Advies nr. 43/2020 van 26 mei 2020

Betreft: Adviesaanvraag betreffende een wetsvoorstel betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking (CO-A-2020-049)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikel 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016*/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening* gegevensbescherming) (hierna AVG)

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van de heer Patrick Dewael, Voorzitter van de Kamer van Volksvertegenwoordigers ontvangen op 15 mei 2020;

Gelet op het verslag van Alexandra Jaspar, directeur van het Kenniscentrum van de Gegevensbeschermingsautoriteit ;

Brengt op 26 mei 2020 het volgend advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Voorziter van de Kamer van Volksvertegenwoordigers heeft aan de Autoriteit gevraagd advies te verstrekken over een wetsvoorstel betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking (hierna "het wetsvoorstel").

2. Dit wetsvoorstel volgt op een ontwerp van koninklijk besluit met hetzelfde onderwerp, waarover de Autoriteit zich in haar advies 34/2020 van 28 april jongstleden heeft uitgesproken en waarnaar de Autoriteit verwijst voor aspecten die in dit advies niet aan de orde komen.

3. In de Toelichting wordt het volgende verduidelijkt «*digitale contactopsporingsapplicaties laten de burgers toe zelf vast te stellen dat ze recent in contact zijn geweest met een besmet persoon, zonder dat ze weten wie de besmette persoon is en zonder dat de plaatsen waar personen geweest zijn, worden bijgehouden, noch in de contactopsporingsapplicatie, noch in een centrale gegevensbank*».

4. Het wetsvoorstel heeft in de eerste plaats tot doel de voorwaarden vast te stellen waaraan contactopsporingsapplicaties voor het beheer van een pandemie op Belgisch grondgebied[1] moeten voldoen om de gegevensverwerking die ze genereren tot een minimum te beperken en om ervoor te zorgen dat de essentiële waarborgen tegen het risico van heridentificatie van de gebruikers van deze applicaties en het behoud van hun rechten en vrijheden aanwezig zijn.

5. Volgens het wetsvoorstel zal Sciensano de beveiligde sleutels van de besmette gebruikers van de applicatie in een logbestand registreren en dit bestand ter beschikking stellen van andere gebruikers van deze applicaties (op basis van deze sleutels zullen andere gebruikers met behulp van hun applicatie de aanwezigheid van een mogelijk gekoppeld tijdelijk serienummer kunnen afleiden, wat vervolgens een waarschuwing zal genereren dat ze een risicovol contact met een besmette persoon hebben gehad). Volgens de Toelichting maakt de gebruikte techniek (DP3T) het dus mogelijk om de uitwisseling van informatie te garanderen dat de gebruikers een risicovol contact hebben gehad zonder dat de gebruikers door de beheerder van de applicatieserver of door andere gebruikers worden geïdentificeerd.

6. De Autoriteit benadrukt dat haar advies uiterst dringend is uitgebracht en zich daarom beperkt tot de essentiële punten.

[1] De titel van het wetsvoorstel moet dienovereenkomstig worden aangepast.

7. Zij is positief over bepaalde verbeteringen die in de tekst zijn aangebracht ten opzichte van het ontwerp van koninklijk besluit dat haar werd voorgelegd: motivering van de proportionaliteit van de gegevensverwerking door middel van de applicaties, motivering voor de bewaartermijn van drie weken, toevoeging dat een niet-gebruiker niet mag worden benadeeld, verplichting voor Sciensano om kruiscontroles van gegevens te voorkomen (over de formulering van deze verplichting, zie hieronder alsook de bijbehorende voetnoot), gebruik van geanonimiseerde gegevens voor epidemiologisch onderzoek, gebruik van het DP3T-systeem op basis van Bluetooth-technologie en cryptografie.

8. De Autoriteit herinnert eraan dat de gegevensbeschermingsautoriteiten van de lidstaten van de Europese Unie via het Europees Comité voor gegevensbescherming (hierna "de ECG" genoemd) gezamenlijk richtsnoeren[i] hebben opgesteld voor het traceren van toepassingen. De Autoriteit benadrukt de noodzaak om er op toe te zien dat deze worden nageleefd.

II. ONDERZOEK

a. Inleiding

9. Het eerste doel van het wetsvoorstel is het bepalen van de voorwaarden waaraan contactopsporingsapplicaties die in het kader van het pandemiebeheer op Belgisch grondgebied worden gebruikt, moeten voldoen en Sciensano te belasten met het beheer van dit opsporingssysteem Voor de duidelijkheid moet de titel van het wetsvoorstel in deze zin worden geherformuleerd.

b. Voorafgaande opmerking over de noodzaak van het gebruik van opsporingsapplicaties en de gegevensverwerking waartoe deze aanleiding geven

10. Aangezien het gekozen protocol een aanzienlijke inbreuk vormt op de privacy van de bevolking, dat, hoewel het goed is toch risico's met zich meebrengt, en gezien het risico van gewenning dat het wijdverbreide gebruik van traceringstechnologieën met zich meebrengt, kan de keuze om het gebruik van dergelijke toepassingen aan de bevolking aan te bieden alleen worden gemaakt als dit niet alleen proportioneel, maar ook noodzakelijk is.

11. Hoewel het proportionele karakter van traceringstoepassingen bij wet kan en moet worden geregeld, zodat de burgers het nodige vertrouwen kunnen krijgen in de werking[2] ervan, hangt de noodzaak af van externe factoren die aanwezig en gerechtvaardigd moeten zijn wanneer ze door de bevoegde autoriteit(en) ter beschikking worden gesteld (dit vereist dat vooraf bepaalde vragen worden gesteld,

[2] De effectiviteit van het gebruik van deze opsporingsapplicaties hangt af van het aantal mensen dat ze installeert en activeert.

in dit verband, en wel deze: Zullen mensen die een risicocontact hebben gehad, getest kunnen worden of zullen ze in quarantaine worden gezet? Ondermijnt het aantal asymptomatische maar besmette mensen niet de effectiviteit van dit soort applicaties? En zie voor de rest punt A van bovengenoemd advies 34/2020). Op basis van de antwoorden op deze vragen zal de bevoegde overheid moeten kunnen certificeren dat haar keuze noodzakelijk en relevant is voor het beheer van de lockdownbeëindiging van de bevolking. Deze keuze moet voldoende worden gedocumenteerd voordat de applicaties voor het publiek beschikbaar worden gesteld en met passende regelmatige tussenpozen. Deze analyse moet worden geïntegreerd in de effectbeoordeling voorafgaand aan de gegevensverwerking, die overeenkomstig artikel 35 van de AVG moet worden uitgevoerd, vooraleer de applicatie(s) en het bijbehorende apparaat worden vrijgegeven.

