



RAAD VAN STATE
afdeling Wetgeving

CONSEIL D'ÉTAT
section de législation

advies 67.424/3
van 26 mei 2020

avis 67.424/3
du 26 mai 2020

over

sur

een wetsvoorstel 'betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking' (*Parl. St. Kamer* 2019-20, nr. 55-1251/001)

une proposition de loi 'relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population' (*Doc. Parl., Chambre*, 2019-20, n° 55-1251/001)

Op 15 mei 2020 is de Raad van State, afdeling Wetgeving, door de Voorzitter van de Kamer van volksvertegenwoordigers verzocht binnen een termijn van vijf werkdagen een 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’ (*Parl. St. Kamer 2019-20, nr. 55-1251/001*).

Het voorstel is door de derde kamer onderzocht op 20 en 22 mei 2020. De kamer was samengesteld uit Jo BAERT, kamervoorzitter, Jeroen VAN NIEUWENHOVE en Koen MUYLLE, staatsraden, Jan VELAERS en Bruno PEETERS, assessoren, en Annemie GOOSSENS, griffier.

Het verslag is uitgebracht door Frédéric VANNESTE, eerste auditeur, en Cedric JENART, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Jeroen VAN NIEUWENHOVE, staatsraad.

Het advies, waarvan de tekst hierna volgt, is gegeven op 26 mei 2020.

*

Le 15 mai 2020, le Conseil d'État, section de législation, a été invité par le Président de la Chambre des représentants à communiquer un avis, dans un délai de cinq jours ouvrables, sur une proposition de loi ‘relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population’ (*Doc. Parl., Chambre, 2019-20, n° 55-1251/001*).

La proposition a été examinée par la troisième chambre les 20 et 22 mai 2020. La chambre était composée de Jo BAERT, président de chambre, Jeroen VAN NIEUWENHOVE et Koen MUYLLE, conseillers d'État, Jan VELAERS et Bruno PEETERS, assesseurs, et Annemie GOOSSENS, greffier.

Le rapport a été présenté par Frédéric VANNESTE, premier auditeur, et Cedric JENART, auditeur adjoint.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Jeroen VAN NIEUWENHOVE, conseiller d'État.

L'avis, dont le texte suit, a été donné le 26 mai 2020.

*

1. Volgens artikel 84, § 1, eerste lid, 3°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, moeten in de adviesaanvraag de redenen worden opgegeven tot staving van het spoedeisende karakter ervan.

In het onderhavige geval wordt het verzoek om spoedbehandeling gemotiveerd als volgt:

“- het opsporen van de contacten van besmette personen en het aansporen van deze contacten om de nodige maatregelen te nemen, is cruciaal om nieuwe besmettingshaarden, die de volksgezondheid bedreigen, te voorkomen;

- digitale contactopsporingsapplicaties die op een smartphone worden geïnstalleerd kunnen de gezondheidsdiensten helpen in het monitoren en doorbreken van het aantal besmettingen en de beperkingen van manuele contactopsporing verhelpen;

- dit wetsvoorstel tracht een algemeen juridisch kader te creëren, onder meer om ervoor te zorgen dat op het Belgisch grondgebied slechts één technologische methode van contactopsporingsapplicaties wordt gebruikt”.

*

2. Overeenkomstig artikel 84, § 3, eerste lid, van de gecoördineerde wetten op de Raad van State, heeft de afdeling Wetgeving zich moeten beperken tot het onderzoek van de bevoegdheid van de steller van de handeling, van de rechtsgrond¹, alsmede van de vraag of aan de te vervullen vormvereisten is voldaan.

*

STREKKING VAN HET WETSVOORSTEL

3. Het voor advies voorgelegde wetsvoorstel strekt ertoe een wettelijk kader te scheppen om het gebruik op vrijwillige basis toe te laten van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van COVID-19. Het bepaalt de functionaliteiten van de digitale contactopsporingsapplicaties, de nadere regels en technische voorwaarden voor het gebruik ervan alsook de waarborgen ter bescherming van de fundamentele rechten en vrijheden van de burgers (artikel 2 van het voorstel).

De doelstellingen van de verwerking van de informatie door digitale contactopsporingsapplicaties worden bepaald, namelijk het kunnen bevestigen van een besmetting van de gebruiker van de applicatie, het verwittigen van gebruikers dat zij zich gedurende een bepaalde tijd in de nabijheid van een besmette persoon hebben bevonden en het uitvoeren van epidemiologisch onderzoek betreffende de verspreiding van COVID-19 (artikel 4, § 1). De informatie mag ook worden gebruikt voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, maar niet voor andere doeleinden (artikel 10).

¹ Aangezien het om een wetsvoorstel gaat, wordt onder “rechtsgrond” de overeenstemming met de hogere rechtsnormen verstaan.

Er worden een aantal vereisten bepaald inzake functionaliteit en veiligheid van die applicaties. De technische specificaties waaraan de applicaties moeten voldoen, moeten op de website van de verwerkingsverantwoordelijke worden vermeld (artikel 4, §§ 2 en 3).

De digitale contactopsporingsapplicaties moeten uitsluitend op vrijwillige basis worden geïnstalleerd, gebruikt en gedeïnstalleerd (artikel 5). Sciensano wordt aangewezen als de verwerkingsverantwoordelijke en moet de voorgeschreven informatie aan de gebruiker verstrekken bij de installatie van de applicatie (artikel 6).

Er wordt bepaald welke gegevens door de digitale contactopsporingsapplicaties worden verwerkt specifiek met het oog op de contactopsporing, welke gegevens niet mogen worden geregistreerd, welke gegevens niet mogen worden gecommuniceerd aan de gebruiker en welke informatie de gebruiker vrijwillig kan ingeven in de applicatie. De doelstelling van de applicatie inzake epidemiologisch onderzoek is facultatief en de gebruiker moet uitdrukkelijk bevestigen dat de informatie in verband met die doelstelling aan Sciensano kan worden meegedeeld (artikel 7).

Bepaalde gegevens met betrekking tot de gebruiker waarvan de besmetting is vastgesteld, worden bijgehouden in een centrale loglijst die wordt beheerd door Sciensano met het oog op de eerste twee voornoemde doelstellingen (artikel 8, § 1). Andere gegevens met betrekking tot besmette personen en personen waarmee ze in contact zijn geweest worden bijgehouden in een centrale databank die wordt beheerd door Sciensano; die gegevens moeten apart worden bewaard van de gegevens in de voormelde loglijst en die gegevens mogen niet met elkaar in verbinding worden gebracht (artikel 8, § 2).

Er wordt bepaald wanneer verscheidene gegevens moeten worden gewist in de eindapparatuur en in de loglijst (artikel 9, §§ 1 en 2) en wanneer de digitale contactopsporingsapplicaties worden gedeactiveerd (artikel 9, § 3).

Voor de verwerking van de informatie in de loglijst en in de databank voorziet de verwerkingsverantwoordelijke in een strikt en adequaat gebruikers- en toegangsbeheer aan de hand van bepaalde opgesomde informaticatechnieken (artikel 11, § 1, eerste lid). De geregistreeerde informatie wordt gedurende drie jaar bewaard (artikel 11, § 1, tweede lid). De verwerkingsverantwoordelijke voorziet in de nodige technische en organisatorische maatregelen om te waarborgen dat de informatie bewaard in de loglijst en in de databank niet met elkaar in verband worden gebracht (artikel 11, § 2).

De aan te nemen wet treedt in werking op de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt en is van toepassing tot (lees: treedt buiten werking op) de dag van de bekendmaking van het koninklijk besluit dat het einde van de COVID-19-epidemie afkondigt (artikel 12).

BEVOEGDHEID

4. De voorgestelde regeling voorziet in een wetgevend kader voor de functionaliteiten en de technologische specificaties van digitale contactopsporingsapplicaties, in het kader van de maatregelen ter voorkoming van de verdere verspreiding van COVID-19. Het is de bedoeling om daarmee zowel het adequaat functioneren van die digitale contactopsporingsapplicaties te waarborgen, alsook om de ermee gepaard gaande verwerking van persoonsgegevens te regelen.

In de toelichting bij het voorstel wordt uiteengezet dat zowel de digitale contactopsporing als de manuele contactopsporing cruciaal zijn om nieuwe besmettingshaarden te voorkomen die de volksgezondheid bedreigen. De manuele opsporing, die onder meer kan gebeuren door middel van call centra, zou evenwel niet altijd even doeltreffend zijn en ook een belangrijke inmenging vormen in de persoonlijke levenssfeer. Digitale contactopsporingsapplicaties zouden daarentegen doeltreffender zijn om de bevolking tijdig te informeren en zouden ook een beperktere inmenging in de persoonlijke levenssfeer inhouden. Het voorstel strekt ertoe het gebruik van deze applicaties met voldoende waarborgen te omkaderen en ervoor te zorgen dat ze voldoen aan de vereisten inzake grondrechten, met toepassing van de *privacy by design*-beginselen² van de algemene verordening gegevensbescherming³ (hierna: AVG), opdat de burger voldoende vertrouwen heeft in de technologie om ze daadwerkelijk te gebruiken, ondanks het strikt vrijwillige karakter ervan.

5. De federale overheid is bevoegd om algemene regels te bepalen inzake de beperking van het recht op eerbiediging van het privéleven,⁴ die als minimumregeling geldt in welke aangelegenheid ook.⁵

Het vrijwillige karakter van de digitale contactopsporingsapplicaties, zoals die worden geregeld in de voorgestelde regeling, neemt niet weg dat het gebruik ervan een inmenging kan vormen in de persoonlijke levenssfeer en dat de federale overheid op algemene wijze eisen kan opleggen met betrekking tot die applicaties vanuit het oogpunt van de bescherming van de gebruikers ervan met betrekking tot de verwerking van persoonsgegevens door middel van deze applicaties.

² Dit houdt in dat de overeenstemming met de vereisten inzake de bescherming van de persoonlijke levenssfeer wordt gewaarborgd door ze in te bouwen in de betrokken applicaties als technische en organisatorische maatregelen waaraan die applicaties moeten voldoen (zie artikel 25 van de AVG, alsook overweging 78 ervan).

³ 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)'.

⁴ GwH 30 april 2003, nr. 50/2003, B.8.10 en GwH 30 april 2003, nr. 51/2003, B.4.12.

⁵ GwH 20 oktober 2004, nr. 162/2004, B.5.2; GwH 19 januari 2005, nr. 16/2005, B.5.2; GwH 14 februari 2008, nr. 15/2008, B.21; GwH 19 juli 2018, nr. 104/2018, B.22.3; GwH 12 maart 2020, nr. 43/2020, B.53.6. Zie ook adv.RvS 61.267/2/AV van 27 juni 2017 over een voorontwerp dat heeft geleid tot de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit', *Parl.St.* Kamer 2016-17, nr. 54-2648/001, 106-116.

Die federale bevoegdheid betreft echter het uitwerken van *algemene* regels. Het vaststellen van specifieke regelingen met betrekking tot de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens betreffende een bepaalde gemeenschaps- of gewestaangelegenheid, is een bevoegdheid van de betrokken gemeenschap of het betrokken gewest.

