden; toen zijn er ook maatregelen genomen, zoals de verdubbeling van de grondwettelijke aanhoudingstermijn tot 48 uren, die thans verworven blijken te zijn.

Professor Élise Degrave (UNamur) stelt dat we ons ervoor moeten hoeden om lichtzinnig in zee te gaan met

avoir préalablement examiné attentivement les alternatives existantes. La première question que nous devons nous poser est de savoir pourquoi nous avons besoin d'eux. Une chose est de leur demander de débloquer les smartphones pour leur permettre de communiquer entre eux, mais c'en est une autre de leur confier le stockage de données, par exemple.

Plutôt que de donner une réponse claire, la CNIL a indiqué que le projet français était tout sauf anodin. La CNIL a posé plusieurs balises et a demandé à pouvoir se prononcer de nouveau une fois que ce projet sera plus précis.

Il convient d'établir une distinction claire entre le SPF Santé publique et la plate-forme *eHealth*. Cette dernière est un instrument régi par la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions. La professeure Degrave se demande s'il ne serait pas possible de gérer l'application de traçage des contacts dans une base de données commune au SPF Santé publique, sans lien avec la plate-forme eHealth, en collaboration avec les Régions et sous la supervision de l'APD.

M. Michael Freilich (N-VA) demande au professeur Preneel pourquoi il a récemment quitté le projet européen concernant une telle application mobile: ne savait-il pas que l'on y travaillait sur le stockage central de données? Que pense au demeurant le professeur de la direction dans laquelle s'engagent pour l'heure notamment la France et l'Allemagne dans ce domaine?

L'intervenant s'attarde ensuite sur la conservation de l'information dans une banque de données et non, par exemple, sur l'appareil d'une personne: les opérateurs télécoms font déjà quelque chose de similaire, notamment le stockage central des données de localisation: quelle est la différence?

En ce qui concerne le contrôle de l'application mobile, l'intervenant demande à M. Stevens comment il peut contrôler les applications mobiles provenant de l'étranger: existe-t-il en quelque sorte une obligation légale lorsque l'application mobile se trouve dans l'App Store?

L'APD dispose-t-elle de spécialistes dans des domaines techniques tels que le code source?

En ce qui concerne par ailleurs le traçage manuel, il s'agit d'une technique très invasive au niveau de la vie privée: où et comment seront par exemple stockées les données des *contact tracers*? Les autorités ne peuvent

de GAFAM, zonder vooraf goed te onderzoeken welke alternatieven er bestaan. De eerste vraag die we ons moeten stellen is waarom we ze nodig hebben. Het is één zaak hen te vragen om smartphones te deblokkeren om ze met elkaar te laten communiceren, maar het is een andere om hen bijvoorbeeld de opslag van gegevens toe te vertrouwen.

Veeleer dan een sluitend antwoord te geven, heeft de CNIL duidelijk gemaakt dat het Franse ontwerp allesbehalve onschuldig is. Het heeft een aantal bakens uitgezet en heeft verzocht zich opnieuw te kunnen uitspreken eens het ontwerp meer voldragen is.

Er moet een duidelijk onderscheid worden gemaakt tussen de FOD Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu en het *eHealth*-platform. Dat laatste is een instrument dat wordt geregeld door de wet van 21 augustus 2008 houdende oprichting en organisatie van het *eHealth*-platform en diverse bepalingen. Professor Degrave vraagt zich af of het niet mogelijk is de contact tracing app te beheren via een gegevensbank die gedeeld wordt met de FOD Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu, zonder link met het *eHealth*-platform, en dit in samenwerking met de gewesten en onder het toezicht van de GBA.

De heer Michael Freilich (N-VA) vraagt aan professor Preneel waarom hij recent is opgestapt uit het Europese project rond een dergelijke app: was het nieuw voor hem dat men daar werkt rond de centrale opslag van gegevens? Wat is trouwens de mening van de professor over de richting waarin met name Frankrijk en Duitsland zich momenteel begeven in deze aangelegenheid?

Vervolgens gaat de spreker in op het bijhouden van de informatie op een databank en dus bijvoorbeeld niet op het toestel van een persoon: vandaag doen de telecomoperatoren al iets dergelijks, met name de centrale opslag van lokalisatiegegevens: wat is dan het verschil?

Wat de controle op de app betreft, vraagt de spreker aan de heer Stevens op welke manier hij apps uit het buitenland kan controleren: is hier sprake van een soort wettelijke verplichting wanneer de app zich bijvoorbeeld bevindt in de App Store?

Beschikt de GBA over specialisten wanneer het gaat om technische zaken als de broncode?

Wat verder de manuele tracering betreft gaat het om een zeer privacy-invasieve techniek: waar en hoe zullen bijvoorbeeld de gegevens van de *contact tracers* worden opgeslagen? De overheid mag deze gegevens niet zelf

conserver elles-mêmes ces données: le *tracer* remettra-t-il alors une farde contenant tous ses contacts à l'intéressé?

Enfin, la législation relative à la protection de la vie privée offre-t-elle actuellement un cadre légal suffisant pour assurer une protection correcte ou faut-il légiférer davantage?

Enfin, dans le cadre des menaces d'espionnage et d'ingérence étrangère, l'intervenant demande à M. Raes si, sur certains appareils chinois, l'application mobile ne peut être piratée par le téléphone même.

Mme Jessika Soors (Ecolo-Groen) demande à M. Stevens si aujourd'hui l'APD rendrait un avis positif sur la proposition de résolution.

En ce qui concerne le calendrier, l'intervenante demande au professeur Preneel à quelle vitesse une application mobile pourrait être déployée dans la réalité, une fois que les ministres compétents ont donné leur approbation. Elle aimerait également en savoir plus sur la complémentarité entre l'application mobile et un éventuel traçage manuel. Enfin, selon les informations parues dans la presse, au moins 60 % de la population devrait utiliser l'application mobile pour en assurer l'efficacité, alors que le professeur affirme que 10 à 15 % est en fait suffisant: cela signifie-t-il que l'application mobile ne serait pas moins efficace si le taux de pénétration était inférieur à 60 %?

Enfin, Mme Soors pose la question suivante à tous les orateurs: abstraction faite de la répartition des compétences entre l'autorité fédérale et les régions et dans la mesure où tous les cadres juridiques seraient en ordre, si les orateurs étaient les ministres compétents pour prendre une décision sur le suivi et la traçabilité, que feraient-ils aujourd'hui?

M. Khalil Aouasti (PS) constate que le professeur Preneel était membre du Centre de connaissances de l'APD: est-ce toujours le cas? S'il en est ainsi et que le centre de connaissances doit rendre un avis sur une éventuelle application mobile, n'y a-t-il pas un conflit d'intérêts? La personne concernée devrait en effet participer en tant qu'expert au développement de l'application et ensuite rendre un avis sur la même application au nom du centre de connaissances.

Un cadre juridique et une habilitation spécifique sont par ailleurs indispensables: alors qu'il s'avère que l'Allemagne dispose déjà d'une loi et que l'assemblée plénière de l'Assemblée nationale française se penche aujourd'hui sur un cadre juridique, après avis de la Commission nationale de l'informatique et des libertés

bijhouden: gaat de *tracer* dan bijvoorbeeld een mapje meegeven aan de betrokkene met al zijn contacten?

Biedt de privacywetgeving vandaag ten slotte een voldoende wettelijk kader voor een juiste bescherming of is er extra wetgeving nodig?

Tot slot vraagt de spreker aan de heer Raes, in het kader van de dreigingen van spionage en buitenlandse inmenging, of op bepaalde Chinese toestellen de app niet kan worden gehackt via de telefoon zelf.

Mevrouw Jessika Soors (Ecolo-Groen) vraagt de heer Stevens of de GBA vandaag een positief advies zou verlenen over het voorstel van resolutie.

Aan professor Preneel vraagt de spreekster, wat de timing betreft, hoe snel een app in de realiteit zou kunnen worden uitgerold, nadat de bevoegde ministers hun fiat zouden hebben gegeven. Daarnaast kreeg zij graag meer uitleg over de complementariteit tussen de app en eventuele manuele *tracing.* Ten slotte zou volgens persberichten minstens 60 % van de bevolking de app moeten gebruiken opdat hij efficiënt zou zijn, terwijl de professor stelt dat 10 % tot 15 % eigenlijk voldoende is: betekent zulks dat de app niet minder efficiënt zou zijn indien de penetratiegraad lager dan 60 % zou zijn?

Ten slotte legt mevrouw Soors aan alle sprekers de volgende vraag voor: abstractie makend van de bevoegdheidsverdeling tussen de federale overheid en de gewesten en voor zover alle wettelijke kaders in orde zouden zijn, indien de sprekers de bevoegde ministers zouden zijn voor een beslissing omtrent *tracking-and-tracing*, wat zouden zij vandaag zouden doen?

De heer Khalil Aouasti (PS) stelt vast dat professor Preneel lid was van het Kenniscentrum van de GBA: is dit nog steeds het geval? Indien zulks het geval is en het Kenniscentrum een advies zou moeten geven over een eventuele app, zou er geen sprake zijn van een belangenconflict? Immers, de betrokkene zou als expert de app mee ontwikkelen en achteraf vanuit het Kenniscentrum advies moeten geven over dezelfde app.

Daarnaast zijn een wettelijk kader en een specifieke machtiging essentieel: nu blijkt dat Duitsland al een wet heeft en de plenaire vergadering van de Franse *Assemblée Nationale* vandaag vergadert over een wettelijk kader, na een advies van de *Commission nationale de l'informatique et des libertés* (CNIL) van 24 april 2020,

(CNIL) du 24 avril 2020, la Belgique va-t-elle suivre la même voie et donc opter pour des dispositions légales?

L'intervenant demande ensuite à M. Stevens s'il est toujours membre du groupe paneuropéen de huit personnes et où on en est à cet égard.

L'APD a-t-elle par ailleurs été invitée à rendre un avis et, si tel est le cas, cet avis – critique à en croire la presse – peut-il être transmis aux membres de la commission?

À l'intention de M. Raes et du professeur Preneel, l'intervenant fait également observer que lors du débat précité tenu à l'Assemblée nationale sur l'algorithme Bluetooth, il s'est avéré qu'en termes de sécurité nationale, ce dernier serait dépassé et qu'il pourrait en outre être facilement piraté notamment par des puissances étrangères; en outre, cet algorithme serait en lice pour servir de norme européenne.

L'intervenant constate par ailleurs que la professeure Degrave n'est pas favorable à ce que la plateforme eHealth gère les données de l'application. Lui-même préférerait cependant que ces données soient gérées par une autorité publique: quels pourraient dans ce cas être les autres candidats?

En ce qui concerne la plateforme eHealth, l'intervenant a constaté sur le site internet de la plateforme qu'un certain nombre d'applications sont déjà proposées pour s'enregistrer: en termes de protection de la vie privée, un certain nombre de ces applications indiquent que les données sont confidentielles, mais qu'elles peuvent être transmises à un des partenaires du réseau eHealth: quel est l'avis de M. Stevens à ce propos?

M. Erik Gilissen (VB) souligne que le développement d'une application collectant des données anonymes par le biais du Bluetooth semble être une bonne solution. Un certain nombre de préoccupations subsistent toutefois en matière de respect de la vie privée. Un stockage décentralisé constitue une solution appropriée, mais il doit être associé au caractère volontaire à 100 % de l'application.

En outre, l'intervenant s'interroge sur le pourcentage minimal d'utilisateurs nécessaire pour que l'application soit efficace.

De plus, le code source doit être transparent et l'application ne doit pas pouvoir être utilisée à d'autres fins. L'utilisateur doit toujours conserver le contrôle des données: comment peut-on le garantir? Comment éviter que

zal België dezelfde weg opgaan en dus ook opteren voor een wettelijke regeling?

Vervolgens vraagt de spreker aan de heer Stevens of hij nog steeds lid is van de pan-Europese groep bestaande uit acht personen en hoever men in dat kader is gevorderd.

Werd verder de GBA om een advies gevraagd en indien zulks het geval is kan dit advies –dat volgens de pers kritisch is – aan de leden van deze commissie worden bezorgd?

Ter attentie van de heer Raes en professor Preneel merkt de spreker verder op dat het in het al vermelde debat van de *Assemblée Nationale* met betrekking tot het bluetooth-algoritme is gebleken dat dit laatste in termen van nationale veiligheid voorbijgestreefd zou zijn en bovendien gemakkelijk zou kunnen worden gehackt, onder andere door buitenlandse mogendheden; bovendien zou dit algoritme een kandidaat zijn voor de Europese standaard.

Verder stelt de spreker vast dat professor Degrave er geen voorstandster van is dat het *eHealth*-platform de gegevens van de applicatie zou beheren. Nochtans geeft hij er de voorkeur aan dat deze gegevens zouden worden beheerd door een openbare overheid: wie zou in dit geval dan nog kandidaat kunnen zijn?

Wat het *eHealth*-platform betreft, heeft de spreker vastgesteld op de website van het platform dat daar al een aantal apps worden voorgesteld om jezelf te registreren: welnu, de privacytermen van een aantal van deze apps stellen dat je gegevens privé zijn maar dat ze wel kunnen worden overgedragen aan één van de partners in het *eHealth*-netwerk: wat is de mening van de heer Stevens hieromtrent?

De heer Erik Gilissen (VB) merkt op dat de ontwikkeling van een app met anonieme gegevens via bluetooth een goede oplossing lijkt. Wel blijven een aantal bezorgdheden bestaan omtrent privacy. Decentrale opslag is een goede oplossing maar moet worden gecombineerd met een 100 % vrijwillig karakter van de app.

Daarnaast vraagt de spreker welk percentage gebruikers minimaal noodzakelijk is opdat de app efficiënt zou zijn.

Verder dient de broncode transparant te zijn en mag de app niet bruikbaar zijn voor andere doeleinden. De gebruiker dient steeds de controle te behouden over de data: hoe kan dit worden verzekerd? Op welke

les données soient utilisées à d'autres fins? Comment répondre en outre à la préoccupation du citoyen concernant le respect de la vie privée et les fuites de données? On constate en effet que les citoyens ne sont pas suffisamment disposés à installer l'application et il apparaît donc que le cadre légal ne constitue qu'une partie du problème.

Mme Nathalie Gilson (MR) constate que la proposition de résolution ne vise que le traçage numérique. Elle apprend en outre que plus de 2 000 personnes seront recrutées pour assurer le traçage physique par l'intermédiaire de centres d'appel: l'intervenante demande à M. Stevens et à Mme Verstrepen comment cette collecte physique de données pourra se dérouler dans le respect de la vie privée.

Ensuite, la membre craint que le risque de manipulation (espionnage, piratage, fuites, etc.) n'augmente si l'on adopte une approche *open source*.

En outre, si les Régions sont effectivement compétentes pour le développement des applications, une interopérabilité est évidemment nécessaire au sein de la Belgique, voire au sein de l'Union européenne, qui a développé une boîte à outils en la matière. De quelle manière une application pourra-t-elle contribuer à rétablir le plus rapidement possible la libre circulation au sein de l'espace européen?

Enfin, l'intervenante revient sur l'efficacité de l'application. Selon des articles de presse, il faut au moins 60 % d'utilisateurs pour que l'application soit efficace, mais l'enquête citée par Mme Verstrepen indique que seulement 6 % de la population est disposée à utiliser l'application. Est-ce la raison pour laquelle on a finalement opté pour le traçage physique? L'intervenante est d'ailleurs beaucoup plus préoccupée par ce traçage physique que par une application en ce qui concerne le respect des droits de l'homme et de la vie privée.

M. Sammy Mahdi (CD&V) s'étonne des observations du professeur Preneel selon lesquelles un taux de participation de 10 à 15 % serait suffisant pour assurer une utilisation efficace de l'application: comment peut-on le prouver? Des simulations réalisées en Suède et aux Pays-Bas ont montré que même un taux de participation de 60 % serait insuffisant s'il n'était pas suffisamment réparti sur l'ensemble du territoire: qu'en pense l'orateur?

En ce qui concerne le Bluetooth, l'intervenant se demande à quelle vitesse cette technologie va évoluer compte tenu des problèmes liés à la présence de plexiglas et de murs. Ces problèmes entraîneront en effet la détection de nombreux faux contacts positifs.

manier kan worden voorkomen dat de data worden gebruikt voor andere doeleinden? Op welke manier kan verder de bezorgdheid van de burger omtrent privacy en datalekken worden aangepakt? Men stelt immers vast dat de burgers onvoldoende bereid zijn om de app te installeren en het blijkt dus dat het wettelijk kader maar een deel van het probleem vormt.

Mevrouw Nathalie Gilson (MR) stelt vast dat het voorstel van resolutie enkel de digitale tracering viseert. Zij verneemt verder dat meer dan 2 000 personen zullen worden aangeworven om aan fysieke tracering te doen via callcenters: de spreekster vraagt aan de heer Stevens en aan mevrouw Verstrepen op welke manier deze fysieke inzameling van gegevens zal kunnen verlopen met respect voor de privacy.

Vervolgens vreest het lid dat het risico voor manipulatie (spionage, hacking, lekken, enzovoort) groter zal zijn indien wordt gewerkt met een opensource-benadering.

Verder zijn de gewesten inderdaad bevoegd voor de ontwikkeling van de apps maar er is uiteraard interoperabiliteit nodig binnen België en zelfs in de schoot van de Europese Unie, die hieromtrent een *toolbox* heeft ontwikkeld: op welke manier zal een app kunnen bijdragen aan het zo snel mogelijk herstellen van het vrij verkeer binnen de Europese ruimte?

Ten slotte gaat de spreekster in op de doelmatigheid van de app: volgens persberichten waren hiervoor minstens 60 % gebruikers nodig, maar uit de door mevrouw Verstrepen aangehaalde enquête is gebleken dat slechts 6 % van de bevolking bereid zou zijn om de app te gebruiken: is het om reden dat uiteindelijk werd geopteerd voor de fysieke tracering? De spreekster maakt zich trouwens veel meer zorgen over deze fysieke tracering dan over een app, wat betreft het respect voor de mensenrechten en de privacy.

De heer Sammy Mahdi (CD&V) is verbaasd over de opmerkingen van professor Preneel dat een participatiegraad van 10 tot 15 % zou volstaan voor een efficiënt gebruik van de app: hoe kan dit worden gestaafd? Uit simulaties in Zweden en Nederland is gebleken dat zelfs 60 % onvoldoende zou zijn indien dit niet voldoende verspreid is over het hele grondgebied: wat is de mening van de expert hieromtrent?

Wat bluetooth betreft, vraagt de spreker hoe snel deze technologie zal evolueren gezien de problemen met onder meer plexiglas en muren: dit zal namelijk zorgen voor vele valse positieven.

En outre, on peut s'interroger sur le nombre de personnes qui possèdent actuellement un smartphone approprié en Belgique. Les téléphones Apple équipés d'un système d'exploitation iOS ne peuvent actuellement pas être utilisés parce qu'ils doivent être actifs. En ce qui concerne les téléphones Android, la dernière mise à jour doit être installée pour pouvoir utiliser l'application. À la lumière de ces éléments, quel est, selon l'expert, le nombre de gsm appropriés actuellement en circulation? On constate d'ailleurs qu'en 2019, un senior sur quatre ne possédait pas de smartphone.

Le professeur Preneel pourrait-il en outre fournir une estimation du coût que représentent le développement et la maintenance de cette application?

Le débat public susmentionné qui a eu lieu aux Pays-Bas a effectivement peut-être été un cirque médiatique, mais il a tout de même montré que des pirates informatiques pouvaient s'introduire dans un gsm par le biais du Bluetooth, indépendamment de l'application, qui peut être sûre en elle-même: qu'en est-il selon l'expert?

À l'attention de M. Raes, l'intervenant souligne qu'il est apparu, aux Pays-Bas, qu'il est possible de renforcer la capacité du Bluetooth au moyen d'un dispositif. Cela générerait de nombreux faux contacts positifs et pourrait inquiéter de nombreuses personnes: quel est l'avis de l'expert à ce sujet?

L'intervenant demande ensuite à M. Stevens s'il estime que l'approche autrichienne est appropriée? Que pense-t-il en outre d'un code source ouvert ("*open source*")? M. Stevens considère-t-il la chasse aux bugs (en anglais "*bug bounties*", une méthode consistant à rétribuer les citoyens pour détecter des failles dans le système) comme une approche adéquate? Que pense l'expert du texte de la proposition de résolution? Serait-il lui-même partisan d'encore renforcer ce texte?

Enfin, l'intervenant demande aux représentants de la Ligue des Droits Humains s'ils sont préoccupés par l'utilisation de l'application par rapport aux activités quotidiennes des intéressés? Il va de soi que les non-utilisateurs ne peuvent pas être sanctionnés, mais ne serait-il pas souhaitable de récompenser, par exemple, l'utilisation de l'application?

M. Egbert Lachaert (Open Vld) comprend les préoccupations relatives au respect de la vie privée: son groupe a cosigné la proposition. Le texte actuel de la proposition de résolution est-il satisfaisant selon l'APD?

Étant donné que les conditions prévues dans la proposition de résolution sont très strictes, il sera très difficile

Bovendien kan men zich afvragen hoeveel mensen vandaag in België een hiervoor geschikte smartphone bezitten? Wat Apple-telefoons betreft met een iOS-besturingssysteem, deze kunnen vandaag niet worden gebruikt omdat ze actief moeten zijn. Voor Android-telefoons is het nodig dat de laatste *update* is geïnstalleerd om de app te kunnen gebruiken. Hoeveel geschikte gsm's zijn er in het licht hiervan momenteel in omloop volgens de expert? Men stelt trouwens vast dat in 2019 een op de vier senioren geen smartphone bezat.

Kan professor Preneel verder een raming geven van de kostprijs voor de ontwikkeling en het onderhoud van deze app?

Het al vermelde openbare debat dat in Nederland heeft plaatsgevonden was inderdaad misschien eerder een mediacircus, maar toch is hieruit gebleken dat hackers zich via bluetooth toegang kunnen verschaffen tot een gsm, los van de app die op zichzelf veilig kan zijn: wat is hiervan aan volgens de expert?

Ter attentie van de heer Raes merkt de spreker op dat in Nederland is gebleken dat het mogelijk is om de capaciteit van bluetooth te versterken door middel van een bluetooth-versterker: zodoende zouden vele valse positieven worden gegenereerd en zouden vele mensen zich ongerust kunnen maken: wat is de mening van de expert hieromtrent?

Aan de heer Stevens vraagt de spreker vervolgens of hij van mening is dat de Oostenrijkse benadering goed is? Wat is verder zijn mening over een opensource-broncode? Vindt de heer Stevens de zogenaamde "*bug bounties*" (waarbij burgers financieel worden beloond om fouten in het systeem op te sporen) een goede benadering? Wat is de mening van de expert over de tekst van het voorstel van resolutie? Zou hij zelf de tekst van de resolutie nog verder versterken?

Ten slotte vraagt de spreker aan de vertegenwoordigers van de Liga voor Mensenrechten of zij zich geen zorgen maken omtrent het gebruik van de app ten opzichte van dagelijkse activiteiten van de betrokkenen? Uiteraard mogen niet-gebruikers niet bestraft worden maar zou het niet wenselijk zijn om bijvoorbeeld het gebruik van de app te belonen?

De heer Egbert Lachaert (Open Vld) begrijpt de bezorgdheden omtrent de privacy: zijn fractie heeft het voorstel mee ondertekend. Volstaat de huidige tekst van het voorstel van resolutie voor de GBA?

Aangezien de voorwaarden in het voorstel van resolutie heel strikt worden geformuleerd, is het heel

de développer une application qui y sera conforme et de garantir qu'un nombre suffisant de citoyens l'utiliseront. L'alternative, c'est-à-dire le suivi des contacts physiques, ne rassure pas vraiment plus l'orateur à l'égard du respect de la vie privée: nous serons dès lors contactés téléphoniquement par différentes personnes physiques qui nous poseront toutes sortes de questions privées; ces informations seront conservées, etc. Quelle est la moins mauvaise de ces deux solutions?

M. Kris Verduyckt (sp.a.) constate que, selon M. Stevens, l'utilisation des données concernant les télécommunications est totalement anonyme alors que la professeure Degrave a fait référence aux travaux du professeur Yves-Alexandre de Montjoye, qui affirme que l'anonymat n'existe pas: qu'en est-il?

Procédera-t-on à un stockage centralisé des données? Qui, le cas échéant, possédera les données: les autorités publiques, les opérateurs de télécommunications ou une société tierce désignée à cette fin?

Quel est par ailleurs l'avis de M. Stevens à propos de la piste *open source* pour l'application?

S'agissant de la technologie Bluetooth, l'intervenant demande au professeur Preneel d'indiquer le temps (la durée) nécessaire pour obtenir un résultat? Est-ce possible, par exemple, lorsque des personnes en voiture attendent côte à côte à un feu rouge? On constate d'ailleurs que la fonction Bluetooth est souvent désactivée par de nombreux utilisateurs.

Il souhaite par ailleurs des précisions sur le pourcentage minimum d'utilisateurs pour qu'une telle application soit efficace. Enfin, n'est-il pas envisageable de procéder à l'actualisation d'applications des services publics existantes, comme "itsme", afin qu'elles disposent de plus de fonctionnalités; cela permettrait également de dépasser plus facilement la barre de 15 à 20 % d'utilisateurs.