12. Alleen de overheidsinstellingen die van de wetgever een opdracht van algemeen belang hebben gekregen, kunnen een dergelijk systeem opzetten (artikel 6.1. e) van de AVG). Deze geregelde gegevensverwerkingen hebben betrekking op bijzondere categorieën gegevens in de zin van artikel 9.1 van de AVG (d.w.z. gegevens betreffende de gezondheid). Bijgevolg moet het vereiste kwaliteitsniveau van de wet die deze applicaties en het bijhorende apparaat omkadert, hoog zijn en moet deze wetgeving waarborgen bieden voor de betrokken personen, gezien het grote risico van inbreuk op hun rechten en vrijheden. In artikel 9.2. i) van de AVG is inderdaad bepaald dat een dergelijke verwerking kan worden uitgevoerd indien dit noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, maar alleen als deze verwerking onderworpen is aan een wettelijke (of regelgevende) norm die voorziet in passende en specifieke maatregelen om de rechten en vrijheden van de betrokkenen te waarborgen.

c. <u>Garanties in verband met de onmogelijkheid om opnieuw te worden geïdentificeerd - Verwerkingsverantwoordelijke - controle op de naleving van de voorwaarden - verplichte voorlegging aan de Autoriteit van de voorafgaande gegevensbeschermingseffectbeoordeling, publicatie van deze beoordeling en het advies van de Autoriteit</u>

13. Het DP3T-protocol biedt een reeks garanties, waaronder het minimaliseren van de verzamelde gegevens (alleen de sleutels van besmette personen worden gedeeld, geen directe uitwisseling van de sociale grafiek), het genereren van sleutels op de telefoon van de gebruiker, evenals bescherming tegen de risico's van kruisingen van gegevens en heridentificatie van de betrokkenen. Hoewel het protocol goed is, sluit het niet alle risico's uit, zoals het risico dat een persoon kan bepalen wie hem of haar heeft besmet of de locatie van de besmette personen. Over deze aspecten wordt verwezen naar het artikel van Serge Vaudenay, professor en directeur van het Security and Cryptography Laboratory (LASEC) aan de Ecole polytechnique fédérale de Lausanne (EPFL) waarin de verschillende mogelijke

aanvallen worden belicht en hoe deze het best kunnen worden aangepakt3. Het is van essentieel belang dat enerzijds het voortbestaan van de risico's in het wetsvoorstel wordt weerspiegeld, zodat met name het Parlement en de betrokken personen niet van deze informatie worden beroofd, en anderzijds (2) de proportionaliteitsanalyse met volledige kennis van zaken kan worden uitgevoerd. Het wetsvoorstel zwijgt echter over de inhoud van dit protocol, over de garanties die het biedt, over de resterende risico's en over de risicobeperkingsstrategieën die op het niveau van de applicatie moeten worden geïmplementeerd.

14. De beschrijving van de werking van de applicaties (in de toelichting, niet in het dispositief van het wetsvoorstel, dat de Autoriteit de aanvrager verzoekt te corrigeren) en van de specificaties waaraan de applicaties moeten voldoen (artikel 4 § 2 van het wetsvoorstel), garandeert niet dat op het niveau van de te kiezen opsporingsapplicatie(s) voldoende beperkingsstrategieën worden opgelegd.

15. in de omschrijving van het protocol ontbreekt het nummer van de versie of het "type" van het protocol dat wordt voorgesteld. Verschillende ontwerpen zijn voorgesteld door het DP3T-consortium.

16. Belangrijke verversingsfrequenties en tijdelijke serienummers zijn essentieel voor de anonimiteit van het systeem en om het risico van tracering te vermijden. Het wetsvoorstel bevat geen informatie over hoe vaak de sleutels en identificatoren "random" (eigenlijk tijdelijk) moeten worden ververst.

17. Een lezing van deze bepaling lijkt er zelfs op te wijzen dat de specificaties die voor de applicaties zijn voorzien, risico's van heridentificatie in principe weer invoeren, die door het DP3T-protocol zijn vernietigd. Uit de lezing van het wetsvoorstel blijkt inderdaad dat de verificatie van de positieve status van een persoon wordt gedaan door de vermelding in de applicatie van zijn of haar telefoonnummer en de datum van de test. De applicatie stuurt vervolgensde sleutel(s) van de persoon naar de server waardoor het mogelijk wordt om deze gedurende enkele weken te traceren. Om aanspraak te kunnen maken op de invoering van een systeem dat werkt met anonieme gegevens en waarbij elke mogelijkheid tot heridentificatie wordt uitgesloten:

    a. moet de aan de gebruiker verstrekte autorisatiecode die hem machtigt om zijn sleutel(s) naar de databank te sturen, worden verstrekt door een andere operator dan de operator die belast is met het beheer van de sleuteldatabank. Zodra de sleutels zijn geverifieerd, moeten de gegevens die een autorisatiecode aan het telefoonnummer en de datum van de test koppelen, worden gewist;

---

[3] Serge Vaudenay, Analysis of DP3T – Between Scylla and Charybdis, 8 avril 2020, EPFL, Lausanne, online bschikbaar op dit adres https://eprint.iacr.org/2020/399.pdf

b. moet het systeem werken met meerdere (en niet één) sleutels, zonder de mogelijkheid om te weten, ook voor Sciensano, dat ze gekoppeld zijn aan dezelfde persoon, ze moeten vaak worden ververst en het moet mogelijk zijn voor de gebruiker om te controleren of de sleutel is veranderd (of zelfs idealiter om achteraf elke generatie van sleutels te verwijderen gedurende een bepaalde periode).