6. De voorgestelde regeling voorziet niet in algemene regels inzake de beperking van het recht op eerbiediging van het privéleven bij de ontwikkeling en het gebruik van alle soorten van digitale contactopsporingsapplicaties. De in het voorstel geregelde digitale contactopsporingsapplicaties worden uitdrukkelijk en in hoofdorde ingezet om besmettingen met COVID-19 op te sporen en te voorkomen, hetgeen tot uiting komt in het opschrift en in verscheidene bepalingen van het voorstel.

De gemeenschappen⁶ zijn echter bevoegd voor de opsporing en de strijd tegen de besmettelijke en de sociale ziekten als een onderdeel van hun bevoegdheden inzake preventieve gezondheidszorg.⁷ Het in contact treden met (mogelijk of vermoedelijk) besmette personen, alsook met personen en collectiviteiten waarmee ze in contact zijn geweest, het verstrekken van aanbevelingen aan deze personen met het oog op de voorkoming van verdere besmettingen, en het opleggen van afzonderingsmaatregelen aan deze personen kan tot die bevoegdheid worden gerekend.⁸ Dat geldt ook voor de verwerking, met die finaliteit, van persoonsgegevens die

⁶ Wat betreft de Franse Gemeenschap is de uitoefening van deze bevoegdheid overeenkomstig artikel 3, 6°, van het bijzonder decreet van 3 april 2014 'relatif aux compétences de la Communauté française dont l'exercice est transféré à la Région wallonne et à la Commission communautaire française' (en de gelijklopende decreten van het Waalse Gewest en de Franse Gemeenschapscommissie) overgedragen aan het Waalse Gewest en de Franse Gemeenschapscommissie.

⁷ Artikel 5, § 1, I, eerste lid, 8°, van de bijzondere wet van 8 augustus 1980 'tot hervorming der instellingen'. Zie ook *Parl.St.* Senaat 1979-80, nr. 434/2, 125 en *Parl.St.* Kamer 1979-80, nr. 627/10, 52. Deze bevoegdheid werd impliciet bevestigd in adv.RvS 34.339/AV van 29 april 2003 over een voorontwerp dat heeft geleid tot het decreet van de Vlaamse Gemeenschap en het Vlaamse Gewest van 21 november 2003 'betreffende het preventieve gezondheidsbeleid', *Parl.St.* Vl.Parl. 2002-03, nr. 1709/1, 147-155, alsook uitdrukkelijk in adv.RvS 38.381/3 van 7 juli 2005 over een ontwerp van koninklijk besluit 'tot vaststelling van de profylactische maatregelen en de verplichte aangifte aan de cel medische bewaking van pathologieën van epidemische aard' en in adv.RvS 53.018/VR van 13 mei 2013 over een ontwerp van koninklijk besluit 'houdende de gezondheidscontrole van het internationale verkeer'.

⁸ De federale voorbehouden bevoegdheid inzake de "nationale maatregelen inzake profylaxis" doet geen afbreuk aan die gemeenschapsbevoegdheid, aangezien die beperkt is tot de verplichte inentingen (adv.RvS 58.118/3 van 28 september 2015 over een voorontwerp dat geleid heeft tot de ordonnantie van 18 december 2015 'houdende instemming met het Samenwerkingsakkoord tussen de Franse Gemeenschap (ONE), de Gemeenschappelijke Gemeenschapscommissie en de Duitstalige Gemeenschap betreffende de aankoop van vaccins om de kinderen, de zwangere vrouwen en de adolescenten te beschermen' *Parl.St.* Ver.Verg. Gem.Gem.Comm. 2015-16, nr. B-41/1, 5-6).

daarmee verband houden.⁹ Op grond van die bevoegdheid hebben de gemeenschappen ondertussen reeds een aantal regelingen uitgewerkt wat de manuele contactopsporing betreft.¹⁰

Zoals in de toelichting bij het voor advies voorgelegde wetsvoorstel wordt erkend,¹¹ behoort de ontwikkeling van digitale contactopsporingsapplicaties die specifiek gericht zijn op het opsporen van COVID-19-besmettingen tot de bevoegdheid van de gemeenschappen. Die bevoegdheid omvat het vaststellen van een regeling voor de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens bij de ontwikkeling en het gebruik van die applicaties.

In zoverre het voor advies voorgelegde wetsvoorstel in regels voorziet die specifiek gericht zijn op digitale contactopsporingsapplicaties om COVID-19-besmettingen op te sporen, wordt dan ook de gemeenschapsbevoegdheid inzake preventieve gezondheidszorg betreden.

7. De digitale contactopsporingsapplicaties strekken er blijkens artikel 4, § 1, derde streepje, van het voorstel ook toe “epidemiologisch onderzoek uit te voeren betreffende de verspreiding van COVID-19 op basis van geanonimiseerde gegevens”, hetgeen kan worden ingepast in de federale bevoegdheden inzake wetenschappelijk onderzoek.¹² In dat opzicht wordt aangesloten bij de surveillance-activiteiten waarmee Sciensano is belast bij artikel 4 van de wet van 25 februari 2018 ‘tot oprichting van Sciensano’.

8. De conclusie is derhalve dat het wetsvoorstel betrekking heeft zowel op federale als op gemeenschapsbevoegdheden.

Het voor advies voorgelegde wetsvoorstel kan in zijn huidige vorm enkel doorgang vinden indien het zou worden omgevormd tot een samenwerkingsakkoord waarvoor parlementaire instemming is vereist. Het zou immers Belgen persoonlijk kunnen binden en het heeft betrekking op aangelegenheden die – gelet op het in artikel 22 van de Grondwet vervatte wettigheidsbeginsel – bij wet moeten worden geregeld.¹³ Een dergelijk samenwerkingsakkoord biedt overigens de meest rechtszekere oplossing.

⁹ Zie de in voetnoten 4 en 5 aangehaalde arresten van het Grondwettelijk Hof. Zie ook adv.RvS 67.407/3 van 20 mei 2020 over een ontwerp van besluit van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie nr. 2020/006 ‘tot het organiseren van het gezondheidkundig contactonderzoek in het kader van de strijd tegen de COVID-19-pandemie’, opmerking 4.1; adv.RvS 67.412/3 van 25 mei 2020 over een voorontwerp van decreet van de Duitstalige Gemeenschap ‘über die Rückverfolgung von Infektionsketten im Rahmen der Bekämpfung der Coronavirus (COVID-19) Gesundheitskrise’, opmerking 4.1.

¹⁰ Zie het decreet van de Vlaamse Gemeenschap van 8 mei 2020 ‘tot organisatie van contactonderzoek in het kader van COVID-19’ en het besluit van de Waalse Regering nr. 35 van 5 mei 2020 ‘organisant le tracing socio-sanitaire dans le cadre de la lutte contre l’épidémie COVID-19’, evenals het in vorige voetnoot vermelde ontwerp van besluit van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie nr. 2020/006 en voorontwerp van decreet van de Duitstalige Gemeenschap.

¹¹ *Parl.St.* Kamer 2019-20, nr. 55-1251/001, 6.

¹² Artikel 6bis, §§ 2 en 3, van de bijzondere wet van 8 augustus 1980.

¹³ Zie artikel 92bis, § 1, tweede lid, van de bijzondere wet van 8 augustus 1980.

Een andere mogelijkheid zou erin kunnen bestaan het voorstel terug te brengen tot een algemene regeling van de verwerking van persoonsgegevens bij het gebruik van digitale contactopsporingsapplicaties. Voor zover die regeling dan de essentiële elementen bevat die overeenkomstig artikel 22 van de Grondwet in een wetgevende norm moeten worden geregeld, kunnen de aspecten van de voorgestelde regeling die specifiek betrekking hebben op de opsporing van COVID-19-besmettingen worden opgenomen in een administratief samenwerkingsakkoord tussen de federale overheid en de gemeenschappen, waarvoor geen parlementaire instemming is vereist.

VORMVEREISTEN

9. Het voorstel bevat bepalingen die de verwerking van persoonsgegevens regelen. Artikel 36, lid 4, van de AVG, gelezen in samenhang met artikel 7, lid 1, c), en overweging 96 van die verordening, voorziet in een verplichting om de toezichthoudende autoriteit, in dit geval de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 ‘tot oprichting van de Gegevensbeschermingsautoriteit’, te raadplegen bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking.

De Gegevensbeschermingsautoriteit heeft weliswaar reeds advies nr. 34/2020 van 28 april 2020 gegeven over een ontwerp van koninklijk besluit ‘nr. XXX tot uitvoering van artikel 5, § 1, 1°, van de wet van 27 maart 2020 die machtiging verleent aan de Koning om maatregelen te nemen in de strijd tegen de verspreiding van het coronavirus COVID-19 (II), met het oog op het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking’.¹⁴

De Raad van State beschikt niet over het ontwerp van koninklijk besluit dat aan de Gegevensbeschermingsautoriteit is voorgelegd en kan dus ook niet nagaan in welke mate het wetsvoorstel dat aan hem om advies is voorgelegd is aangepast om tegemoet te komen aan de opmerkingen die in het advies van de Gegevensbeschermingsautoriteit zijn geformuleerd. Evenmin kan hij nagaan of er geen nieuwe bepalingen zijn toegevoegd in vergelijking met dat ontwerp. Enkel in de mate dat het wetsvoorstel louter een overname is van dat ontwerp van koninklijk besluit en de doorgevoerde aanpassingen louter het gevolg zijn van de opmerkingen van de Gegevensbeschermingsautoriteit, kan ervan worden uitgegaan dat de Gegevensbeschermingsautoriteit niet opnieuw moet worden geraadpleegd.

10. Een aantal bepalingen van het voorstel moeten worden beschouwd als technische voorschriften in de zin van artikel 1, lid 1, f), van richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 ‘betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij’, meer bepaald als regels betreffende diensten van de informatiemaatschappij in de zin van artikel 1, lid 1, e), van die richtlijn.

¹⁴ Zie <https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/AD34-2020.pdf>.

Dergelijke technische voorschriften moeten overeenkomstig artikel 5 van richtlijn (EU) 2015/1535 worden aangemeld bij de Europese Commissie. In dat geval geldt een wachtperiode van (minstens) drie maanden vooraleer het wetsvoorstel kan worden aangenomen, overeenkomstig artikel 6 van de richtlijn. Die wachtperiode geldt evenwel niet, overeenkomstig artikel 6, lid 7, als een lidstaat om dringende redenen wegens een ernstige en onvoorziene situatie die verband houdt met de bescherming van (onder meer) de gezondheid van mensen, op zeer korte termijn technische voorschriften moet uitwerken en deze onmiddellijk daarop moet vaststellen en invoeren, zonder dat raadpleging mogelijk is. In dat geval is de mededeling aan de Commissie nog steeds vereist; in de mededeling moet de reden voor de urgentie worden vermeld. De Commissie spreekt zich dan zo spoedig mogelijk uit over de mededeling.

Bijgevolg moet het voorstel worden aangemeld bij de Europese Commissie, waarbij dan de urgentie van de goedkeuring ervan kan worden uiteengezet ter verantwoording van het niet in acht nemen van de voorgeschreven wachtermijn.