Le membre demande à M. Raes si la technologie Bluetooth peut être facilement piratée? Il observe que, de plus, ce n'est pas vraiment une technologie stable, comme le savent tous ceux qui ont essayé de connecter un smartphone à une voiture par le Bluetooth.

L'intervenant attire l'attention de la Ligue des droits de l'Homme sur le fait qu'il y a, selon lui, un clivage entre les générations: les jeunes ont en effet déjà le sentiment que leurs données se trouvent un peu partout et adopteront dès lors plus facilement cette technologie. Par ailleurs, le membre craint qu'il s'agisse d'une obligation sociale, notamment de la part des employeurs.

moeilijk om een dergelijke app te ontwikkelen en ervoor te zorgen dat voldoende burgers de app ook gebruiken. Het alternatief, namelijk de fysieke *contact tracing*, stelt de spreker niet meteen meer gerust wat het privéleven betreft: we zullen worden opgebeld door verschillende fysieke personen die ons allerlei privévragen zullen stellen, deze informatie wordt opgeslagen enzovoort: wat is de minst slechte oplossing van de twee?

De heer Kris Verduyckt (sp.a) stelt vast dat volgens de heer Stevens het gebruik van telecomgegevens op een volledig anonieme manier gebeurt terwijl professor Degrave toch verwees naar het werk van professor Yves-Alexandre de Montjoye, die beweert dat anonimiteit niet bestaat. Wat is hiervan aan?

Zal worden voorzien in een centrale opslag van de gegevens? Wie zal eventueel de gegevens bezitten: de overheid, de telecomoperatoren of nog een aangestelde derde firma?

Wat is verder de mening van de heer Stevens omtrent een opensource-benadering voor de app?

Aan professor Preneel vraagt de spreker, wat de bluetooth-technologie betreft, hoe lang (duurtijd) contact nodig is om een hit te verkrijgen? Is dit bijvoorbeeld mogelijk wanneer men naast elkaar staat te wachten in de wagen aan een rood licht? Men stelt trouwens vast dat de bluetooth-functie door veel gebruikers vaak wordt afgezet.

Daarnaast kreeg hij graag meer uitleg over het minimale gebruikerspercentage opdat een dergelijke app efficiënt zou zijn. Is het ten slotte niet denkbaar dat men overgaat tot een update van bestaande overheidsapps, zoals "itsme", zodat deze meer functionaliteiten hebben; zodoende zou men ook gemakkelijker boven de 15 tot 20 % gebruikers uitkomen.

Aan de heer Raes vraagt de spreker of de bluetooth-technologie gemakkelijk kan worden gehackt? Bovendien gaat het niet echt om stabiele technologie zoals iedereen weet die getracht heeft om zijn smartphone via bluetooth te connecteren met de wagen.

Ter attentie van de Liga voor Mensenrechten merkt de spreker op dat er volgens hem sprake is van een generatieverschil: jongeren hebben immers nu al het idee dat hun gegevens nu al overal verspreid zitten en zullen deze technologie dan ook gemakkelijker omarmen. Daarnaast vreest de spreker dat het zal gaan om een sociale verplichting, onder meer vanwege de werkgevers.

Enfin, l'intervenant constate, comme le professeure Degrave, que les GAFAM ne sont effectivement pas des entreprises philanthropiques: comment sera-t-il possible de tenir ces entreprises à l'écart du processus? À moins que nous n'ayons besoin d'elles parce que la technologie s'appuie sur leurs systèmes …

Monsieur Nabil Boukili (PVDA-PTB) fait observer que dans un avis récent, l'autorité néerlandaise chargée des données personnelles (*Autoriteit Persoonsgegevens*, AP) indique que les données de localisation sont toujours des données personnelles. Ce qui implique que le consentement de la personne concernée doit donc être toujours demandé afin de pouvoir traiter ces informations. Toute personne qui sait où quelqu'un vit ou travaille et qui combine ces données avec les données de localisation "anonymisées" de nombreuses personnes peut utiliser cette combinaison pour déterminer à qui elles appartiennent. Il est important de souligner qu'il est impossible de rendre ce type de données anonymes, car elles ne sont jamais irréversibles. Quelle est la position de l'APD à ce sujet? Les données de localisation "anonymes" existent-elles?

L'article 35, 1, du RGPD stipule: "Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires."

Question à M Stevens: l'APD peut-elle garantir que, compte tenu de la grande importance sociale de cette discussion, ces analyses d'impact des différentes applications envisagées seront rendues publiques?

Le professeur Preneel, chef du groupe de recherche Cosic KUL, collabore au protocole DP-3T également cité dans la résolution. Le protocole DP-3T a été développé autour de l'idée d'utiliser le "BLE-RSSI" (Bluetooth *Low-Energy – Received Signal Strength Indicator)* pour déterminer à quel moment différentes personnes ont été à proximité les unes des autres sur une durée déterminée. Le principe est que la proximité d'un autre smartphone, qui utilise la même technologie, agit comme un proxy pour la transmission du coronavirus. Chaque fois que vous vous trouvez à proximité d'une personne compatible pendant un certain temps, celle-ci est stockée. Si un nombre suffisant de personnes utilisent une telle

Ten slotte stelt de spreker samen met professor Degrave vast dat de GAFAM inderdaad geen filantropische instellingen zijn: op welke manier zal men deze bedrijven uit het proces kunnen weghouden? Tenzij we ze nodig hebben omdat de technologie immers draait op hun systemen…

De heer Nabil Boukili (PVDA-PTB) wijst erop dat de Nederlandse instantie die bevoegd is inzake persoonsgegevens (de Autoriteit Persoonsgegevens – AP) in een recent advies aangeeft dat locatiegegevens altijd persoonsgegevens zijn. Derhalve moet steeds de toestemming van de betrokkene worden gevraagd om die informatie te mogen verwerken. Om het even wie die weet waar iemand woont of werkt en die deze gegevens kruist met de van tal van mensen beschikbare "geanonimiseerde" locatiegegevens, kan bepalen om wiens gegevens het gaat. Het is belangrijk erop te wijzen dat dergelijke gegevens onmogelijk anoniem kunnen worden gemaakt omdat ze nooit onomkeerbaar zijn. Wat is het standpunt van de GBA daaromtrent? Bestaat er zoiets als "anonieme" locatiegegevens?

Artikel 35, 1, van de AVG luidt als volgt: "Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Één beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.".

Vraag aan de heer Stevens: kan de GBA, in het licht van het grote maatschappelijke belang van deze discussie, waarborgen dat deze impactanalyses van de verschillende overwogen toepassingen openbaar zullen worden gemaakt?

Professor Preneel, hoofd van de onderzoeksgroep Cosic van de KUL, werkt mee aan het DP-3T protocol, dat eveneens in het voorstel van resolutie wordt vermeld. Het DP-3T protocol werd ontwikkeld rond het idee om de bluetooth *Low-Energy – Received Signal Strength Indicator* (afgekort BLE-RSSI) te gebruiken, met de bedoeling te bepalen op welk tijdstip verschillende mensen gedurende een bepaalde periode in mekaars nabijheid zijn geweest. Als principe geldt dat de nabijheid van een andere smartphone die van dezelfde technologie gebruik maakt, fungeert als een *proxy* voor de overdracht van het coronavirus. Telkens als iemand zich gedurende een bepaalde tijdspanne in

application tout au long de la journée, il serait possible de retrouver les personnes qui ont été en contact avec un patient positif au COVID-19 dans le cadre d'une stratégie de test et de suivi. La valeur ajoutée de l'application est que les personnes qui auraient été oubliées ou inconnues au patient pourraient être identifiées par cette méthode pour autant qu'elles utilisent également l'application.

M. Boukili a quelques questions fondamentales sur les prémisses sur lesquelles repose le fonctionnement du protocole et celles-ci concernent le taux d'adoption nécessaire, l'efficacité du protocole et la manière dont une large adoption d'une telle application peut changer notre société.

Pour ce qui concerne le taux d'adoption nécessaire, est-ce que le professeur Preneel peut indiquer quel est le pourcentage minimum de la population qui doit installer l'application?

Environ combien de smartphones en Belgique sont équipés du BLE, la variante spécifique du protocole Bluetooth utilisé dans ces appareils? Le site web Ars Technica note que près de 60 % des smartphones dans le monde ne disposent pas de cette technologie et qu'il s'agit principalement des modèles les plus anciens et les moins chers.

L'efficacité dépend de la manière dont le BLE-RSSI peut estimer correctement les distances entre les personnes. Cette estimation est-elle précise et dépend-elle de facteurs externes tels que des obstacles peu élevés qui peuvent bloquer les signaux alors que la transmission du virus est possible, ou à l'inverse, des murs qui bloquent la transmission du virus mais qui ne sont pas remarqués dans le protocole. Combien de résultats faux positifs et faux négatifs le professeur attend-il?

Le 8 avril, le professeur Serge Vaudenay de l'EPFl à Lausanne, en Suisse, a publié une analyse du protocole DP-3T en préimpression dans laquelle il fait quelques remarques critiques sur la manière dont la technologie peut être utilisée de manière abusive. Le 21 avril, le "dépôt Github" du protocole DP-3T a publié une vue d'ensemble intitulée "Évaluation des risques en matière de confidentialité et de sécurité des systèmes de traçage numérique de proximité", dans laquelle différentes versions sont examinées. Il va sans dire qu'une analyse académique approfondie est nécessaire avant de demander à tout le monde dans la société de se promener avec une balise Bluetooth. La lecture de ces sources nous donne

de buurt van een compatibele persoon bevindt, wordt die persoon opgeslagen. Mochten voldoende mensen een dergelijke toepassing de hele dag door gebruiken dan zou het mogelijk zijn om na te gaan wie met een COVID-19-positieve patiënt in contact is gekomen als onderdeel van een test- en opvolgingsstrategie. De toegevoegde waarde van de applicatie bestaat erin dat mensen die zouden zijn vergeten of die onbekend zijn voor de patiënt, met die methode zouden kunnen worden geïdentificeerd op voorwaarde dat ook zij de applicatie gebruiken.

De heer Boukili heeft enkele fundamentele vragen omtrent de premissen waarop de werking van het protocol berust. Ze hebben betrekking op de noodzakelijke adoptiegraad, op de doeltreffendheid van het protocol en op de manier waarop een ruime aanwending van een dergelijke toepassing onze samenleving kan veranderen.

Kan professor Preneel in verband met de noodzakelijke adoptiegraad aangeven wat het minimumpercentage is van de bevolking dat de applicatie moet installeren?

Hoeveel smartphones ongeveer zijn in België uitgerust met BLE, de specifieke variant van het bij die toestellen gebruikte bluetooth-protocol? Op de webstek *Ars Technica* wordt aangegeven dat wereldwijd bijna 60 % van de smartphones niet over die technologie beschikken en dat het daarbij vooral om de oudste en de goedkoopste modellen gaat.

De doeltreffendheid hangt af van de mate waarin de BLE-RSSI de afstand tussen de personen correct kan inschatten. Is die inschatting nauwkeurig en kan ze worden beïnvloed door externe factoren zoals lage obstakels die de signalen kunnen blokkeren terwijl het virus wel degelijk kan worden overgedragen? Of is het omgekeerd ook mogelijk dat muren die de overdracht van het virus tegengehouden, niet door het protocol worden opgemerkt? Hoeveel valse positieve en negatieve resultaten verwacht de professor?

Op 8 april 2020 heeft professor Serge Vaudenay van de *École polytechnique fédérale de Lausanne* in Zwitserland een voorpublicatie van een analyse van het DP-3T-protocol uitgebracht, waarbij hij enkele kritische kanttekeningen plaatst bij deze technologie, omdat ze namelijk kan worden misbruikt. Op 21 april werd op de website GitHub, waarop het DP-3T-protocol wordt gehost, een algemene beschouwing gepubliceerd, getiteld "*Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems*". Daarin werden verschillende versies onderzocht. Het spreekt voor zich dat een grondige academische analyse noodzakelijk is alvorens aan iedereen in de samenleving te vragen steeds een

matière à réflexion. Est-ce que le professeur Preneel peut expliquer ce qui suit dans ce contexte?

Que signifie "*wardriving*" dans le deuxième document et est-ce que ce risque peut-être exclu dans le cadre d'un système de traçage basé sur le Bluetooth?

Peut-on exclure que les utilisateurs de toute forme de traçage Bluetooth puissent être suivis pendant un certain temps une fois qu'ils connaissent la "clé maîtresse" qui génère les "*Ephemeral IDs*"?

Est-il possible d'exclure la possibilité que les gouvernements utilisent les données de l'application, telles que le nombre de contacts sociaux que vous avez, pour vérifier si les personnes sont en quarantaine? Eventuellement après avoir donné un mandat d'accès?

Est-il possible d'exclure la possibilité que l'état de santé des personnes connues soit rendu accessible en les recherchant de manière ciblée?

Est-il possible d'exclure la possibilité que les pays ou régions où les différentes applications sont utilisées soient également enregistrés dans l'application? Et, du point de vue de la protection de la vie privée et du principe de minimisation des informations, est-il préférable qu'une application soit développée au niveau fédéral ou au niveau des entités fédérées?

Ensuite, le ministre a déjà déclaré à plusieurs reprises que le déploiement d'une application appartient aux entités fédérées. Comme le coronavirus ne s'arrête pas à la frontière linguistique, cela signifie qu'un protocole doit être mis en place pour que les différentes applications puissent échanger des données entre elles.

Qu'est-ce que la Ligue des Droits Humains en pense? Le développement de différentes applications devant communiquer entre elles ne risque-t-il pas d'entraîner des risques supplémentaires pour leurs utilisateurs, notamment le risque de fuites dues à l'échange de données entre différentes applications?

Est-ce que la Ligue des Droits Humains craint que la crise actuelle soit utilisée pour mettre en place des mécanismes de contrôle à grande échelle qui ne seront pas supprimés progressivement après la crise?

On estime que 50 à 80 % de la population doit utiliser une telle application avant qu'elle fonctionne. L'orateur vient de demander au professeur Preneel quel devrait être ce pourcentage selon lui. En tout cas, ce pourcentage

bluetooth-baken op zak te hebben. De lezing van die bronnen geeft stof tot nadenken. Kan professor Preneel in dat verband nadere toelichting geven bij de hierna volgende punten?

Wat betekent de term "*wardriving*" in het tweede document en kan dat risico in het raam van een op bluetooth gebaseerd traceringssysteem worden uitgesloten?

Kan worden uitgesloten dat de gebruikers van om het even welke vorm van bluetooth-tracering gedurende een bepaalde tijd kunnen worden gevolgd nadat ze de hoofdsleutel die "*Ephemeral IDs*" genereert, hebben weten te achterhalen?

Kan de mogelijkheid worden uitgesloten dat de regeringen de gegevens van de app (bijvoorbeeld het aantal sociale contacten) zullen gebruiken om te controleren of de personen in quarantaine zijn, eventueel nadat een toegangsmachtiging werd gegeven?

Kan de mogelijkheid worden uitgesloten dat de gezondheidstoestand van de personen die gekend zijn toegankelijk wordt gemaakt door ze gericht op te sporen?

Kan de mogelijkheid worden uitgesloten dat de landen en de regio's waar de verschillende apps worden gebruikt ook in de app worden geregistreerd? Uit het oogpunt van de bescherming van de persoonlijke levenssfeer en van het beginsel van gegevensminimalisatie rijst ten slotte de vraag of een app bij voorkeur op het federaal niveau dan wel op deelstaatniveau dient te worden ontwikkeld.

Voorts heeft de minister al meermaals verklaard dat de uitrol van een app een bevoegdheid van de deelstaten is. Aangezien het coronavirus niet stopt aan de taalgrens, betekent zulks dat een protocol moet worden ingesteld opdat de diverse apps onderling gegevens zouden kunnen uitwisselen.

Wat denkt de *Ligue des Droits Humains* daarvan? Dreigt de ontwikkeling van diverse apps die onderling moeten communiceren geen bijkomende risico's voor de gebruikers ervan met zich te brengen, in het bijzonder het risico op lekken ten gevolge van de gegevensuitwisseling tussen verschillende applicaties?

Vreest de *Ligue des Droits Humains* dat de huidige crisis zal worden aangewend om middelen voor grootschalige controle in te zetten die na de crisis niet geleidelijk zullen worden afgeschaft?

Opdat een dergelijke app zou werken, moet ze naar schatting door 50 tot 80 % van de bevolking worden gebruikt. De spreker heeft professor Preneel gevraagd hoe hoog dat percentage volgens hem moet zijn. Het is

est très élevé. À titre de comparaison: 65 % des Belges ont un profil Facebook, moins de gens ont l'application Facebook sur leur portable. Le ministre De Backer lui-même a souligné qu'en Autriche, la Croix-Rouge a fait beaucoup de publicité pour une application COVID-19 et que seuls 3 à 4 % de la population utilisent efficacement l'application.

Outre le fait qu'une grande partie de la population pourrait ne pas vouloir utiliser une application corona, le membre souligne que tout le monde ne possède pas un smartphone. En particulier, les personnes âgées, les enfants ou les personnes en situation de pauvreté.

Qu'est-ce que la Ligue pense de l'accessibilité d'une application? Est-ce qu'il n'y a pas de risque d'effet Matthieu, laissant de côté précisément les personnes vulnérables qui en ont le plus besoin?

Finalement, l'orateur pose une question à M. Raes: les experts nous disent que la technologie Bluetooth est facile à pirater. Quelles sont les conditions requises pour qu'un système protège utilement son intégrité? Un smartphone commercial répond-il à ces exigences?

Mme Catherine Fonck (cdH) aborde d'abord la question de la faisabilité de l'application: est-il possible de fournir un calendrier concernant la disponibilité d'une application de ce type en Belgique?

S'agissant de la question de l'efficacité, elle demande s'il est possible de fournir une projection de la capacité de dépistage nécessaire pour qu'une telle application puisse apporter toute sa plus-value.

En effet, il a été rapporté dans la presse qu'au moins 60 % de la population devrait installer l'application: quelle est la validité scientifique de ce chiffre et s'agit-il d'un pourcentage de la population générale ou des personnes qui présentent des symptômes? Ce pourcentage est-il un ordre de grandeur isolé ou doit-il être considéré en combinaison avec le *tracing* manuel?

Elle s'adresse ensuite aux membres de la *Task Force* "*Data & Technology Against Corona*": peuvent-ils indiquer si le gouvernement a déjà travaillé ou non à l'élaboration d'une base juridique pour ces applications?

Il existe certes déjà un cadre légal, notamment sur la protection de la vie privée et la prophylaxie des maladies transmissibles, qui s'inscrit dans un cadre sanitaire européen global. Mais n'est-il pas également nécessaire de prévoir une base légale pour la participation

in elk geval heel hoog. Ter vergelijking: 65 % van de Belgen heeft een Facebookprofiel, maar het aantal gebruikers met de Facebook-app op hun gsm ligt lager. Minister De Backer heeft zelf benadrukt dat in Oostenrijk het Rode Kruis veel reclame voor een COVID-19-app heeft gemaakt, maar dat slechts 3 tot 4 % van de bevolking de app doeltreffend gebruikt.

Het lid benadrukt dat het niet alleen zou kunnen dat een groot deel van de bevolking de corona-app niet wenst te gebruiken, maar dat bovendien niet iedereen over een smartphone beschikt. De spreker denkt daarbij in het bijzonder aan de ouderen, aan de kinderen of aan de mensen in armoede.

Wat denkt de *Ligue des Droits Humains* over de toegankelijkheid van een app? Dreigt er geen Mattheuseffect te ontstaan, waarbij precies de kwetsbare personen die ze het meest nodig hebben uit de boot vallen?

Tot slot heeft de spreker een vraag voor de heer Raes. De deskundigen geven aan dat de bluetooth-technologie gemakkelijk gehackt kan worden. Welke voorwaarden moeten vervuld zijn zodat een systeem de integriteit ervan terdege beschermt? Voldoet een commerciële smartphone aan die vereisten?

Mevrouw Catherine Fonck (cdH) gaat vooreerst in op de haalbaarheid van de operatie: is het mogelijk om een timing te verstrekken met betrekking tot de beschikbaarheid van een dergelijke app in België?

Wat daarnaast de efficiëntie betreft vraagt zij of het mogelijk is om een projectie te geven van de noodzakelijke testcapaciteit opdat een dergelijke app zijn volledige meerwaarde zou kunnen realiseren.

Men heeft inderdaad in de pers vernomen dat minstens 60 % van de bevolking de app zou moeten installeren: welke is de wetenschappelijke validiteit van dit cijfer en gaat het hier een percentage van de algemene bevolking of van diegenen die symptomen vertonen? Is deze 60 % een op zichzelf staande grootheid of moet dit percentage worden gezien in combinatie met manuele *tracing*?

Vervolgens richt zij zich tot de leden van de taskforce "*Data & Technology Against Corona*"*:* kunnen zij zeggen of de regering al heeft gewerkt rond een wettelijke basis voor deze apps of is zulks niet het geval?

Verder bestaat er uiteraard al een wettelijk kader, onder meer de wetgeving op de privacy en op de profylaxis van besmettelijke ziekten, die zich situeert in een globaal Europees sanitair kader. Is het niet nodig om daarnaast ook een wettelijke basis te voorzien voor

des 2 000 traceurs de contact, qui ne sont pas soumis au secret médical et qui présentent donc chacun des risques individuels en termes de respect de la vie privée des citoyens? L'intervenante donne l'exemple de fichiers Excel qui seraient accessibles à ces 2 000 participants: cela ne pose-t-il pas un risque d'atteinte à la vie privée au moins aussi grand que l'installation d'applications de suivi strictement réglementées?

La Commission nationale française de l'informatique et des libertés (CNIL), composée d'experts en matière de respect de la vie privée, a ouvert la porte à une application de ce type le week-end dernier: quelle est l'attitude des experts vis-à-vis de l'avis donné à ce sujet par la CNIL qui, en substance, ne voit pas d'ingérence dans la vie privée, dans l'application proposée, dès lors que son utilisation n'est pas imposée? (*https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid*).

Enfin, la membre se demande si les critiques très inquiétantes sur le rôle des GAFAM dans ce dossier sont toujours pertinentes dès lors que, techniquement, ils ne libèrent que le Bluetooth et donnent, de plus, pour la première fois, accès à leurs codes. En outre, Google ne créerait pas d'application mais remplirait seulement le rôle d'interface.

Mme Sophie Rohonyi (DéFI) souhaite tout d'abord poser quelques questions à MM. Stevens et Raes. On a appris que les centres d'appel auront besoin de 2 000 collaborateurs pour le suivi des contacts. Où en est le recrutement à cet égard? De qui s'agira-t-il? Quelles sont les exigences en matière de diplômes? Une formation spécifique est-elle prévue?

Il se murmure que les mutuelles vont pouvoir répondre à l'appel d'offres de l'autorité fédérale, compte tenu de leur expérience en matière de dossiers médicaux confidentiels. Est-ce exact et cela offre-t-il des garanties suffisantes en termes de respect de la vie privée?

En ce qui concerne le rôle des entités fédérées, en particulier des Régions, l'intervenante demande quelle Région sera compétente par example à l'égard d'une personne qui travaille à Bruxelles, qui y a ses contacts, mais qui est domiciliée en Flandre ou en Wallonie? Ou s'agira-t-il d'un centre d'appel unique cofinancé par les trois régions?

En ce qui concerne le rôle de l'Union européenne, la membre demande comment une harmonisation minimale entre les États membres peut être assurée dans le respect de la vie privée. Que pensent les experts des recommandations de l'Union européenne en la matière? Par l'intermédiaire de la KUL, 130 chercheurs

de participatie van de 2 000 *contact tracers* die niet onderworpen zijn aan het medisch beroepsgeheim en die daardoor elk een individueel risico vormen voor de privacy van de burgers? De spreekster geeft het voorbeeld van Excelbestanden die toegankelijk zouden zijn voor deze 2 000 deelnemers: levert dit niet op zijn minst even grote risico's voor inbreuken op de privacy als de installatie van strikt gereglementeerde *tracing* apps?

De Franse CNIL, die bestaat uit experten inzake privacy, heeft het afgelopen weekend de deur geopend voor een dergelijke applicatie: wat is de houding van de experten ten opzichte van het advies dat de CNIL hieromtrent heeft verstrekt, dat ten gronde geen inbreuken op het privéleven ziet in de voorgestelde applicatie, aangezien het gebruik ervan niet wordt opgelegd? (*https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid*).

Ten slotte vraagt het lid zich af of de zeer verontrustende kritieken op de rol van de GAFAM in dit dossier nog wel pertinent zijn mits zij op technisch vlak enkel bluetooth zouden vrijgeven en bovendien voor het eerst ooit toegang geven tot hun codes; bovendien maakt Google zelf geen app maar vervult het enkel de rol van interface.

Mevrouw Sophie Rohonyi (DéFI) wenst eerst enkele vragen te stellen aan de heren Stevens en Raes. Er werd vernomen dat de callcenters 2 000 medewerkers zouden nodig hebben voor contact tracing: hoe ver is men gevorderd met de aanwerving van de betrokkenen? Over wie gaat het? Welke zijn de diplomavereisten? Wordt een specifieke vorming voorzien?