Het systeem lijkt echter informatie te genereren dat een besmette persoon (niet rechtstreeks geïdentificeerd) langdurig contact heeft gehad met een andere besmette persoon (ook niet rechtstreeks geïdentificeerd) en/of met tussenpozen X, wat over het algemeen niet denkbaar is in het geval van een anoniem systeem waarbij de sleutels van dezelfde persoon niet onder elkaar gekoppeld zijn.

De beschrijving van het systeem garandeert niet dat Sciensano de betrokkenen niet telefonisch zal contacteren (wat zou betekenen dat hun telefoonnummer zou worden bewaard en dat het systeem in feite niet op anonieme basis zou werken).

18. Met het oog op zowel de rechtszekerheid als de leesbaarheid van het wetsvoorstel is de Autoriteit van mening dat het begrip "opsporingsapplicatie" in artikel 3 moet worden gedefinieerd. In deze definitie wordt gespecificeerd dat deze applicaties waarborgen bieden tegen het risico van heridentificatie van hun gebruikers, zoals uiteengezet in de toelichting[4] (applicatie op basis van het DP3T-cryptografiesysteem waarmee de gebruiker kan worden geïnformeerd dat hij een risicovol contact heeft gehad met een besmette persoon zonder te weten wie de besmette persoon is en zonder dat de locaties van deze personen worden verzameld in de applicatie voor het traceren van contacten of in een centrale gegevensbank). Bovendien zal deze definitie op nuttige wijze duidelijk maken dat een opsporingsapplicatie in geen geval de realtime overdracht van informatie van een risicocontact naar een besmette persoon mogelijk maakt.

19. In artikel 6 van het wetsvoorstel wordt Sciensano aangewezen als verwerkingsverantwoordelijke.

20. De Autoriteit dedecteert een aanzienlijk risico in verband met het feit dat, naast hetgeen in punt 15 hierboven is vermeld en ondanks het feit dat het wetsvoorstel Sciensano verplicht om maatregelen te nemen zodat de gegevens die door deze instantie overeenkomstig het wetsvoorstel worden verzameld, niet worden gekruist met andere gegevens uit andere databanken[5]; via een ander normatief ontwerp

[4] In de toelichting wordt het volgende verduidelijkt "*digitale contactopsporingsapplicaties laten de burgers toe zelf vast te stellen dat ze recent in contact zijn geweest met een besmet persoon, zonder dat ze weten wie de besmette persoon is en zonder dat de plaatsen waar personen geweest zijn, worden bijgehouden, noch in de contactopsporingsapplicatie, noch in een centrale gegevensbank*».

[5] De formulering van artikel 11 § 2 laat overigens te wensen over aangezien wordt gepreciseerd "*de informatie bewaard in de loglijst en databank bedoeld in art. 8, §§ 1 en 2 in geen geval met elkaar in verbinding worden gebracht*". Welnu, de loglijst is beschreven in artikel 8 § 1 en het is de onderzoeksdatabank van Sciensano die in artikel 8 § 2 van het wetsvoorstel wordt bedoeld. In plaats daarvan moet worden verduidelijkt dat elke koppeling van gegevens die via de opsporingsapplicaties worden

dat in goedkeuringsfase[6] zit (zie het gerelateerde advies van de Autoriteit gepubliceerd op 25 mei 2020), aan deze instantie al het beheer is toegewezen van een grote databank van personen die besmet zijn met het coronavirus COVID 19. De Autoriteit herinnert eraan dat een van de essentiële onderdelen van opsporingsapplicaties, niet alleen wat betreft de bescherming van de privacy, maar ook wat betreft het vertrouwen dat zij bij de bevolking moet wekken, erin bestaat te zorgen voor de uitwisseling van informatie tussen besmette personen en hun risicocontacten en hen tegelijkertijd te beschermen tegen het risico dat zij opnieuw worden geïdentificeerd.

21. Bovendien moet worden gespecificeerd in verband met welke gegevensverwerkingen deze aanwijzing plaatsvindt. Anders biedt deze aanwijzing niet de vereiste voorspelbaarheid en duidelijkheid. Naar wat de Autoriteit heeft kunnen begrijpen, gaat het de verwerkingsverantwoordelijke aan te wijzen die zal op teren voor de applicaties(s) die de wettelijk vereiste kenmerken hebben en die de aan het gebruik ervan gekoppelde server zal beheren (logbestand opslaan en aan alle gebruikers de beveiligde sleutels van besmette gebruikers ter beschikking stellen met het oog op het genereren van de waarschuwing voor het bestaan van een risicocontact met de betrokken gebruikers). De auteur van het wetsvoorstel moet de aanwijzing van de verwerkingsverantwoordelijke vervolledigen door aan te geven in verband met welke verwerking van persoonsgegevens deze aanwijzing plaatsvindt. Bovendien, als het, zoals de Autoriteit kan begrijpen, Sciensano is die zal beslissen welke opsporingsapplicaties worden gebruikt en ter beschikking gesteld van het publiek in België, moet dit ook duidelijk worden gemaakt.

22. De Autoriteit herinnert er ook aan dat het gebruik van één enkele applicatie het risico zou verminderen dat de applicaties niet aan de technische en wettelijke vereisten voldoen en aanzienlijke risico's voor de vertrouwelijkheid van de gegevens van de burgers met zich meebrengen. Daarom beveelt de Autoriteit aan een artikel aan het wetsvoorstel toe te voegen om te specificeren dat Sciensano de verantwoordelijkheid op zich neemt om te controleren en ervoor te zorgen dat de aan het publiek aangeboden applicaties voldoen aan alle vereiste wettelijke specificaties, alsmede aan die van de ECG. Een aanvullende garantie voor de betrokken personen, die passend lijkt te zijn, is dat in het wetsvoorstel wordt bepaald dat Sciensano, voordat een opsporingsapplicatie aan het publiek ter beschikking wordt gesteld, haar DPIA met betrekking tot die applicatie aan de Autoriteit moet voorleggen voor een voorafgaand advies, met de verplichting om de DPIA en het advies van de Autoriteit over deze DPIA te publiceren.

