7-189/1

SÉNAT DE BELGIQUE

SESSION DE 2019-2020

9 OCTOBRE 2020

Proposition de résolution relative à la conformité des mesures de suivi des contacts prises dans le cadre de la lutte contre le coronavirus avec les normes internationales en matière de traitement des données à caractère personnel

(Déposée par M. Rik Daems et consorts)

DÉVELOPPEMENTS

Le suivi des contacts (*contact tracing*) est une mesure importante à mettre en œuvre afin de réduire le taux de contamination au coronavirus. Lorsque des personnes ont été en contact avec une personne dont la contamination par le virus a été établie par un test, elles en sont informées. Elles peuvent alors se mettre spontanément en quarantaine. Ce suivi des contacts s'effectue fréquemment à l'aide d'applications qui évoquent parfois *Big Brother* et qui suscitent une vive controverse sociétale et politique. Leurs défenseurs y voient un moyen efficace de mettre en lumière et d'arrêter la propagation du coronavirus alors que leurs adversaires s'inquiètent surtout de la manière dont elles traitent nos données à caractère personnel. Pour autant qu'il soit correct, c'est-à-dire conforme aux normes internationales, le traitement des données à caractère personnel ne saurait être un obstacle au développement de telles applications.

C'est la société Devside qui développe l'application «corona» belge. Elle a été désignée par le Comité interfédéral belge *Testing & Tracing*. Concrètement, la Belgique reçoit le code source de l'Allemagne qu'il suffit d'adapter au système de santé belge. La partie *back-end* de l'application, c'est-à-dire les serveurs centraux avec lesquels communique l'application, est fournie par l'entreprise Ixor. Lorsqu'un patient présente les symptômes du coronavirus, le code généré de manière aléatoire est enregistré à un niveau central. L'application assure elle-même le suivi des contacts au moyen de la

BELGISCHE SENAAT

ZITTING 2019-2020

9 OKTOBER 2020

Voorstel van resolutie over de overeenstemming van de contactopsporingsmaatregelen in de strijd tegen het coronavirus met de internationale normen met betrekking tot de verwerking van persoonsgegevens

(Ingediend door de heer Rik Daems c.s.)

TOELICHTING

Om de besmettingsgraad van het coronavirus in te dijken, is de zogenaamde *«contact tracing»* een belangrijke stap. Mensen worden ingelicht wanneer ze met iemand in contact zijn gekomen die positief heeft getest op de aanwezigheid van het virus. Zij kunnen zichzelf dan in quarantaine plaatsen. Vaak gebeurt deze *contact tracing* via apps die soms een hoog bigbrothergehalte hebben. Dergelijke apps leiden tot een sterke maatschappelijke en politieke discussie. Voorstanders van dergelijke applicaties zien er een belangrijk hulpmiddel in om de verdere verspreiding van het coronavirus in kaart te brengen en te stoppen, tegenstanders kijken dan vooral naar de manier waarop ze omgaan met onze persoonlijke gegevens. De verwerking van persoonsgegevens mag geen obstakel vormen voor het bouwen van zo'n app als de verwerking van persoonsgegevens juist gebeurt, dat wil zeggen in overeenstemming met internationale normen.

De Belgische corona-app wordt gebouwd door het bedrijf Devside. Dat bedrijf werd aangewezen door het Belgische Interfederaal Comité voor *Testing & Tracing*. Concreet krijgt België de broncode van Duitsland en moet die enkel nog aangepast worden aan het Belgische gezondheidssysteem. Het bedrijf Ixor zal de *backend* van de app verzorgen, zijnde de centrale servers waarmee de app communiceert. Wanneer een patiënt coronasymptomen vertoont wordt de willekeurig gegenereerde code centraal opgeslagen. De app zelf maakt de *contact tracing* mogelijk via bluetooth. De Duitse applicatie

technologie bluetooth. L'application allemande utilise le protocole *Decentralized Privacy Preserving Proximity Tracing* (protocole DP3T) basé sur l'interface de programmation applicative (*application programming interface* – API) de Google et d'Apple.

Toutes les mesures relatives au traitement automatisé des données à caractère personnel, parmi lesquelles les applications de suivi de contacts pour smartphone (en cas de suspicion de contamination), doivent être tout à fait conformes aux normes énoncées dans la Convention 108 (et éventuellement la Convention 108+) du Conseil de l'Europe, ainsi qu'à la recommandation CM/Rec (2020)1 du Comité des ministres du Conseil de l'Europe. Lorsqu'il s'agit d'appliquer des systèmes d'intelligence artificielle, il est possible de solliciter l'accompagnement spécialisé d'organes tels que le Comité consultatif de la Convention 108.

Il est capital que les mesures prises par les autorités nationales (en l'espèce, la Belgique) soient conformes aux lignes directrices émises dans les Conventions 108 et 108+ afin de garantir les libertés individuelles.