11. Ten slotte rijst de vraag of de voorgestelde regeling onder het toepassingsgebied valt van de dienstenrichtlijn.¹⁵ Het ter beschikking stellen van een digitale contactopsporingsapplicatie moet worden beschouwd als een dienst, waarvan het mogelijk is dat die tegen een vergoeding wordt aangeboden, of die vergoeding nu afkomstig is van de overheid of – eventueel via reclame-inkomsten – van de gebruiker. Het wetsvoorstel waarborgt alleszins niet dat de applicaties worden aangeboden als een niet-economische dienst van algemeen belang.¹⁶ De uitzondering voor de diensten van de gezondheidszorg¹⁷ kan ook niet worden ingeroepen, omdat de applicaties geen betrekking hebben op activiteiten die in de lidstaat waar de dienst wordt verricht, zijn voorbehouden aan beoefenaren van gereguleerde beroepen in de gezondheidszorg.¹⁸

Het is dan ook mogelijk dat de dienstenrichtlijn toepasselijk is,¹⁹ zodat het voorstel moet worden getoetst aan de artikelen 14 en 15 ervan met betrekking tot de eisen die worden gesteld aan de uitoefening van een dienstenactiviteit op het grondgebied van België.²⁰ Op het eerste gezicht lijkt het voorstel geen verboden eisen als bedoeld bij artikel 14 te bevatten, evenmin als niet-discriminerende eisen als bedoeld bij artikel 15, lid 2. De Raad van State beschikt evenwel niet over het vereiste technische inzicht in de specifieke eisen ten aanzien van de digitale contactopsporingsapplicaties om daarover een sluitend oordeel te kunnen vellen. In voorkomend geval zou toch nog een aanmelding bij de Europese Commissie overeenkomstig artikel 15, lid 7, van de dienstenrichtlijn vereist kunnen zijn.

¹⁵ Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 ‘betreffende diensten op de interne markt’.

¹⁶ Zie artikel 2, lid 2, a), van de dienstenrichtlijn.

¹⁷ Zie artikel 2, lid 2, f), van de dienstenrichtlijn.

¹⁸ *Handboek voor de implementatie van de Dienstenrichtlijn*, Europese Commissie, 2007, p. 12. Zie ook overweging 22 bij de dienstenrichtlijn.

¹⁹ De uitzonderingsgronden in artikel 2, lid 2, c) en i), lijken alleszins ook niet toepasselijk in dit geval.

²⁰ Er wordt immers niet voorzien in een vergunningsstelsel, zodat niet moet worden getoetst aan de artikelen 9 tot 13 van de dienstenrichtlijn.

ALGEMENE OPMERKINGEN

12. Gelet op het vrijwillige karakter van de digitale contactopsporingsapplicaties staat of valt de werkzaamheid ervan met een voldoende hoge dekkingsgraad, met andere woorden het aantal burgers dat de applicatie in gebruik neemt.²¹ Die dekkingsgraad zal bepalend zijn voor de mate waarin de applicaties daadwerkelijk een complementaire rol kunnen spelen naast de manuele contactopsporing die door de gemeenschappen wordt geïmplementeerd. Daarbij moet ook rekening worden gehouden met de grootschalige verwerking van persoonsgegevens die gepaard gaat met het gebruik van die applicaties. Die verwerking moet immers, overeenkomstig artikel 5, lid 1, c), van de AVG beperkt zijn tot wat noodzakelijk is voor de beoogde doeleinden. Het komt er dus op aan dat noodzakelijkheidsbeginsel te verzoenen met een voldoende hoge dekkingsgraad.

De hoofdindienster van het voorstel verklaarde daarover het volgende:

“Het gebruik van een contactopsporingsapplicatie kan niet beschouwd worden als de ultieme en allesomvattende oplossing voor het terugdringen van COVID-19 besmettingen. Inderdaad, niet iedereen beschikt over een smartphone en zij die dat wel doen zullen misschien niet allemaal de contactopsporingsapplicatie gebruiken. Dat neemt niet weg dat een app complementair werkt ten opzichte van manuele tracing en enkele van de gebreken van manuele tracing oplost (in het bijzonder de moeilijkheid voor een persoon om zich alle (korte) contacten te herinneren die hij/zij binnen een bepaalde periode heeft gehad, laat staan om voor al die personen contactgegevens te kunnen bezorgen).

Het wetsvoorstel gaat uit van het gebruik van Bluetooth technologie vermits er gewerkt wordt met proximateitsdata en niet geolokalisatiedata op basis van GPS. Het gebruik van exacte lokalisatiegegevens is echter veel meer privacy-intrusief en wordt niet ondersteund op Europees niveau. (...)

(...)

Dit is een vraag die zeer complex is en waarop met de huidige stand van zaken van de wetenschap geen eenvoudig antwoord kan geformuleerd worden. Ten eerste hangt dit af van hoe dekkingsgraad juist gedefinieerd is: een mogelijk definitie is of men kan bepalen met een voldoende nauwkeurigheid of persoon A voldoende lang voldoende dicht bij persoon B is geweest? Hierbij kan men twee soorten fouten maken: het kan zijn dat een persoon A toch voldoende dicht en voldoende lang bij persoon B geweest is, maar dat dit niet blijkt uit de Bluetooth metingen (vals negatief) of dat persoon A niet voldoende lang en voldoende dicht bij persoon B geweest is, terwijl Bluetooth metingen het tegendeel aangeven (vals positief). In de voorbije maanden zijn er al een groot aantal experimenten geweest, die aangeven dat men de parameters zo kan instellen dat de valse negatieve en valse positieve waarden aanvaardbaar zijn (het gaat om een trade-off waarbij het vergroten van valse negatieven leidt tot verkleinen van valse positieven en omgekeerd). Maar dit volstaat niet om te weten of de app effectief is: empirische resultaten wijzen uit dat slechts 1 op de 20 risicovolle contacten toch leidt tot een besmetting. Dus zelfs als men heel accuraat alle risicovolle contacten in kaart kan brengen, zal het aantal daadwerkelijk besmette mensen niet nauwkeurig bepaald kunnen worden. Men weet daarnaast ook niet exact hoe de kans op besmetting varieert als functie

²¹ Zie <https://ukhumanrightsblog.com/2020/05/01/what-are-the-data-privacy-considerations-of-contact-tracing-apps/>. Zie ook *Parl.St.* Kamer 2019-20, nr. 55-1251/001, 4: “De doeltreffendheid van een contactopsporingsapplicatie is exponentieel evenredig met het aantal personen dat eenzelfde applicatie installeert en activeert.”

van duur en afstand van het contact; dit hangt af van een groot aantal parameters die moeilijk te meten zijn zoals windrichting en luchtvochtigheid. Maar deze onzekerheid betekent absoluut niet dat de app niet effectief zou zijn.

De impact van de app hangt ook af van de fractie van de bevolking die de app daadwerkelijk gebruikt. Er zijn een aantal modellen opgesteld, die uiteenlopende resultaten geven. Sommige modellen geven aan dat minstens 60% van de bevolking de app zou moeten gebruiken om een impact te hebben op de COVID-19 epidemie. Maar dergelijke modellen steunen op een groot aantal aannames. Zo zou het kunnen zijn dat de app wel degelijk effectief is met een gebruik van 20% als 80% van de 20-jarigen de app gebruikt en slechts 10% van de oudere bevolkingsgroepen.

Vragen over de dekkingsgraad en nauwkeurigheid kunnen ook gesteld worden bij manueel contact tracing: mensen weten niet meer exact met wie ze voldoende lang in contact geweest zijn, of ze zijn niet bereid om die informatie te geven. Het kan ook zijn dat men bijvoorbeeld op het openbaar vervoer vrij langdurig dicht bij een persoon heeft gezeten, terwijl men de naam of contactinformatie van die persoon niet kent. Dus ook hier heeft men valse negatieven en valse positieven. De twee soorten van contactopsporing moeten als complementair beschouwd worden.

Epidemiologen zijn het erover eens dat contactopsporing essentieel is om een epidemie onder controle te brengen. Contactopsporing moet ook niet 99% accuraat zijn om voldoende impact te hebben. Omwille van technologische beperkingen kon contactopsporing tot op heden alleen manueel gebeuren en was er geen andere keuze. Op basis van de huidige stand van zaken van de wetenschap zijn er goede indicaties dat een contactopsporingsapp wel degelijk kan werken, complementair aan manuele contactopsporing. Als een contactopsporingsapp ontworpen is volgens de principes van 'privacy by design' (zoals voorgesteld), is ze minder intrusief dan manuele contactopsporing. Als toch zou blijken dat de app helemaal niet effectief is, kan ze gemakkelijk gestopt worden. Gezien de uitzonderlijke situatie, lijkt de app wel degelijk noodzakelijk te zijn en te voldoen aan de voorwaarden dat ze een minimale inmenging vormt."

Er kan worden aangenomen dat, gezien de snelheid waarmee het wetgevend kader moet worden uitgewerkt, een voorafgaandelijke effectbeoordeling van de voorgestelde regeling niet haalbaar is.²² Een evaluatie ervan, onder meer wat betreft de doeltreffendheid, wordt in het vooruitzicht gesteld bij artikel 12, derde lid, van het voorstel, namelijk zes maanden na de inwerkingtreding van de aan te nemen regeling. Aangezien het hier gaat om een nieuwe technologie en gelet op het belang van een nauwgezette opvolging van de zo-even geschetste afweging tussen een voldoende hoge dekkingsgraad en het noodzakelijkheidsbeginsel van de met de applicaties gepaard gaande verwerking van persoonsgegevens,²³ is het raadzaam om het tijdstip van die evaluatie te vervroegen en desgevallend te voorzien in herhaalde evaluaties of zelfs in een mechanisme van permanente opvolging.

²² De Raad van State is zich ervan bewust dat naar aanleiding van het door de bevoegde Kamercommissie aangenomen 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', reeds hoorzittingen en een omstandige bespreking hebben plaatsgevonden (*Parl.St.* Kamer 2019-20, nrs. 55-1182/005 en 55-1182/006). Uit die bespreking blijkt echter ook dat er vooralsnog onvoldoende wetenschappelijke evidentie beschikbaar is over de haalbare en vereiste dekkingsgraad.

²³ Zie over dat laatste element ook <https://www.ejiltalk.org/contact-tracing-apps-and-human-rights/>.

In dat verband moet ook worden gewezen op de gegevensbeschermingseffectbeoordeling die de verwerkingsverantwoordelijke moet uitvoeren voor het begin van de verwerkingsactiviteiten, overeenkomstig artikel 35 van de AVG, “[w]anneer 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”. Dat is hier ook het geval,²⁴ zodat die gegevensbeschermingseffectbeoordeling hoe dan ook zal moeten worden uitgevoerd, naast de zo-even aangehaalde evaluatie van de aan te nemen regeling zelf.