23. Zoals de ECG verlangt, moet ook de volledige broncode van elke applicatie worden gepubliceerd en de Autoriteit dringt erop aan dat deze publicatie lang genoeg vóór de datum waarop de applicatie ter

verzameld met andere persoonsgegevens verboden is, evenals elke poging om gebruikers van een opsporingsapplicatie opnieuw te identificeren.

[6] Wetsvoorstel tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19, Kamer van Volksvertegenwoordigers, doc. 55, 1249/1.

beschikking wordt gesteld, plaatsvindt om de analyse ervan door specialisten mogelijk te maken. Ze beveelt aan dat al de" builds " verifieerbaar zijn.

d. Doelstellingen van de gegevensverwerking door middel van digitale contactopsporingsapplicaties en het beginsel van de minimale gegevensverwerking.

24. In artikel 4 van het wetsvoorstel wordt getracht de doeleinden van de verwerking van persoonsgegevens te bepalen die met behulp van opsporingsapplicaties zullen worden uitgevoerd.

25. In de eerste plaats wordt ten onrechte gesteld dat de applicaties gegevensverwerkingen uitvoeren. Het is niet de applicatie die de gegevensverwerking uitvoert, maar een natuurlijke of rechtspersoon. Dit moet gecorrigeerd worden. Bovendien moet niet alleen worden gespecificeerd aan welke algemene functionaliteiten de opsporingsapplicaties moeten beantwoorden, maar moet ook duidelijk worden gespecificeerd welke gegevensverwerking door Sciensano wordt uitgevoerd om de werking van het opsporingssysteem te garanderen.

26. Voorts is de formulering van het eerste en het tweede doeleinde problematisch en moet worden verbeterd. Volgens ons begrip van het systeem moeten opsporingsapplicaties beschikbaar worden gesteld aan gebruikers om de uitwisseling van informatie mogelijk te maken dat zij een risicovol contact hebben gehad met een besmette gebruiker, zonder dat de gebruikers worden geïdentificeerd door de beheerder van de applicatieserver of door de gebruikers zelf. Het doorgeven van informatie dat een gebruiker besmet is, is daarom niet een eerste doeleinde van de applicatie, maar alleen een basisvoorwaarde.

27. Bovendien houdt het minimaliseringsbeginsel van de AVG in dat alleen gegevens mogen worden verwerkt die strikt noodzakelijk en relevant zijn voor het nagestreefde doel. Gelet op de definitie van risicocontacten die door de FOD Volksgezondheid en het Crisiscentrum is vastgesteld (contact van minder dan 1,5 meter met een besmette persoon gedurende meer dan 15 minuten), is de Autoriteit dan ook van oordeel dat alleen dergelijke contacten (in voorkomend geval met een aanvaardbare foutmarge van het type "contact van minder dan 4 meter afstand voor meer dan 10 minuten") moeten worden opgevangen (vooral omdat de Bluetooth-technologie het mogelijk maakt contacten tot 100 meter afstand op te vangen, wat duidelijk disproportioneel is voor het nagestreefde doel). De formulering van het doeleinde zal op deze basis moeten worden herzien en met het oog op de rechtszekerheid moet een definitie van het begrip "risicocontact" overeenkomstig de officiële aanbevelingen in artikel 3 van het wetsontwerp worden opgenomen.

28. Met betrekking tot het derde doeleinde, bedoeld in artikel 4 van het wetsvoorstel (epidemiologisch onderzoek) is de Autoriteit van mening dat deze doelstelling niet specifiek hoeft te worden gedefinieerd in het wetsvoorstel omdat naleving van de relevante bepalingen van de AVG en de WVG inzake onderzoek volstaat. Dit is des te meer het geval omdat artikel 10 van het wetsvoorstel voorziet in een verbod op de verdere verwerking van gegevens die zijn verzameld in het kader van het beheer van dit opsporingssysteem, met uitzondering van de verdere verwerking ten behoeve van wetenschappelijk en statistisch onderzoek overeenkomstig artikel 89 van het AVG en titel 4 van de kaderwet. Dit ondanks het feit dat de Autoriteit heeft begrepen dat de server, afgezien van het verzamelen van aanvullende gegevens voor onderzoeksdoeleinden die niet noodzakelijk zijn voor het traceren, geen aanvullende informatie verzamelt die niet reeds openbaar is[7].

29. Als het doel echter is om uitsluitend voor dit onderzoeksdoel aanvullende gegevens te verzamelen (wat blijkt uit de manier waarop een deel van het systeem is opgezet), ziet de Autoriteit een fundamenteel probleem in deze aanvullende verzameling en doelstelling, die het risico van heridentificatie en het opstellen van de sociale grafiek van individuen met zich meebrengt, terwijl het doel van de voorgestelde wet is om opsporingsapplicaties te moduleren om het risico van heridentificatie tot een minimum te beperken. Bovendien rechtvaardigt noch het wetsvoorstel, noch de toelichting de proportionaliteit van deze verzameling voor het beoogde doel.

30. De toevoeging van dit epidemiologische onderzoeksdoel is schadelijk voor het begrip van het project en kan leiden tot verwarring bij de burgers. De Autoriteit beveelt daarom aan de bepalingen van het wetsvoorstel met betrekking tot omkadering van het onderzoek te schrappen, vooral omdat sommige daarvan in strijd zijn met de garantie dat dergelijk onderzoek zal worden uitgevoerd met behulp van anonieme gegevens.

e. <u>Vereiste parameters voor de opsporingsapplicaties - beginsel van de minimale gegevensverwerking van de AVG</u>

31. Hoewel het wetsvoorstel terecht bepaalt dat de installatie en het gebruik van een opsporingsapplicatie vrijwillig zal zijn, is het belangrijk dat de parameters van dergelijke toepassingen in overeenstemming zijn met de AVG. Dit is het voorwerp van artikel 4 § 2, dat de vereiste functionaliteiten voor de opsporingsapplicaties vaststelt.