Er wordt gefluisterd dat de mutualiteiten zouden ingaan op de offerteaanvraag van de federale overheid gezien hun ervaring met confidentiële medische dossiers: is dit correct en biedt dit voldoende garanties op het vlak van de bescherming van het privéleven?

Wat de rol van de gefedereerde entiteiten en met name de gewesten betreft vraagt de spreekster welk gewest bijvoorbeeld bevoegd zou zijn indien het gaat om een persoon die werkzaam is in Brussel en daar zijn contacten heeft maar gedomicilieerd is in Vlaanderen of in Wallonië? Of zou het gaan om één enkel callcenter dat door de drie gewesten samen wordt gefinancierd?

Wat de rol van de Europese Unie aangaat vraagt het lid hoe een minimale harmonisatie tussen de lidstaten kan worden voorzien met respect voor het privéleven? Wat is de mening van de experten over de aanbevelingen van de Europese Unie in deze materie? 130 onderzoekers nemen via de KUL deel aan een Europees project met

participent à un projet européen visant à mettre au point une norme européenne permettant aux applications mobiles de fonctionner au-delà des frontières. Qu'en pensent les experts?

Le traçage doit par ailleurs aller de pair avec un dépistage massif, mais compte tenu des problèmes qui se sont posés dans les maisons de repos ainsi que dans les hôpitaux et auprès des personnes présentant des symptômes, on peut émettre certains doutes. Quid de la liberté du médecin de procéder à un test ou à la mise en quarantaine? Le médecin disposera-t-il encore d'une marge d'appréciation?

Qu'est-ce qui garantit que l'on pourra continuer à empêcher que l'intéressé puisse savoir qui l'a contaminé?

De quelle manière peut-on éviter que des données soient sauvegardées avant leur suppression automatique?

Compte tenu du caractère sensible des données médicales, tant le RGPD que la législation relative à la protection de la vie privée disposent que ces données ne peuvent être traitées que par des personnes soumises au secret médical. Ces opérations de traçage pourront-elles se dérouler sans le contrôle d'une personne soumise au secret médical?

L'intervenante, renvoyant au professeur Preneel, fait observer que les signaux Bluetooth peuvent avoir une force différente selon que l'appareil se trouve par exemple dans une poche ou dans la main de la personne. Cet élément n'entraîne-t-il pas un risque de faux positifs et de faux négatifs?

Renvoyant à la professeure Degrave, l'intervenante indique qu'elle comprend les réserves relatives aux GAFAM, mais quelle autre solution y a-t-il?

M. Gilles Vanden Burre (Ecolo-Groen) souligne, à l'intention de M. Stevens, que l'application mobile doit être considérée au regard de différents groupes cibles. La fracture numérique étant très importante en Belgique, l'utilisation de la technologie est beaucoup moins évidente – comme l'illustre l'accès aux smartphones et leur détention par les malades et les personnes âgées – dans les groupes marginalisés ou pour les enfants. Comment éviter de favoriser ainsi certaines catégories de citoyens?

L'intervenant demande par ailleurs des recommandations concrètes en ce qui concerne le traçage manuel. Des garanties spécifiques sont-elles nécessaires au sujet, par exemple, de la confidentialité ou de la durée de stockage maximale de certaines données?

het oog op het op punt stellen van een Europese standaard opdat de app over de grenzen heen zou werken: wat is de mening van de experten hieromtrent?

De tracering dient verder gepaard te gaan met massaal testen, maar gezien de problemen die zich hebben voorgedaan in de woonzorgcentra alsook in de ziekenhuizen en bij de mensen met symptomen kan men hierbij toch bedenkingen hebben: wat met de vrijheid van de arts om over te gaan tot een test of tot quarantaine: zal er morgen nog sprake zijn van een appreciatiemarge voor de betrokken arts?

Welke garantie bestaat er verder dat kan worden verhinderd dat de betrokkene kan zien wie hem of haar heeft besmet?

Op welke manier kan verder worden vermeden dat gegevens worden opgeslagen vooraleer ze "uitdoven"?

Gezien het gevoelig karakter van medische gegevens preciseren zowel de AVG als de privacywetgeving dat deze gegevens enkel kunnen worden gemanipuleerd door personen die onderworpen zijn aan een medisch beroepsgeheim: zullen deze traceringsoperaties kunnen verlopen zonder toezicht van een persoon die onder het medisch geheim valt?

Ter attentie van professor Preneel merkt de spreekster op dat bluetooth-signalen een verschillende sterkte kunnen hebben naargelang bijvoorbeeld het toestel zich in de jaszak of een hand van de betrokkene bevindt: bestaat hierdoor niet het risico op valse positieven en valse negatieven?

Ter attentie van professor Degrave begrijpt de spreekster de reserves wat de GAFAM betreft, maar wat is het alternatief?

De heer Gilles Vanden Burre (Ecolo-Groen) merkt op, ter attentie van de heer Stevens, dat men de app dient te situeren ten opzichte van verschillende doelgroepen: aangezien de digitale kloof in België heel groot is, is dit heel wat minder vanzelfsprekend, wat blijkt uit de toegang tot en het bezit van smartphones bij zieken en bejaarden, in gemarginaliseerde groepen alsook voor kinderen: hoe zal men vermijden dat bepaalde categorieën van burgers hier worden bevoordeeld?

Daarnaast vraagt de spreker naar concrete aanbevelingen met betrekking tot de manuele tracering: zijn specifieke waarborgen nodig met betrekking tot bijvoorbeeld vertrouwelijkheid of maximum opslagduur van bepaalde gegevens?

Mme Kathleen Verhelst (Open Vld) s'enquiert de la probabilité que l'on parvienne effectivement à mettre au point une application mobile, compte tenu des considérations formulées en matière de participation, de respect de la vie privée, de coûts, de risques, etc.?

Est-il possible de fournir une estimation du coût total du déploiement de cette application? Le rendement global du projet a-t-il été évalué?

Sommes-nous soumis à des pressions internationales qui nous invitent à participer à une initiative européenne?

Qu'adviendra-t-il s'il apparait *a posteriori* que l'application n'est guère utile mais qu'entre-temps, beaucoup de protections ont été abandonnées en termes de respect de la vie privée?

Il est par ailleurs très positif de travailler à la fois sur les aspects technologiques, juridiques et de sécurité, mais nous sommes tellement concentrés sur la conception des dimensions technologiques et juridiques que nous risquons de définir d'ores et déjà la société de demain avant même d'avoir organisé d'avoir un débat social à ce sujet. Ne pourrions-nous pas attendre les résultats des autres pays, et organiser, dans l'intervalle, un débat de fond à ce sujet?

Ne pourrait-on pas faire en sorte que cette application soit également mutuellement avantageuse pour le citoyen et bénéficie dès lors d'une plus large adhésion?

Mme Katleen Bury (VB) évoque le cadre légal. La Ligue des droits de l'Homme a parlé d'un conflit d'intérêts dans le cas où un membre de la *task force* émettrait également un avis par la suite. Qu'en est-il?

Comment la vie privée sera-t-elle préservée? Comment les données seront-elles rendues anonymes? Ne s'agira-t-il pas plutôt d'un pseudo-anonymat qui n'empêchera pas de retracer ultérieurement l'identité de la personne? La membre n'a en effet aucun mal à imaginer que les compagnies d'assurance, par exemple, seront très intéressées de savoir qui a été malade puisque cette maladie a un impact sur presque tous les organes humains.

M. Jaak Raes (VSSE) constate que beaucoup de questions ont trait à la technologie Bluetooth et en particulier au risque de voir celle-ci détournée dans le but de soustraire illégalement des données de sécurité aux détenteurs d'appareils Bluetooth.

L'orateur répète que le père spirituel de cette technologie a pris la plume cette semaine pour en expliquer les limites. Le Bluetooth suscite des attentes importantes. Bien que de nombreuses personnes disposent d'un

Mevrouw Kathleen Verhelst (Open Vld) vraagt hoe groot de kans is dat men werkelijk tot een app komt, wanneer men rekening houdt met overwegingen inzake participatie, privacy, kosten, risico's, enzovoort?

Is het mogelijk om een inschatting te geven van de volledige kostprijs van de uitrol van een dergelijke app? Werd het rendement van dit hele opzet nader bekeken?

Is er sprake van internationale druk om mee te doen met een Europees initiatief?

Wat als achteraf zou blijken dat de app toch niet echt nuttig is maar ondertussen toch veel privacy zou zijn opgegeven?

Het is verder een zeer goede zaak dat men zowel op technologisch, juridisch als veiligheidsvlak tegelijk aan het werk is, maar men is zodanig bezig met het uitwerken van de technologische en juridische aspecten dat het risico bestaat dat we nu al de maatschappij van de toekomst gaan bepalen in plaats van vooraf een maatschappelijk debat te voeren. Zou men niet kunnen wachten op de resultaten van andere landen en ondertussen een grondig debat voeren?

Kan men er niet voor zorgen dat deze app ook andere *win-win*-aspecten oplevert voor de burger en op die manier ook meer gedragen zal zijn?

Mevrouw Katleen Bury (VB) gaat in op het wettelijk kader: de Liga voor Mensenrechten sprak van een belangenconflict indien een lid van de taskforce achteraf ook een advies uitbrengt: wat is hiervan aan?

Op welke manier zal de privacy worden gewaarborgd? Hoe zullen de gegevens worden geanonimiseerd? Gaat het niet eerder om een pseudo-anonimiteit waarbij men achteraf alsnog kan traceren over wie het gaat? Het lid kan zich immers perfect inbeelden dat bijvoorbeeld verzekeringsinstellingen zeker interesse zullen tonen om te weten wie ziek is geweest, aangezien de ziekte een impact heeft op nagenoeg alle menselijke organen.

De heer Jaak Raes (VSSE) stelt vast dat vele vragen betrekking hebben op de bluetooth-technologie, in het bijzonder het risico dat deze zou worden misbruikt om op illegale wijze veiligheidsgegevens te ontfutselen aan de houder van een bluetooth-apparaat.

De spreker herhaalt dat de geestelijke vader van deze technologie eerder deze week in de pen klom om de grenzen ervan toe te lichten. De verwachtingen omtrent bluetooth zijn hooggespannen. Hoewel zeer veel

smartphone équipé de cette technologie, il ne s'agit souvent pas de la version la plus récente pourvue d'une nouvelle radio qui permet d'évaluer les distances de façon très précise.

La Sûreté de l'État estime que la technologie Bluetooth actuellement utilisée par la plupart des appareils est susceptible d'être piratée et qu'elle n'offre donc pas une garantie de sécurité absolue. Les applications les plus modernes peuvent éventuellement être plus performantes à cet égard. On peut bien entendu réduire les risques en évitant de lier des données à caractère personnel aux radios Bluetooth, mais cela rendra le *tracing* individuel prévu dans la lutte contre le coronavirus impossible. Il convient donc de limiter autant que possible l'échange d'autres données à caractère personnel ou d'enregistrer celles-ci le cas échéant sur un autre serveur.

La Sûreté de l'État n'est pas compétente pour la désignation des *contact tracers*. Les citoyens doivent pouvoir être certains que les informations communiquées seront traitées correctement. L'orateur trace un parallèle avec les personnes qui travaillent au sein des services de renseignement et qui sont, elles aussi, potentiellement vulnérables. Il faut pouvoir accorder sa confiance, mais il faut aussi pouvoir la retirer dès le premier signe d'abus. Eu égard à la présence d'un facteur humain, il n'est pas absolument exclu que des informations sensibles soient un jour utilisées de façon inappropriée dans le cadre du *contact tracing*. Mais ce risque peut être minimisé grâce à certaines mesures de sécurité, comme l'interdiction faite aux *contact tracers* d'emporter les informations recueillies en dehors de leur lieu de travail.

M. Freilich a évoqué le risque d'espionnage. L'orateur renvoie à cet égard à ce qu'il a expliqué devant cette commission au cours de l'audition relative au déploiement de la technologie 5G (DOC 55 0981/001, p. 12). Il avait indiqué à l'époque que dans ce domaine, les services de sécurité ont une approche géostratégique de l'analyse des risques, qui tient compte d'un certain nombre de caractéristiques du pays dont provient la technologie. Les critères appliqués en l'espèce sont les suivants: le caractère potentiellement autoritaire du pays d'origine du fournisseur; la mesure dans laquelle un fournisseur peut agir indépendamment de son autorité nationale (les opérations commerciales du fournisseur concerné sont-elles indépendantes des préoccupations et/ou des ingérences nationales?); l'existence et l'application d'une législation nationale qui donne à un État (non membre de l'UE) une emprise sur les entreprises et la mesure dans laquelle cette législation est compatible avec la législation de l'UE; l'indépendance de l'ordre judiciaire dans le pays en question (à défaut de quoi les services peuvent par exemple être contraints de commettre des

mensen beschikken over een smartphone die is uitgerust met bluetooth-technologie, gaat het veelal niet om de modernste versie met een nieuwe radio die toelaat om zeer nauwkeurig afstanden in te schatten.

De Staatsveiligheid meent dat de bluetooth-technologie zoals die thans wordt gebruikt door de meeste toestellen, vatbaar is voor hacking en dus geen absolute veiligheidsgarantie biedt. De modernste applicaties kunnen eventueel meer veiligheidswaarborgen bieden. Men kan uiteraard op veilig spelen door de koppeling tussen persoonsgegevens en bluetooth-radio's te vermijden, maar op die manier maakt men ook de individuele tracing ter bestrijding van de coronacrisis onmogelijk. De aanbeveling is dus om zo weinig mogelijk andere persoonsgebonden informatie uit te wisselen of deze eventueel op te slaan op een server.

De Staatsveiligheid is niet bevoegd inzake de aanstelling van de *contact tracers*. Burgers moeten erop kunnen vertrouwen dat de meegedeelde informatie op een correcte wijze zal worden behandeld. De spreker trekt een parallel met mensen die werken binnen de inlichtingendiensten, die evenzeer potentieel kwetsbaar zijn. Men moet vertrouwen kunnen schenken, maar bij het eerste signaal van wangedrag moet dat vertrouwen ook kunnen worden ingetrokken. Er is een menselijke factor in het spel, dus het valt niet absoluut uit te sluiten dat er ooit ongepast gebruik zou worden gemaakt van gevoelige informatie in het kader van contact tracing. Maar dat risico kan worden geminimaliseerd door bepaalde veiligheidsmaatregelen, zoals het verbod voor *contact tracers* om de verkregen informatie mee te nemen buiten de werkplek.

De heer Freilich verwees naar de mogelijke dreiging van spionage. In dit verband herinnert de spreker aan de uiteenzetting die hij gaf in deze commissie tijdens de hoorzitting over de uitrol van 5G-technologie (DOC 55 0981/001, blz. 12). Hij legde toen uit dat de veiligheidsdiensten de risicoanalyse in dat verband geostrategisch benaderen, rekening houdend met een aantal karakteristieken van het land waaruit de technologie afkomstig is. Er worden daarbij met name de volgende criteria gehanteerd: het mogelijk autoritaire karakter van het land van afkomst van de leverancier; de mate waarin een leverancier zich onafhankelijk kan opstellen ten opzichte van zijn nationale overheid (staat de bedrijfsvoering van de betrokken leverancier los van nationale bekommeringen en/of inmenging?); het bestaan en de toepassing van nationale wetgeving die een (niet-EU-)Staat greep geeft op bedrijven, en de mate waarin die compatibel is met EU-wetgeving; de onafhankelijkheid van de gerechtelijke werking in het land in kwestie (bij gebreke waarvan diensten bijvoorbeeld kunnen verplicht worden inbreuken te plegen); en ten slotte de

infractions); la publicité des opérations commerciales et la mesure dans laquelle des facteurs tels que des aides d'État (cachées) ou une direction d'entreprise ou un actionnariat non transparents perturbent le fonctionnement normal du marché. M. Raes estime que ces critères s'appliquent *mutatis mutandis* à la technologie Bluetooth.

M. Raes indique en conclusion qu'il existe un risque de piratage et que pour réduire celui-ci au maximum, il s'indique d'échanger le moins possible de données à caractère personnel et surtout d'enregistrer celles-ci sur un serveur. La Sûreté de l'État n'est pas opposée au développement d'une application visant à lutter contre le coronavirus, à condition qu'il soit suffisamment tenu compte des aspects sécuritaires. Notre pays ne peut pas manquer ce rendez-vous, d'autant que nous serons sans doute confrontés dans le futur à une recrudescence du virus.

M. David Stevens (APD) estime qu'il est parfaitement possible de cumuler la qualité de membre de la *task force* et de président de l'APD sans qu'il soit question de confusion d'intérêts. L'orateur illustre son propos par un exemple. Toutes les applications liées au coronavirus doivent être agréées par la *task force* avant d'être proposées sur *Google Play* ou sur l'*App Store*. Pour obtenir cet agrément – une sorte d'autorisation – l'application doit réussir un test préliminaire rapide réalisé par la *task force*. Des dizaines de tests ont ainsi déjà été effectués. L'orateur indique que ce contrôle est très performant. Les applications qui présentent des failles importantes en matière de vie privée sont écartées. Si l'APD ne faisait pas partie de la *task force*, des applications de ce type seraient commercialisées et l'APD exercerait son contrôle régulier, mais elle serait contrainte de le faire *a posteriori*. Le test préliminaire, qui n'entraîne pas d'approbation formelle, constitue une forme de *privacy by design.* M. Stevens est heureux de faire partie de la *task force*, au sein de laquelle il veille à garantir la protection de la vie privée. Il n'y a donc pas de confusion d'intérêts et il n'y en aura pas davantage si l'APD devait, dans une phase ultérieure, rendre un avis ou réaliser une analyse d'impact relative à la protection des données concernant une application précédemment soumise à un test.

L'APD peut bel et bien contrôler des applications à l'étranger, même si c'est plus compliqué que dans un contexte national. Le RGPD contient des règles à cet effet. La question pertinente est de savoir où se trouve le principal établissement de celui qui est responsable du traitement. Pour les applications axées sur la Belgique, l'APD peut être compétente et est en tout cas concernée, et elle prendra contact avec son homologue dans le pays où est localisé l'établissement principal de celui

openheid van bedrijfsvoering en de mate waarin factoren zoals (verdoken) overheidssteun of niet-transparante bedrijfsleiding of aandeelhouderschap een normale marktwerking verstoren. De heer Raes is van mening dat deze criteria *mutatis mutandis* van toepassing zijn op bluetooth-technologie.

Tot besluit van zijn betoog stelt de heer Raes dat het risico op hacking bestaat en dat het, om dat risico maximaal te beperken, aanbeveling verdient zo weinig mogelijk persoonsgegevens uit te wisselen en deze vooral op te slaan op een server. De Veiligheid van de Staat is niet tegen de ontwikkeling van een app ter bestrijding van het coronavirus, gesteld dat er voldoende oog is voor de veiligheidsaspecten. Ons land mag deze boot missen, niet het minst omdat we in de toekomst wellicht zullen worden geconfronteerd met nieuwe opstoten.

De heer David Stevens (GBA) is van oordeel dat er geenszins sprake is van belangenvermenging bij het gelijktijdig uitoefenen van de functies van lid van de taskforce en voorzitter van de GBA. Hij illustreert dit aan de hand van een voorbeeld. Alle apps die te maken hebben met het coronavirus hebben een toezegging nodig vanwege de taskforce alvorens ze op Google Play of de App Store mogen terechtkomen. Die toezegging, een soort machtiging, volgt op het succesvol ondergaan van een snelle, preliminaire test door de taskforce. Tientallen tests werden zo al uitgevoerd. Volgens de spreker is deze check een uitstekende zaak. Apps die ernstige privacy-gebruiken vertonen worden eruit gefilterd. Mocht de GBA geen deel uitmaken van de taskforce, zouden zulke apps op de markt komen en zou de GBA haar reguliere toezicht uitoefenen, doch men zou noodgedwongen achter de feiten aanhollen. De preliminaire test, die geen formele goedkeuring inhoudt, is in wezen een manifestatie van *privacy by design.* De heer Stevens is dan ook verheugd deel uit te maken van de taskforce, waar zijn enige bekommernis de bescherming van de privacy is. Van enige belangenvermenging is dus geen sprake, ook niet wanneer de GBA in een later fase een advies of een gegevensbeschermingseffectbeoordeling zou dienen uit te brengen over een app die eerder een test onderging.

De GBA kan wel degelijk toezicht uitoefenen op apps in het buitenland, zij het dat dit moeilijker is dan in een nationale context. De AVG bevat daaromtrent regels. De relevante vraag is waar de belangrijkste vestiging zich bevindt van degene die verantwoordelijk is voor de verwerking. Voor apps die zich op de België richten is de GBA mogelijk bevoegd en in ieder geval betrokken, en zal zij contact nemen met haar tegenhanger in het land waar de hoofdvestiging van de app-aanbieder

qui propose l'application. Dans le cadre de l'application "corona", cette question de compétence jouera sans doute un rôle moins important, vu que l'on créera un cadre légal dont la territorialité pourra faire partie.

L'orateur confirme qu'une expertise spécialisée suffisante est disponible au sein de l'APD. En interne, l'APD compte cinq ingénieurs ICT, qui sont associés activement à ce dossier. Par ailleurs, l'APD peut également s'appuyer sur douze experts externes, six au sein de la Chambre contentieuse et six au sein du Centre de connaissances, notamment le professeur Preneel et le professeur de Montjoye.

Faut-il se baser sur la même logique pour le traçage manuel que pour les applications de suivi des contacts? La réponse est nuancée. Les mêmes principes, à savoir ceux relatifs à la protection de la vie privée, sont pertinents, comme la transparence, la minimalisation, le *privacy by design,* etc. Une différence fondamentale est cependant que, dans la variante manuelle, une contamination a été constatée et on vise une relation de personne à personne (également avec les personnes avec lesquelles la personne contaminée a eu des contacts), alors que, dans le cas de l'application, il s'agit d'enregistrer des contacts entre personnes d'une manière aussi anonyme que possible. Ce type d'application n'est pas la panacée. Il s'agit d'une tentative de soutenir le traçage manuel des contacts de manière judicieuse. Le traçage des contacts manuel et automatisé doit être considéré comme complémentaire, la répartition des compétences étant réglée en ce sens que la première forme doit être organisée au niveau régional.

M. Stevens répond à la question visant à savoir si le cadre légal est efficace que, conformément aux recommandations européennes, il faut viser un intérêt général, ce qui requiert une base légale. L'orateur ne se prononce pas quant à savoir s'il doit s'agir d'une loi ou d'un arrêté royal. On ne peut en aucun cas se contenter d'un simple consentement, ce qui permettrait à certaines grandes entreprises technologiques de lancer la même application.

L'orateur indique qu'il est en effet toujours associé au Comité européen de la protection des données (*European Data Protection Board* ou EDPB), qui rassemble les représentants des autorités nationales de protection des données de l'UE. L'APD a d'ailleurs collaboré très activement à l'élaboration des recommandations européennes.

Selon M. Stevens, on ne peut exclure que, sur le site internet de la Taskforce, certaines applications énumérées ne satisfassent pas entièrement aux obligation du RGPD. La Taskforce se limite en effet à un screening

gelokaliseerd is. In het kader van de corona-app zal die bevoegdheidskwestie wellicht minder spelen, nu hiervoor een wettelijk kader zal worden geschapen waarvan de territorialiteit deel kan uitmaken.

De spreker bevestigt dat er binnen de GBA voldoende gespecialiseerde expertise voorhanden is. Intern telt de GBA vijf ICT-ingenieurs in haar rangen, die actief worden betrokken bij dit dossier. Daarnaast kan de GBA ook bogen op twaalf externe experten, zes in de Geschillenkamer en zes in het Kenniscentrum, waaronder professor Preneel en professor de Montjoye.

Dient voor manuele tracing dezelfde logica te gelden als voor de tracing apps? Het antwoord is genuanceerd. Dezelfde principes, met name op het vlak van privacy, zijn relevant, zoals transparantie, minimalisatie, *privacy by design* enzovoort. Een fundamenteel verschil is echter dat er bij de manuele variant een besmetting werd vastgesteld en er een één-op-één-relatie wordt beoogd (ook met de personen met wie de besmette persoon in contact is geweest), daar waar het er bij de app om draait om op een zo anoniem mogelijke wijze contacten tussen personen te registreren. Zo'n app is geen wondermiddel. Het is een poging om de manuele contact tracing zinvol te ondersteunen. Manuele en geautomatiseerde contact tracing moeten als complementair worden beschouwd, waarbij de bevoegdheidsverdeling derwijze geregeld is dat die eerste vorm op gewestelijk niveau moet worden georganiseerd.

Op de vraag of het wettelijk kader afdoende is, antwoordt de heer Stevens dat, conform de Europese aanbevelingen, er een algemeen belang dient te worden nagestreefd, wat een wettelijke basis vereist. De spreker laat in het midden of dat een wet dan wel een genummerd KB dient te zijn. In geen geval mag worden volstaan met een loutere toestemming, wat bepaalde grote technologiebedrijven zou toelaten om dezelfde app te gaan lanceren.

De spreker geeft aan inderdaad nog steeds betrokken te zijn bij het Europees Comité voor Gegevensbescherming (*European Data Protection Board* of EDPB), waarin de vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten in de EU zijn vertegenwoordigd. De GBA heeft overigens zeer actief meegewerkt aan uitwerking van de Europese richtlijnen.