13. Artikel 6, § 2, van het voorstel schrijft voor dat de verwerkingsverantwoordelijke, op het moment van het installeren van een contactopsporingsapplicatie, aan de gebruiker de informatie moet verstrekken zoals bepaald in artikel 13 van de AVG. Artikel 7, § 5, van het voorstel bepaalt dat de doelstelling van de applicatie met betrekking tot wetenschappelijk onderzoek²⁵ (en de erbij horende verwerking van de persoonsgegevens bedoeld in artikel 8, § 2, van het voorstel) optioneel is en dat de gebruiker uitdrukkelijk moet bevestigen dat die persoonsgegevens aan de verwerkingsverantwoordelijke kunnen worden meegedeeld.

De impact op de persoonlijke levenssfeer van de optionele bijkomende verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek is aanzienlijk groter dan die van de loutere contactopsporing. Dat blijkt zowel uit de omstandigheid dat die gegevens worden verwerkt in een centrale databank, veeleer dan in een gedecentraliseerd systeem zoals voor de contactopsporing, als uit de gevoeliger aard van de persoonsgegevens die in die centrale databank worden opgenomen.

Het is dan ook raadzaam om hetzij artikel 6, § 2, hetzij artikel 7, § 5, aan te vullen met de meer specifieke verplichting om eenvoudige en voor de gebruiker begrijpelijke informatie te verstrekken omtrent de doeleinden van de twee soorten van gegevensverwerking en de ermee verband houdende verwerking van persoonsgegevens, met vervolgens de mogelijkheid om toegang te krijgen tot meer gedetailleerde informatie, bijvoorbeeld op de website van Sciensano.²⁶ Daarbij zou het verschil tussen die twee soorten gegevensverwerking duidelijk moeten worden uiteengezet. Op die manier zou ook beter worden tegemoetgekomen aan de informatievereisten vervat in artikel 12 van de AVG.

14. Nergens in het voorstel wordt bepaald wie toegang heeft tot de centrale databank bedoeld in artikel 8, § 2, met het oog op wetenschappelijk onderzoek, ook niet in artikel 11, § 1, dat betrekking heeft op het gebruikers- en toegangsbeheer. De hoofdindienster van het voorstel verklaarde daaromtrent het volgende:

“Het wetsvoorstel voorziet niet uitdrukkelijk in de opsomming van de departementen of personen binnen Sciensano die toegang krijgen tot de loglijst en de databank. Dit is ook niet noodzakelijk en wordt nooit vereist door de

²⁴ In die zin ook advies nr. 34/2020 van 28 april 2020 van de Gegevensbeschermingsautoriteit, opmerkingen 23 en 48.

²⁵ Zie artikel 4, § 1, derde streepje, van het voorstel.

²⁶ In die zin ook advies nr. 34/2020 van 28 april 2020 van de Gegevensbeschermingsautoriteit, opmerking 24.

Gegevensbeschermingsautoriteit. Sciensano dient echter een toegangs- en gebruiksbeheer op te zetten op basis van gebruikersprofielen. De toegang en het gebruik van de loglijst en databank worden ook geregistreerd en deze gegevens zijn toegankelijk zowel voor de gegevensbeschermingsfunctionaris van Sciensano alsook voor de Gegevensbeschermingsautoriteit.

De gemeenschappen en gewesten beschikken op basis van dit wetsvoorstel niet over de mogelijkheid om toegang te krijgen tot de loglijst en de databank.”

Uit het advies van de Gegevensbeschermingsautoriteit kan worden afgeleid dat in de aan haar voorgelegde tekst bepalingen voorkwamen over de toegang tot en de mededeling van gegevens van de centrale loglijst en de centrale databank, namelijk het verbod van mededeling van de gegevens in de centrale loglijst aan derden en de mogelijkheid van raadpleging van de centrale databank door de “bevoegde autoriteiten van de gewesten [lees: de gemeenschappen]”. De Gegevensbeschermingsautoriteit beval juist aan om die bepalingen nog aan te scherpen.²⁷ Indien het daadwerkelijk de bedoeling is om aan geen enkele instantie buiten (departementen of personeelsleden van) Sciensano toegang te verlenen tot de centrale loglijst en de centrale databank, kan dat beter uitdrukkelijk worden bepaald. In het andere geval moet worden bepaald welke instanties wel toegang kunnen krijgen overeenkomstig artikel 11, § 1, van het voorstel.

ONDERZOEK VAN DE TEKST

Artikel 2

15.1. Artikel 2, tweede lid, van het voorstel bevat geen normatieve bepaling en moet worden weggelaten.

15.2. Het eerste lid is dan weer te vaag geformuleerd: indien het daadwerkelijk de bedoeling is het gebruik van digitale contactopsporingsapplicaties *toe te laten* voor de in artikel 4, § 1, bepaalde doelstellingen, wordt impliciet ook beoogd het gebruik van digitale contactopsporingsapplicaties voor die doelstellingen en die niet voldoen aan hetgeen in het voorstel wordt bepaald, te verbieden, althans voor de geldigheidsduur van de aan te nemen regeling. Dit zou uitdrukkelijk moeten worden bepaald.

Tevens rijst de vraag hoe de voormelde maatregelen gehandhaafd kunnen worden. Er kan wellicht beter worden voorzien in administratieve sancties of strafsancities voor het aanbieden van niet-conforme applicaties.

Artikel 4

16. Artikel 4, § 3, van het voorstel bepaalt dat op de website van de verwerkingsverantwoordelijke de technische specificaties vermeld worden waaraan de digitale contactopsporingsapplicaties moeten voldoen.

²⁷ Advies nr. 34/2020 van 28 april 2020, opmerkingen 39 en 40.

Indien daarmee wordt bedoeld dat op de website van Sciensano een weergave wordt bekendgemaakt van de voorwaarden die vervat zijn in de voorgestelde regeling, bestaat daartegen geen bezwaar, op voorwaarde dat die weergave overeenstemt met deze regeling.

Indien daarentegen wordt bedoeld dat Sciensano *bijkomende* technische specificaties kan opstellen en bekendmaken waaraan die applicaties moeten voldoen, wordt een regelgevende bevoegdheid toegekend aan Sciensano. Het verlenen van verordenende bevoegdheid aan een openbare instelling, zoals Sciensano, is in beginsel niet in overeenstemming met de algemene publiekrechtelijke beginselen omdat erdoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en een rechtstreekse parlementaire controle ontbreekt. Bovendien ontbreken de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking, de preventieve controle van de Raad van State, afdeling Wetgeving, en de duidelijke plaats in de hiërarchie der normen. Dergelijke delegaties kunnen dan ook enkel worden gebillijkt voor zover zij zeer beperkt zijn en een niet-beleidsmatige karakter hebben, door hun detailmatige of hoofdzakelijk technische draagwijdte. De instellingen die de betrokken reglementering dienen toe te passen moeten hierbij zowel aan rechterlijke controle als aan politieke controle onderworpen zijn.²⁸

Artikel 5

17. Artikel 5, eerste lid, van het voorstel bepaalt dat het installeren, het gebruiken en het de-installeren van een digitale contactopsporingsapplicatie uitsluitend op vrijwillige basis gebeurt. De vraag rijst evenwel of die bepaling in haar algemene formulering voldoende rekening houdt met artikel 8 van de AVG, dat voorwaarden bepaalt voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij en dat voorschrijft dat voor kinderen jonger dan 16 jaar (of eventueel tot jonger dan 13 jaar)²⁹, de toestemming of machtiging tot toestemming is vereist van de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De verwerkingsverantwoordelijke moet, met inachtneming van de beschikbare technologie, redelijke inspanningen doen om te controleren of die vereiste (machtiging tot) toestemming is gegeven. Ook al is de voormelde verordeningsbepaling rechtstreeks toepasselijk en is ze dus bindend voor de verwerkingsverantwoordelijke, toch kan worden overwogen om het wetsvoorstel aan te vullen met bepalingen die die eis concretiseren voor de betrokken applicatie.

²⁸ Vergelijk met de toetsingscriteria die het Grondwettelijk Hof gebruikt om delegaties van verordenende bevoegdheid door de wetgever aan een autonome administratieve overheid of een gedecentraliseerde openbare instelling te beoordelen; zie GwH 11 juni 2015, nr. 86/2015, B.22.4 en GwH 9 juni 2016, nr. 89/2016, B.9.6.4: “De artikelen 33, 105 en 108 van de Grondwet verzetten zich niet ertegen dat, in een bepaalde technische materie, de wetgever specifieke uitvoerende bevoegdheden toevertrouwt aan een autonome administratieve overheid die zowel aan de jurisdictionele controle als aan de parlementaire controle is onderworpen, en verbieden de wetgever niet om delegaties te verlenen aan een uitvoerend orgaan, op voorwaarde dat die betrekking hebben op de uitvoering van maatregelen waarvan het doel door de bevoegde wetgever is bepaald, in het bijzonder in technische en ingewikkelde materies.”; zie GwH 19 november 2015, nr. 162/2015, B.8.4: “Artikel 33 van de Grondwet en artikel 20 van de bijzondere wet van 8 augustus 1980 [tot hervorming der instellingen] staan niet eraan in de weg dat de wetgever specifieke uitvoerende bevoegdheden toevertrouwt aan een gedecentraliseerde openbare instelling die aan een bestuurlijk toezicht en aan een rechterlijke toetsing is onderworpen.”

²⁹ Indien ervoor wordt gekozen om een lagere leeftijd dan 16 jaar te hanteren overeenkomstig artikel 8, lid 1, tweede alinea, van de AVG.

18. Artikel 5, tweede lid, van het voorstel houdt in dat het al dan niet installeren, het al dan niet gebruiken en het al dan niet de-installeren van een digitale contactopsporingsapplicatie geen aanleiding kan geven tot enige burgerrechtelijke of strafrechtelijke maatregel, tot enige discriminerende handeling of tot enig voordeel of nadeel. Op de vraag wat wordt bedoeld met de term “enig voordeel of nadeel”, antwoordde de hoofdindienster van het voorstel als volgt:

“Deze bepaling werd toegevoegd op vraag van de Gegevensbeschermingsautoriteit. De GBA benadrukte dat het weigeren van het gebruiken van een contactopsporingsapplicatie niet tot enig nadeel zou mogen leiden. Omgekeerd echter mag de keuze voor het gebruiken van een applicatie ook niet tot enig voordeel leiden. Het betreft dus een bepaling vanuit de bezorgdheid dat er geen discriminerende handelingen, in positieve en negatieve zin zouden mogen plaatsvinden. Een nadere beschrijving van een voordeel of nadeel is echter moeilijk aangezien de brede waaier van mogelijke toepassingen in de praktijk. De casuïstiek zal dit moeten uitwijzen.”

In de toelichting bij het voorstel wordt voorts verduidelijkt dat de suggestie van de Gegevensbeschermingsautoriteit om te voorzien in burgerlijke, administratieve of strafrechtelijke sancties voor degenen die de toegang tot een goed of dienst zouden koppelen aan het gebruik van de applicaties,³⁰ niet wordt gevolgd en dat zal worden voorzien in promotiecampagnes om het gebruik van de applicaties aan te moedigen.³¹

Het op sluitende wijze omschrijven van de term “enig voordeel of nadeel” in de tekst van het voorstel zelf is allicht onmogelijk, maar dat neemt niet weg dat het op basis van de huidige tekst en de toelichting erbij niet duidelijk is of de applicatie bijvoorbeeld gebundeld kan worden met andere, voor de gebruiker interessante toepassingen, of dat aan het gebruik van de applicatie bepaalde kortingen kunnen worden verbonden, enzovoort. Het is dan ook raadzaam om de casuïstiek toch enigszins te schetsen naar aanleiding van de parlementaire bespreking.