[7] Dit ondanks het feit dat de Autoriteit heeft begrepen dat de server, afgezien van het verzamelen van aanvullende gegevens voor onderzoeksdoeleinden die niet nodig zijn voor het traceren, geen aanvullende informatie verzamelt die niet reeds openbaar is.

32. In het algemeen is de Autoriteit van mening dat, om te zorgen voor een betere leesbaarheid en voorspelbaarheid en voor rechtszekerheid met betrekking tot deze technische functionaliteiten die nodig zijn om het risico op heridentificatie te voorkomen (onomkeerbaarheid van hashing, frequentie van verandering van niet-gepersonaliseerde tijdelijke serienummers), de hiernavolgende begrippen moeten worden gedefinieerd in artikel 3 van het wetsvoorstel:
    a. Beveiligde sleutel (in de definitie zal het nuttig zijn dat alleen cryptografische algoritmen die voldoen aan de huidige stand van de techniek kunnen worden gebruikt om de integriteit en vertrouwelijkheid van de uitwisselingen te waarborgen) ;
    b. Gebruiker van een digitale opsporingsapplicatie;
    c. Tijdelijk niet-gepersonaliseerd (en niet "random") serienummer.

33. Met betrekking tot artikel 4 § 2, zesde streepje, waarin de grenzen worden vastgesteld voor het verzamelen en opslaan van gegevens door en in de eindapparatuur van de gebruikers via Bluetooth-technologie, verwijst de Autoriteit naar haar opmerkingen in het vorige punt over het beginsel van minimalisering van de gegevensverwerking. Deze bepaling zal dienovereenkomstig worden aangepast om te voldoen aan de AVG.

34. Bovendien moet een verbod om enige identificator te verzamelen die gekoppeld is aan de terminal van de gebruiker (terminal mac-adres,...). worden toegevoegd als garantie voor de betrokkenen tegen heridentificatie. Ook een nadere omschrijving van het gebruik van de Bluetooth-technologie verdient het om te worden opgenomen in het dispositief van het wetsvoorstel aangezien dit een specifiek kenmerk van het systeem is. De Autoriteit dringt er voorts op aan dat in de lijst van specificaties wordt vermeld dat de applicaties elke mogelijkheid tot geolokalisering van gebruikers moeten verhinderen.

35. Bovendien zal in artikel 4 § 2, laatste streepje, op nuttige wijze worden gespecificeerd welke bevoegde overheid verantwoordelijk zal zijn voor het uitschakelen van de digitale opsporingsapplicaties zodra deze niet langer nodig zijn voor het beheer van de lockdownbeëindiging.

36. Artikel 4 §3 van het wetsvoorstel bepaalt het volgende "*Op de website van de verwerkingsverantwoordelijke worden de technische specificaties vermeld waaraan de digitale contactopsporingsapplicaties moeten voldoen*". De Autoriteit is van mening dat het aan de Koning is om deze technische modaliteiten vast te stellen, rekening houdend met de richtsnoeren van de ECG, en dat het aan Sciensano is om ervoor te zorgen dat de applicaties aan deze technische modaliteiten voldoen. Bovendien moet in het dispositief van de wet worden gespecificeerd dat deze technische modaliteiten ervoor moeten zorgen dat de in de paragrafen twee van hetzelfde artikel bedoelde functies worden geëerbiedigd en dat zij ervoor zorgen dat de gebruikers van de opsporingsapplicatie worden beschermd tegen het risico op heridentificatie door een derde partij.

37. In dit verband is het in het algemeen van belang dat alle gegevensstromen met betrekking tot de werking van het traceringssysteem op zijn minst voldoende worden beveiligd om elke aanval en elk misbruik van het systeem voor kwaadaardige doeleinden te voorkomen. Het gaat om de beveiliging van de volgende gegevensstromen: server naar applicaties, applicaties naar de overheid die verantwoordelijk is voor het ontvangen van meldingen van besmette personen en gegevensstromen tussen de applicaties zelf (tussen de eindapparatuur van de gebruikers van de applicatie). Het is belangrijk dat deze technische maatregelen in dergelijke veiligheidsmaatregelen voorzien. Het gebruik van een vertrouwelijk derdenplatform lijkt hiervoor onontbeerlijk.

f. <u>Vrijwillig karakter van het gebruik van de opsporingsapplicatie</u>

38. Het is van fundamenteel belang dat het wetsvoorstel bepaalt dat de installatie, het gebruik en de verwijdering van een opsporingsapplicatie moet worden uitgevoerd zodra en alleen als een gebruiker de wens daartoe heeft geuit. Hoewel dit duidelijk de bedoeling is van de auteur van het wetsvoorstel, moet dit duidelijk worden omschreven.

39. De auteur van het wetsvoorstel heeft de suggestie van de Autoriteit in haar advies 34/2020 om te voorzien in civielrechtelijke en/of administratieve en/of strafrechtelijke sancties voor eenieder die de toegang tot een goed of dienst zou koppelen aan het gebruik van een opsporingsapplicatie, niet gevolgd. In de toelichting wordt dit gemotiveerd door het feit dat er campagnes worden overwogen om het gebruik van een opsporingsapplicatie te bevorderen. De Autoriteit is van mening dat promotiecampagnes kunnen worden gevoerd zonder dat het gebruik van dergelijke aanvragen hoeft te worden gekoppeld aan de toegang tot een goed of dienst. Als een dergelijke voorwaardelijkheid in de praktijk zou worden uitgevoerd, zou dit het vrijwillige karakter van het gebruik van de toepassing teniet doen. Om het vertrouwen van het publiek te waarborgen, is het belangrijk dat het vrijwillige karakter van dit systeem door middel van sancties wordt gewaarborgd. De Autoriteit beveelt ook aan om in de voorgestelde wet expliciet een bepaling op te nemen waarin wordt bevestigd dat het gebruik van opsporingsapplicaties in ieder geval strikt vrijwillig is en zal blijven, dat er in dit verband geen enkele druk op de burgers zal worden uitgeoefend en dat deze vrijwilligheid in alle onderdelen van het dispositief zal worden weerspiegeld: installatie van de applicatie, activering van de communiatie met Bluetooth, contact opnemen met een professionele zorgverlener, melding van een positieve diagnose of een positief opsporingsresultaat van COVID-19 in de applicatie, uitvoeren van een opsporing na ontvangst van een melding, verwijderen van de applicatie.