Volgens de heer Stevens valt het niet uit te sluiten dat op de website van de taskforce apps staan opgelijst die niet volledig beantwoorden aan de verplichtingen van de AVG. De taskforce beperkt zich immers tot een

préliminaire des applications, qui n'est pas suivi d'une approbation formelle; il est impossible, en quelques semaines, de soumettre des dizaines d'applications à une analyse approfondie du respect des conditions liées à la protection de la vie privée. Cette mission limitée est d'ailleurs aussi explicitement mentionnée sur le site internet. Il est possible – et ce n'est absolument pas problématique d'un point de vue éthique ou déontologique – que la Chambre contentieuse doive se pencher, à un stade ultérieur, sur une application mentionnée sur le site internet.

Comme l'a fait remarquer à juste titre M. Gilissen, il règne chez les citoyens une certaine inquiétude concernant les fuites de données et les violations de la vie privée dans le cadre des applications de suivi des contacts. Selon M. Stevens, c'est normal et c'est même une bonne chose que cette question fasse l'objet d'un débat de société, y compris au sein de cette commission. Il se réjouit d'ailleurs que l'on ait tenu compte, dès le début de cette initiative, des préoccupations en matière de respect de la vie privée. L'ensemble des compétences du ministre concerné n'y est sans doute pas étranger.

Les fuites de données sont indissociablement liées à la réalité technologique et ne sont jamais à exclure. Cela ne signifie cependant pas qu'il ne faut pas s'en protéger.

M. Stevens est assez favorable aux logiciels à source ouverte. Le fait que le code source soit rendu public est un signe de transparence et laisse supposer que le développeur n'a rien à cacher. Cela indique que l'on travaille de façon décentralisée, ce qui est absolument préférable à une banque de données centrale de personnes contaminées et de contacts. Cependant, il faut bien sûr prendre en compte les risques liés aux applications à source ouverte, à savoir les risques sur le plan de la sécurité nationale.

Selon M. Stevens, l'approche autrichienne, dans le cadre de laquelle les aspects centraux de la contamination sont enregistrés par l'autorité de contrôle du respect de la vie privée, ne semble pas, à première vue, un exemple attrayant. Il s'agit d'un rôle opérationnel qui peut éventuellement être confié à un sous-traitant, moyennant un cadre contractuel correct. L'APD, qui est une autorité de contrôle et, en cette qualité, peut infliger des sanctions (même aux pouvoirs publics), ne devrait pas assumer un tel rôle; cela créerait une confusion d'intérêts.

L'orateur est favorable à l'idée d'une implication citoyenne (qui passerait par exemple par des "chasses aux bugs" ou "*bug bounties*"). L'objectif central est de mettre en place un dispositif qui inspire confiance aux citoyens

preliminaire *screening* van de apps, waarop geen formele goedkeuring volgt; het is niet mogelijk om binnen het tijdsbestek van enkele weken tientallen apps aan een grondige analyse van de privacyvoorwaarden te onderwerpen. Deze beperkte missie staat overigens ook expliciet vermeld op de website. Het is mogelijk – en vanuit ethisch of deontologisch oogpunt geenszins problematisch – dat de Geschillenkamer zich in een later stadium zou dienen te buigen over een op de website vermelde app.

Zoals de heer Gilissen terecht opmerkte, heerst er bij de burgers enige bezorgdheid over datalekken en schendingen van de privacy in het kader van de tracing apps. Volgens de heer Stevens is dit normaal en is het zelfs een goede zaak dat hieromtrent een maatschappelijk debat wordt gevoerd, inclusief in deze commissie. Het stemt hem trouwens tevreden dat de bekommernissen inzake privacy van bij het prille begin van dit initiatief zijn meegenomen. Wellicht is het takenpakket van de bevoegde minister daaraan niet vreemd.

Datalekken zijn onlosmakelijk verbonden met de technologische realiteit en vallen nooit uit te sluiten. Dit betekent uiteraard niet dat men zich daartegen niet hoeft te wapenen.

De heer Stevens staat eerder positief ten opzichte van opensource-*software*. Het publiek beschikbaar stellen van de broncode getuigt van transparantie en doet vermoeden dat de ontwikkelaar niets te verbergen heeft. Het duidt op een decentrale werking, wat absoluut te verkiezen valt boven een centrale gegevensbank van besmette personen en contacten. De risico's verbonden met opensource-apps, met name op het vlak van de nationale veiligheid, moeten uiteraard wel worden meegenomen.

De Oostenrijkse benadering, waarbij de centrale aspecten van de besmetting door de toezichthouder op het vlak van privacy zelf worden opgenomen, lijkt de heer Stevens op het eerste gezicht geen aantrekkelijk voorbeeld. Dit is een operationele rol die eventueel aan een onderaannemer kan worden toevertrouwd, middels een deftig contractueel kader. De GBA, die een toezichthouder is en in die hoedanigheid sancties kan opleggen (zelfs aan de overheid), zou een dergelijke rol niet moeten opnemen; dit zou neerkomen op een belangenvermenging.

De spreker is de idee van burgerbetrokkenheid (bijvoorbeeld via "*bug bounties*") genegen. De centrale doelstelling is om iets te bouwen waar de burgers vertrouwen in hebben en mee de schouders willen onderzetten.

et qu'ils sont désireux de soutenir. Cette démarche s'inscrit également dans la philosophie du mouvement "numérique au service de l'intérêt général" ou "*data for good*", qui inspire également le niveau européen. L'orateur estime qu'à l'heure actuelle, la politique menée dans notre pays tient suffisamment compte de cette préoccupation. Ce n'est pas le cas partout: certains pays (par exemple la France) ont recours à des applications non décentralisées ou qui n'utilisent pas la technologie Bluetooth (Pologne). D'autres pays envisagent même d'imposer l'application.

Mme Soors a demandé si l'APD pourrait émettre un avis positif sur la proposition de résolution à l'examen. Abstraction faite du fait que l'APD n'a pas de compétence consultative formelle à l'égard des propositions de résolution, M. Stevens estime que le texte contient de nombreux éléments positifs: décentralisation, utilisation de la technologie Bluetooth et caractère volontaire de l'utilisation de l'application sont, à ses yeux, autant d'éléments essentiels pour apprécier la proportionnalité générale de la mesure envisagée. Quant à savoir si l'application envisagée se révélera efficace dans la lutte contre le coronavirus, rien ne permet malheureusement de l'affirmer avec certitude avant de l'avoir testée.

D'aucuns ont demandé comment la proposition de résolution pourrait être renforcée. L'orateur se félicite de (la qualité de) l'audition mais souligne qu'il reste des progrès à faire en termes de transparence du débat, en particulier en ce qui concerne la discussion relative à la base légale de l'application envisagée et le choix de l'instrument juridique (loi ou AR numéroté). L'orateur n'estime pas pour autant que nous devrions imiter nos voisins néerlandais, chez qui la sélection de l'application s'est opérée intégralement sur la place publique. Cette méthode ne fait que créer une illusion de transparence. L'AP, pendant néerlandais de l'APD, a été forcée de reconnaître, malgré toute son ouverture, qu'elle ne disposait pas de suffisamment d'informations pour porter un jugement pertinent sur les applications.

Différentes observations ont été formulées sur le couplage avec d'autres données et le rôle que la plateforme eHealth et la BCSS pourraient jouer à cet égard. M. Stevens n'a pas connaissance de ce couplage. Il suggère que la proposition de résolution pourrait être renforcée en insérant de manière plus explicite, dans le texte, l'interdiction de couplage avec d'autres données. De même, les rôles et les responsabilités des différents acteurs publics pourraient être précisés dans la proposition de résolution ou, mieux encore, dans la future loi ou le futur arrêté royal numéroté.

Enfin, compte tenu de la complémentarité entre le traçage de contacts manuel et le traçage numérique et

Dit strookt ook met de filosofie van "*data for good*" die ook het Europese niveau inspireert. De spreker meent dat het beleid in ons land momenteel voldoende rekening houdt met die bekommernis. Dit is niet overal het geval; in sommige landen wordt gewerkt aan apps die niet decentraal zijn (Frankrijk) of die niet werken met bluetooth-technologie (Polen). Er zijn ook landen die overwegen om de app te verplichten.

Mevrouw Soors vroeg of de GBA een positief advies zou verlenen omtrent het voorliggende voorstel van resolutie. Abstractie makend van het feit dat de GBA geen formele adviesbevoegdheid heeft inzake voorstellen van resolutie, meent de heer Stevens dat de tekst veel goede zaken bevat: decentralisatie, het gebruik van bluetooth-technologie en het vrijwillig karakter van de app zijn voor de spreker drie wezenlijke elementen in de beoordeling van de algemene proportionaliteit van de voorgenomen maatregel. Of de app effectief zal zijn in de strijd tegen het coronavirus kunnen we helaas niet op voorhand met zekerheid weten.

De vraag werd gesteld hoe het voorstel van resolutie nog zou kunnen worden versterkt. De spreker is verheugd over de (kwaliteit van de) hoorzitting, maar meent dat er nog stappen kunnen worden gezet op het vlak van de transparantie van het debat. Dat is met name het geval voor de discussie over de wettelijke basis voor de app en de keuze van het juridische instrument (wet of genummerd KB). Daarmee wil de spreker niet gezegd hebben dat we moeten vervallen in de Nederlandse situatie, waar de selectie van een app integraal op het publieke forum plaatsvond. Hierdoor wordt slechts een illusie van transparantie gecreëerd. De Nederlandse tegenhanger van de GBA, de AP, moest spijts alle openheid toegeven dat ze over onvoldoende informatie beschikte om een zinvol oordeel te kunnen vellen over de apps.

Verschillende opmerkingen betroffen de koppeling met andere gegevens en de rol die het *eHealth*-platform en de KBSZ daarbij zouden opnemen. De heer Stevens heeft geen weet van zulke koppeling. Hij suggereert dat het voorstel van resolutie zou kunnen worden versterkt door het verbod op de koppeling met andere gegevens explicieter op te nemen in de tekst. Ook zouden de rollen en verantwoordelijkheden van de verschillende overheidsactoren kunnen worden verduidelijkt in het voorstel van resolutie of, beter nog, in de toekomstige wet of genummerd KB.

Gelet op de complementariteit tussen manuele en digitale contact tracing en de verschillende

les différents niveaux de pouvoirs où ils sont organisés, la proposition de résolution pourrait être renforcée en y renvoyant à la mise en place d'un consensus entre les différentes entités qui composent la Belgique.

M. Verduyckt a demandé des précisions sur l'anonymat des données télécoms utilisées par le groupe de travail pour cartographier la mobilité des citoyens. Le résultat final de ce traitement est un chiffre (public) indiquant combien d'appareils mobiles ont été utilisés pendant combien de temps dans une localité dont le code postal n'est pas le code postal propre de l'utilisateur. L'orateur cite l'exemple de son propre déplacement à Bruxelles en matinée: si son téléphone portable figurait déjà dans les données – ce qui supposerait l'arrivée d'au moins 29 autres téléphones à Bruxelles à partir du même code postal – il ne serait pas possible de déterminer l'itinéraire qu'il a emprunté. On peut débattre de la question de savoir si ces informations sont anonymes. En tout état de cause, l'anonymisation est suffisante à la lumière de l'objectif poursuivi. Comme cela a été indiqué précédemment, le résultat final est un nombre qui, en soi, est totalement anonyme bien qu'il ait été obtenu en traitant des données à caractère personnel. La loi sur les télécommunications prévoit d'ailleurs la possibilité d'un traitement anonymisé de ces données télécoms. Les trois opérateurs de téléphonie mobile rendent les données anonymes et les agrègent, après quoi un partenaire externe opérant dans un cadre contractuel strict les analyse et génère l'indicateur de mobilité.

En réponse à la question de M. Boukili, visant à savoir s'il existe, en définitive, des données de localisation anonymisées, M. Stevens indique que c'est le cas au travers de la conversion en chiffres.

Eu égard aux risques liés à l'utilisation des applications de traçage, il est logique que l'on évalue l'impact sur la protection des données. Ce point pourrait, du reste, également être intégré dans la proposition de résolution.

L'orateur n'a aucune idée du temps nécessaire pour développer une application de traçage. Ce calendrier relève d'une décision politique qui ne fait aucune différence dans la perspective de la protection des données.

M. Stevens ne dispose pas non plus d'informations sur les profils des personnes qui travailleront dans les centres d'appel. En tout état de cause, les aspects de cette question liés à la vie privée sont minimes. Mieux vaut adresser cette question aux ministres compétents.

La réponse à la question de M. Vanden Burre sur la manière d'empêcher l'exclusion de certains groupes tels

bevoegdheidsniveaus waarop zij worden georganiseerd, zou het voorstel van resolutie ten slotte kunnen worden versterkt door daarin een verwijzing op te nemen naar het creëren van draagvlak over de verschillende entiteiten van dit land heen.

De heer Verduyckt vroeg hoe het zat met de anonimiteit van telecomgegevens die worden aangewend door de taskforce om de mobiliteit van de burgers in kaart te brengen. Het eindresultaat van die verwerking is een (publiek) cijfer van hoeveel mobiele toestellen hoeveel tijd in een andere postcode dan hun eigen postcode hebben doorgebracht. De spreker geeft het voorbeeld van zijn eigen verplaatsing naar Brussel deze ochtend; als zijn mobiel toestel al in de cijfers zou voorkomen – wat veronderstelt dat minstens 29 andere toestellen vanuit dezelfde postcode naar Brussel zouden zijn gekomen – dan valt daar bijvoorbeeld niet uit af te leiden welk traject hij heeft gevolgd. Of dit anoniem is, is voer voor discussie. Het is alleszins voldoende geanonimiseerd in het licht van de nagestreefde doelstelling. Het eindresultaat is, zoals gezegd, een aantal, dat op zich volstrekt anoniem is, zij het dat het wordt bereikt door een verwerking van persoonsgegevens. De telecomwet voorziet overigens in de mogelijkheid van een geanonimiseerde verwerking van die telecomgegevens. De drie mobiele operatoren anonimiseren en aggregeren de gegevens, waarna een binnen een strikt contractueel kader opererende externe partner de analyse doet en de mobiliteitsindicator genereert.

Op de vraag van de heer Boukili of geanonimiseerde lokalisatiegegevens überhaupt bestaan, antwoordt de heer Stevens bevestigend, namelijk door omzetting naar cijfers.

Gelet op de risico's verbonden met het gebruik van tracing apps, is het logisch dat er een gegevensbeschermingseffectbeoordeling zal worden uitgevoerd. Dit zou overigens eveneens kunnen worden toegevoegd in het voorstel van resolutie.

De spreker heeft geen zicht op de timing voor de tracing app. Dit is een beleidsbeslissing die vanuit het perspectief van de gegevensbescherming geen verschil maakt.

De heer Stevens heeft evenmin informatie omtrent de profielen van de personen die werkzaam zullen zijn in de callcenters. De privacyaspecten van die kwestie zijn alleszins minimaal. Deze vraag kan best worden gesteld aan de bevoegde ministers.

Het antwoord op de vraag van de heer Vanden Burre hoe kan worden vermeden dat bepaalde groepen zoals

que les enfants et les seniors réside dans la complémentarité. Outre le traçage automatisé, il existera de toute façon une variante manuelle. L'application de traçage doit venir en appui du traçage manuel, et garantir, en particulier, que ce dernier reste gérable.

M. Stevens peut difficilement évaluer dans quelle mesure il est probable que l'application devienne réalité. Il serait préférable que Mme Verhelst adresse cette question au ministre compétent. L'orateur confirme toutefois que si elle se concrétise, il s'agira d'une variante, protégeant suffisamment la vie privée des citoyens selon l'APD, ce qui implique qu'elle incorporera les trois caractéristiques décrites comme étant des garanties essentielles (Bluetooth, sur base volontaire, décentralisée). L'orateur souligne encore que certains pays, en Europe également, s'emploient à développer des systèmes dans lesquels ce n'est pas le cas.

L'orateur n'a pas subi de pressions internationales afin de participer à l'initiative européenne. Comme cela a déjà été mentionné, l'APD a collaboré très activement aux directives du CEPD, dans lesquelles figurent les garanties précitées.

S'il devait apparaître que l'application n'est pas utile, il faudra mettre fin anticipativement à son utilisation. L'orateur estime qu'il est opportun que cette éventualité soit prévue dans la proposition de résolution. Cela s'inscrit également dans le cadre des principes en vigueur en matière de protection de la vie privée.

L'orateur ne considère pas qu'il est indiqué d'attendre que des résultats étrangers soient disponibles. Premièrement, il est assez urgent de déployer le suivi des contacts. En outre, l'orientation que suivront la plupart des pays est connue; les limites ont été exposées par le CEPD, lesquelles permettent de se mettre au travail. Il est d'ailleurs connu qu'il n'est pas possible de transposer tout simplement des exemples provenant d'autres pays dans un autre contexte national.

À la question de Mme Bury de savoir si les données collectées seront réellement anonymes et s'il ne sera pas possible à un stade ultérieur d'encore les associer à des personnes, M. Stevens répond que le caractère décentralisé de la banque de données offre des garanties suffisantes en la matière.

Le professeur Bart Preneel (KUL) donne davantage de précisions au sujet de la différence entre le PEPP-PT et le DP-3T. Début mars, la KUL a rejoint un grand consortium européen conduit par des acteurs allemands (PEPP-PT). Le but consistait à proposer une solution à la fois centralisée et décentralisée au sein de ce consortium. La structure de décision de ce consortium

kinderen en ouderen worden uitgesloten, schuilt in de complementariteit; naast de geautomatiseerde tracing zal er in ieder geval een manuele variant zijn. De tracing app moet de manuele tracing ondersteunen, en er met name voor zorgen dat die laatste beheersbaar blijft.

De heer Stevens kan moeilijk inschatten hoe groot de kans is dat de app er werkelijk komt. Mevrouw Verhelst zou deze vraag best tot de bevoegde ministers richten. De spreker bevestigt wel dat als hij er komt, het in een variant zal zijn waarbij, naar de mening van de GBA, de privacy van de burgers voldoende beschermd zal zijn, wat impliceert dat hij de drie als essentiële waarborgen omschreven kenmerken (bluetooth, vrijwillig, decentraal) incorporeert. De spreker wijst er nogmaals op dat bepaalde, ook Europese landen, werken aan systemen waarin dit niet het geval is.

De spreker heeft geen internationale druk ervaren om te participeren in het Europese initiatief. De GBA heeft zoals al gezegd zeer actief meegewerkt aan de richtlijnen van de EDPB waarin voormelde garanties zijn opgenomen.

Mocht de app niet nuttig blijken, dan dient hij vroegtijdig worden stopgezet. De spreker vindt het een goede zaak dat deze eventualiteit voorzien is in het voorstel van resolutie. Een en ander strookt ook met de geldende principes inzake privacy.

De spreker meent niet dat het aangewezen is om te wachten tot er buitenlandse resultaten beschikbaar zijn. Vooreerst is er een zekere tijdsdruk om de contact tracing uit te rollen. Bovendien kennen we de richting die de meeste landen zullen uitgaan; de krijtlijnen werden uitgezet door de EDPB. Daarmee kunnen we nu aan de slag. Overigens is het bekend dat voorbeelden uit andere landen zich niet zomaar laten transponeren in een andere nationale context.

Op de vraag van mevrouw Bury of de verzamelde gegevens werkelijk anoniem zullen zijn en of niet het mogelijk zal zijn deze in een later stadium alsnog te linken aan personen, antwoordt de heer Stevens dat het decentrale karakter van de gegevensbank ter zake voldoende waarborgen biedt.

Professor Bart Preneel (KUL) geeft verdere toelichting over het verschil tussen PEPP-PT en DP-3T. Begin maart heeft de KUL zich aangesloten bij een groot Europees consortium geleid door Duitse spelers (PEPP-PT). De bedoeling was om binnen dat consortium zowel een centrale als een decentrale oplossing voor te stellen. De beslissingsstructuur van dat consortium was echter

n'était toutefois guère transparente et, sous l'impulsion de l'Allemagne, le consortium continuait à défendre une solution centralisée auprès du monde extérieur. Finalement, le groupe d'étude de l'orateur a décidé de se retirer du consortium après à peine un mois. Le week-end passé, l'Allemagne a également signalé qu'elle privilégiait la solution décentralisée. La France est le seul grand pays qui travaille encore sur la solution centralisée au sein du PEPP-PT, avec son protocole ROBERT développé par l'Inria. Hier, des scientifiques français ont toutefois exprimé leur inquiétude à cet égard dans une lettre ouverte. Le Royaume-Uni est le dernier pays qui souhaite encore une solution centralisée indépendamment du PEPP-PT.

L'Europe souhaite une solution pour tous les pays mais tente de combler le retard qu'elle a en partie accumulé par rapport aux faits. Les États membres ont agi très vite et l'UE essaie d'aligner les différents pays par le biais de recommandations.

L'interopérabilité limitée des différentes solutions constitue un problème de taille. Le fait de recueillir les informations concernant les chiffres aléatoires reçus dans une banque de données centralisée ou non centralisée relève d'une approche fondamentalement différente. Si une solution centralisée est associée à une solution décentralisée, le résultat est en quelque sorte le pire des deux mondes, à savoir la perte maximale de protection de la vie privée et l'efficience minimale. L'orateur s'attend à ce que des critiques acerbes soient formulées en Europe au cours des prochaines semaines au sujet de ce qu'il arriverait si un ressortissant d'un pays qui a opté pour une solution décentralisée voyageait à destination d'un pays qui a mis en œuvre une solution centralisée.

La principale raison pour laquelle l'orateur opte pour une solution décentralisée est que celle-ci présente moins de risques de piratage; la banque de données ne contient que des chiffres aléatoires qui ne sont pas réutilisables à d'autres fins. Le prix à payer pour ce risque inférieur de piratage est que les attaques locales, au moyen d'une antenne Bluetooth et d'une caméra, sont un peu plus aisées. De telles infractions sont toutefois également possibles sans application. Il s'agit essentiellement d'une mise en balance: est-on plus préoccupé par un abus centralisé ou par des attaques locales?

Des questions ont été posées au sujet du taux de pénétration exigé de l'application. Nul ne le sait en réalité; une étude indique que 60 % est le minimum requis, mais il se pourrait tout autant que ce taux soit supérieur ou inférieur. Les chiffres qui résultent des études dépendent dans une large mesure des hypothèses utilisées. Il ne fait toutefois pas de doute qu'une application ne fonctionnera pas si le taux de pénétration est inférieur

weinig transparant en op aansturen van Duitsland bleef het consortium naar de buitenwereld toe een centrale oplossing verdedigen. Uiteindelijk heeft de onderzoeksgroep van de spreker na een kleine maand besloten om uit het consortium te stappen. Afgelopen weekend heeft Duitsland aangegeven ook de voorkeur te geven aan een decentrale oplossing. Het enige grote land dat nog aan een centrale oplossing werkt binnen PEPP-PT is Frankrijk, met zijn door Inria ontwikkeld ROBERT-systeem. Gisteren echter hebben Franse wetenschappers in een open brief hun bezorgdheid hieromtrent geuit. Los van PEPP-PT is het Verenigd Koninkrijk het laatste land dat nog een centrale oplossing wil.

Europa wil één oplossing voor alle landen maar loopt voor een stuk achter de feiten aan. De lidstaten hebben zeer vlug gehandeld en de EU tracht de verschillende landen op één lijn te krijgen middels aanbevelingen.

Een groot probleem betreft de beperkte interoperabiliteit van de verschillende oplossingen. Of je informatie over ontvangen random getallen al of niet in een centrale gegevensbank verzamelt, is een fundamenteel verschillende benadering. Als je een centrale en een decentrale oplossing gaat koppelen, krijg je in zekere zin het slechtste van twee werelden: maximaal privacyverlies en minimale efficiëntie. De spreker verwacht dat er de komende weken in Europa nog een hartig woordje zal worden gepraat over wat er zou gebeuren als een burger vanuit een land dat voor een decentrale oplossing opteerde, naar een land dat een centrale oplossing implementeerde, zou reizen.

De hoofdreden waarom de spreker kiest voor een decentrale oplossing is dat het risico op *hacks* lager ligt; de gegevensbank bevat enkel random getallen, die niet herbruikbaar zijn voor andere doeleinden. De prijs die men betaalt voor dat lagere risico op *hacks* is dat lokale aanvallen, met een bluetooth-antenne en een camera, iets gemakkelijker zijn. Zulke overtredingen zijn echter ook mogelijk zonder een app. Het is in wezen een afweging: is men meer bezorgd over centraal misbruik of over lokale aanvallen?

Er werden vragen gesteld omtrent de vereiste penetratiegraad van de app. Eigenlijk weet men het niet; één studie zegt dat 60 % minimaal vereist is, maar het zou evengoed kunnen dat het meer of minder is. Uit studies voortvloeiende cijfers hangen in hoge mate af van de gebruikte veronderstellingen. Dat een app niet zal werken als de penetratie minder dan 10 % bedraagt, is echter een uitgemaakte zaak. Wat telt is de bevolking

à 10 %. Ce qui importe est de convaincre la population de l'utilité et de la sécurité de l'application afin d'obtenir un taux de pénétration aussi élevé que possible.