Artikel 9

19. Artikel 9, § 3, tweede lid, van het voorstel bepaalt dat het deactiveren van de digitale contactopsporingsapplicaties niet afhankelijk mag zijn van de-installatie door de gebruiker. Deze bepaling is niet erg duidelijk. Indien wordt bedoeld dat de applicatie wordt gedeactiveerd op de in het eerste lid bedoelde dag, ook indien een gebruiker de applicatie pas later de-installeert, kan dat beter met zoveel woorden worden bepaald.

Artikel 11

20. Artikel 11, § 1, tweede lid, van het voorstel schrijft voor dat de geregistreeerde informatie wordt bewaard gedurende drie jaar. Op de vraag waarom wordt gekozen voor een bewaartermijn van drie jaar, antwoordde de hoofdindienster van het voorstel:

“Dit is noodzakelijk om inbreuken op de toegangsregels achteraf nog te kunnen vaststellen.”

³⁰ Advies nr. 34/2020 van 28 april 2020 van de Gegevensbeschermingsautoriteit, opmerking 21.

³¹ *Parl.St.* Kamer 2019-20, nr. 55-1251/001, 11.

De vraag rijst of een dergelijke termijn volstaat gezien de strafrechtelijke aard van de sancties die verbonden zijn aan ongeoorloofde toegang tot de gegevens en de verjaringstermijn voor dergelijke inbreuken.³²

Artikel 12

21. Artikel 12, tweede lid, van het voorstel heeft betrekking op de buitenwerkingtreding³³ van de aan te nemen regeling. Indien gekozen wordt voor een wetgevend samenwerkingsakkoord overeenkomstig hetgeen wordt uiteengezet in opmerking 8, tweede alinea, zal moeten worden voorzien in een aangepaste regeling van de buitenwerkingtreding, die dan niet afhankelijk kan worden gemaakt van het nemen van een koninklijk besluit. Er zal dan voor een andere werkwijze van buitenwerkingtreding moeten worden gekozen die rechtszeker is en kenbaar voor alle burgers.

22. In elk geval acht de Raad van State het denkbaar – en misschien zelfs wenselijk – dat de buitenwerkingtreding van de aan te nemen regeling wordt gedifferentieerd. Zo kan onder meer aan de artikelen 6, § 1, 10 en 11 van het voorstel een langere geldingsduur worden verleend.

23. Wat betreft de evaluatiebepaling in artikel 12, derde lid, van het voorstel kan in de eerste plaats worden verwezen naar opmerking 12, waarin wordt aangedrongen op een verkorting van de termijn van zes maanden na de inwerkingtreding van de aan te nemen regeling.

Op de vraag of deze evaluatiebepaling normatief is bedoeld of louter een voornemen inhoudt, antwoordde de hoofdindienster van het voorstel: “Dit is een voornemen.”

Om de redenen die reeds in opmerking 12 zijn uiteengezet, is de evaluatie van de aan te nemen regeling te belangrijk om beperkt te blijven tot een louter voornemen. Dat betekent niet noodzakelijk dat een evaluatiebepaling moet worden opgenomen in deze tekst, maar wel dat die evaluatie daadwerkelijk en liefst sneller dan pas na zes maanden moet plaatsvinden.

*

³² In die zin ook advies nr. 34/2020 van 28 april 2020 van de Gegevensbeschermingsautoriteit, opmerking 41.

³³ Veeleer dan de formulering “is van toepassing tot”.

1. Conformément à l'article 84, § 1^{er}, alinéa 1^{er}, 3^o, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la demande d'avis doit indiquer les motifs qui en justifient le caractère urgent.

En l'occurrence, l'urgence est motivée comme suit :

« - het opsporen van de contacten van besmette personen en het aansporen van deze contacten om de nodige maatregelen te nemen, is cruciaal om nieuwe besmettingshaarden, die de volksgezondheid bedreigen, te voorkomen;

- digitale contactopsporingsapplicaties die op een smartphone worden geïnstalleerd kunnen de gezondheidsdiensten helpen in het monitoren en doorbreken van het aantal besmettingen en de beperkingen van manuele contactopsporing verhelpen;

- dit wetsvoorstel tracht een algemeen juridisch kader te creëren, onder meer om ervoor te zorgen dat op het Belgisch grondgebied slechts één technologische methode van contactopsporingsapplicaties wordt gebruikt ».

*

2. Conformément à l'article 84, § 3, alinéa 1^{er}, des lois coordonnées sur le Conseil d'État, la section de législation a dû se limiter à l'examen de la compétence de l'auteur de l'acte, du fondement juridique¹ et de l'accomplissement des formalités prescrites.

*

PORTÉE DE LA PROPOSITION DE LOI

3. La proposition de loi soumise pour avis a pour objet de créer un cadre légal pour permettre l'utilisation, sur une base volontaire, d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19. Elle détermine les fonctionnalités des applications numériques de traçage de contacts, les modalités et les conditions technologiques relatives à leur utilisation, ainsi que les garanties de protection des droits et libertés fondamentaux des citoyens (article 2 de la proposition).

La proposition définit les finalités du traitement des informations par des applications numériques de traçage de contacts, à savoir la possibilité de confirmer une contamination de l'utilisateur de l'application, prévenir les utilisateurs qu'ils ont été à proximité d'une personne contaminée pendant un certain temps et effectuer des recherches épidémiologiques sur la propagation du COVID-19 (article 4, § 1^{er}). Les informations peuvent également être traitées à des fins archivistiques dans l'intérêt public, de recherche scientifique ou historique, ou statistiques, mais pas à d'autres fins (article 10).

¹ S'agissant d'une proposition de loi, on entend par « fondement juridique » la conformité avec les normes supérieures.

La proposition fixe une série d'exigences en matière de fonctionnalités et de sécurité de ces applications. Les spécifications techniques auxquelles les applications doivent satisfaire doivent être mentionnées sur le site internet du responsable du traitement (article 4, §§ 2 et 3).

Les applications numériques de traçage de contacts doivent exclusivement être installées, utilisées et désinstallées sur une base volontaire (article 5). Sciensano est désignée comme responsable du traitement et doit fournir les informations prescrites à l'utilisateur au moment de l'installation de l'application (article 6).

La proposition détermine les données que les applications numériques de traçage de contacts traitent spécifiquement en vue du dépistage des contacts, les données qui ne peuvent pas être enregistrées, les données qui ne peuvent pas être communiquées à l'utilisateur et les informations que l'utilisateur peut volontairement insérer dans l'application. En ce qui concerne la recherche épidémiologique, l'objectif de l'application est facultatif et l'utilisateur doit expressément confirmer que les informations y relatives peuvent être communiquées à Sciensano (article 7).

Certaines données relatives à l'utilisateur dont la contamination a été constatée sont sauvegardées dans une liste log centrale gérée par Sciensano en vue des deux premiers objectifs précités (article 8, § 1^{er}). D'autres données relatives aux personnes contaminées et aux personnes avec lesquelles elles ont été en contact sont sauvegardées dans une banque de données centrale gérée par Sciensano ; ces données doivent être conservées séparément des données de la liste log précitée et elles ne peuvent pas être interconnectées (article 8, § 2).

La proposition fixe le moment auquel différentes données doivent être effacées dans l'équipement terminal et dans la liste log (article 9, §§ 1^{er} et 2) ainsi que celui auquel les applications numériques de traçage de contacts sont désactivées (article 9, § 3).

Pour le traitement des informations enregistrées dans la liste log et dans la banque de données, le responsable du traitement prévoit une gestion stricte et adéquate des accès et des utilisateurs en utilisant certaines techniques informatiques qui sont énumérées (article 11, § 1^{er}, alinéa 1^{er}). Les informations enregistrées sont conservées pendant trois ans (article 11, § 1^{er}, alinéa 2). Le responsable du traitement prévoit les mesures techniques et organisationnelles nécessaires afin de garantir que les informations conservées dans la liste log et la banque de données ne sont pas interconnectées (article 11, § 2).

La loi à adopter entre en vigueur le jour de sa publication au Moniteur belge et est d'application jusqu'au (lire : cesse d'être en vigueur le) jour de la publication de l'arrêté royal proclamant la fin de l'état d'épidémie du coronavirus COVID-19 (article 12).

COMPÉTENCE

4. La réglementation en projet prévoit un cadre légal pour les fonctionnalités et les spécifications technologiques des applications numériques de traçage de contacts, dans le contexte des mesures de prévention de la propagation du COVID-19. Elle vise à la fois à garantir le fonctionnement adéquat de ces applications numériques de traçage de contacts et à régler le traitement des données à caractère personnel y afférent.

Selon les développements de la proposition, tant le traçage numérique que le traçage manuel des contacts sont d'une importance primordiale pour éviter de nouveaux foyers de contamination qui menacent la santé publique. Le traçage manuel, qui peut notamment être effectué par des call centers ne serait toutefois pas toujours aussi efficace et impliquerait aussi une ingérence importante dans la vie privée. Des applications numériques de traçage de contacts seraient en revanche plus efficaces pour informer la population à temps et impliqueraient également une ingérence plus limitée dans la vie privée. La proposition vise à encadrer l'utilisation de ces applications par des garanties suffisantes et à faire en sorte qu'elles répondent aux exigences en matière de droits fondamentaux, en application des principes *privacy by design*² du règlement général sur la protection des données³ (ci-après : RGPD), de sorte que la technologie inspire une confiance suffisante au citoyen pour qu'il en fasse une utilisation effective, en dépit de son caractère strictement volontaire.

5. L'autorité fédérale est compétente pour fixer des règles générales relatives à la limitation du droit au respect de la vie privée⁴, qui a valeur de réglementation minimale pour toute matière⁵.

Le caractère volontaire des applications numériques de traçage de contacts, réglées dans la réglementation proposée, n'empêche pas que leur utilisation peut constituer une ingérence dans la vie privée et que l'autorité fédérale peut, d'une manière générale, soumettre ces applications à des exigences au regard de la protection de leurs utilisateurs en ce qui concerne le traitement des données à caractère personnel au moyen de ces applications.

² Ce principe implique que le respect des exigences en matière de protection de la vie privée soit garanti en les intégrant dans les applications concernées en tant que mesures techniques et organisationnelles auxquelles ces applications doivent répondre (voir l'article 25 du RGPD, ainsi que son considérant 78).

³ Règlement (UE) n° 2016/679 du Parlement et du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)'.

⁴ C.C., 30 avril 2003, n° 50/2003, B.8.10 et C.C., 30 avril 2003, n° 51/2003, B.4.12.