g. Transparantie van de gegevensverwerking die door het gebruik van de applicatie wordt gegenereerd

40. In artikel 6, § 2 wordt verwezen naar de informatieplicht van Sciensano krachtens artikel 13 van de AVG. Wat de modaliteiten voor het verstrekken van deze informatie betreft, wordt verwezen naar overweging 24 van bovengenoemd advies 34/2020 van de Autoriteit. Hieraan zal bijzondere aandacht moeten worden besteed. Het vertrouwen van potentiële gebruikers kan alleen worden opgebouwd als zij duidelijk en voldoende worden geïnformeerd over de manier waarop het contactapplicatiesysteem zal werken en over het volledige scala aan gegevensverzamelingen en -uitwisselingen dat het zal genereren, alsmede over de concrete en operationele doeleinden ervan.

h. Lokale gegevensopslag in de eindapparaten van de gebruikers en in het centrale logbestand

41. Artikel 7 van het wetsvoorstel heeft betrekking op het bewaren van gegevens die worden gebruikt of gegenereerd in het kader van het gebruik van opsporingsapplicaties.

42. In de eerste plaats moet de vaagheid rond deze bepaling met betrekking tot de categorieën van personen die instaan voor het bewaren van de beoogde gegevens (beveiligde sleutels, niet-gepersonaliseerde tijdelijke serienummers die door applicaties worden gegenereerd, tijdzones met inbegrip van een datum en een 6 uur durend deel van de dag waarop het contact tussen de gebruikers plaatsvond, alsmede de afstand en de duur van het contact) worden weggenomen. Ons begrip van het systeem is dat deze gegevens lokaal worden opgeslagen in de eindapparatuur van de gebruikers. Dit moet nader worden gepreciseerd.

43. Bovendien moeten deze gegevens, overeenkomstig het hierboven uiteengezette principe van de minimale gegevensverwerking, beperkt worden tot het strikt noodzakelijke minimum wat betreft het begrip risicocontact zoals bepaald door de FOD Volksgezondheid en het crisiscentrum (cf. supra). Dit artikel zal dienovereenkomstig worden aangepast.

i. Inzamelen van het telefoonnummer en de informatie dat de gebruiker van de opsporingsapplicatie is besmet.

44. Artikel 7 § 2 bepaalt "*De gebruiker kan vrijwillig volgende informatie ingeven in de contactopsporingsapplicatie*:

a. de met COVID-19 vastgestelde besmetting[8] ;

[8] Zoals wij het begrijpen, lijkt het ons beter de informatie te beogen volgens dewelke de gebruiker die over een dergelijke privésleutel beschikt, besmet is door COVIC-19.

b. *het telefoonnummer van de gebruiker*. »

45. De verzameling van het telefoonnummer van de gebruiker is ontegenzeggelijk de zwakke schakel in het systeem dat de auteur van het wetsvoorstel beoogt. Dit telefoonnummer verbreekt immers de garantie van niet-identificatie van de gebruiker.

46. De Autoriteit begrijpt echter uit de toelichting dat dit telefoonnummer noodzakelijk is voor Sciensano om een verificatie-SMS naar de gebruiker te sturen na verificatie en vaststelling van de authenticiteit van de gebruikte opsporingsapplicatie. Zodra deze sms-code is ingevoerd in de applicatie, zal Sciensano toestemming geven aan de applicatie van de gebruiker om de beveiligde sleutel en de vermoedelijke datum van besmetting te uploaden naar het centrale logbestand met de beveiligde sleutels van alle besmette gebruikers.

47. Zoals hierboven vermeld, beveelt de Autoriteit het gebruik van codes voor eenmalig gebruik ten zeerste aan voor het valideren van de verzending van sleutels naar de server, zonder het telefoonnummer in de applicatie in te voeren. Indien de vermelding van het telefoonnummer toch onontbeerlijk is, is de Autoriteit van mening dat het niet alleen noodzakelijk is om in artikel 7 § 2,van het wetsvoorstel dit ene en enige doel van het gebruik van het telefoonnummer van de gebruiker te specificeren[9] (met verbod op verdere verwerking), maar ook om in het dispositief van het wetsvoorstel expliciet te bepalen dat enerzijds de autorisatiecode (definitie in te voegen in artikel 3 van het wetsvoorstel) een random gegenereerde code is die niet gekoppeld is aan enige identificatiegegevens van de gebruiker of zijn eindapparaat en dat anderzijds het telefoonnummer van de gebruiker door Sciensano wordt gewist direct na het versturen van een sms naar de besmette gebruiker. Wat dit laatste punt betreft, moet de duidelijkheid van de formulering van de laatste bepaling (en de hierboven aanbevolen aanvullende garanties) worden verbeterd, indien het de bedoeling is dat de auteur van het wetsvoorstel voorziet in artikel 9, §1, lid 3 in de onmiddellijke schrapping door Sciensano van het telefoonnummer en de informatie dat de houder van dit telefoonnummer besmet is

48. Artikel 7,§ 3 van het wetsvoorstel bepaalt het tijdstip waarop de gebruiker wordt gevraagd zijn of haar telefoonnummer in de opsporingsapplicatie in te voeren, d.w.z. het tijdstip waarop hij of zij zich bij de zorgverlener bevindt voor de PCR-test die wordt uitgevoerd om na te gaan of hij of zij al dan niet besmet is. In dit verband heeft de Autoriteit vragen over de keuze van dit moment die haar voorbarig lijkt, aangezien het - gelet op het doel waarvoor dit telefoonnummer wordt gebruikt - dit blijkbaar pas aan de gebruiker zal worden aangeboden op het moment dat hij op de hoogte wordt gesteld van het positieve resultaat van zijn test. Bij gebrek aan motivering zal de auteur van het wetsvoorstel de bepaling van dit moment in die zin wijzigen.