Qu'en est-il des personnes qui ne possèdent pas un smartphone approprié et quelle est la taille de ce groupe? Le professeur Preneel a posé cette dernière question aux opérateurs mais n'a pas encore pu obtenir de réponse. Les opérateurs disposent en tout état de cause de cette information; ils savent précisément de combien de personnes il s'agit. À l'étranger, une prospection a d'ailleurs déjà été réalisée au sujet de la possibilité de donner un Bluetooth-*token* aux personnes dépourvues de smartphone. De tels appareils existent déjà, seul le logiciel devrait être adapté, ce qui prendrait quelques semaines. Le coût d'un tel appareil est estimé à 5 à 10 euros. Il faut d'abord examiner si le système fonctionne correctement sur les smartphones, mais si tel est le cas, il sera possible d'envisager de déployer ces Bluetooth *tokens* sur une base volontaire.

Le professeur Preneel conteste que son appartenance à la chambre contentieuse de l'APD puisse constituer un conflit d'intérêts.

L'application basée sur le protocole DP-3T est conçue de manière à ne pas pouvoir être utilisée à d'autres fins. Les situations gagnant-gagnant comportent des risques pour la vie privée et ne sont volontairement pas recherchées.

Plusieurs députés se sont inquiétés des faux positifs et des faux négatifs. Les citoyens peuvent contribuer eux-mêmes à éviter les faux positifs en désactivant la fonction Bluetooth de leur smartphone ou l'application dans certaines situations (par exemple à leur domicile). Le protocole DP-3T permet également à l'utilisateur de supprimer ultérieurement les données existantes des fichiers. On ne connaîtra le nombre de faux négatifs qu'une fois que le système aura été déployé à grande échelle. L'orateur pense qu'il est possible d'obtenir de bons résultats à cet égard.

La Suisse deviendra, à partir du 11 mai, le premier pays à déployer l'application (décentralisée). L'Autriche, l'Estonie et l'Espagne lui emboîteront le pas. Il se sera écoulé environ quatre semaines entre la décision du gouvernement suisse et le déploiement de l'application. Le code de cette application étant en accès libre, nous pourrons bénéficier des développements et des expériences des autres pays. Nous pourrons (ré)utiliser de nombreux éléments fondamentaux; il faudra uniquement adapter l'interface réservée aux autorités sanitaires et au monde médical à la situation belge. L'orateur estime

te overtuigen van het nut en de veiligheid van de app, om een zo hoog mogelijke penetratiegraad te verkrijgen.

Wat met mensen die geen geschikte smartphone hebben en hoe groot is die groep? Professor Preneel richtte deze laatste vraag aan de operatoren maar mocht nog geen antwoord krijgen. In ieder geval is het zo dat de operatoren over die informatie beschikken; zij weten precies over hoeveel mensen het gaat. In het buitenland werd overigens al verkennend onderzoek verricht naar de mogelijkheid om mensen zonder smartphone een bluetooth-token te geven. Zulke toestellen bestaan al, enkel de software zou dienen te worden aangepast, wat enkele weken zou kosten. De kost van zo'n toestel wordt geschat op 5 tot 10 euro. Eerst moet worden bekeken of het systeem goed werkt op smartphones, maar als dat het geval is kan eraan worden gedacht om zulke bluetooth-tokens op vrijwillige basis uit te rollen.

Professor Preneel ontkent dat zijn lidmaatschap van de Geschillenkamer van de GBA een belangenconflict zou doen rijzen.

De app in het DP-3T protocol is zo ontworpen dat hij niet kan worden gebruikt voor andere doeleinden. Winwinsituaties leiden tot privacy-risico's en worden bewust niet opgezocht.

Verschillende vraagstellers waren bezorgd over valse positieven en valse negatieven. Die eerste kan de burger alvast zelf helpen vermijden, door zijn bluetooth-functie of de app in bepaalde situaties (bijvoorbeeld thuis) uit te schakelen. Het DP-3T protocol biedt ook de mogelijkheid voor de gebruiker om achteraf bestaande gegevens uit de bestanden te verwijderen. Het aantal valse negatieve meldingen zal moeten blijken uit de metingen, eens het systeem is uitgerold op grote schaal. De spreker denkt dat het haalbaar is om ter zake goede resultaten te boeken.

Zwitserland zal als eerste de (decentrale) app uitrollen, en wel vanaf 11 mei. Oostenrijk, Estland en Spanje zullen volgen. Er zullen ongeveer een viertal weken zitten tussen de Zwitserse beslissing en de uitrol. Gelet op het feit dat de code opensource is, zullen wij kunnen profiteren van de ontwikkelingen en ervaringen in andere landen. We zullen veel bouwstenen kunnen (her)gebruiken; enkel de interface met de gezondheidsautoriteiten en de medische wereld zal dienen te worden aangepast aan de Belgische situatie. De spreker schat dan ook dat, als we voortgang maken met de beslissing, een

donc que, si nous prenons un décision en ce sens, il devrait être possible de procéder au déploiement de l'application en Belgique une à deux semaines après son déploiement en Suisse.

Comment s'assurer que les versions de l'application installées sur les appareils des utilisateurs correspondent au code source qui sera publié? Il s'agit d'un problème bien connu. Il existe deux manières de vérifier que le code source et le code compilé (le code machine ou le code programme) correspondent. La première solution fonctionne toujours: il est possible de vérifier le code programme en détail et s'assurer qu'il correspond au code source. Cette méthode prend beaucoup de temps mais, pour la partie critique du code (comme les opérations cryptographiques), elle est certainement envisageable et offre de solides garanties. La deuxième solution consiste à utiliser une compilation déterministe (ou une compilation reproductible), ce qui permet de recompiler le code source pour une plateforme donnée et de vérifier si l'on obtient un résultat identique. Cette méthode n'est pas encore applicable à toutes les langues et à toutes les plateformes. Cette solution sera certainement utilisée dans le cadre du protocole DP-3T si elle est envisageable, et elle l'est probablement pour une partie du code.

Mme Olivia Venet (Ligue des Droits Humains) indique que l'atteinte controversée à la vie privée doit être prévue par la loi et doit être nécessaire dans une société démocratique. L'oratrice fustige le manque de réflexion et d'analyse d'impact permettant d'évaluer cette nécessité. En effet, les autorités sont déjà en train de recruter des personnes qui seront chargées de tracer les contacts des personnes infectées, sans avoir décidé que cette méthode constitue réellement la meilleure solution à cet égard. Mme Venet rejoint la professeure Degrave lorsque celle-ci indique qu'il existe un risque réel que nous nous enfermions dans un processus que les organes législatifs n'ont pas réellement eu l'occasion d'analyser, d'examiner et à propos duquel ils n'ont pas pu se prononcer. L'oratrice estime que le cadre légal doit prendre la forme non pas d'un arrêté royal mais d'une loi, qui devra être soumise à l'avis de l'APD et du Conseil d'État.

L'oratrice ne souhaite absolument pas contester que la préoccupation première du président de l'APD est la protection de la vie privée, mais elle s'interroge toujours sur sa participation à la *task force*, au sein de laquelle les participants examineront des solutions, parviendront à un compromis et rédigeront un texte. Comment pourrait-on dès lors s'attendre à ce que l'APD, qui est présidée par un membre de cette même *task force*, rende un avis critique sur ce texte? Pour Mme Venet, il faut établir une distinction claire entre ces fonctions et il faudra, au besoin, que le président se retirer des délibérations.

uitrol in België één à twee weken na de Zwitserse uitrol mogelijk moet zijn.

Hoe zal men kunnen garanderen dat de versies van de app die op de toestellen van gebruikers geïnstalleerd worden, overeenkomen met de broncode die vrijgegeven wordt? Het betreft een algemeen gekend probleem. Er zijn twee manieren om na te gaan of broncode en gecompileerde code (machinecode of programmacode) overeenkomen. De eerste werkt altijd: men kan de programmacode in detail nakijken en verifiëren of die overeenkomt met de broncode. Dat is heel tijdrovend, maar voor het kritische deel van de code (zoals de cryptografische operaties) is dat zeker haalbaar en geeft dat sterke waarborgen. Een tweede oplossing is gebruik maken van deterministische compilatie (*deterministic compilation* of *reproducible builds*). In dat geval kan men de broncode hercompileren voor een bepaald platform en nagaan of men identiek hetzelfde resultaat bekomt. Dit is nog niet mogelijk voor alle talen en platformen. Deze oplossing zal zeker gebruikt worden binnen DP-3T als het haalbaar is; waarschijnlijk kan dat voor een deel van de code.

Mevrouw Olivia Venet (Ligue des Droits Humains) stelt dat de kwestieuze inbreuken op de bescherming van het privéleven bij wet moeten zijn voorzien en noodzakelijk moeten zijn in een democratische samenleving. De spreekster hekelt het feit dat er onvoldoende reflectie en impactanalyse is om die noodzakelijkheid te kunnen beoordelen. Men is thans al bezig met de rekrutering van de *contact tracers*, zonder dat beslist is dat dat werkelijk de beste oplossing is. Mevrouw Venet treedt professor Degrave bij wanneer zij stelt dat het risico reëel is dat we vastzitten in een proces waarbij de volksvertegenwoordiging niet terdege de kans heeft gekregen om de kwestie te onderzoeken, te bespreken en zich erover uit te spreken. De spreekster vindt dat het wettelijk kader de vorm moet aannemen van een wet – niet van een genummerd KB – na het advies te hebben ingewonnen van de GBA en de Raad van State.

De spreekster wil hoegenaamd niet ontkennen dat de voornaamste bekommering van de voorzitter van de GBA de privacybescherming is, maar blijft zich toch vragen stellen bij zijn deelname aan de taskforce. Binnen die schoot bespreekt men samen oplossingen, bereikt men een compromis, en werkt men een tekst uit. Hoe kan men dan verwachten dat de GBA, met aan het roer een lid van de taskforce, een kritisch advies uitbrengt over zo'n tekst? Volgens mevrouw Venet moet er een strikte functiescheiding zijn en moet de voorzitter zich desnoods terugtrekken uit de beraadslagingen.

L'oratrice s'inquiète des risques de dérives. Elle est convaincue que les applications doivent servir à renforcer les capacités des citoyens, et pas à les contrôler. Les institutions sont au service des citoyens. Ce n'est qu'avec eux que nous parviendrons à lutter effectivement contre le virus. Les institutions ne sont pas les ennemis des citoyens, et vice versa. C'est la philosophie qui doit présider à l'élaboration d'un cadre légal.

Il est certain que la garantie de l'anonymat est compromise au sein des *call centers*. Affirmer que des numéros de téléphone constituent des données anonymes ne tient pas debout. Un problème réel se pose à cet égard.

L'oratrice est opposée à l'octroi de récompenses dans le cadre de l'application. En effet, si des récompenses sont prévues, il ne peut plus être question d'une utilisation sur base volontaire, ce qui ouvre la porte à des discriminations et d'utilisation abusive des données. Le cadre légal devra poser des balises en la matière et devra par ailleurs aussi régler des questions telles que la suppression et la conservation des données.

Mme Venet conclut en soulignant que des pays du monde entier ainsi que la Haut-Commissaire des Nations Unies aux droits de l'homme mettent en garde contre les risques de dérives et de restrictions illégales des libertés fondamentales. Les textes qui devront être rédigés par le Parlement devront protéger les citoyens contre ces risques, même en temps de crise.

Mme Kati Verstrepen (Liga voor Mensenrechten) indique qu'il faut se montrer vigilant à l'égard du suivi et du traçage physique. Dans le cadre du traçage manuel, le traitement anonyme des données est tout simplement impossible. Il faut par conséquent établir un cadre légal définissant très clairement les conditions dans lesquelles ce suivi et ce traçage physique peuvent avoir lieu. Il est inconcevable de procéder déjà au recrutement des personnes chargées du traçage des contacts alors qu'aucune réflexion sur un cadre légal n'a été menée jusqu'à présent.

En ce qui concerne les applications de traçage des contacts, l'oratrice redoute le phénomène de pression sociale, qui aura pour conséquence que l'accès aux services privés ou publics (par exemple l'horeca ou les transports en commun) ou même à l'emploi (par exemple le système des titres-services) sera subordonné à l'utilisation de l'application. Ce débat devra certainement être mené dans le cadre de celui sur le caractère volontaire de l'utilisation de l'application.

De spreekster is beducht voor uitwassen. Het is haar overtuiging dat de apps moeten dienen om de burger toe te laten zijn capaciteiten te versterken, eerder dan om hem te controleren. De instellingen staan ten dienste van de burgers; enkel samen met hen zullen we erin slagen het virus effectief te bestrijden. De instellingen zijn niet de vijand van de burgers en omgekeerd. Het is die geestesgesteldheid die moet primeren bij het uitwerken van een wettelijk kader.

De anonimiteit staat wel degelijk onder druk bij de callcenters. Het gaat niet op om te beweren dat telefoonnummers anonieme gegevens zijn. Er is daar een reëel probleem.

De spreekster staat afkerig tegen het gebruik van beloning in het kader van de app. In dat geval is er immers geen sprake meer van gebruik op vrijwillige basis, wat de deur openzet voor discriminatie en misbruik van de gegevens. Het wettelijk kader moet hieraan paal en perk stellen, en moet trouwens ook zaken regelen zoals de bewaring en het wissen van de gegevens.

Mevrouw Venet merkt ten slotte op dat overal ter wereld, ook door de vertegenwoordigster van het Hoog Commissariaat voor de Mensenrechten van de VN, wordt gewaarschuwd voor misbruiken en ongeoorloofde inperkingen van de fundamentele vrijheden. De teksten die door het Parlement worden opgesteld moeten de burgers daartegen in bescherming nemen, ook in tijden van crisis.

Mevrouw Kati Verstrepen (Liga voor Mensenrechten) stelt dat alertheid op zijn plaats is ten overstaan van de fysieke tracking-and-tracing. Bij de manuele variant is een geanonimiseerde verwerking van de gegevens simpelweg onmogelijk. Er moet dan ook een wettelijk kader komen dat zeer duidelijk omschrijft onder welke voorwaarden zulke fysieke *tracking-and-tracing* kan plaatsvinden. Het is onvoorstelbaar dat men *al contact tracers* aan het rekruteren is terwijl er nog niet eens is nagedacht over een wettelijk kader.

Wat de *contact tracing apps* betreft is de spreekster bevreesd voor sociale druk, waarbij toegang tot private of publieke diensten (bijvoorbeeld horeca, openbaar vervoer) of zelfs tewerkstelling (bijvoorbeeld het systeem van de dienstencheques) afhankelijk zullen worden gesteld van het gebruik van de app. Dit debat moet zeker worden gevoerd tegen de achtergrond van het vrijwillig karakter van de app.

Un député a évoqué le fossé générationnel en indiquant que ce seront surtout les jeunes qui adopteront cette technologie et se poseront moins de questions sur la protection du respect de leur vie privée. Compte tenu de son caractère anonyme, l'enquête de la Ligue ne peut pas confirmer cette affirmation, mais le fait est que de très nombreux individus inquiets envoient des questions à la Ligue au sujet de la protection de la vie privée des jeunes.

Le danger que la crise actuelle serve à mettre en place des mécanismes de contrôle qui ne seront pas désactivés par la suite est réel. L'oratrice fait un parallèle avec la menace terroriste qui pesait il y a quelques années. Des mesures qui avaient été prises à cette époque, comme le doublement à 48 heures de la durée de détention prévue par la Constitution, semblent désormais acquises.

La professeure Élise Degrave (UNamur) affirme qu'il ne faut pas s'engager à la légère avec les GAFAM sans avoir préalablement examiné attentivement les alternatives existantes. La première question que nous devons nous poser est de savoir pourquoi nous avons besoin d'eux. Une chose est de leur demander de débloquer les smartphones pour leur permettre de communiquer entre eux, mais c'en est une autre de leur confier le stockage de données, par exemple.

Plutôt que de donner une réponse claire, la CNIL a indiqué que le projet français était tout sauf anodin. La CNIL a posé plusieurs balises et a demandé à pouvoir se prononcer de nouveau une fois que ce projet sera plus précis.

Il convient d'établir une distinction claire entre le SPF Santé publique et la plate-forme *eHealth*. Cette dernière est un instrument régi par la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions. La professeure Degrave se demande s'il ne serait pas possible de gérer l'application de traçage des contacts dans une base de données commune au SPF Santé publique, sans lien avec la plate-forme eHealth, en collaboration avec les Régions et sous la supervision de l'APD.

Een vraagsteller refereerde aan het generatieverschil, waarbij vooral jongeren deze technologie zouden omarmen en zich minder vragen stellen wat de bescherming van hun privacy betreft. Uit de bevraging door de Liga zal het niet blijken, want die is anoniem, maar feit is dat de Liga erg veel bezorgde vragen omtrent privacy krijgt van jonge mensen.

Het gevaar dat de huidige crisis wordt aangewend om een aantal controlemechanismen te installeren die later niet worden teruggeschroefd, is reëel. De spreekster trekt een parallel met de terrorismedreiging enkele jaren geleden; toen zijn er ook maatregelen genomen, zoals de verdubbeling van de grondwettelijke aanhoudingstermijn tot 48 uren, die thans verworven blijken te zijn.

Professor Élise Degrave (UNamur) stelt dat we ons ervoor moeten hoeden om lichtzinnig in zee te gaan met de GAFAM, zonder vooraf goed te onderzoeken welke alternatieven er bestaan. De eerste vraag die we ons moeten stellen is waarom we ze nodig hebben. Het is één zaak hen te vragen om smartphones te deblokkeren om ze met elkaar te laten communiceren, maar het is een andere om hen bijvoorbeeld de opslag van gegevens toe te vertrouwen.

Veeleer dan een sluitend antwoord te geven, heeft de CNIL duidelijk gemaakt dat het Franse ontwerp allesbehalve onschuldig is. Het heeft een aantal bakens uitgezet en heeft verzocht zich opnieuw te kunnen uitspreken eens het ontwerp meer voldragen is.

Er moet een duidelijk onderscheid worden gemaakt tussen de FOD Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu en het *eHealth*-platform. Dat laatste is een instrument dat wordt geregeld door de wet van 21 augustus 2008 houdende oprichting en organisatie van het *eHealth*-platform en diverse bepalingen. Professor Degrave vraagt zich af of het niet mogelijk is de contact tracing app te beheren via een gegevensbank die gedeeld wordt met de FOD Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu, zonder link met het *eHealth*-platform, en dit in samenwerking met de gewesten en onder het toezicht van de GBA.

ANNEXE

AVIS DE LA COMMISSION DE LA JUSTICE

RAPPORT

FAIT AU NOM DE LA COMMISSION
DE LA JUSTICE
PAR
M. **Christoph D'HAESE**

SOMMAIRE

Pages
I. Exposé introductif de Mme Jessika Soors, auteure principale de la proposition de résolution DOC 55 1182/001 96
II. Discussion 97

BIJLAGE

ADVIES VAN DE COMMISSIE VOOR JUSTITIE

VERSLAG

NAMENS DE COMMISSIE
VOOR JUSTITIE
UITGEBRACHT DOOR
DE HEER **Christoph D'HAESE**

INHOUD

Blz
I. Inleidende uiteenzetting van mevrouw Jessika Soors, hoofdindienster van voorstel van resolutie DOC 55 1182/001 96
II. Bespreking....97

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Kristien Van Vaerenbergh

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Christoph D'Haese, Sophie De Wit, Kristien Van Vaerenbergh	Yngvild Ingels, Sander Loones, Wim Van der Donckt, Valerie Van Peel
Ecolo-Groen	Zakia Khattabi, Jessika Soors, Stefaan Van Hecke	Julie Chanson, Marie-Colline Leroy, Cécile Thibaut, Tinne Van der Straeten
PS	Khalil Aouasti, Laurence Zanchetta, Özlem Özen	Ludivine Dedonder, Mélissa Hanus, Ahmed Laaouej, Patrick Prévot
VB	Katleen Bury, Marijke Dillen	Tom Van Grieken, Dries Van Langenhove, Reccino Van Lommel
MR	Nathalie Gilson, Philippe Pivin	Mathieu Bihet, Magali Dock, Caroline Taquin
CD&V		Els Van Hoof, Servais Verherstraeten
PVDA-PTB	Nabil Boukili	Greet Daems, Marco Van Hees
Open Vld	Katja Gabriëls	Egbert Lachaert, Goedele Liekens
sp.a	Ben Segers	John Crombez, Karin Jiroflée

C. — Membres sans voix délibérative / Niet-stemgerechtigde leden:

cdH	Vanessa Matz
DéFI	Sophie Rohonyi

MESDAMES, MESSIEURS,

Lors de sa réunion du 22 avril 2020, la Conférence des présidents a chargé votre commission de rendre à la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique un avis sur les aspects de la proposition de résolution relatifs au respect de la vie privée. Votre commission a discuté de cet avis lors de sa réunion du 29 avril 2020.

I. — **EXPOSÉ INTRODUCTIF L'AUTEURE PRINCIPALE DE LA PROPOSITION DE RÉSOLUTION DOC 55 1182/001**

Mme Jessika Soors (Ecolo-Groen) renvoie tout d'abord aux développements de sa proposition de résolution.

Elle souligne que cette résolution n'est pas en soi un plaidoyer en faveur d'une application mobile contre le COVID-19. Cette résolution indique par contre clairement que si la décision est prise d'utiliser une telle application, elle doit s'inscrire dans une stratégie plus large de sortie. En d'autres termes, il convient de réfléchir à la façon de relier une telle application aux personnes qui sont dépistées, aux conditions de quarantaine, etc. Conformément à la proposition de résolution à l'examen, cette application mobile doit répondre aux normes les plus élevées possible en matière de respect de la vie privée ainsi que de protection des informations et des données personnelles.

Cette résolution porte sur le choix d'un stockage de données décentralisé, d'une technologie Bluetooth anonyme, de l'utilisation de cette application sur une base volontaire. La décision de partager davantage de données en cas de contamination ne pourra être prise qu'au su et avec l'autorisation de la personne concernée.

La proposition de résolution à l'examen fait référence à l'initiative DP3T, qui est le seul modèle à passer avec succès, tant dans notre pays qu'à l'étranger, les nombreux audits et contrôles qui ont été réalisés dans l'intervalle.

Il convient par ailleurs de travailler en *open source* et *open coding*, ce qui offrira une grande transparence du modèle sur lequel l'application mobile sera construite.

La proposition de résolution à l'examen prévoit également des dispositions relatives à la conservation et à la destruction des données. Elle stipule qu'une fois la crise passée, l'application mobile ne pourra plus être utilisée, que les données devront être détruites et

DAMES EN HEREN,

De Conferentie van voorzitters heeft tijdens haar vergadering van 22 april 2020 uw commissie gelast om over de aspecten van het voorstel van resolutie die de privacy betreffen een advies te geven aan de commissie voor Economie, Consumentenbescherming en Digitale Agenda. Uw commissie heeft tijdens haar vergadering van 29 april 2020 over dit advies vergaderd.

I. — **INLEIDENDE UITEENZETTING VAN DE HOOFDINDIENSTER VAN HET VOORSTEL VAN RESOLUTIE DOC 55 1182/001**

Mevrouw Jessika Soors (Ecolo-Groen) verwijst in de eerste plaats naar de schriftelijke verantwoording bij haar voorstel van resolutie.

Zij benadrukt hierbij dat deze resolutie geen pleidooi is voor een app tegen COVID-19 op zich. De resolutie stelt daarentegen duidelijk dat als er zou worden besloten om gebruik te maken van zo'n app, dit dient te kaderen in een bredere exit strategie. D.w.z. dat er moet worden nagedacht over hoe zo'n app kan worden gelinkt aan personen die worden getest, aan de quarantainevoorwaarden en dergelijke. Overeenkomstig het ter bespreking voorliggende voorstel van resolutie dient deze app voorts aan de hoogst mogelijke standaard wat privacy en bescherming van de informatie en persoonsgegevens betreft, te voldoen.

De resolutie betreft de keuze voor een gedecentraliseerde gegevensopslag, voor de anonieme bluetooth-technologie, voor het gebruik van de app op vrijwillige basis. Wanneer wordt beslist om bij besmetting meer gegevens te delen dan is dit enkel mogelijk met medeweten en goedkeuring van de betrokken persoon.

De resolutie verwijst naar het DP3T initiatief dat het enige model is dat zowel in het binnen- als het buitenland standhoudt bij de vele doorlichtingen en checks die inmiddels werden gevoerd.

Voorts dient er met *open source* en *open coding* te worden gewerkt. Aldus is er heel wat transparantie over het model waarop de app wordt gebouwd.

De resolutie voorziet ook in bepalingen inzake de bewaring en de vernietiging van de gegevens. Er wordt gestipuleerd dat eens de crisis voorbij is ook een einde dient te komen aan het gebruik van de app, dat de gegevens dienen te worden vernietigd en dat een audit

qu'un audit devra être réalisé pour vérifier que tout s'est déroulé correctement.

Enfin, la proposition de résolution à l'examen aborde plusieurs préoccupations liées à l'efficacité d'une telle application mobile. Ses auteurs n'ont pas l'ambition de formuler une réponse sur ce point ni de plaider dans un sens ou l'autre. Nombre d'experts ont toutefois déjà fait la remarque que le *tracing* manuel, une piste aujourd'hui étudiée par les régions, et l'utilisation d'une application mobile peuvent être complémentaires. Beaucoup de choses dépendront de la mesure dans laquelle les citoyens sont disposés à utiliser l'application mobile. Il est dès lors important, si l'on met en place une telle application, que celle-ci bénéficie d'un soutien suffisant de la population. Cet objectif peut être atteint notamment en montrant que cette application mobile a, en toute transparence, fait l'objet d'un débat au Parlement, que l'on a opté pour la protection de la vie privée dès la conception de cette application.