⁵ C.C., 20 octobre 2004, n° 162/2004, B.5.2 ; C.C., 19 janvier 2005, n° 16/2005, B.5.2 ; C.C., 14 février 2008, n° 15/2008, B.21 ; C.C., 19 juillet 2018, n° 104/2018, B.22.3 ; C.C., 12 mars 2020, n° 43/2020, B.53.6. Voir également l'avis C.E. 61.267/2/AG du 27 juin 2017 sur un avant-projet devenu la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', *Doc. parl.*, Chambre, 2016-17, n° 54-2648/001, pp. 106-116.

Cette compétence fédérale concerne cependant l'élaboration de *règles générales*. L'établissement de règles spécifiques relatives à la protection de personnes physiques lors du traitement de données à caractère personnel concernant une matière communautaire ou régionale spécifique est une compétence de la communauté ou de la région concernée.

6. La réglementation proposée ne prévoit pas de règles générales restreignant le droit au respect de la vie privée dans le cadre du développement et de l'utilisation de toutes sortes d'applications numériques de traçage de contacts. Les applications numériques de traçage de contacts réglées dans la proposition sont expressément et principalement instaurées pour dépister et prévenir les contaminations par le COVID-19, ce qu'expriment l'intitulé et différentes dispositions de la proposition.

Les communautés ⁶ sont cependant compétentes pour le dépistage et la lutte contre les maladies contagieuses et sociales en tant que composante de leurs compétences en matière de médecine préventive ⁷. L'entrée en contact avec des personnes (potentiellement ou présumées) infectées, ainsi qu'avec des personnes et des collectivités avec lesquelles elles ont été en contact, la formulation de recommandations à ces personnes en vue de prévenir d'autres infections et l'imposition de mesures de confinement à ces mêmes personnes peuvent être réputées relever de cette compétence ⁸. Il en va de même pour le traitement ayant la même finalité de données à caractère personnel qui y sont liées ⁹. Sur la base de cette compétence, les communautés ont entre-temps déjà élaboré un certain nombre de réglementations concernant le traçage manuel des contacts ¹⁰.

⁶ En ce qui concerne la Communauté française, l'exercice de cette compétence a été transféré à la Région wallonne et à la Commission communautaire française conformément à l'article 3, 6°, du décret spécial du 3 avril 2014 'relatif aux compétences de la Communauté française dont l'exercice est transféré à la Région wallonne et à la Commission communautaire française' (et aux décrets parallèles de la Région wallonne et de la Commission communautaire française).

⁷ Article 5, § 1^{er}, I, alinéa 1^{er}, 8°, de la loi spéciale du 8 août 1980 'de réformes institutionnelles'. Voir également *Doc. parl.*, Sénat, 1979-80, n° 434/2, p. 125 et *Doc. parl.*, Chambre, 1979-80, n° 627/10, p. 52. Cette compétence a été implicitement confirmée dans l'avis C.E. 34.339/AG du 29 avril 2003 sur un avant-projet devenu le décret de la Communauté flamande et de la Région flamande du 21 novembre 2003 'betreffende het preventieve gezondheidsbeleid', *Doc. parl.*, Parl. fl., 2002-03, n° 1709/1, pp. 147-155, ainsi que expressément dans les avis C.E. 38.381/3 du 7 juillet 2005 sur un projet d'arrêté royal 'établissant les mesures prophylactiques et la déclaration obligatoire à la cellule de vigilance sanitaire de pathologies présentant un caractère épidémique' et C.E. 53.018/VR du 13 mai 2013 sur un projet d'arrêté royal 'relatif au contrôle sanitaire du trafic international'.

⁸ La compétence réservée à l'autorité fédérale concernant « les mesures prophylactiques nationales » ne porte pas atteinte à cette compétence communautaire, dès lors qu'elle est limitée aux vaccinations obligatoires (avis C.E. 58.118/3 du 28 septembre 2015 sur un avant-projet devenu l'ordonnance du 18 décembre 2015 'portant assentiment à l'accord de coopération entre la Communauté française (ONE), la Commission communautaire commune et la Communauté germanophone relatif à l'achat de vaccins destinés à protéger les enfants, les femmes enceintes et les adolescents', *Doc. parl.*, Ass. réun., Comm. comm. comm., 2015-16, n° B-41/1, pp. 5-6).

⁹ Voir les arrêts de la Cour constitutionnelle cités dans les notes 4 et 5. Voir également l'avis C.E. 67.407/3 du 20 mai 2020 sur un projet d'arrêté du Collège réuni de la Commission communautaire commune n° 2020/006 'organisant le suivi sanitaire des contacts dans le cadre de la lutte contre la pandémie COVID-19', observation 4.1 ; l'avis C.E. 67.412/3 du 25 mai 2020 sur un avant-projet de décret de la Communauté germanophone 'über die Rückverfolgung von Infektionsketten im Rahmen der Bekämpfung der Coronavirus (COVID-19) Gesundheitskrise', observation 4.1.

¹⁰ Voir le décret de la Communauté flamande du 8 mai 2020 'tot organisatie van contactonderzoek in het kader van COVID-19' et l'arrêté du Gouvernement wallon n° 35 du 5 mai 2020 'organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID-19', ainsi que le projet d'arrêté du Collège réuni de la Commission

Comme le reconnaissent les développements de la proposition de loi soumise pour avis¹¹, le développement des applications numériques de traçage de contacts qui visent spécifiquement à dépister les contaminations par le COVID-19 relève de la compétence des communautés. Cette compétence comporte la mise en place d'une réglementation visant à protéger les personnes physiques lors du traitement des données à caractère personnel dans le cadre du développement et de l'utilisation de ces applications.

Dans la mesure où la proposition de loi soumise pour avis règle spécifiquement des applications numériques de traçage de contacts visant à dépister des contaminations par le COVID-19, elle empiète dès lors sur la compétence communautaire en matière de médecine préventive.

7. Selon l'article 4, § 1^{er}, troisième tiret, de la proposition, les applications numériques de traçage de contacts visent également à « effectuer des recherches épidémiologiques sur la propagation du COVID-19 sur [la] base de données anonymisées », ce qui peut s'inscrire dans les compétences fédérales en matière de recherche scientifique¹². À cet égard, cette disposition se rattache aux activités de surveillance dont Sciensano est chargée par l'article 4 de la loi du 25 février 2018 'portant création de Sciensano'.

8. En conclusion, la proposition de loi concerne à la fois des compétences fédérales et des compétences communautaires.

Dans sa forme actuelle, la proposition de loi soumise pour avis ne peut se concrétiser que si elle est transformée en un accord de coopération pour lequel l'assentiment parlementaire est requis. Cet accord pourrait en effet lier les Belges individuellement et il concerne des matières qui - eu égard au principe de légalité inscrit à l'article 22 de la Constitution - doivent être réglées par la loi¹³. Pareil accord de coopération offre au demeurant la meilleure sécurité juridique.

On pourrait également envisager de refondre la proposition en une réglementation générale du traitement des données à caractère personnel lors de l'utilisation des applications numériques de traçage de contacts. Dans la mesure où cette réglementation comporte alors les éléments essentiels qui, conformément à l'article 22 de la Constitution, doivent être réglés dans une norme législative, les aspects de la réglementation proposée qui concernent spécifiquement le dépistage des contaminations par le COVID-19 peuvent être inscrits dans un accord de coopération administratif conclu entre l'autorité fédérale et les communautés, pour lequel l'assentiment parlementaire n'est pas requis.

communautaire commune n° 2020/006 et l'avant-projet de décret de la Communauté germanophone, mentionnés dans la note précédente.

¹¹ *Doc. parl.*, Chambre, 2019-20, n° 55-1251/001, p. 6.

¹² Article 6*bis*, §§ 2 et 3, de la loi spéciale du 8 août 1980.

¹³ Voir l'article 92*bis*, § 1^{er}, alinéa 2, de la loi spéciale du 8 août 1980.

FORMALITÉS

9. La proposition contient des dispositions qui règlent le traitement des données à caractère personnel. L'article 36, paragraphe 4, du RGPD, combiné avec l'article 7, paragraphe 1, c), et le considérant 96 de ce règlement, impose l'obligation de consulter l'autorité de contrôle, en l'occurrence l'Autorité de protection des données visée dans la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.

L'Autorité de protection des données a certes déjà donné l'avis n° 34/2020 du 28 avril 2020 sur un projet d'arrêté royal 'n° XXX portant exécution de l'article 5, § 1^{er}, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population'¹⁴.

Le Conseil d'État ne dispose pas du projet d'arrêté royal qui a été soumis à l'Autorité de protection des données et n'est dès lors pas à même de vérifier dans quelle mesure la proposition de loi qui lui a été soumise pour avis a été adaptée pour rencontrer les observations formulées dans l'avis de l'Autorité de protection des données. Il ne peut pas non plus vérifier si de nouvelles dispositions n'ont pas été ajoutées par rapport à ce projet. Ce n'est que dans la mesure où la proposition de loi se borne à reproduire ce projet d'arrêté royal et les adaptations apportées résultent uniquement des observations formulées par l'Autorité de protection des données que l'on peut considérer que celle-ci ne doit pas de nouveau être consultée.

10. Un certain nombre de dispositions de la proposition doivent être considérées comme des règles techniques au sens de l'article premier, paragraphe 1, f), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 'prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information', plus particulièrement comme des règles relatives aux services de la société de l'information au sens de l'article premier, paragraphe 1, e), de cette directive.

¹⁴ Voir <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/AV34-2020.pdf>

Conformément à l'article 5 de la directive (UE) 2015/1535, de telles règles techniques doivent être notifiées à la Commission européenne. Dans ce cas, un délai d'attente de trois mois (au moins) s'applique avant que la proposition de loi puisse être adoptée, conformément à l'article 6 de la directive. Toutefois, conformément à l'article 6, paragraphe 7, ce délai d'attente ne s'applique pas lorsqu'un État membre, pour des raisons urgentes tenant à une situation grave et imprévisible qui a trait à la protection (notamment) de la santé des personnes, doit élaborer à très bref délai des règles techniques pour les arrêter et les mettre en vigueur aussitôt, sans qu'une consultation soit possible. Dans ce cas, la communication à la Commission est toujours requise ; la communication doit mentionner le motif qui justifie l'urgence. La Commission se prononce ensuite sur la communication dans les plus brefs délais.

Par conséquent, la proposition doit être notifiée à la Commission européenne, l'urgence de son adoption pouvant alors être exposée pour justifier le non-respect du délai d'attente prescrit.

11. Enfin, la question se pose de savoir si la réglementation proposée relève du champ d'application de la directive « services »¹⁵. La mise à disposition d'une application numérique de traçage de contacts doit être considérée comme un service, qui peut éventuellement être fourni contre rémunération, que cette rémunération émane de l'autorité ou – éventuellement par voie de recettes publicitaires – de l'utilisateur. La proposition de loi ne garantit nullement que les applications sont proposées en tant que service non économique d'intérêt général¹⁶. L'exception pour les services de soins de santé¹⁷ ne peut pas non plus être invoquée, dès lors que les applications ne concernent pas des activités réservées à une profession de santé réglementée dans l'État membre où le service est fourni¹⁸.