[9] Onder voorbehoud van wat hierboven is geschreven met betrekking tot het verzoek van de Autoriteit.

j. Centralisatie van de gegevens door Sciensano

49. Artikel 8 van het wetsvoorstel bepaalt de lijst van gegevens die centraal worden bewaard door Sciensano, zowel ten behoeve van het beheer van het systeem van digitale opsporingsapplicaties als ten behoeve van het onderzoek.

50. De Autoriteit heeft geen opmerkingen over de lijst van gecentraliseerde gegevens voor het eerste doeleinde, behalve dat deze lijst uitputtend moet zijn. Er moet worden gepreciseerd dat alleen deze informatie wordt gecentraliseerd.

51. Wat de in artikel 8 § 2, bedoelde lijst van gegevens betreft, verwijst de Autoriteit naar haar opmerking hierboven over het doel van de opsporing. Aangezien het hoofddoel van het wetsvoorstel is om een systeem met opsporingsapplicaties zodanig te reguleren dat deze onder andere voldoen aan het beginsel van gegevensminimalisering, lijkt het niet relevant om te voorzien in het verzamelen van aanvullende gegevens ten behoeve van opsporing die niet noodzakelijk zijn voor het opsporingsdoeleinde (aantal ontmoetingen van de gebruiker met een besmette persoon en voor elke ontmoeting het aantal dagen sinds de datum van de COVID-besmetting). Bovendien kan de Autoriteit de proportionaliteit van deze gegevens niet beoordelen bij gebrek aan uitleg in de toelichting en een motivering waarom deze gegevens nodig zijn om de voorgestelde onderzoeken uit te voeren en de noodzaak om ze op deze manier te verzamelen in vergelijking met andere verzamelmethoden die momenteel worden toegepast voor het epidemiologische onderzoek dat reeds plaatsvindt.

k. Bewaartermijn van gegevens in de eindapparatuur en in het gecentraliseerde logbestand en deactivering van digitale opsporingsapplicaties

52. In artikel 9 van het wetsontwerp wordt de bewaartermijn voor de gegevens[10] die zowel bij de eindapparaten van de gebruikers als in het centrale bestand van Sciensano worden verzameld, vastgesteld op maximaal drie weken, hetgeen in het licht van de in de toelichting gegeven uitleg relevant en noodzakelijk lijkt voor het bereiken van het nagestreefde doel.

53. Artikel 9 §3 bepaalt dat opsporingsapplicaties worden **gedeactiveerd** zodra een koninklijk besluit dat het einde van de epidemische toestand van het coronavirus COVID-19 afkondigt, in het Belgisch Staatsblad is gepubliceerd. Aangezien het mogelijk is dat de opsporingsapplicaties vóór die tijd niet meer nodig zijn, is de Autoriteit van mening dat in het wetsvoorstel moet worden gespecificeerd dat

[10] Wat de lijst van de genoemde gegevens betreft, wordt verwezen naar de eerdere opmerkingen van de Autoriteit over het beginsel van minimalisering van de gegevens. Deze bepaling zal op dit punt dienovereenkomstig worden aangepast.

de deactivering van het systeem op een vast moment moet worden vastgesteld (die in het wetsvoorstel moet worden opgenomen), met de mogelijkheid voor de bevoegde minister om het te verlengen, mits dit wordt gemotiveerd.

l. Verdere verwerking voor onderzoeksdoeleinden

54. Artikel 10 van het wetsvoorstel voorziet, als waarborg voor de rechten en vrijheden van de gebruikers, in een verbod op de verdere verwerking van de verzamelde gegevens, met uitzondering van de verwerking voor onderzoeks- en statistische doeleinden.

55. De autoriteit merkt op dat artikel 10, tweede lid, moet verwijzen naar het gehele artikel 89 en niet alleen naar de leden 2 en 3, aangezien lid 1 vereist dat het beginsel van de minimale gegevensverwerking in het kader van het uitvoeren van onderzoek en het gebruik van gegevens waarmee de betrokkenen niet of niet meer kunnen worden geïdentificeerd, in acht wordt genomen zodra dit volstaat voor het doeleinde van het onderzoek. Bovendien lijkt het, in het licht van artikel 4 van het wetsvoorstel, passend om eenvoudigweg te specificeren dat een dergelijke verdere verwerking zal worden uitgevoerd op basis van geanonimiseerde gegevens.

m. Gebruikers- en toegangsbeheer

56. Artikel 11 van het wetsvoorstel voorziet in een systeem voor het beheer van de toegang en de gebruikers tot de loglijst en de databank die met het oog op epidemiologisch onderzoek zal worden opgezet.

57. De Autoriteit zet vraagtekens bij het nut van dit artikel, aangezien volgens artikel 4 enerzijds epidemiologisch onderzoek zal worden uitgevoerd op basis van geanonimiseerde gegevens en anderzijds het beheer van het logbestand volgens de Autoriteit bij Sciensano zal worden gecentraliseerd en alleen toegankelijk zal zijn voor gebruikers van de applicatie die door hun aard niet opnieuw kunnen worden geïdentificeerd.

58. Indien het de bedoeling van de auteur van het wetsvoorstel is om andere personen dan de gebruikers van opsporingsapplicaties toegang te verlenen tot deze databanken, is het absoluut noodzakelijk dat het dispositief van de wet deze ontvangers en de omstandigheden en redenen waarom zij toegang zouden moeten hebben, identificeert en de rechtmatigheid en proportionaliteit van deze toegang rechtvaardigt. Zonder een nadere omschrijving in de toelichting kan de Autoriteit het rechtmatige en proportionele karakter van een dergelijke toegang niet beoordelen en heeft zij in dit verband ernstige twijfels, aangezien op basis van de toelichting een dergelijke toegang niet gerechtvaardigd of noodzakelijk lijkt voor het bereiken van het doel van het traceringssysteem.