Il est important que le choix du respect de la vie privée lors de l'utilisation d'une telle application soit fait dès le début du processus. Le modèle de l'application détermine en effet la manière dont l'aspect du respect de la vie privée et de la protection des données est traité. Si l'on s'engage sur une voie aujourd'hui, on ne pourra plus en changer par la suite.

L'audition organisée le 28 avril 2020 au sein de la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique a montré la nécessité d'élaborer un cadre juridique. L'amendement n° 1 (DOC 55 1182/002) de MM. Aouasti (PS) et Lacroix (PS) répond à ce besoin et reçoit donc le soutien de l'intervenante.

II. — **DISCUSSION**

M. Khalil Aouasti (PS) est favorable à la proposition de résolution, moyennant l'amendement n° 1 qui garantit un cadre légal.

L'orateur s'étonne d'avoir reçu l'avis de Autorité de protection des données (APD) concernant un projet d'arrêté royal sur la mise en place d'une application de *tracing*. Les députés ont donc appris que l'APD avait remis un tel avis au moment même où les membres de la commission Économie, de la Protection des consommateurs et de l'Agenda numérique discutaient des conséquences et des objectifs liés au fait de travailler via un arrêté royal ou via une loi. Où est le respect du travail parlementaire? C'est le parlement qui contrôle le

moet worden uitgevoerd om na te gaan of alles correct is verlopen.

Tot slot zijn er een aantal bekommernissen omtrent de effectiviteit van zo'n app. De indieners hebben niet de ambitie om hierop een antwoord te formuleren of om het ene dan wel het andere te bepleiten. Veel experts hebben evenwel al opgemerkt dat de manuele *tracing*, een piste die de regio's nu onder de loep nemen, en het gebruik van een app aan elkaar complementair kunnen zijn. Veel zal afhangen van de mate waarin de burgers bereid zijn om de app te gebruiken. Het is daarom belangrijk dat als zo'n app er komt, er ook voldoende draagvlak bij de bevolking wordt gecreëerd. Dit kan onder meer door aan te tonen dat in alle transparantie over deze app een debat in het Parlement werd gevoerd, dat bij de keuze voor de app een *privacy by design*-keuze werd gemaakt.

Het is belangrijk dat de keuze voor privacy bij het gebruik van zo'n app bij de aanvang van het proces wordt gemaakt. Het model van de app bepaalt immers hoe goed met het privacy-aspect en de bescherming van gegevens wordt omgegaan. Als nu een bepaalde weg wordt ingeslagen, is het niet meer mogelijk om nadien koerswijzigingen door te voeren.

De tijdens de in de commissie voor Economie, Consumentenbescherming en Digitale Agenda gehouden hoorzitting van 28 april 2020 heeft de nood aan een wettelijk kader aangetoond. Amendement nr. 1 (DOC 55 1182/002) van de heren Aouasti (PS) en Lacroix (PS) komt hieraan tegemoet en draagt dan ook haar goedkeuring weg.

II. — **BESPREKING**

De heer Khalil Aouasti (PS) kan zich vinden in het ter bespreking ingediende voorstel van resolutie, op voorwaarde dat amendement nr. 1 (dat beoogt in een wettelijk raamwerk te voorzien) wordt aangenomen.

De spreker is verwonderd een advies van de Gegevensbeschermingsautoriteit inzake een ontwerp van koninklijk besluit betreffende het inzetten van een opsporingsapp te hebben ontvangen. De volksvertegenwoordigers hebben dus vernomen dat de Gegevensbeschermingsautoriteit dat advies heeft verleend op het eigenste moment dat in de commissie voor Economie, Consumentenbescherming en Digitale Agenda werd gedebatteerd over de gevolgen en de bedoelingen van de keuze om via een koninklijk besluit

gouvernement. L'orateur n'apprécie pas cette manière de travailler. Le président de l'APD , qui était présent aux auditions de la commission Économie, savait pourtant qu'il avait été saisi d'un arrêté royal: pourquoi ne pas l'avoir dit aux députés?

Le groupe de l'orateur n'est pas favorable à une application de *tracing*. Cependant, comme il constate que tout va très vite et sans beaucoup de consultation sur ce sujet, l'orateur souligne le besoin de mettre en place des balises claires. Premièrement, cela doit passer par une loi. Il faut un vrai débat démocratique. Comme l'a dit la Ligue des Droits Humains, c'est la loi qui doit définir la technique et non l'inverse. La technique devra s'adapter aux règles, aux principes et aux balises définies par la loi.

Par ailleurs, la critique essentielle de l'avis de l'APD est que l'efficacité de l'application n'est absolument pas démontrée. Il faut fixer les critères et les données techniques pour que l'efficacité soit avérée. Quid de la participation de la personne et de la proportion de la population participante? Si l'efficacité de l'application devait être démontrée, ce dont doute l'APD, il y aurait énormément de balises à prévoir.

Par ailleurs, comme l'a dit la Sûreté de l'État, la gestion du stockage doit être entre les mains d'une autorité publique indépendante.

Il faut en outre un consentement spécifique, libre et éclairé. Il ne doit donc y avoir aucune condition mise au téléchargement de cette application. La personne doit savoir exactement à quoi elle consentit. Le consentement doit aussi être éclairé: il faut donc transmettre l'identité du responsable du traitement, ses finalités, le code source, la durée de conservation des données. La système doit aussi être strictement limité au temps nécessaire et à la durée de la pandémie. L'APD a dit dans son avis que les durées mentionnées actuellement dans le projet d'arrêté royal ne permettent pas de comprendre en quoi on prendrait en considération un temps nécessaire.

Il est important de plus qu'il y ait un comité de monitoring: pendant le suivi de la gestion de ces données, un comité de monitoring composé de personnes

dan wel via een wet tewerk te gaan. Waar is het respect voor de parlementaire werkzaamheden? Het toezicht op de regering komt het Parlement toe. De spreker kan die manier van doen niet smaken. De voorzitter van de Gegevensbeschermingsautoriteit, die de hoorzittingen in de commissie Economie heeft bijgewoond, wist nochtans dat hem een ontwerp van koninklijk besluit voor advies was voorgelegd. Wat heeft hem belet dat aan de volksvertegenwoordigers mee te delen?

De fractie van de spreker is geen voorstander van een opsporingsapp. Aangezien hij echter vaststelt dat alles zeer snel gaat, zonder noemenswaardig overleg, dringt hij erop aan duidelijke krachtlijnen uit te tekenen. Eerst en vooral moet die app bij wet worden ingesteld, na een heus democratisch debat. Zoals de *Ligue des Droits Humains* stelde, moet de wet de techniek aansturen, niet omgekeerd. De techniek zal zich moeten schikken naar de wettelijk bepaalde regels, beginselen en krachtlijnen.

Het belangrijkste punt van kritiek in het advies van de Gegevensbeschermingsautoriteit is overigens dat de efficiëntie van een dergelijke app helemaal niet is bewezen. Er moeten criteria en technische gegevens worden vastgelegd om die efficiëntie aan te tonen. *Quid* met de medewerking van de betrokkene en welk aandeel van de bevolking moet eraan deelnemen? Mocht worden aangetoond dat die app efficiënt is – wat de Gegevensbeschermingsautoriteit betwijfelt –, dan zou zulks zeer sterk moeten worden gereglementeerd.

Voorts heeft de Veiligheid van de Staat erop gewezen dat de opgeslagen gegevens door een onafhankelijk overheidsorgaan moeten worden beheerd.

Bovendien is de specifieke, vrije en geïnformeerde toestemming van de betrokkene vereist. Het downloaden van die app mag dus aan geen enkele voorwaarde worden gekoppeld. De betrokkene moet precies weten waarmee hij/zij instemt. Hij/zij moet dus goed worden geïnformeerd, wat inhoudt dat de identiteit van de verwerkingsverantwoordelijke, diens bedoelingen, de broncode en de bewaringstermijn van de gegevens moeten worden meegedeeld. Het gebruik van de app moet daarenboven strikt worden beperkt tot de tijd die nodig is en tot de duur van de pandemie. In haar advies heeft de Gegevensbeschermingsautoriteit aangegeven dat uit de in het voorliggende ontwerp van koninklijk besluit opgenomen termijnen niet kan worden opgemaakt in hoeverre de regeling slechts voor de "nodige" tijd zou worden gehandhaafd.

Daarenboven is het belangrijk dat een en ander wordt opgevolgd door een monitoringcomité: bij de opvolging van het beheer van die data moet een dergelijk comité,

indépendantes, y compris de l'APD en tant qu'autorité indépendante, doit pouvoir veiller à ce que l'usage fait des données ne puisse pas être dévoilé.

Il y a aussi des conditions de sécurité qui ont été déterminées par la Sûreté de l'État.

Enfin, il faut de la transparence absolue. L'orateur regrette que cette transparence ne soit pas présente à l'heure actuelle. C'est pourtant une condition essentielle.

M. John Crombez (sp.a) se rallie aux propos de l'intervenant précédent. Le membre demande ensuite à la représentante du ministre dans quel cadre cet examen devra avoir lieu.

La représentante du ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord, indique qu'un premier texte a été rédigé en tenant compte des points évoqués dans la proposition de résolution. Ce texte sera déposé à la Chambre sous la forme d'un projet de loi. Il sera adapté aux observations de l'Autorité de protection des données. La représentante du ministre présume que le projet de loi sera examiné en commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique.

M. Christoph D'Haese (N-VA) salue l'initiative des auteurs, grâce à laquelle le débat peut être mené au niveau où il doit être mené. L'intervenant attire toutefois l'attention des membres sur le fait que cette matière, qui touche à la vie privée, devrait être débattue en commission de la Justice.

La question se pose de savoir comment la technologie peut nous aider à traverser la crise du coronavirus de façon sûre et conviviale, à éviter ou à reporter autant que possible une situation dans laquelle notre système de soins de santé serait à nouveau confronté à un risque de surcharge, et donc à éviter un nouveau confinement. Et comment peut-elle nous aider à retrouver une vie normale aussi rapidement que possible? Cette question nous préoccupe depuis le début de cette pandémie et la voilà enfin inscrite à l'ordre du jour de cette commission. Le membre présume qu'un débat interne intense est mené – ou a été mené – à ce sujet au sein des autres groupes, comme dans son propre groupe. Il est frappant de constater que ce dossier semble revêtir un caractère *quasi* éthique. Car si de nombreux parlementaires se sont déjà forgé, depuis longtemps, une opinion bien précise au sujet de l'utilisation d'une éventuelle application de suivi dans le cadre de la crise du coronavirus, ils se posent aussi beaucoup de questions à propos du respect

bestaande uit onafhankelijke leden (onder meer van de Gegevensbeschermingsautoriteit als onafhankelijk orgaan), erop kunnen toezien dat het gebruik van de gegevens niet in de openbaarheid kan worden gebracht.

De Veiligheid van de Staat heeft tevens een aantal veiligheidsvoorwaarden opgelijst.

Tot slot wordt opgemerkt dat absolute transparantie vereist is. De spreker betreurt dat die momenteel ontbreekt, hoewel dit een zeer belangrijke vereiste is.

De heer John Crombez (sp.a) sluit zich aan bij de vorige spreker en had ook graag van de vertegenwoordigster van de minister vernomen binnen welk kader deze bespreking zich dient te situeren.

De vertegenwoordigster van de minister van Digitale Agenda, Telecommunicatie en Post, belast met Administratieve Vereenvoudiging, Bestrijding van de sociale fraude, Privacy en Noordzee, deelt mee dat op basis van de in het voorstel van resolutie aangehaalde punten een eerste tekstversie werd opgesteld dat als wetsontwerp in de Kamer zal worden ingediend. De tekst zal worden aangepast aan de bemerkingen van de Gegevensbeschermingsautoriteit. De spreekster gaat er van uit dat het wetsontwerp in de commissie voor Economie, Consumentenbescherming en Digitale Agenda zal worden besproken.

De heer Christoph D'Haese (N-VA) dankt de indieners voor hun initiatief dat ervoor gezorgd heeft dat het debat wordt gevoerd daar waar het thuishoort. Hij vestigt de aandacht van de leden er evenwel op dat deze aangelegenheid, die de privacy betreft, in de commissie voor Justitie dient te worden besproken.

De vraag stelt zich hoe technologie ons op een veilige en vriendelijke manier kan helpen om ons verder doorheen deze coronatoestand te loodsen? Om er mee voor te zorgen dat de kans op een nieuwe dreiging van overbelasting van ons gezondheidssysteem en bijhorend risico op een nieuwe *lockdown* wordt vermeden of zo lang mogelijk wordt afgewend? En dat we zo snel mogelijk weer een zo normaal mogelijk leven kunnen gaan leiden. Dat is een kwestie die al sedert het begin van deze pandemie de gemoederen bedaart, en nu eindelijk in deze commissie op de tafel belandt. Het lid vermoedt dat ook de andere fracties een even intens intern debat daarover hebben gevoerd of aan het voeren zijn als de zijne. Het is opvallend om vast te stellen dat dit dossier een haast ethisch karakter lijkt te hebben. Heel veel parlementsleden hebben voor zichzelf al lang een uitgesproken standpunt gevormd met betrekking tot een mogelijke corona-*tracing*-app, maar zitten anderzijds wél nog met heel veel vragen rond privacy en effectiviteit.

de la vie privée et de l'efficacité de cette application. L'intervenant appelle donc le ministre compétent à sortir de sa réserve, en matière de vie privée, et à indiquer clairement dans quel cadre ce débat doit avoir lieu. Il demande à la représentante du ministre de préciser les mesures qui seront éventuellement adoptées, ainsi que le calendrier prévu en la matière.

L'audition organisée le 28 avril 2020 en commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique est apparue très utile, car elle a permis de répondre à de nombreuses questions. Certains orateurs ont en outre soulevé, à cette occasion, des questions prioritaires qui pourraient peut-être être intégrées dans la proposition de résolution afin de la renforcer.

L'intervenant estime qu'il convient de limiter l'examen au sein de cette commission aux points concernant le cadre de la vie privée. Les éléments qui relèvent davantage de l'Agenda numérique devraient être abordés en commission de l'Économie.

M. D'Haese évoque ensuite les points suivants:

— Au cours de l'audition précitée, la quasi-totalité des orateurs ont recommandé la mise en place d'un cadre légal pour le traitement des données. L'amendement n° 1 présenté par MM. Aouasti et Lacroix (DOC 55 1182/002) répond à cette préoccupation.

— Il a également été souligné, au cours de l'audition, que la proposition de résolution ne tient peut-être pas suffisamment compte de la répartition des compétences. Une demande 1c. visant à travailler en étroite collaboration avec les entités fédérées en vue de l'adoption éventuelle d'une application corona a en effet manifestement été ajoutée en dernière minute sur l'épreuve. Il conviendrait peut-être effectivement d'indiquer plus précisément dans la proposition de résolution quelles sont les compétences respectives des régions et de l'autorité fédérale dans le cadre de la recherche des contacts et de l'adoption éventuelle d'une application corona. Il faudrait ensuite faire la clarté sur la question de savoir si cette application sera, oui ou non, adoptée.

— Pour garantir le respect du RGPD, il conviendra aussi de réaliser une analyse d'impact relative à la protection des données (AIPD). Une demande pourrait être insérée à cet effet dans la proposition de résolution.

Hij roept de bevoegde minister dan ook op om uit zijn "privacy kot" te komen teneinde duidelijk te stellen binnen welk kader deze discussie zich dient te situeren. Hij vraagt de vertegenwoordigster van de minister dan ook om te verduidelijken wat er komt en wat niet, en in voorkomend geval tegen wanneer?

De tijdens de in de commissie voor Economie, Consumentenbescherming en Digitale Agenda gehouden hoorzitting van 28 april 2020 is zeer nuttig gebleken voor het verder uitklaren van een flink aantal van vraagtekens. Een aantal sprekers reikten daar bovenop nog een aantal aandachtspunten aan die misschien mee opgenomen kunnen worden in het voorstel van resolutie om het nog verder te versterken.

De spreker acht het aangewezen dat de bespreking zich in deze commissie beperkt tot die aspecten die verband houden met het privacy-kader. Insteken die meer betrekking hebben op het aspect Digitale Agenda dienen te worden aangekaart bij de bespreking in de commissie voor Economie.

De heer D'Haese haalt vervolgens de volgende punten aan.

— Tijdens voormelde hoorzitting hebben bijna al de genodigde sprekers gesteld dat het aangewezen is om voor de gegevensverwerking in een wettelijk kader te voorzien. Het door de heren Aouasti en Lacroix ingediende amendement nr. 1 (DOC 55 1182/002) komt alvast tegemoet aan deze bekommernis.

— Verder werd ook aangehaald dat het voorstel van resolutie misschien wat te veel voorbij gaat aan de bevoegdheidsverdeling. Op de drukproef werd kennelijk inderdaad nog snel op de valreep een verzoek 1c. ingevoegd om in nauw overleg met de deelstaten tewerk te gaan voor wat betreft een eventuele corona-app. Het verdient misschien inderdaad aanbeveling om toch wat nauwkeuriger in de resolutie af te bakenen waarvoor de gewesten dan wel de federale overheid precies bevoegd zijn in het kader van het contactonderzoek en de eventuele corona-app. Voorts is het aangewezen dat er zekerheid bestaat over deze app. Komt hij er nu of niet?

— Naleving van de GDPR zou ook de noodzaak van een zogeheten DPIA of gegevensbeschermingsimpactanalyse met zich meebrengen. Daarvoor zou ook een verzoek kunnen worden toegevoegd in het voorstel van resolutie.

La proposition de la *Liga voor Mensenrechten* d'étendre la proposition de résolution au traçage manuel des contacts est une suggestion à laquelle le groupe N-VA n'adhère pas. L'intervenant souligne que cela ne relève pas, en effet, de la compétence du législateur fédéral, mais bien de la compétence des régions.

L'intervenant conclut en indiquant que s'il est tenu compte de ces observations, le groupe N-VA rendra un avis positif à la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique.

M. John Crombez (sp.a) déplore que cette discussion ne soit menée que maintenant, à la fin du mois d'avril. Si des applications de suivi des contacts sont nécessaires pour mettre la population en sécurité, il faut que ces applications soient mises en œuvre, et le cadre légal nécessaire aurait déjà dû être établi précédemment. On a déjà perdu beaucoup de temps. Comme l'intervenant précédent, le membre estime que l'évaluation finale du cadre de cette problématique appartient à la commission de la Justice. Il importe que cette problématique soit évaluée à la lumière du Règlement (UE) 2016/679. En effet, la protection des droits fondamentaux et la protection des libertés fondamentales sont, en la matière, des principes de base évidents.

L'intervenant souligne qu'il convient qu'un régulateur public, l'Autorité de protection des données, puisse accéder, dès le début des travaux, complètement et inconditionnellement, à toutes les informations, afin que le respect des droits fondamentaux et des libertés fondamentales puisse être assuré.

Aux questions concernant la décentralisation, la technologie Bluetooth et la base volontaire, s'ajoute la question du caractère temporaire. Il importe en effet de mettre en place un cadre pouvant être activé en cas de besoin mais qui pourra ensuite être désactivé.

En ce qui concerne les compétences, l'intervenant souligne que s'il est vrai que les compétences sont réparties entre différents niveaux – la question de la répartition ayant en effet été source de confusion à la suite de diverses affirmations – , il est parfaitement possible que les différents niveaux de pouvoir se mettent d'accord sur le déroulement des opérations en vue de la protection des citoyens.

M. Crombez souligne que son groupe a cosigné la proposition de résolution et qu'il la soutient donc.

M. Nabil Boukili (PVDA-PTB) désapprouve lui aussi fortement la forme avec laquelle le gouvernement traite le sujet, en se moquant du parlement. Il est vicieux de faire croire qu'on met une question en débat public alors

Een suggestie die de N-VA-fractie niet meeneemt, is het voorstel van de Liga voor Mensenrechten om het voorstel van resolutie uit te breiden naar manuele *contact tracing*. De spreker benadrukt dat dit immers niet de bevoegdheid van de federale wetgever maar wel die van de gewesten uitmaakt.

De spreker besluit dat als met deze opmerkingen rekening wordt gehouden de N-VA-fractie een positief advies kan uitbrengen aan de commissie voor Economie, Consumentenbescherming en Digitale Agenda.

De heer John Crombez (sp.a) betreurt dat pas nu, eind april, deze discussie wordt gevoerd. Als er *tracing*-apps nodig zijn om de bevolking in veiligheid te stellen dan moeten die er komen en had het wettelijk kader al voorhanden moeten zijn. Er is al veel tijd verloren. Net als de vorige spreker is het lid van oordeel dat de eindbeoordeling van het kader waarin deze problematiek wordt gegoten toekomt aan de commissie voor Justitie. Het is belangrijk dat deze problematiek wordt afgetoetst aan de Verordening (EU) 2016/679. De bescherming van de grondrechten en van de fundamentele vrijheden zijn in deze kwestie immers evidente uitgangspunten.

De spreker wijst op de noodzaak van een publieke regulator, zijnde de Gegevensbeschermingsautoriteit, die van in het begin volledige en onvoorwaardelijke toegang moet hebben tot alle informatie opdat de naleving van de grondrechten en de fundamentele vrijheden kan worden verzekerd.

Naast decentralisatie, bluetooth-technologie, vrijwilligheid, is er ook het aspect tijdelijkheid. Het is immers belangrijk dat een kader wordt gecreëerd dat bij nood kan worden geactiveerd maar dat daarna ook kan worden uitgezet.

Wat de bevoegdheden betreft, benadrukt de spreker dat, als deze verspreid zouden liggen over verschillende niveaus, want daarover is naar aanleiding van diverse uitspraken nogal verwarring gerezen, het perfect mogelijk is om in functie van de bescherming van de burgers tussen de verschillende bevoegdheidsniveaus af te spreken hoe de zaken zullen verlopen.

De heer Crombez stipt aan dat zijn fractie het voorstel van resolutie heeft meeondertekend en derhalve steunt.

Ook *de heer Nabil Boukili (PVDA-PTB)* acht het bijzonder verwerpelijk hoe de regering met deze kwestie omgaat door het Parlement een neus te zetten. Het is pervers de illusie te wekken dat een kwestie publiekelijk

qu'on fait déjà un arrêté royal indépendamment des différentes positions qui seront développées au parlement.

Les auditions en commission de l'Économie ont mis en exergue une double équation. D'un côté, on a une application dont on doute de l'efficacité. Même les défenseurs de l'application indiquent que des problèmes peuvent survenir, qu'il faut un pourcentage important de la population qui l'utilise pour qu'elle ait un impact – ce qui n'est pas garanti –, etc. En outre, c'est un élément complémentaire à une série de mesures faisant partie d'une vision globale. Le reste n'est pourtant pas encore mis en place d'une manière concrète.

De l'autre côté, il y a une atteinte grave à la vie privée et aux droits démocratiques.

Le PVDA-PTB est donc opposé à la mise en place de cette application. On ne peut pas se lancer dans une aventure aussi hasardeuse qui mettrait en danger la vie privée des Belges.

Il faut donc une législation claire sur le traçage, car, même sans application on risque des atteintes à la vie privée.

La proposition de résolution renforce l'aspect éthique dans lequel il faut travailler. L'orateur la soutient donc. Ces mesures devront être prises dans un cadre juridique légal.

L'orateur insiste enfin pour que le débat soit aussi mené en commission de la Justice.

M. Sammy Mahdi (CD&V) constate que la manière dont cette problématique est abordée est peu transparente. Il partage donc la frustration des intervenants précédents à ce sujet.

L'audition organisée le 28 avril 2020 au sein de la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique a permis de clarifier de nombreux points, en particulier au travers de l'exposé de la Sûreté de l'État, qui a indiqué que la technologie pouvait être piratée et souligné les risques liés à l'utilisation de cette technologie tant par d'autres États que par des organisations extrémistes. Il convient d'établir un cadre juridique strict et clair qui permettra de garantir la protection des citoyens.

L'intervenant salue l'initiative de Mme Soors, qui veille à ce que les choses soient traitées dans l'ordre: à ce

wordt besproken en tegelijk reeds een koninklijk besluit voor te bereiden, zonder rekening te houden met de diverse standpunten die in het Parlement zullen worden ingenomen.

De hoorzittingen in de commissie voor Economie hebben een dubbel euvel aan het licht gebracht. Eensdeels is er een app waarvan de efficiëntie in twijfel wordt getrokken. Zelfs de voorstanders ervan wijzen erop dat zich problemen kunnen voordoen, dat de deelname van een groot deel van de bevolking vereist is om een impact te hebben (waarbij die deelname niet is gegarandeerd) enzovoort. Bovendien is die app een aanvulling op een aantal maatregelen die zijn ingebed in een alomvattende visie. De overige maatregelen zijn evenwel nog niet concreet uitgerold.

Anderdeels worden de persoonlijke levenssfeer en de democratische rechten ernstig geschonden.