Concrètement, pour être conformes aux normes internationales, toutes les mesures (nationales) prises devront se conformer aux recommandations suivantes:

– les personnes concernées doivent être informées du traitement de leurs données personnelles;

– les données à caractère personnel ne peuvent être traitées que pour autant que cela soit nécessaire et proportionné à la finalité légitime, déterminée et explicite poursuivie;

– le traitement des données doit être précédé d'un examen de son impact potentiel;

– la protection des données personnelles est garantie dès la conception (*privacy by design*) et des mesures appropriées sont prises afin de garantir la sécurité des données. La recommandation CM/Rec (2019)2 du Comité des ministres en matière de protection des données relatives à la santé donne des orientations spécifiques en la matière;

– les personnes concernées peuvent exercer leurs droits, notamment celui de corriger les données conservées à leur sujet et d'introduire un recours en cas de violations supposées de ces droits;

– le principe de la légitimité est respecté, ce qui implique que:

maakt gebruik van het *Decentralized Privacy Preserving Proximty Tracingprotocol* (DP3T-protocol), waarbij de *application programming interface* (API) van Google en Apple als basis dient.

Alle maatregelen met betrekking tot geautomatiseerde verwerking van persoonsgegevens, waaronder smartphoneapplicaties voor het opsporen van contacten (bij vermoeden van besmetting) moeten volledig in overeenstemming zijn met de normen van Verdrag 108 (en waar relevant, Verdrag 108+) van de Raad van Europa, samen met de Aanbeveling CM/Rec (2020) 1 van het Comité van ministers van de Raad van Europa. Bij toepassing van kunstmatige intelligentiesystemen, kan gebruikt worden gemaakt van de deskundige begeleiding van organen zoals het Raadgevend Comité van Verdrag 108.

Het is belangrijk dat de maatregelen van nationale overheden (*in casu* België) in overeenstemming zijn met de richtlijnen uitgeschreven in Verdrag 108 en 108+ om de vrijheden van individuen te verzekeren.

Concreet wil de overeenstemming met internationale normen zeggen dat alle genomen (nationale) maatregelen volgende aanbevelingen moeten volgen:

– betrokkenen moeten geïnformeerd worden over de verwerking van hun persoonlijke gegevens;

– persoonsgegevens worden alleen verwerkt voor zover dat nodig is en dit in verhouding staat tot het expliciete, gespecificeerde en legitieme doel dat wordt nagestreefd;

– er wordt een effectbeoordeling uitgevoerd voordat de gegevensverwerking begint;

– «*privacy by design*» is gegarandeerd en er worden passende maatregelen genomen om de veiligheid van gegevens te beschermen. CM/Rec (2019) 2 over de bescherming van gezondheidsgerelateerde gegevens van de aanbeveling van het Comité van ministers geven in dit verband specifieke richtlijnen;

– betrokkenen hebben het recht om hun rechten uit te oefenen, onder meer om de gegevens die over hen worden bewaard te corrigeren en om verhaal te halen voor vermeende schendingen van die rechten;

– het rechtmatigheidsbeginsel wordt gerespecteerd, dat wil zeggen:

a) le traitement des données ne peut être effectué que sur la base du consentement de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi;

b) le fondement légitime englobe entre autres le traitement de données nécessaire aux fins de sauvegarde des intérêts vitaux des individus et le traitement de données nécessaire pour des motifs d'intérêt public, comme dans le cas de la gestion d'une épidémie mortelle;

– le traitement à grande échelle de données à caractère personnel n'est possible que s'il est scientifiquement prouvé qu'il offre potentiellement des avantages pour la santé publique plus importants que d'autres solutions moins invasives;

– selon la Convention 108+ (voir article 11), une exception n'est admise que «dès lors qu'une telle exception est prévue par une loi, qu'elle respecte l'essence des droits et libertés fondamentales, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique»:

a) si des restrictions sont appliquées, ces mesures doivent être exclusivement prises sur une base temporaire et seulement pour une période explicitement limitée à la durée de l'état d'urgence;

b) il est crucial que des précautions spécifiques soient prises et que l'assurance soit donnée que les données à caractère personnel bénéficieront à nouveau d'une protection totale dès que l'état d'urgence sera levé;

c) pour le traitement de données à l'aide de systèmes d'intelligence artificielle, voir les lignes directrices relatives à l'intelligence artificielle et à la protection des données émises par le Comité consultatif instauré par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

La présente proposition de résolution a pour thème une compétence communautaire transversale. En effet, diverses instances sont habilitées à traiter des données à caractère personnel et responsables du développement d'une application «corona». Les Communautés sont ainsi compétentes pour le développement de l'application «corona» car il s'intègre dans leur compétence en matière de prévention des maladies. Ce sont aussi les entités fédérées qui doivent ratifier la Convention. En revanche, c'est l'Autorité fédérale de protection des données qui veille au respect des principes fondamentaux de la protection des données.