59. Bovendien wordt in het wetsvoorstel niet gespecificeerd dat gebruikers van de applicatie toegang hebben tot het logbestand, zodat hun applicatie de privésleutel van besmette gebruikers kan lezen om het tijdelijke serienummer te genereren en te controleren of dit nummer is opgenomen in hun eigen contacten op hun eindapparaat (wat een waarschuwingsbericht zal genereren dat ze een risicovol contact met een besmette persoon hebben gehad). Omwille van de voorspelbaarheid en duidelijkheid moet dit in het wetsvoorstel worden gespecificeerd.

n. <u>Keuze van het bericht dat door de overheid in het waarschuwingsbericht wordt verzonden aan gebruikers die een risicovol contact hebben gehad met een besmette persoon</u>

60. Het doel van het wetsvoorstel is niet om te bepalen welk type bericht zal worden gecommuniceerd aan gebruikers die risicovol contact hebben gehad met een besmette persoon. Er wordt echter verwezen naar overweging 30 van advies 34/2020. Het is belangrijk dat de vrije wil van de gebruikers van opsporingsapplicaties behouden blijft.

OM DIE REDENEN,

Is de Autoriteit van mening dat, indien de noodzaak van de terbeschikkingstelling van opsporingsapplicaties voor het beheer van de lockdownbeëindiging wordt aangetoond, de voorwaarden die ervoor instaan dat het gebruik ervan in overeenstemming is met de AVG, nog altijd moeten worden ingevoerd en de Autoriteit is van mening dat het wetsvoorstel hiertoe moet worden aangepast aan de opmerkingen in dit advies, meer bepaald:

1. Uitleg over de essentiële onderdelen van het DP3T-protocol, de garanties die het biedt, de restrisico's en de redenen waarom geconcludeerd moet worden dat de gegevensverwerkingen die zouden worden uitgevoerd toch proportioneel zijn;
2. Uitleg over de werking van het opsporingsysteem, met name om ervoor te zorgen dat de risico's die door het DP3T-protocol worden beperkt, niet opnieuw worden ingevoerd door applicaties en/of een systeem dat heridentificatie mogelijk maakt;
3. Specificatie in artikel 6 van de categorieën van gegevensverwerkingen waarvoor de verwerkingsverantwoordelijke is aangesteld, toewijzing van de opdracht om na te gaan of de voor het publiek beschikbaar gestelde applicaties voldoen aan de wettelijke specificaties;
4. Invoeren van een verplichte voorlegging aan de Autoriteit van de DPIA('s) die moeten worden uitgevoerd en invoeren van de publiciteitsmaatregelen van deze DPIA('s) en de adviezen van

de GBA over deze DPIA('s);

5. Invoeren van publiciteitsmaatregelen voor de volledige broncode van de geselecteerde applicatie(s), en dit, voldoende vooraf ;
6. Herformulering van het doel waarvoor het opsporingssysteem is opgezet;
7. Verwijdering van het onderzoeksdoeleinde van het opsporingssysteem en bijgevolg de daaruit voortvloeiende aanpassing van het wetsvoorstel;
8. Verbetering van de leesbaarheid van het wetsvoorstel en de voorspelbaarheid van de verwerkingen die zullen voortvloeien uit het gebruik van opsporingsapplicaties door het toevoegen van de definities van belangrijke concepten zoals opsporingsapplicatie, gebruiker, risicocontact, autorisatiecode, beveiligde sleutel, niet-gepersonaliseerd tijdelijk serienummer, bevoegde minister, ..;
9. Naleving van het beginsel van de minimale gegevensverwerking bij het vaststellen van de gegevens die moeten worden verzameld en verwerkt in het kader van het ingevoerd opsporingssysteem en dit op niveau van meerdere artikelen van het wetsvoorstel;
10. Toevoeging, naast de technische functionaliteiten die worden opgelegd aan de opsporingsapplicaties, dat de deactivering kan worden uitgevoerd door de bevoegde minister en belasten van de Koning met het bepalen van de technische specificaties waaraan de applicaties zullen moeten voldoen;
11. Oplegging van sancties aan eenieder die het gebruik van opsporingsapplicaties zou koppelen aan de toegang tot een goed of dienst (cons. 31);
12. Verduidelijking dat het bewaren van gegevens op grond van artikel 7 betrekking heeft op het bewaren van gegevens in de eindapparatuur van de gebruiker (zie cons. 34);
13. Vaststelling van specifieke garanties om het risico van heridentificatie op basis van het telefoonnummer van de besmette gebruiker te beperken (zie cons. 39);
14. Vaststelling van het tijdstip waarop de gebruiker wordt verzocht zijn telefoonnummer mee te delen overeenkomstig het proportionaliteitsbeginsel (zie cons.40) ;
15. Preciseren dat de lijst van gegevens die door Sciensano zijn gecentraliseerd ten behoeve van het beheer van het opsporingssysteem, een limitaitieve lijst is (cons. 42) ;
16. Toevoeging aan artikel 9, §3 dat de opsporingsapplicaties wordt gedeactiveerd zodra de bevoegde minister heeft vastgesteld dat deze niet meer nodig zijn voor het beheer van de beëindiging van de lockdown (cons. 45) ;
17. Preciseren In artikel 10 dat de verdere verwerking voor onderzoeksdoeleinden van de gegevens verzameld door Sciensano in het kader van het beheer van de opsporingsapplicaties zal plaatsvinden op basis van geanonimiseerde gegevens (zie cons. 47) ;
18. Rectificatie van artikel 11 betreffende toegang en gebruikersbeheer overeenkomstig de consideransen 48 tot en met 50 en schrapping van elke bepaling waaruit een uitwisseling van gegevens kan worden afgeleid die niet noodzakelijk is voor het beheer van de opsporingsapplicaties;

19. Preciseren over welke toegangen de gebruikers van opsporingsapplicaties zullen beschikken (cons. 51).

De Autoriteit beveelt eveneens aan:

1. Dat de analyse van de noodzaak van het besluit om dit soort applicaties te gebruiken naar behoren wordt gedocumenteerd en geïntegreerd wordt in de DPIA die moet worden uitgevoerd;
2. Dat bijzondere aandacht wordt besteed aan de wijze waarop de betrokkenen worden geïnformeerd over de werking van de opsporingsapplicaties en de uitwisseling van gegevens die zij genereren;
3. dat de vrije wil van de gebruikers van opsporingsapplicaties behouden blijft (cons. 52).

(get.) Alexandra Jaspar
Directeur van het Kenniscentrum

[i] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020.