PVDA-PTB is derhalve gekant tegen de invoering van die app. Het geeft geen pas zich in een zo hachelijk avontuur te storten dat de privacy van de Belgen op de helling zou zetten.

De opsporingswetgeving moet dus duidelijk zijn; zelfs zonder app dreigt immers de persoonlijke levenssfeer te worden geschonden.

Aangezien het ter bespreking voorliggende voorstel van resolutie meer belang hecht aan het ethisch aspect van de zaak, zal de spreker het steunen. Deze maatregelen zullen moeten worden genomen binnen een wettelijk juridisch kader.

Tot slot dringt de spreker erop aan het debat ook in de commissie voor Justitie te voeren.

De heer Sammy Mahdi (CD&V) stelt vast dat de manier waarop met deze problematiek wordt omgegaan van weinig transparantie getuigt. Hij sluit zich dan ook aan bij de frustraties hierover van de vorige sprekers.

De tijdens de in de commissie voor Economie, Consumentenbescherming en Digitale Agenda gehouden hoorzitting van 28 april 2020 heeft op vele punten duidelijkheid gebracht, niet in het minst door de Staatsveiligheid die heeft aangegeven dat de technologie gehackt kan worden en heeft gewezen op de gevaren van zowel andere Staten als van extremistische organisaties om hiermee aan de slag te gaan. Er is nood aan een streng en duidelijk juridisch kader dat de bescherming van de burgers garandeert.

De spreker is tevreden met het initiatief van mevrouw Soors dat ervoor zorgt dat in de juiste volgorde wordt

que l'on commence par prévoir un cadre juridique avant de s'interroger sur la manière dont la technologie peut être utilisée. Ces dernières années et décennies, partout dans le monde, des gouvernements ont en effet utilisé certaines technologies avant de s'interroger sur leurs éventuels effets pervers, ce qui a posé de nombreux problèmes à l'égard de la protection de la vie privée. Cette problématique doit d'abord être examinée au Parlement, de préférence au sein de la commission de la Justice, afin que les verrous juridiques soient clairs pour tout le monde.

M. Mahdi se réjouit que la résolution contienne plusieurs éléments qui revêtent une grande importance pour son groupe. En réponse à l'observation de M. Crombez relative aux compétences, il indique que le fait que cette discussion ait traîné en longueur n'est pas illogique compte tenu de ce qui se passe dans les autres pays. Il renvoie en l'occurrence à l'Allemagne, qui a d'abord opté en faveur du PEPP-PT, système européen centralisé, mais qui a décidé, il y a quelques jours, de faire marche arrière. La technologie n'est pas claire pour tout le monde. Il importe dès lors d'identifier, si nécessaire, les méthodes qui pourraient être utilisées pour garantir également le respect de la vie privée. La résolution à l'examen opte résolument pour le DP3T et la décentralisation dès lors que l'échange de données peut présenter des risques. Il est en effet possible, comme l'a également indiqué la *Liga voor Mensenrechten* au cours des auditions, que, si cette application existe, la pression soit grande, par exemple, pour que les gens utilisent les transports en commun, avec cette application ou non, pour aller travailler, avec cette application ou non.

En ce qui concerne le caractère volontaire, le membre attire l'attention sur le manque d'adhésion. L'Université d'Anvers a indiqué que 50 % de ses répondants avaient répondu qu'ils ne voulaient pas l'utiliser pour des raisons de confidentialité et que 80 % des répondants étaient inquiets. Il est donc nécessaire d'assurer la transparence à propos de cette application et de la manière dont elle devrait se développer. Le code source doit être public et la procédure doit être *open source*. La société civile et le plus grand nombre possible d'experts devront y être associés. C'est la seule façon de rassurer les citoyens et de les convaincre d'utiliser cette application. Aujourd'hui, le simple fait de déployer une application soulève un grand nombre de questions. M. Mahdi est donc satisfait que la résolution prévoie une condition. Si cette application doit être conçue, elle devra être bien conçue. Les données des citoyens ne pourront pas être diffusées ou échangées avec des autorités et des organisations susceptibles d'en abuser. Le caractère temporaire des données est un autre point important qui préoccupe les citoyens.

gehandeld: eerst voorzien in een juridisch kader en dan pas kijken hoe de technologie kan worden gebruikt. De voorbije jaren en decennia hebben over de hele wereld regeringen immers eerst technologie gebruikt om pas naderhand na te gaan wat de mogelijke perverse effecten ervan kunnen zijn, wat tot heel wat privacy problemen heeft geleid. Deze problematiek moet eerst in het Parlement, bij voorkeur in de commissie voor Justitie, worden behandeld opdat de juridische grendels voor eenieder duidelijk zijn.

De heer Mahdi is verheugd dat de resolutie een aantal elementen bevat die voor zijn fractie van groot belang zijn. Wat de bemerking van de heer Crombez betreft over de bevoegdheden, antwoordt hij dat het feit dat deze discussie heeft aangesleept niet onlogisch is als men kijkt naar wat er in de andere landen gaande is. Hij verwijst in deze naar Duitsland waar eerst werd gekozen voor PEPP-PT, het Europese systeem dat gecentraliseerd is, maar waar dan enkele dagen geleden werd beslist om dit toch niet te doen. De technologie is niet voor iedereen duidelijk. Het is derhalve belangrijk om te kijken, mocht het nodig zijn, welke methodes gebruikt kunnen worden om daarnaast ook de privacy te garanderen. In deze resolutie wordt resoluut gekozen voor DP3T, voor decentralisering omdat de uitwisseling van gegevens voor gevaren kan zorgen. Het is immers mogelijk, zoals ook de Liga voor Mensenrechten tijdens de hoorzitting heeft gesteld, dat mocht die app er komen er grote druk kan ontstaan om bijvoorbeeld het openbaar vervoer te gebruiken, al dan niet met die app, om te gaan werken, al dan niet met app.

Inzake vrijwilligheid vestigt het lid de aandacht op het gebrek aan draagvlak. De Universiteit Antwerpen heeft meegedeeld dat 50 % van hun respondenten heeft aangegeven omwille van privacy-redenen er geen gebruik van te willen maken; 80 % van de respondenten maakt zich ongerust. Er is dus nood aan transparantie over deze app en de manier waarop deze zich moet ontwikkelen. De broncode moet openbaar zijn, de procedure moet *open source* zijn. Het sociale middenveld en zoveel mogelijke experts moeten erbij worden betrokken; alleen op die manier zullen de burgers worden gerustgesteld en gebruik maken van de app. Vandaag, zomaar een app uitrollen, roept nogal wat vragen op. De heer Mahdi is dan ook tevreden over de voorwaardelijke zin die wordt gebruikt in de resolutie. Als die app er zou moeten komen dan moet het goed in elkaar steken. De gegevens van de burgers mogen niet worden verspreid of uitgewisseld met mogendheden en organisaties die daarvan misbruik kunnen maken. Ook de tijdelijkheid van de gegevens is een belangrijk aspect waarover de burgers zich zorgen maken.

Pour conclure, l'intervenant indique qu'il soutient la proposition de résolution à l'examen. Il conviendra également de déterminer comment le traçage manuel permettra également de garantir la protection de la vie privée des citoyens. M. Mahdi forme le vœu qu'à l'avenir, il soit garanti, au-delà des clivages partisans, que la législation relative à la vie privée, en particulier en ce qui concerne les progrès technologiques, soit élaborée dans la transparence, en prévoyant d'abord un cadre juridique clair, avant d'examiner quelle technologie peut être utilisée.

Mme Sophie Rohonyi (DéFI) indique qu'il faut veiller à ne pas emprunter le chemin qu'ont pris certains États qui profitent de cette crise sanitaire pour restreindre les libertés individuelles et pour cadenasser le rôle du parlement dont la mission première est de contrôler le gouvernement.

L'oratrice a des craintes sur ce dernier point. Tout le monde semblait d'accord sur la nécessité d'une base légale pour ce *tracing*. Aujourd'hui, on apprend que l'APD a rendu un avis sur un avant-projet d'arrêté royal. Il semble difficile de croire que le président de l'APD n'était pas au courant.

Sur quelle base le gouvernement travaille-t-il finalement? Il faudra en tout cas tenir compte des garde-fous prévus par cette proposition de résolution.

Pour que l'atteinte à nos droits et libertés soient proportionnée, comme le prévoit la Constitution et la Convention européenne des droits de l'homme, il faut des garde-fous précis, mais aussi un débat transparent et public, et une base légale. Un arrêté de pouvoirs spéciaux peut-il être considéré comme une loi au sens de l'article 22 de la Constitution et de l'article 8 de la CEDH? L'oratrice considère au contraire qu'il faudra une loi.

Le *tracing*, même s'il constitue un élément-clé du déconfinement, reste une atteinte aux droits fondamentaux qui doit être accompagnée de garde-fous, en particulier lorsqu'il s'agit de données médicales, donc sensibles. Leur traitement ne peut se justifier que dans des circonstances exceptionnelles bien déterminées et sous un contrôle strict. Le professeur Elise Degrave a notamment souligné les risques en termes de discrimination d'un tel traitement.

Dans ce contexte, le *tracing* ne peut pas se mettre en place par le biais d'un arrêté de pouvoirs spéciaux,

De spreker besluit dat hij zich achter het ter bespreking voorliggende voorstel van resolutie kan scharen. Er moet ook verder worden nagegaan op welke manier de manuele *tracing* ook de privacy van de burgers kan garanderen. De heer Mahdi drukt de hoop uit dat in de toekomst over de partijgrenzen heen erover zal worden gewaakt dat wetgeving over privacy, en zeker met betrekking tot technologische vooruitgang, op een transparante manier tot stand komt met eerst een duidelijk juridisch kader, om pas daarna te kijken welke technologie kan worden gebruikt.

Mevrouw Sophie Rohonyi (DéFI) waarschuwt dat België niet dezelfde weg mag inslaan als bepaalde andere Staten die deze gezondheidscrisis aanwenden om de individuele vrijheden in te perken en de rol van hun parlement, waarvan de belangrijkste taak erin bestaat toezicht te houden op de regering, aan banden te leggen.

Dat laatste punt verontrust de spreekster. Iedereen leek het erover eens dat die *tracing* een wettelijke basis vereist. Thans vernemen we dat de GBA een advies over een voorontwerp van koninklijk besluit heeft uitgebracht. Het valt moeilijk te geloven dat de voorzitter van de GBA niet op de hoogte was.

Op basis waarvan werkt de regering uiteindelijk? Er zal in elk geval rekening moeten worden gehouden met de in dit voorstel van resolutie aangehaalde maatregelen om misbruiken tegen te gaan.

Om buitenproportionele aantastingen van onze rechten en vrijheden te beletten – die waarborg moet er zijn krachtens de Grondwet en het Europees Verdrag voor de Rechten van de Mens – zijn er niet alleen duidelijke regels nodig om dergelijke aantastingen tegen te gaan, maar ook een transparant en publiek debat, alsmede een wettelijke basis. Kan een volmachtenbesluit worden beschouwd als een wet in de zin van artikel 22 van de Grondwet en artikel 8 van het EVRM? De spreekster is integendeel van oordeel dat er nood is aan een wet.

Hoe belangrijk *tracing* ook is om uit de *lockdown* te raken, het is en blijft een aantasting van de grondrechten, waar beschermende maatregelen tegenover moeten staan – zeker indien het om medische en dus gevoelige gegevens gaat. De verwerking van die gegevens zou enkel mogen worden toegestaan indien dit vanwege uitzonderlijke en welomlijnde omstandigheden te rechtvaardigen valt én indien er een strikt toezicht op wordt uitgeoefend. Zo heeft professor Elise Degrave uitdrukkelijk gewezen op het risico dat een dergelijke gegevensverwerking tot ongelijke behandeling kan leiden.

In het licht daarvan mag *tracing* niet tot stand komen via een volmachtenbesluit; gebeurt dat toch, dan zal

au défaut de quoi la confiance dans le gouvernement, mais aussi la confiance des citoyens, sera entamée. Or, il est indispensable, pour un *tracing* efficace, que les citoyens aient confiance dans ce système.

L'oratrice soutient bien entendu la proposition de résolution et les garde-fous que celle-ci prévoit.

Ces garde-fous doivent être considérés comme un ensemble de conditions cumulatives, notamment celle de la transparence du débat.

La tâche sera difficile. Il faudra opérer un équilibre entre les droits et libertés individuelles, notamment la protection de la vie privée, et la préservation de notre santé, qui est aussi un droit fondamental.

Il va falloir avoir une lecture pragmatique de la situation. Le déconfinement sera entamé si la situation épidémiologique le permet, et il va falloir vivre avec le virus qui sera toujours présent. Il faudra se protéger les uns et les autres et isoler les personnes contaminées.

Mme Rohonyi reconnait la plus-value de ce système, moyennant les garde-fous mentionnés et une stratégie claire et précise en termes de *testing*. La proposition de résolution est une très bonne base et elle lance au gouvernement des messages clairs.

L'oratrice pose deux questions à la représentante du ministre De Backer:

1. Qu'en est-il du recrutement et du fonctionnement des *call-centers*? Les mutuelles seront-elles mobilisées? Cela constitue-t-il une garantie suffisante en termes de protection de la vie privée? Qui va faire quoi au sein de ces *call-centers*?

2. Qu'en est-il de la composition de la *task force* "*data against corona*"? Il faut avoir de la transparence sur cette composition et connaitre les possibles conflits d'intérêts.

L'oratrice annonce le dépôt d'amendements qui aura lieu en commission de l'Économie.

M. Khalil Aouasti (PS) rejoint cette demande concernant la composition de la *task force*. Dans quel délai ce texte sera-t-il déposé? En outre, il faudra demander un nouvel avis de l'APD. L'orateur a le sentiment que le

het vertrouwen in de regering maar ook het vertrouwen van de burgers worden geschaad. *Tracing* kan echter slechts werken indien de burgers vertrouwen hebben in het systeem.

De spreekster steunt uiteraard het voorstel van resolutie en de daarin vervatte maatregelen om misbruiken tegen te gaan.

Die maatregelen moeten worden opgevat als een geheel van cumulatieve voorwaarden, zoals die van een transparant debat.

Het wordt een moeilijke opdracht: er is nood aan een balans tussen de individuele rechten en vrijheden (meer bepaald de bescherming van de persoonlijke levenssfeer) en de bescherming van onze gezondheid, die evenzeer een grondrecht is.

De situatie zal pragmatisch moeten worden benaderd. De *lockdown*-maatregelen zullen worden afgebouwd indien de epidemiologische toestand dit mogelijk maakt; we zullen moeten leven met het virus, dat nog altijd aanwezig zal zijn. We zullen elkaar moeten beschermen en de besmette personen in afzondering brengen.

Mevrouw Rohonyi erkent dat dit systeem een meerwaarde heeft indien het gepaard gaat met de voormelde maatregelen om misbruiken tegen te gaan, en met een duidelijke en nauwkeurige teststrategie. Het voorstel van resolutie vormt een heel goede basis en bevat duidelijke aandachtspunten ten behoeve van de regering.

De spreekster stelt de vertegenwoordigster van minister De Backer twee vragen:

1. *Quid* met het aantrekken van personeel en de werking van de callcenters? Zullen ter zake de ziekenfondsen worden ingeschakeld, en vormt dat een voldoende waarborg voor de bescherming van de persoonlijke levenssfeer? Wie zal wat doen in die callcenters?

2. *Quid* met de samenstelling van de taskforce *data against corona*? Er moet transparantie zijn omtrent die samenstelling en het moet duidelijk zijn waar eventueel belangenconflicten kunnen rijzen.

De spreekster kondigt aan amendementen te zullen indienen in de commissie voor Economie.

De heer Khalil Aouasti (PS) sluit zich aan bij de vraag over de samenstelling van de taskforce. Voorts vraagt de spreker wanneer dit voorstel zal worden ingediend. Ook zal de GBA om een nieuw advies moeten worden

président de l'APD a menti par omission au parlement concernant l'avis rendu sur le projet d'arrêté royal.

M. Gilles Vandenburre (Ecolo-Groen) se réjouit qu'il y ait un débat démocratique dans ce parlement sur ce sujet. C'était l'objectif de cette proposition de résolution. Le Parlement doit garder le *leadership* sur ce débat fondamental. Le fait que beaucoup de groupes aient cosignés ce texte permet d'avoir une assise démocratique très large pour pouvoir avancer. C'est un élément très important.

L'orateur regrette fortement que l'avis de l'APD ait été demandé sur un avant-projet d'arrêté royal. Cela donne le sentiment qu'on essaie de court-circuiter le parlement. Le travail parlementaire ne peut pas se faire doubler via un arrêté royal.

Trois balises ont été mises fortement en évidence: la décentralisation, l'aspect volontaire et le fait que tout soit ouvert et transparent (open data/open source/open code). Ce sont des valeurs fondamentales dans ce débat.

Comment l'aspect du traçage manuel va-t-il être prévu dans le cadre juridique en préparation? Il faut avoir de la clarté à cet égard.

Il faut pouvoir avancer rapidement sur ce sujet dans le cadre d'un débat démocratique.

Mme Nathalie Gilson (MR) indique que son groupe n'a pas signé la proposition de résolution car elle ne va pas assez loin, selon son groupe.

Toutes nos libertés ont été mises sous cloche, à juste titre. La question est de savoir comment on va évoluer vers le déconfinement. Comment peut-on protéger nos services hospitaliers tout en déconfinant progressivement? La réflexion sur l'utilisation du traçage, en complément à d'autres méthodes, peut-être une des pistes pour aller vers le déconfinement.

L'oratrice souligne que son groupe a déposé une dizaine d'amendements sur la proposition de résolution en commission de l'Économie.

Le début de l'intervention de l'intervenante précédente, membre du parti libéral, stupéfie *M. Christoph D'Haese (N-VA)*. Il s'agit d'un débat constitutionnel. Il est inadmissible d'affirmer que la résolution ne va pas assez loin. Quel est le point de vue du ministre compétent à

verzocht. De spreker heeft het gevoel dat wat het advies over het ontwerp van koninklijk besluit betreft, de voorzitter van de GBA een en ander voor het Parlement heeft verzwegen.

De heer Gilles Vanden Burre (Ecolo-Groen) is verheugd dat dit Parlement een democratisch debat over het onderwerp voert. Zulks was de bedoeling van dit voorstel van resolutie. Het Parlement moet met betrekking tot dit fundamenteel debat de leiding blijven nemen. Doordat veel fracties dit voorstel van resolutie mee hebben ondertekend, kan het op een heel brede democratische basis steunen om vooruitgang te boeken; dat is een heel belangrijk aspect van de zaak.

De spreker betreurt echt dat over een voorontwerp van koninklijk besluit het advies van de GBA werd gevraagd, want dat geeft de indruk dat men het Parlement buitenspel probeert te zetten. De parlementaire werkzaamheden mogen niet ongedaan worden gemaakt door een koninklijk besluit.

Drie kernelementen worden in de verf gezet: decentralisering, vrijwilligheid en het feit dat alles open en transparant moet gebeuren (*open data*/*open source*/*open code*). In dit debat zijn dat fundamentele waarden.

Hoe zal het aspect "manuele *tracing*" in het op stapel staande juridisch raamwerk worden geregeld? Ter zake is duidelijkheid vereist.

Er moet in dit verband snel vooruitgang kunnen worden geboekt, binnen een democratisch debat.

Mevrouw Nathalie Gilson (MR) geeft aan dat haar fractie het voorstel van resolutie niet heeft ondertekend omdat het volgens de MR niet ver genoeg gaat.

Alle onze vrijheden werden – terecht – ingeperkt. De vraag is hoe men naar een afbouw van de *lockdown*-maatregelen zal toewerken. Hoe kunnen onze ziekenhuisdiensten goed blijven werken wanneer tegelijk de *lockdown* geleidelijk zal worden afgebouwd? De denkoefening aangaande het gebruik van *tracing*, ter aanvulling van andere methodes, kan een van de denksporen zijn om de *lockdown* af te bouwen.

De spreekster benadrukt dat haar fractie in de commissie voor Economie een tiental amendementen op het voorstel van resolutie heeft ingediend.

Het begin van de uiteenzetting van de vorige spreekster, die lid is van de liberale partij, slaat *de heer Christoph D'Haese (N-VA)* met verstomming. Het gaat hier over een grondwettelijke discussie. Het gaat dan niet op om nu te stellen dat de resolutie niet ver genoeg gaat.

l'égard des droits et des libertés en la matière? En est-il le gardien?

M. Khalil Aouasti (PS) demande à Mme Gilson si son groupe compte rendre un avis négatif à la proposition de résolution? Est-ce à dire que les sept ministres libéraux ne soutiennent pas le processus gouvernemental?

Mme Nathalie Gilson (MR) précise qu'elle se limitera à une intervention de type juridique sur ce texte. Elle se réjouit qu'un projet de loi sera débattu au parlement sur cette question du *tracing*.

En ce qui concerne la proposition de résolution, il ne faudrait pas oublier de se référer expressément à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Par ailleurs, il faut bien distinguer *tracking* et *tracing*. Le *tracking* revient à suivre les déplacements des personnes, alors que le *tracing* signifie trouver un moyen de les avertir du fait qu'ils ont croisé des personnes positives au COVID-19 et les faire prendre certaines mesures. L'oratrice rappelle que des porteurs asymptomatiques peuvent transmettre le virus. Le traçage manuel déjà utilisé pour la tuberculose notamment ne sera donc pas efficace en l'espèce.

En ce qui concerne le comité éthique, l'oratrice est favorable à la mise en place d'un organe de consultation obligatoire, tout au long du processus limité dans le temps d'utilisation d'une application de traçage.

Mme Gilson rappelle que les Régions sont compétentes pour la mise en œuvre de ce traçage et l'application, cependant, c'est le niveau fédéral qui reste compétent pour la protection de la vie privée, qu'on parle d'une application ou de traçage manuel. Il est très important que cette résolution touche aussi cet aspect.

Beaucoup sont inquiets du traçage manuel, qui serait beaucoup plus invasif sur la vie privée et son efficacité ne serait pas maximale car on ne connait pas toujours toutes les personnes croisées. Ces personnes-là ne seront donc jamais averties via les *call-centers*.

Il faut faire référence au traçage manuel et aux garde-fous à imposer pour protéger le traitement des données

Wat is het standpunt van de bevoegde minister over de rechten en vrijheden in deze? Is hij de bewaker ervan?

De heer Khalil Aouasti (PS) vraagt mevrouw Gilson of haar fractie een negatief advies zal uitbrengen over het voorstel van resolutie? Betekent zulks dat de zeven Franstalige liberale ministers het optreden van de regering niet steunen?

Mevrouw Nathalie Gilson (MR) geeft aan dat ze zich in haar betoog zal beperken tot de juridische aspecten van het voorstel. Zij is verheugd dat in dit Parlement een wetsontwerp omtrent *tracing* zal worden besproken.

Wat het voorstel van resolutie betreft, mag niet uit het oog worden verloren uitdrukkelijk te verwijzen naar de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Voorts moet een duidelijk onderscheid worden gemaakt tussen *tracking* en *tracing:* bij *tracking* worden de verplaatsingen van de mensen gevolgd, terwijl *tracing* inhoudt dat een middel wordt uitgewerkt om mensen te verwittigen dat zij in contact waren met anderen die een positieve COVID-19-test hebben afgelegd en dat die mensen bepaalde maatregelen moeten nemen. De spreekster brengt in herinnering dat wie het virus draagt maar geen symptomen vertoont, het virus kan overdragen. De manuele *tracing* die onder meer bij tuberculose al wordt toegepast, zal in dit geval dus niet doeltreffend zijn.

Wat het ethisch comité betreft, is de spreekster ervoor gewonnen te voorzien in de instelling van een raadgevend orgaan dat gedurende het volledige, in tijd beperkte gebruik van een *track & trace app* verplicht moet worden geconsulteerd.

Mevrouw Gilson wijst erop dat de gewesten bevoegd zijn voor de tenuitvoerlegging van die *tracing* en voor de app; het federale niveau blijft echter bevoegd inzake bescherming van de persoonlijke levenssfeer, zowel wat een app betreft als bij manuele *tracing*. Het is van het grootste belang dat ook dat aspect in dit voorstel van resolutie aan bod komt.

Velen zijn ongerust over manuele *tracing*, die een veel grotere impact op de persoonlijke levenssfeer zou hebben en bovendien niet maximaal doeltreffend zou zijn omdat men niet altijd weet met wie er contact is geweest. Die personen zullen dus nooit via de *call centers* worden verwittigd.

In het voorstel van resolutie moet worden gewezen op het aspect "manuele *tracing*" en op de op te leggen

à caractère personnel. En outre, la proposition de résolution devrait prévoir une référence aux Guidelines du Comité européen de la protection des données. Ce document daté du 21 avril 2020 contient toute une série de recommandations qui devraient être incluses dans la résolution.

En outre, la résolution devrait faire référence au principe de minimisation, notamment l'article 25.1. du RGPD, et à la licéité et la finalité du système qui sera mis en œuvre. La licéité doit être choisie sur la base des articles 6 ou 9 du RGPD, sachant que le consentement n'est pas la seule base possible compte tenu de l'intérêt public, de la sauvegarde des droits et libertés de la personne concernée. Cela permettra d'empêcher l'utilisation de l'application pour d'autres finalités, telles que le contrôle des mesures de distanciation sociale ou de quarantaine par exemple.