a) de verwerking van gegevens kan worden uitgevoerd op basis van de toestemming van de betrokkene of op een andere legitieme basis die wettelijk is vastgelegd;

b) legitieme grondslag omvat met name gegevensverwerking die nodig is voor de vitale belangen van individuen, en gegevensverwerking op basis van algemeen belang, zoals in het geval van monitoring van een levensbedreigende epidemie;

– grootschalige verwerking van persoonsgegevens is alleen mogelijk wanneer, op basis van wetenschappelijk bewijs, de potentiële voordelen voor de volksgezondheid zwaarder doorwegen dan de voordelen van andere alternatieve oplossingen die minder ingrijpend zijn;

– volgens Verdrag 108+ (zie artikel 11) worden slechts uitzonderingen toegestaan «voorzien door de wet, bij eerbiediging van de fundamentele rechten en vrijheden en vormt dit een noodzakelijke en evenredige maatregel in een democratische samenleving»:

a) indien beperkingen worden toegepast, moeten die maatregelen uitsluitend op voorlopige basis worden genomen en alleen voor een periode die uitdrukkelijk beperkt is tot de noodtoestand;

b) het is van cruciaal belang dat er specifieke voorzorgsmaatregelen worden genomen en dat de verzekering wordt gegeven dat persoonlijke gegevens volledig worden beschermd zodra de noodtoestand is opgeheven;

c) voor gegevensverwerking met behulp van kunstmatige-intelligentiesystemen, zie verdere richtlijnen inzake kunstmatige intelligentie en gegevensbescherming van de adviescommissie van het gegevensbeschermingsverdrag.

Dit onderwerp betreft een transversale aangelegenheid met de Gemeenschappen. Er zijn namelijk verschillende instanties bevoegd voor de verwerking van persoonsgegevens en de ontwikkeling van een corona-app. Zo zijn de Gemeenschappen bevoegd voor het ontwikkelen van de corona-app daar dit onder de bevoegdheid van de ziektepreventie valt. Het zijn ook de deelstaten die het verdrag moeten ratificeren. Het is echter de federale Gegevensbeschermingsautoriteit die ervoor zorgt dat de grondbeginselen van gegevensbescherming correct worden nageleefd.

PROPOSITION DE RÉSOLUTION

Le Sénat,

Demande aux différents gouvernements de notre pays:

1) de ratifier la Convention 108+ du Conseil de l'Europe. Celle-ci a été signée par la Belgique le 10 octobre 2018 mais n'a pas encore été ratifiée à ce jour. Des pays comme la Bulgarie, la Croatie, la Lituanie, la Pologne et la Serbie nous ont précédés;

2) d'assurer que la Belgique (et dès lors les entités fédérées) se conforme aux normes internationales édictées dans les Conventions 108 et 108+ du Conseil de l'Europe (voir supra);

3) de publier le code source de l'application de suivi des contacts. Le principal avantage de cette publicité du code source est la transparence à l'égard de la population. L'entreprise (et les autorités publiques) garanti(ssen)t la fiabilité de l'application en prouvant sur quel code elle est basée, ce qui aura pour effet pratique positif de permettre une localisation rapide des *bugs* dans l'application;

4) d'assortir les applications de compilations reproductibles *(reproducible builds)*. Celles-ci constituent un maillon de la chaîne de confiance. Elles prouvent que l'application a été compilée à partir du code source public, ce qui permet à quiconque de vérifier qu'aucune erreur n'a été introduite durant le processus de développement.

Le 10 septembre 2020.

VOORSTEL VAN RESOLUTIE

De Senaat,

Vraagt aan de verschillende regeringen van ons land om:

1) Verdrag 108+ van de Raad van Europa te ratificeren. Het verdrag werd op 10 oktober 2018 ondertekend door België maar is tot op heden nog niet geratificeerd. Landen zoals Bulgarije, Kroatië, Litouwen, Polen en Servië gaan ons voor;

2) te verzekeren dat België (en bijgevolg de deelstaten) zich aan de internationale normen houdt zoals vastgelegd in Verdrag 108 en 108+ van de Raad van Europa (zie eerder);

3) de broncode van de contacttracingapp openbaar te maken. Het grootste voordeel van deze publiek beschikbare broncode is de transparantie ten aanzien van de bevolking. Het bedrijf (en de overheid) geven garanties dat de app betrouwbaar is door te bewijzen op welke broncode de app gebaseerd is. Een praktisch positief gevolg is de snelle lokalisering van *bugs* in de app;

4) de apps te voorzien van *«reproducible builds»*. Deze builds fungeren als onderdeel van de vertrouwensketen. Ze bewijzen dat de app gecompileerd is uit de publieke broncode wat iedereen in staat stelt om te verifiëren dat er geen fouten zijn geïntroduceerd tijdens het bouwproces.

10 september 2020.

Rik DAEMS.
Willem-Frederik SCHILTZ.
Gaëtan VAN GOIDSENHOVEN.
Jean-Paul WAHL.

Imprimerie centrale – Centrale drukkerij