Il est dès lors possible que la directive « services » s'applique¹⁹, de sorte que la proposition doit être examinée au regard des articles 14 et 15 de cette directive en ce qui concerne les exigences prévues pour l'exercice d'une activité de service sur le territoire de la Belgique²⁰. À première vue, la proposition ne semble pas contenir d'exigences interdites au sens de l'article 14, ni d'exigences non discriminatoires au sens de l'article 15, paragraphe 2. Le Conseil d'État ne dispose toutefois pas de l'expertise requise concernant les exigences spécifiques relatives aux applications numériques de traçage de contacts pour pouvoir apprécier ce point de manière concluante. Le cas échéant, une notification à la Commission européenne, conformément à l'article 15, paragraphe 7, de la directive « services » pourrait néanmoins encore être requise.

¹⁵ Directive n° 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 'relative aux services dans le marché intérieur'.

¹⁶ Voir l'article 2, paragraphe 2, a), de la directive « services ».

¹⁷ Voir l'article 2, paragraphe 2, f), de la directive « services ».

¹⁸ *Manuel relatif à la mise en œuvre de la directive « services »*, Commission européenne, 2007, p. 12. Voir également le considérant 22 de la directive « services ».

¹⁹ Les motifs d'exception prévus à l'article 2, paragraphe 2, c) et i), ne semblent en tout cas pas non plus s'appliquer en l'espèce.

²⁰ Puisqu'un régime d'autorisation n'est en effet pas prévu, il n'y a pas lieu d'effectuer un contrôle au regard des articles 9 à 13 de la directive « services ».

OBSERVATIONS GÉNÉRALES

12. Eu égard au caractère volontaire des applications numériques de traçage de contacts, leur efficacité dépendra d'un taux de couverture suffisamment élevé, en d'autres termes du nombre de citoyens qui utiliseront l'application²¹. Ce taux de couverture déterminera la mesure dans laquelle les applications pourront effectivement jouer un rôle complémentaire, à côté du traçage manuel de contacts mis en œuvre par les communautés. Par ailleurs, il faut également tenir compte du traitement à grande échelle de données à caractère personnel, qui accompagne l'utilisation de ces applications. En effet, conformément à l'article 5, paragraphe 1, c), du RGPD, ce traitement doit être limité à ce qui est nécessaire pour les objectifs visés. Il importe donc de concilier le principe de nécessité avec un taux de couverture suffisamment élevé.

À ce sujet, l'auteure principale de la proposition a déclaré ce qui suit :

« Het gebruik van een contactopsporingsapplicatie kan niet beschouwd worden als de ultieme en allesomvattende oplossing voor het terugdringen van COVID-19 besmettingen. Inderdaad, niet iedereen beschikt over een smartphone en zij die dat wel doen zullen misschien niet allemaal de contactopsporingsapplicatie gebruiken. Dat neemt niet weg dat een app complementair werkt ten opzichte van manuele tracing en enkele van de gebreken van manuele tracing oplost (in het bijzonder de moeilijkheid voor een persoon om zich alle (korte) contacten te herinneren die hij/zij binnen een bepaalde periode heeft gehad, laat staan om voor al die personen contactgegevens te kunnen bezorgen).

Het wetsvoorstel gaat uit van het gebruik van Bluetooth technologie vermits er gewerkt wordt met proximateitsdata en niet geolokalisatiedata op basis van GPS. Het gebruik van exacte lokalisatiegegevens is echter veel meer privacy-intrusief en wordt niet ondersteund op Europees niveau. (...)

(...)

Dit is een vraag die zeer complex is en waarop met de huidige stand van zaken van de wetenschap geen eenvoudig antwoord kan geformuleerd worden. Ten eerste hangt dit af van hoe dekkingsgraad juist gedefinieerd is: een mogelijk definitie is of men kan bepalen met een voldoende nauwkeurigheid of persoon A voldoende lang voldoende dicht bij persoon B is geweest? Hierbij kan men twee soorten fouten maken: het kan zijn dat een persoon A toch voldoende dicht en voldoende lang bij persoon B geweest is, maar dat dit niet blijkt uit de Bluetooth metingen (vals negatief) of dat persoon A niet voldoende lang en voldoende dicht bij persoon B geweest is, terwijl Bluetooth metingen het tegendeel aangeven (vals positief). In de voorbije maanden zijn er al een groot aantal experimenten geweest, die aangeven dat men de parameters zo kan instellen dat de valse negatieve en valse positieve waarden aanvaardbaar zijn (het gaat om een trade-off waarbij het vergroten van valse negatieven leidt tot verkleinen van valse positieven en omgekeerd). Maar dit volstaat niet om te weten of de app effectief is: empirische resultaten wijzen uit dat slechts 1 op de 20 risicovolle contacten toch leidt tot een besmetting. Dus zelfs als men heel accuraat alle risicovolle contacten in kaart kan brengen, zal het aantal daadwerkelijk besmette mensen niet nauwkeurig bepaald kunnen worden. Men weet daarnaast ook niet exact hoe de kans op besmetting varieert als functie

²¹ Voir <https://ukhumanrightsblog.com/2020/05/01/what-are-the-data-privacy-considerations-of-contact-tracing-apps/>. Voir également *Doc. parl.*, Chambre, 2019-20, n°55-1251/001, p. 4 : « L'efficacité d'une application de traçage de contacts est exponentiellement proportionnelle [au] nombre de personnes qui installent et activent cette même application ».

van duur en afstand van het contact; dit hangt af van een groot aantal parameters die moeilijk te meten zijn zoals windrichting en luchtvochtigheid. Maar deze onzekerheid betekent absoluut niet dat de app niet effectief zou zijn.

De impact van de app hangt ook af van de fractie van de bevolking die de app daadwerkelijk gebruikt. Er zijn een aantal modellen opgesteld, die uiteenlopende resultaten geven. Sommige modellen geven aan dat minstens 60% van de bevolking de app zou moeten gebruiken om een impact te hebben op de COVID-19 epidemie. Maar dergelijke modellen steunen op een groot aantal aannames. Zo zou het kunnen zijn dat de app wel degelijk effectief is met een gebruik van 20% als 80% van de 20-jarigen de app gebruikt en slechts 10% van de oudere bevolkingsgroepen.

Vragen over de dekkingsgraad en nauwkeurigheid kunnen ook gesteld worden bij manueel contact tracing: mensen weten niet meer exact met wie ze voldoende lang in contact geweest zijn, of ze zijn niet bereid om die informatie te geven. Het kan ook zijn dat men bijvoorbeeld op het openbaar vervoer vrij langdurig dicht bij een persoon heeft gezeten, terwijl men de naam of contactinformatie van die persoon niet kent. Dus ook hier heeft men valse negatieven en valse positieven. De twee soorten van contactopsporing moeten als complementair beschouwd worden.

Epidemiologen zijn het erover eens dat contactopsporing essentieel is om een epidemie onder controle te brengen. Contactopsporing moet ook niet 99% accuraat zijn om voldoende impact te hebben. Omwille van technologische beperkingen kon contactopsporing tot op heden alleen manueel gebeuren en was er geen andere keuze. Op basis van de huidige stand van zaken van de wetenschap zijn er goede indicaties dat een contactopsporingsapp wel degelijk kan werken, complementair aan manuele contactopsporing. Als een contactopsporingsapp ontworpen is volgens de principes van 'privacy by design' (zoals voorgesteld), is ze minder intrusief dan manuele contactopsporing. Als toch zou blijken dat de app helemaal niet effectief is, kan ze gemakkelijk gestopt worden. Gezien de uitzonderlijke situatie, lijkt de app wel degelijk noodzakelijk te zijn en te voldoen aan de voorwaarden dat ze een minimale inmenging vormt ».

Vu la rapidité avec laquelle le cadre législatif doit être mis en place, il peut être admis qu'une analyse d'impact préalable de la réglementation proposée n'est pas réalisable²². L'article 12, alinéa 3, de la proposition prévoit une évaluation de la réglementation proposée, notamment en ce qui concerne l'efficacité, à savoir six mois après l'entrée en vigueur de la réglementation à adopter. Dès lors qu'il s'agit en l'occurrence d'une nouvelle technologie et eu égard à l'importance d'un suivi minutieux de la mise en balance précitée entre un taux de couverture suffisamment élevé et le principe de nécessité du traitement de données à caractère personnel accompagnant les applications²³, il est conseillé d'avancer le moment de cette évaluation et, le cas échéant, de prévoir des évaluations répétées ou même un mécanisme de suivi permanent.

²² Le Conseil d'État est conscient que dans le cadre de la 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', adoptée par la commission de la chambre compétente, des audiences et une discussion circonstanciée ont déjà eu lieu (*Doc. parl.*, Chambre, 2019-20, n^{os} 55-1182/005 et 55-1182/006). Toutefois, il ressort également de cette discussion que les preuves scientifiques concernant le taux de couverture réalisable et requis dont on dispose à l'heure actuelle sont insuffisantes.

²³ Voir également à propos de ce dernier élément <https://www.ejiltalk.org/contact-tracing-apps-and-human-rights/>.

À cet égard, il faut également relever l'analyse d'impact relative à la protection des données que le responsable du traitement doit effectuer avant le début des activités de traitement, conformément à l'article 35 du RGPD, « [l]orsqu'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 ». Tel est également le cas en l'espèce²⁴, de sorte que cette analyse d'impact relative à la protection des données devra de toute façon être effectuée, outre l'évaluation précitée de la réglementation à adopter proprement dite.

13. L'article 6, § 2, de la proposition dispose qu'au moment de l'installation d'une application numérique de traçage de contacts, le responsable du traitement doit fournir à l'utilisateur les informations prévues à l'article 13 du RGPD. L'article 7, § 5, de la proposition prévoit que l'objectif de l'application en ce qui concerne la recherche scientifique²⁵ (et le traitement des données à caractère personnel y afférent, visé à l'article 8, § 2, de la proposition) est optionnel et que l'utilisateur doit confirmer explicitement que ces données à caractère personnel peuvent être communiquées au responsable du traitement.

L'impact sur la vie privée du traitement complémentaire optionnel des données à caractère personnel en vue de la recherche scientifique est nettement plus important que celui du simple traçage de contacts. Cette constatation ressort tant de la circonstance que ces données sont traitées dans une banque de données centrale plutôt que dans un système décentralisé comme pour le traçage de contacts, que de la nature plus sensible des données à caractère personnel qui sont sauvegardées dans cette banque de données centrale.

Il est dès lors conseillé de compléter soit l'article 6, § 2, soit l'article 7, § 5, par l'obligation plus spécifique de fournir des informations simples et compréhensibles pour l'utilisateur sur les finalités des deux types de traitement des données et du traitement des données à caractère personnel y relatif, en permettant ensuite l'accès à une information plus détaillée, par exemple sur le site internet de Sciensano²⁶. Par ailleurs, la différence entre ces deux types de traitement des données devrait être clairement exposée. Ce faisant, les exigences en matière d'informations contenues à l'article 12 du RGPD seraient également mieux rencontrées.