L'oratrice se réjouit du choix du protocole DP-3T dans la proposition de résolution, avec un serveur décentralisé qui semble le plus protecteur de la vie privée.

La proposition de résolution demande au gouvernement fédéral de "garantir la sécurisation des données collectées ou enregistrées en les cryptant et en les protégeant efficacement contre le piratage" (point J). Lors des auditions, la question s'est posée de savoir si les codes en *open source* n'allaient pas favoriser un risque de piratage. Il faut se pencher sur ce point. Il est important que le code soit ouvert et qu'on applique un système de "privacy by design". En outre, le couplage des données avec d'autres banques de données existantes doit être absolument interdit.

Le point n demande que "les données qui, compte tenu du délai d'incubation du coronavirus, ne sont plus nécessaires, après un certain nombre de semaines, pour constater les infections, soient automatiquement supprimées,"; d'un autre côté, le point m demande de "garantir que les données ne pourront en tout cas être communiquées que dans le cadre de la recherche médicale et scientifique qui concerne le coronavirus". En outre le point u demande "de garantir la suppression définitive des données, à titre de finalité établie, sauf pour l'utilisation des donnéessous forme agrégée et anonyme pour la recherche scientifique ou le traitement de plaintes". L'oratrice est d'avis que les formulations de ces trois points devraient être revues juridiquement pour s'assurer d'un effacement automatique de toutes les données. Cela pourra être le cas après trois semaines,

waarborgen ter bescherming van de persoonlijke gegevens die worden verwerkt. Bovendien zou in deze tekst ook moeten worden verwezen naar de richtsnoeren van het Europees Comité voor de gegevensbescherming; dat document van 21 april 2020 omvat een hele reeks aanbevelingen, die in het voorstel van resolutie zouden moeten worden opgenomen.

Bovendien zou de resolutie moeten verwijzen naar het beginsel van de minimale gegevensverwerking (inzonderheid naar artikel 25.1 van de AVG), alsook naar de rechtmatigheid en het doel van het ten uitvoer te leggen systeem. De rechtmatigheid moet worden bepaald op grond van de artikelen 6 of 9 van de AVG; toestemming is immers niet de enige mogelijke basis, rekening houdend met het openbaar belang alsook de vrijwaring van de rechten en vrijheden van de betrokken persoon. Aldus kan worden voorkomen dat de app wordt gebruikt voor andere doeleinden (bijvoorbeeld toezicht op de maatregelen inzake *social distancing* en quarantaine).

Het verheugt de spreekster dat in het voorstel van resolutie is gekozen voor het DP-3T-protocol, met een gedecentraliseerde server, die de bescherming van de persoonlijke levenssfeer wellicht het best kan waarborgen.

In het voorstel van resolutie wordt de federale regering verzocht "ervoor te zorgen dat de verzamelde of geregistreerde data veilig zijn, door ze te versleutelen en afdoende te beschermen tegen de aanvallen van hackers" (verzoek 1, j). Tijdens de hoorzittingen rees de vraag of *open source*-codes vatbaarder zijn voor hacking. Hier moet dieper op worden ingegaan. Het is belangrijk dat het om een open code gaat en dat een *privacy by design*-systeem wordt toegepast. Voorts moet volstrekt worden verboden dat de data worden gekoppeld aan andere bestaande gegevensbanken.

In verzoek 1, n, wordt gevraagd dat "data die niet meer nodig zijn om besmettingen vast te stellen na een beperkt aantal weken, gebaseerd op de incubatieperiode van het coronavirus (…) automatisch vernietigd worden". Verzoek 1, m, beoogt er voor te zorgen dat de data louter mogen worden doorgegeven binnen de gezondheidszorg en voor wetenschappelijk onderzoek in verband met het coronavirus. Tot slot stelt verzoek 1, u. het volgende: "de onherroepelijke vernietiging van de data als vaststaande finaliteit te garanderen, uitgezonderd het gebruik van de data in geaggregeerde en anonieme vorm voor wetenschappelijk onderzoek of klachtbehandeling". De spreekster vindt dat de formulering van die drie verzoeken juridisch zou moeten worden afgetoetst om er te zeker van te zijn dat alle gegevens automatisch worden verwijderd. Volgens de gehoorde deskundigen

d'après les experts entendus. Pourquoi garder les données plus longtemps?

Par ailleurs, il faudra une analyse d'impact et une consultation de l'APD. En outre, il faut assurer le contrôle du traçage par l'APD tout au long du processus de manière à garantir la transparence.

Il faut un traitement similaire de toutes les données récoltées via la traçage manuel et via le *tracing*. Même si le traçage manuel est une compétence régionale, il faudrait obtenir plus d'informations sur l'aspect de protection de la vie privée qui reste une compétence fédérale.

Enfin, Mme Gilson souligne l'importance d'avoir une interopérabilité des applications entre les Régions au niveau belge mais aussi entre les États de l'Union européenne. L'oratrice rappelle un des acquis essentiels de l'Europe qu'est la liberté de circulation. Il faut pouvoir la retrouver au plus vite. L'interopérabilité est essentielle dans cette perspective.

M. Sammy Mahdi (CD&V) demande des éclaircissements à propos de la manière dont le ministre De Backer entend traiter cette problématique: dans un arrêté de pouvoirs spéciaux ou sous la forme d'un projet de loi? Il espère que le Parlement pourra jouer son rôle dans cette problématique importante.

M. Nabil Boukili (PVDA-PTB) demande que le ministre s'engage expressément à mettre en place un cadre juridique sur ce sujet via un projet de loi.

La représentante du ministre répond que la composition du groupe de travail sera publiée en toute transparence sur le site web. En ces temps de pandémie, les décisions doivent pouvoir être prises rapidement et il faut pouvoir faire appel, à cette fin, à l'expertise nécessaire. C'est la raison pour laquelle l'Autorité de protection des données fait partie de ce groupe de travail.

Le gouvernement fédéral n'est pas compétent à l'égard du centre d'appels. Elle précise que celui-ci est déjà utilisé pour le dépistage de la tuberculose et d'autres maladies. Le cadre légal nécessaire est donc déjà disponible.

Renvoyant à la question posée à ce sujet par M. D'Haese, elle répond que le ministre De Backer est effectivement le garant des droits et des libertés, surtout en matière de respect de la vie privée, souvent au grand dam de certains.

kan een verwijdering na drie weken; waarom de gegevens dan langer bewaren?

Voorts is er nood aan een impactanalyse en moet de GBA worden geraadpleegd. Daarenboven moet diezelfde GBA kunnen toezien op de *tracing* gedurende het hele proces, teneinde de transparantie te waarborgen.

Alle gegevens die manueel dan wel via de *tracing-app* worden verzameld, moeten op een zelfde manier worden verwerkt. Hoewel manuele *tracing* een gewestbevoegdheid is, zou meer informatie moeten worden ingewonnen omtrent het aspect "privacybescherming", waarvoor de Federale Staat nog steeds bevoegd is.

Tot slot wijst mevrouw Gilson op het belang van de interoperabiliteit van de apps, zowel die waarvoor de gewesten in België kiezen als die van de lidstaten op EU-niveau. De spreekster herinnert aan een van de grote verworvenheden van Europa: de vrijheid van verkeer. Die moet zo snel mogelijk worden herwonnen. In dat opzicht is interoperabiliteit van essentieel belang.

De heer Sammy Mahdi (CD&V) had graag verduidelijking bekomen over de manier waarop minister De Backer dit vraagstuk wil aanpakken: zal dat gebeuren met een volmachtenbesluit dan wel met een wetsontwerp? De spreker hoopt dat het Parlement in deze belangrijke aangelegenheid zijn rol kan spelen.

De heer Nabil Boukili (PVDA-PTB) vraagt dat de minister er zich uitdrukkelijk toe verbindt ter zake het raamwerk te creëren via een wetsontwerp.

De vertegenwoordigster van de minister antwoordt dat de samenstelling van de taskforce op een transparante manier op de website zal worden bekendgemaakt. In deze tijden van pandemie moeten op een snelle manier beslissingen kunnen worden genomen en dient hierbij beroep te kunnen worden gedaan op de nodige expertise, vandaar dat de Gegevensbeschermingsautoriteit deel uitmaakt van deze taskforce.

De federale regering is niet bevoegd voor het *call center*. Zij verduidelijkt dat dit *call center* al wordt gebruikt voor het opsporen van tuberculose en andere ziekten. Het nodige wettelijke kader is dus reeds voorhanden.

Verwijzend naar de vraag ter zake van de heer D'Haese antwoordt zij dat minister De Backer weldegelijk de bewaker is van de rechten en vrijheden en zeker wanneer het om privacy gaat, vaak tot ergernis van sommigen.

Le premier projet de texte du ministre sur cette problématique se fondait sur la loi de pouvoirs spéciaux, sans pour autant préjuger de sa forme finale. Ce texte allait évidemment être examiné au sein du gouvernement avant d'être présenté au Parlement. Le ministre souhaitait que l'Autorité de protection des données lui confirme le plus rapidement possible que le premier projet de texte respectait les garanties requises en matière de protection de la vie privée, ce qui explique le premier avis demandé. C'est toutefois la nécessité d'un cadre juridique avec les garanties nécessaires en matière de protection de la vie privée qui a incité le ministre à rédiger ce texte sous la forme d'un projet de loi. Ledit projet tiendra compte de l'avis précité, qui y sera par ailleurs annexé. Une fois que les procédures requises seront remplies, ledit projet de loi sera déposé au Parlement le plus rapidement possible.

M. Christoph D'Haese (N-VA) remercie la représentante du ministre pour ces précisions et souligne l'importance du débat, ce qui explique les questions ciblées et parfois ardues qui ont été posées.

Le fait que les noms des membres de la *task force* ne soient pas encore connus n'inspire pas beaucoup de confiance en matière de préservation des droits et des libertés. Une mission aussi importante, qui touche à des droits fondamentaux, ne peut pas être réglée dans le plus grand secret par les responsables politiques. Voilà pourquoi M. D'Haese souligne l'importance de la transparence. Ce dossier constitue le talon d'Achille libéral de notre démocratie, qui est à l'heure actuelle fortement sous pression.

M. Khalil Aouasti (PS) a le sentiment que le ministre fait acte de repentance. C'est une bonne chose. Cependant, le 9 avril dernier, l'intervenant a demandé au ministre les noms des membres de cette *task force*, sans obtenir de réponse. Le 23 avril, il a à nouveau interpellé le ministre sur ses intentions. Le ministre a répondu que les Régions allaient se charger du *tracing,* mais que le fédéral établirait un cadre légal si on devait faire usage d'une application. C'est le 23 avril que le ministre a adressé son projet d'arrêté royal, soit le même jour. Pourquoi n'a-t-il pas mentionné ceci dans sa réponse aux parlementaires? Ses intentions étaient pourtant claires. Où est la transparence dans les faits? L'intervenant regrette ce mensonge de la part du ministre De Backer.

La transparence est absolument indispensable dans ce dossier. Si on veut une adhésion de la population, en vue de sauver des vies *in fine*, il faut cette transparence. Il n'est pas tolérable que les parlementaires découvrent des éléments au compte-goutte en posant des questions.

Het eerste tekstontwerp van de minister over deze problematiek ging uit van de volmachtenwet, zonder voorafname over welke vorm de tekst uiteindelijk ging aannemen. Vanzelfsprekend ging deze tekst worden besproken binnen de regering om dan aan het Parlement te worden voorgelegd. De minister wenste zo snel mogelijk van de Gegevensbeschermingsautoriteit duidelijkheid te bekomen of het eerste tekstontwerp voldeed aan de vereiste privacywaarborgen, vandaar het eerste gevraagde advies. Het is evenwel de nood aan een wettelijk kader met de noodzakelijke privacywaarborgen dat de minister ertoe heeft aangezet om dit te gieten in een wetsontwerp. Het wetsontwerp zal met dit advies, dat eveneens bij het wetsontwerp zal worden gevoegd, rekening houden. Na de afhandeling van de vereiste procedures zal het zo snel mogelijk in het Parlement worden ingediend.

De heer Christoph D'Haese (N-VA) bedankt de vertegenwoordigster van de minister voor de verduidelijking en benadrukt de belangrijkheid van het debat, vanwaar de gerichte en soms scherpe vragen.

Het feit dat de leden van de taskforce nog niet gekend zijn, geeft niet veel vertrouwen in de bewaking van de rechten en vrijheden. Een dergelijke belangrijke taak die grondrechten betreft, wordt niet geregeld in een politiek achterkamertje. De heer D'Haese benadrukt het belang van transparantie. Dit dossier is de liberale achillespees van de democratie die op dit ogenblik zwaar onder druk staat.

De heer Khalil Aouasti (PS) heeft het gevoel dat de minister tot inkeer komt. Dat is goed. Op 9 april had de spreker de minister echter gevraagd wie de leden van die taskforce waren, zonder daarop antwoord te krijgen. Op 23 april vroeg hij de minister opnieuw opheldering over zijn bedoelingen. De minister antwoordde dat de gewesten zouden instaan voor de *tracing,* doch dat federaal een wettelijk kader zou worden geregeld indien van een app gebruik zou worden gemaakt. Maar op 23 april, diezelfde dag dus, bezorgde de minister zijn ontwerp van koninklijk besluit. Waarom heeft hij dat niet vermeld in zijn antwoord aan de parlementsleden? Zijn bedoelingen waren nochtans duidelijk. *Quid* met de transparantie? De spreker betreurt de misleidende aanpak van minister De Backer.

In dit dossier is transparantie onontbeerlijk. Indien men wil kunnen bogen op steun van de bevolking, *in fine* om levens te redden, dan moet die transparantie er zijn. Het is ontoelaatbaar dat de parlementsleden slechts door vragen te stellen met mondjesmaat elementen te weten komen.

M. Gilles Vandenburre (Ecolo-Groen) partage entièrement ce besoin de transparence dans ce dossier. Par ailleurs, il est interpellé par la confusion des genres. Le président de l'APD, ainsi qu'un autre membre, sont membres de la *task force.* Cette dernière fait des propositions, qui sont validées par des avis de l'APD. Il y a un problème de mélange de genres. Il faut clarifier ces aspects-là des choses qui sont très interpellantes.

Enfin, la représentante du ministre confirme-t-elle que dans le projet de loi en préparation, il n'y a pas de référence ou de balise par rapport au *tracing* manuel?

M. John Crombez (sp.a) constate que la plupart des membres estiment que si le développement d'une telle application est nécessaire pour protéger la population, il convient de créer un cadre à cet effet. Mais il souligne ensuite qu'il est fondamental de faire preuve de transparence et de clarté puisque des droits fondamentaux sont en jeu. C'est pourquoi l'intervenant répète que la commission de la Justice est la commission indiquée pour examiner cette problématique et que l'Autorité de protection des données devrait devenir une instance de régulation disposant d'un accès total et inconditionnel aux informations et aux systèmes utilisés. Le ministre indique qu'il importe de faire preuve de rapidité en la matière, mais nous sommes entre-temps le 29 avril.

M. Nabil Boukili (PVDA-PTB) se sent berné par le ministre. Le ministre dit que l'application n'est pas nécessaire, alors qu'il prépare en même temps un texte qui est envoyé à l'APD pour avis. Comment lui faire confiance dans ces conditions?

Il faut une proposition de loi discutée de manière approfondie et qui fasse l'objet d'un vrai débat parlementaire, et pas un arrêté royal. Le ministre doit faire preuve de transparence et de clarté.

Quid de l'application? Sera-t-elle abandonnée ou pas finalement? Il ne faut plus de contradiction entre ce qu'il se dit et ce qu'il se fait.

Par ailleurs, qui va composer la *task force*? Il faut le savoir. *Quid* des représentants de la Ligue des Droits Humains, ou encore de Google et d'Apple, dont les intérêts sont autres que la protection des droits de l'homme? Il faut que le parlement obtienne ces informations.

M. Sammy Mahdi (CD&V) fait observer que le Parlement se montre critique parce qu'il reste sur sa faim. En effet, on nous annonce en mars le développement d'une application, pour devoir constater en avril que le flou règne toujours à ce sujet. L'intervenant se réjouit

De heer Gilles Vanden Burre (Ecolo-Groen) treedt die nood aan transparantie volledig bij. Voorts verbaast het hem hoe zaken door elkaar worden gehaald. De voorzitter van de GBA, evenals een ander lid, zijn leden van de taskforce*.* Die taskforce doet voorstellen, die vervolgens via adviezen van de GBA worden gevalideerd. Die gang van zaken schept verwarring en wekt verbazing. Een en ander moet worden uitgeklaard.

Bevestigt de vertegenwoordigster van de minister tot slot dat het in uitzicht gestelde wetsontwerp geen verwijzingen naar of krijtlijnen inzake de manuele *tracing* omvat?

De heer John Crombez (sp.a) stelt vast dat de meesten van oordeel zijn dat als er een app nodig is om de bevolking te beschermen hiervoor een kader moet worden gecreëerd. Maar daarnaast benadrukt hij dat aangezien het hier gaat over grondrechten, transparantie en duidelijkheid van fundamenteel belang zijn. De spreker herhaalt daarom dat de commissie voor Justitie de aangewezen commissie is om deze problematiek te bespreken en dat de Gegevensbeschermingsautoriteit de regulator dient te worden met volledige en onvoorwaardelijke toegang tot de informatie en de gebruikte systemen. Er wordt gesteld dat snelheid in deze belangrijk is, maar inmiddels is het 29 april.

De heer Nabil Boukili (PVDA-PTB) voelt zich door de minister voor de gek gehouden. De minister zegt dat de app niet nodig is, terwijl hij tegelijkertijd een tekst voorbereidt die ter advies aan de GBA wordt voorgelegd. Hoe kan men hem in die omstandigheden vertrouwen?

Er is geen koninklijk besluit maar een wetsvoorstel nodig, dat grondig wordt besproken en waarover een echt parlementair debat plaatsvindt. De minister moet transparant en duidelijk zijn.

Quid met de app? Komt die er nu wel of niet? De tweespalt tussen woord en daad moet stoppen.

Wie zal voorts de taskforce samenstellen? Dat moet geweten zijn. *Quid* met de vertegenwoordigers van de *Ligue des Droits Humains*, of van Google en van Apple, die andere belangen hebben dan de mensenrechten te beschermen? Het Parlement moet over die informatie beschikken.

De heer Sammy Mahdi (CD&V) merkt op dat het Parlement kritisch is omdat het hongerig is geworden. Immers, in maart wordt meegedeeld dat er een app komt, om dan in april te moeten vaststellen dat onzekerheid nog steeds troef is. De aankondiging van de indiening

dès lors de l'annonce du dépôt d'un projet de loi. Il est impatient d'en connaître le contenu, mais regrette que le ministre n'ait pas communiqué plus tôt sur ses projets en la matière. S'agissant de la *task force*, l'intervenant indique que si les données des citoyens enregistrées dans une application anti-coronavirus sont aussi bien protégées que les noms des membres de la *task force*, le Parlement n'a pas à s'inquiéter. Il regrette par conséquent le manque de communication à cet égard. Il importe que les citoyens ne doivent plus s'inquiéter du traitement réservé à leurs données personnelles.

Mme Nathalie Gilson (MR) remercie la représentante du ministre et se réjouit que le ministre ait déjà avancé sur le sujet. Elle attend les communications sur le sujet pour que le parlement puisse aussi avancer dans le débat sur cette question.

La représentante du ministre répond que le ministre De Backer a déjà signalé que la *taskforce* comprend des représentants du cabinet de la Santé publique, du cabinet de l'Agenda numérique, de telecomprivacy, de la plateforme eHealth, de Sciensano, du SPF Santé publique et l'Autorité de protection des données. En outre, un comité d'éthique composé du professeur Nuria Oliver, *data scientist*, du professeur Herman Goosens, épidémiologiste, et de maître Jean-Marc van Gysegem, avocat spécialisé en droit médical, et du professeur Jean-Noël Missa, bioéthicien, a été mis en place pour soutenir le *telecomworkstream*.

Concernant l'observation relative à rapidité avec laquelle le ministre souhaite agir, la représentante précise que le ministre a démarré l'élaboration d'un cadre concernant la protection de la vie privée, lorsqu'il était question de la mise en place d'une application. Elle souligne que cela ne relève pas de la compétence du ministre De Backer de décider de travailler ou pas avec une application d'identification des contacts. Mais si cette décision devait être prise, une base légale qui prévoit un cadre relatif à la protection de la vie privée aura tout de même été élaborée au niveau fédéral pour l'application d'identification des contacts.

En ce qui concerne la question portant sur le contenu de l'arrêté royal, elle répond que celui-ci correspond bien au texte de la résolution.

M. Khalil Aouasti (PS) précise que c'est l'identité des personnes qui composent la *task force* qui est demandée. Le fait de communiquer cette information semble poser problème au ministre.

van een wetsontwerp stemt hem dan ook tevreden. Hij is dan ook benieuwd naar de inhoud ervan maar betreurt dat de minister niet eerder heeft meegedeeld waarmee hij op dit vlak bezig is. Wat de taskforce betreft, stipt de spreker aan dat als de gegevens van de burgers bij een corona-app op dezelfde manier worden beschermd als de samenstelling van de taskforce, het Parlement zich geen zorgen hoeft te maken. Hij betreurt dan ook de gebrekkige communicatie hieromtrent. Het is belangrijk dat de burgers zich geen zorgen meer moeten maken over hun eigen persoonsgegevens.

Mevrouw Nathalie Gilson (MR) bedankt de vertegenwoordigster van de minister en vindt het positief dat de minister op dit stuk vooruitgang heeft geboekt. Ze kijkt uit naar de toekomstige mededelingen, zodat het parlement het debat daaromtrent voort kan voeren.

De vertegenwoordigster van de minister antwoordt dat minister De Backer reeds heeft meegedeeld dat de taskforce bestaat uit vertegenwoordigers van het kabinet Volksgezondheid, het kabinet Digitale Agenda, telecomprivacy, EHealth-platform, Sciensano, de FOD Volksgezondheid en de Gegevensbeschermingsautoriteit. Daarnaast werd er ook voor de steun aan de *telecomworkstream* een ethisch comité opgericht bestaande uit professor Nuria Oliver, *data scientist*, professor Herman Goosens, epidemioloog, meester Jean-Marc van Gysegem, advocaat in medisch recht, en professor Jean-Noël Missa, bioethicist.

In verband met de opmerking over de snelheid waarmee de minister wenst te handelen, verduidelijkt de vertegenwoordigster dat de minister gestart is met de opmaak van een privacykader, wanneer sprake was van de invoering van een app. Ze benadrukt dat het niet de bevoegdheid is van minister De Backer om te beslissen over het wel of niet te werken met een contactopsporingsapp. Maar mocht die beslissing er komen dan is er toch al op federaal niveau werk gemaakt van een wettelijke basis die een privacykader voorziet voor de contactopsporingsapp.

Wat de vraag over de inhoud van het koninklijk besluit betreft, antwoordt zij dat dit KB de tekst van de resolutie goed volgt.

De heer Khalil Aouasti (PS) wijst erop dat wordt gevraagd naar de identiteit van de mensen die de taskforce vormen. Die informatie communiceren blijkt voor de minister een heus probleem.

Mme Jessika Soors (Ecolo-Groen) propose de poursuivre le débat au sein de la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique, en présence du ministre compétent.

M. Christoph D'Haese (N-VA) souhaite connaître les noms des membres de la *taskf orce*, savoir par qui et quand ils ont été nommés, s'ils sont rémunérés et sur quelle base légale ils ont été désignés?

Mme Kristien Van Vaerenbergh, présidente de la commission de la Justice, constate pour conclure cette discussion que les représentants des groupes qui ont pris la parole se sont exprimés en général favorablement au sujet de la proposition de résolution à l'examen, étant entendu que quelques réserves et propositions ont été émises. Les points de vue respectifs tels qu'ils figurent dans le présent rapport sont transmis à la commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique afin d'y étoffer le débat.

Les rapporteurs, *La présidente,*

Christoph D'HAESE Kristien VAN VAERENBERGH

Mevrouw Jessika Soors (Ecolo-Groen) stelt voor om het debat verder te voeren in de commissie voor Economie, Consumentenbescherming en Digitale Agenda, in aanwezigheid van de persoon van de bevoegde minister.

De heer Christoph D'Haese (N-VA) wenst de namen van de leden van de taskforce te kennen, te vernemen wie en wanneer ze werden aangesteld of ze worden vergoed en op welke wettelijke basis ze werden aangewezen?

Mevrouw Kristien Van Vaerenbergh, voorzitter van de commissie voor Justitie, stelt tot besluit van deze bespreking vast dat de vertegenwoordigers van de fracties die het woord hebben genomen zich over het algemeen positief hebben uitgelaten over het ter bespreking voorliggende voorstel van resolutie, met dien verstande dat ook enkele bedenkingen en voorstellen werden geformuleerd. De respectieve standpunten zoals opgenomen in dit verslag worden aan de commissie voor Economie, Consumentenbescherming en Digitale Agenda overgezonden teneinde aldaar het debat te stofferen.

De rapporteur, *De voorzitter,*

Christoph D'HAESE Kristien VAN VAERENBERGH

Imprimerie centrale – Centrale drukkerij