14. La proposition ne prévoit nulle part qui a accès à la banque de données centrale visée à l'article 8, § 2, en vue de la recherche scientifique, pas même l'article 11, § 1^{er}, qui concerne la gestion des accès et des utilisateurs. À ce propos, l'auteure principale de la proposition a déclaré ce qui suit :

²⁴ Voir en ce sens également l'avis n° 34/2020 du 28 avril 2020 de l'Autorité de protection des données, observations 23 et 48.

²⁵ Voir l'article 4, § 1^{er}, troisième tiret, de la proposition.

²⁶ Voir en ce sens également l'avis n° 34/2020 de l'Autorité de protection des données du 28 avril 2020, observation 24.

« Het wetsvoorstel voorziet niet uitdrukkelijk in de opsomming van de departementen of personen binnen Sciensano die toegang krijgen tot de loglijst en de databank. Dit is ook niet noodzakelijk en wordt nooit vereist door de Gegevensbeschermingsautoriteit. Sciensano dient echter een toegangs- en gebruiksbeheer op te zetten op basis van gebruikersprofielen. De toegang en het gebruik van de loglijst en databank worden ook geregistreerd en deze gegevens zijn toegankelijk zowel voor de gegevensbeschermingsfunctionaris van Sciensano alsook voor de Gegevensbeschermingsautoriteit.

De gemeenschappen en gewesten beschikken op basis van dit wetsvoorstel niet over de mogelijkheid om toegang te krijgen tot de loglijst en de databank ».

Il se déduit de l'avis de l'Autorité de protection des données que le texte qui lui a été soumis comportait des dispositions relatives à l'accès aux données de la liste log centrale et de la banque de données centrale, et à leur communication, à savoir l'interdiction de communiquer les données sauvegardées dans la liste log centrale à des tiers et la possibilité de consulter la banque de données centrale par les « autorités compétentes des régions [lire : des communautés] ». L'Autorité de protection des données recommandait précisément de clarifier encore ces dispositions²⁷. Si l'intention est effectivement de n'accorder l'accès à la liste log centrale et à la banque de données centrale à aucune instance autre que (les départements ou les membres du personnel de) Sciensano, il vaudrait mieux le mentionner expressément. Dans le cas contraire, il faut prévoir quelles instances peuvent effectivement y avoir accès, conformément à l'article 11, § 1^{er}, de la proposition.

EXAMEN DU TEXTE

Article 2

15.1. L'article 2, alinéa 2, de la proposition ne contient pas de disposition normative et doit être omis.

15.2. L'alinéa 1^{er} est quant à lui formulé de manière trop vague : s'il s'agit effectivement de *permettre* l'utilisation d'applications numériques de traçage de contacts pour les objectifs visés à l'article 4, § 1^{er}, l'on vise aussi implicitement à interdire l'utilisation pour ces objectifs d'applications numériques de traçage de contacts, qui ne sont pas conformes aux dispositions de la proposition, du moins pour la période d'application de la réglementation à adopter. Il conviendrait de le prévoir expressément.

²⁷ Avis n° 34/2020 du 28 avril 2020, observations 39 et 40.

En outre se pose la question de savoir comment assurer le respect des mesures précitées. Mieux vaut sans doute prévoir des sanctions administratives ou pénales pour la mise à disposition d'applications non conformes.

Article 4

16. L'article 4, § 3, de la proposition dispose que le site du responsable du traitement mentionne les spécifications techniques auxquelles les applications numériques de traçage de contacts doivent satisfaire.

S'il agit ainsi de publier sur le site Internet de Sciensano les conditions inscrites dans la réglementation proposée, rien ne s'y oppose, à condition que la reproduction de celles-ci soit conforme à cette réglementation.

Si l'intention est par contre que Sciensano puisse rédiger et publier des spécifications techniques *supplémentaires* auxquelles ces applications doivent satisfaire, un pouvoir réglementaire est octroyé à Sciensano. L'attribution d'un pouvoir réglementaire à un organisme public, comme Sciensano, n'est en principe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique²⁸.

²⁸ Comparer avec les critères d'évaluation qu'utilise la Cour constitutionnelle pour apprécier les délégations de pouvoir réglementaire par le législateur à une autorité administrative autonome ou à un organisme public décentralisé; voir C.C., 11 juin 2015, n° 86/2015, B.22.4 et C.C., 9 juin 2016, n° 89/2016, B.9.6.4 : « Les articles 33, 105 et 108 de la Constitution ne s'opposent pas à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome soumise tant au contrôle juridictionnel qu'au contrôle parlementaire et n'interdisent pas au législateur d'accorder des délégations à un organe exécutif, pour autant qu'elles portent sur l'exécution de mesures dont le législateur compétent a déterminé l'objet, en particulier dans les matières techniques et complexes »; voir C.C., 9 novembre 2015, n° 162/2015, B.8.4 : « L'article 33 de la Constitution et l'article 20 de la loi spéciale du 8 août 1980 [de réformes institutionnelles] ne s'opposent pas à ce que le législateur confie des compétences exécutives spécifiques à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel ».

Article 5

17. L'article 5, alinéa 1^{er}, de la proposition dispose que l'installation, l'utilisation et la désinstallation d'une application numérique de traçage de contacts se fait uniquement sur une base volontaire. La question se pose toutefois de savoir si cette disposition, dans sa formulation générale, tient compte suffisamment de l'article 8 du RGPD, qui fixe des conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information et qui prescrit que pour les enfants âgés de moins de 16 ans (ou qui éventuellement ne sont pas âgés de moins de 13 ans)²⁹, le consentement doit être donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Compte tenu des moyens technologiques disponibles, le responsable du traitement doit raisonnablement s'efforcer de vérifier que ce consentement requis est donné (ou autorisé). Bien que la disposition réglementaire précitée soit directement applicable et qu'elle soit dès lors contraignante pour le responsable du traitement, il peut néanmoins être envisagé de compléter la proposition de loi par des dispositions qui concrétisent cette obligation pour l'application concernée.

18. Aux termes de l'article 5, alinéa 2, de la proposition, l'installation ou la non-installation, l'utilisation ou la non-utilisation et la désinstallation ou la non-désinstallation d'une application numérique de traçage de contacts ne peut en aucun cas donner lieu à une mesure civile ou pénale, à quelque action discriminatoire ou à quelque avantage ou désavantage. À la question de savoir quelle est la portée des termes « quelque avantage ou désavantage », l'auteure principale de la proposition a répondu comme suit :

« Deze bepaling werd toegevoegd op vraag van de Gegevensbeschermingsautoriteit. De GBA benadrukte dat het weigeren van het gebruiken van een contactsporsingsapplicatie niet tot enig nadeel zou mogen leiden. Omgekeerd echter mag de keuze voor het gebruiken van een applicatie ook niet tot enig voordeel leiden. Het betreft dus een bepaling vanuit de bezorgdheid dat er geen discriminerende handelingen, in positieve en negatieve zin zouden mogen plaatsvinden. Een nadere beschrijving van een voordeel of nadeel is echter moeilijk aangezien de brede waaier van mogelijke toepassingen in de praktijk. De casuïstiek zal dit moeten uitwijzen ».

En outre, les développements de la proposition précisent que la suggestion de l'Autorité de protection des données de prévoir des sanctions civiles, administratives ou pénales pour les personnes qui lieraient l'accès à un bien ou à un service à l'utilisation des applications³⁰ n'est pas suivie et que l'on prévoira des campagnes de promotion pour encourager l'utilisation des applications³¹.

²⁹ Si l'on choisit d'appliquer un âge inférieur à 16 ans, conformément à l'article 8, paragraphe 1, deuxième alinéa, du RGPD.

³⁰ Avis n° 34/2020 de l'Autorité de protection des données du 28 avril 2020, observation 21.

³¹ *Doc. parl.*, Chambre, 2019-20, n° 55-1251/001, p. 11.

Il est probablement impossible de définir de manière concluante les termes « quelconque avantage ou désavantage » dans le texte de la proposition même, mais il n'en demeure pas moins que sur la base du texte actuel et de ses développements, on n'aperçoit pas clairement si, par exemple, l'application peut être liée à d'autres applications intéressantes pour l'utilisateur ou si certaines réductions peuvent être associées à l'utilisation de l'application, etc. Il est dès lors conseillé de développer quelque peu la casuistique dans le cadre des débats parlementaires.

Article 9

19. L'article 9, § 3, alinéa 2, de la proposition dispose que la désactivation des applications numériques de traçage de contacts ne doit pas dépendre de la désinstallation par l'utilisateur. Cette disposition n'est pas très claire. Si elle signifie que l'application est désactivée le jour mentionné à l'alinéa 1^{er}, même si un utilisateur ne désinstalle l'application qu'ultérieurement, mieux vaut le prévoir explicitement.

Article 11

20. L'article 11, § 1^{er}, alinéa 2, de la proposition prévoit que les informations enregistrées sont sauvegardés pendant trois ans. À la question de savoir pourquoi l'on opte pour une durée de conservation de trois ans, l'auteure principale de la proposition a répondu :

« Dit is noodzakelijk om inbreuken op de toegangsregels achteraf nog te kunnen vaststellen ».

On peut se demander si un tel délai suffit au vu de la nature pénale des peines attachées à l'accès non autorisé aux données et du délai de prescription pour ce type d'infractions³².

Article 12

21. L'article 12, alinéa 2, de la proposition concerne la fin de vigueur³³ de la réglementation à adopter. Si l'on opte pour un accord de coopération législatif conformément à l'observation 8, alinéa 2, il faudra prévoir un régime de fin de vigueur adapté, qui ne pourra alors pas être subordonné à l'adoption d'un arrêté royal. Il conviendra dans ce cas d'opter pour un autre dispositif de fin de vigueur, qui sera juridiquement sûr et connu de tous les citoyens.

³² Voir en ce sens également l'avis n° 34/2020 de l'Autorité de protection des données du 28 avril 2020, observation 41.

³³ Plutôt que la formulation « est d'application jusqu'au ».

22. En tout état de cause, le Conseil d'État estime qu'il est concevable – et peut-être même souhaitable – de différencier la fin de vigueur de la réglementation à adopter. Ainsi, les articles 6, § 1^{er}, 10 et 11 de la proposition, notamment, pourraient se voir attribuer une durée de validité plus longue.

23. En ce qui concerne le système d'évaluation prévu à l'article 12, alinéa 3, de la proposition, il peut être renvoyé en premier lieu à l'observation 12, qui recommande de raccourcir le délai de six mois après l'entrée en vigueur de la réglementation à adopter.

À la question de savoir si ce système d'évaluation a un caractère normatif ou s'il s'agit seulement d'une intention, l'auteure principale de la proposition a répondu : « Dit is een voornemen ».

Pour les motifs déjà invoqués dans l'observation 12, l'évaluation de la réglementation à adopter est trop importante pour qu'elle soit limitée à une simple intention. Cela ne signifie pas nécessairement qu'un système d'évaluation doit être inscrit dans le texte même, mais que cette évaluation doit effectivement avoir lieu, et de préférence dans un délai plus court que six mois.

DE GRIFFIER - LE GREFFIER

DE VOORZITTER - LE PRÉSIDENT

Annemie GOOSSENS

Jo BAERT