

14-06-2022

Betreft: brief betreffende van het wetsontwerp inzake het verzamelen en bewaren van identificatiegegevens en metagegevens in de sector elektronische communicatie en de verstrekking van deze gegevens aan de autoriteiten

Geachte leden van het parlement,

U bespreekt momenteel het wetsontwerp inzake het verzamelen en bewaren van identificatiegegevens en metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten.

European Digital Rights (EDRI) is een vereniging die 47 mensenrechtenorganisaties uit heel Europa vertegenwoordigt die opkomen voor rechten en vrijheden in de digitale omgeving. Ons netwerk houdt zich al bijna twintig jaar bezig met de kwestie van dataretentie. Onze leden hebben met beleidsmakers gesproken over de risico's voor de grondrechten die een dergelijke maatregel met zich meebrengt, waar mogelijk technische expertise geleverd en wetgeving voor de rechter gebracht in Ierland, Oostenrijk, Duitsland, Tsjechië, het Verenigd Koninkrijk, Frankrijk enz. wanneer deze in strijd was met nationale en Europese grondrechten. De Liga voor Mensenrechten, die zich inzet om het draagvlak voor de mensenrechten in België te verbreden, heeft aan deze inspanningen bijgedragen.

Wij zijn verheugd over de poging van de Belgische wetgevers om een wettelijk kader te scheppen in overeenstemming met de jurisprudentie van het Hof van Justitie van de Europese Unie voor de bewaring van verkeers- en locatiegegevens. Regelingen voor het bewaren van gegevens die op grond van het EU-recht onwettig zijn, moeten worden afgeschaft en zo spoedig mogelijk worden vervangen door oplossingen die de strikte noodzakelijkheids- en evenredigheidstoets doorstaan die door de rechtbanken is vastgesteld.

Het is dan ook van essentieel belang dat het nieuwe wetsontwerp dat u momenteel bespreekt, geen maatregelen invoert die de effecten van de vorige wet op de grondrechten zouden herhalen en die in strijd zouden zijn met de arresten van het Belgisch Grondwettelijk Hof en het Hof van Justitie van de Europese Unie.

Uit onze lezing blijkt helaas dat dit wetsontwerp, in zijn huidige vorm en indien het zonder de nodige aanpassingen wordt aangenomen, een gevaar zou betekenen voor de grondrechten van burgers, zoals het recht op privacy en gegevensbescherming, de vrijheid van meningsuiting en van informatie, de persvrijheid en de waarborgen inzake het beroepsgeheim, en mogelijk een gevaarlijk precedent zou scheppen voor andere lidstaten.

Wij hebben de volgende ernstige tekortkomingen vastgesteld die het parlement dringend moet verhelpen om te voorkomen dat de richtlijn in de toekomst door de rechter ongeldig wordt verklaard¹:

- **De strikte noodzaak van de Belgische wet op de bewaring van gegevens moet worden bewezen en niet worden aangenomen:** Naar aanleiding de vernietiging van de vorige dataretentiewet door het Belgisch Grondwettelijk Hof waarschuwden politievertegenwoordigers dat zonder dataretentie de politie "doof en blind"² zou worden en betoogden dat het een onmisbare

¹ Voor meer details raden wij aan het advies van de Ligue des Droits Humains te lezen over het wetsontwerp van 17 maart 2022 betreffende het verzamelen en bewaren van identificatiegegevens en metagegevens in de sector elektronische communicatie en het verstrekken van deze gegevens aan de autoriteiten, 05.2022, <https://www.liguedh.be/wp-content/uploads/2022/05/Avis-LDH-DATA-RETENTION-2022-final.pdf>

² *The Brussels Times*, Phone data investigations: Belgian law could be hanging by a thread, 31.03.2021, <https://www.brusselstimes.com/162697/phone-data-investigations-belgian-law-could-be-hanging-by-a-thread-pilote-constitutional-court-service-providers-record-european-court-justice-crime-privacy>

maatregel was³. Politieke verklaringen alleen, waarin wordt gewezen op het veronderstelde nut van gegevensbewaring, volstaan echter niet om aan te tonen dat het in bulk bewaren van telecommunicatiegegevens noodzakelijk is voor het onderzoek naar strafbare feiten. Het loutere nut van een instrument voor rechtshandavingsinstanties voldoet niet aan de wettigheidstoets, met inbegrip van de noodzaak en de evenredigheid. In plaats daarvan is een op feiten gebaseerde beoordeling van de doeltreffendheid van de maatregel vereist, alsmede een onderzoek naar minder ingrijpende opties waarmee hetzelfde doel kan worden bereikt.

- **Gerichte gegevensbewaring mag niet leiden tot de facto massale gegevensbewaring:** Volgens de jurisprudentie van het Hof van Justitie mogen metagegevens slechts gedurende een beperkte periode worden bewaard, op een gerichte manier die wordt bepaald door een geografisch criterium. De belangrijkste conclusie is dat de verplichting om elektronische communicatiegegevens te bewaren de uitzondering moet zijn, en niet de regel. In het wetsontwerp worden bepaalde geografische gebieden gekozen op basis van het percentage zware criminaliteit en hun aard, die een hoog risico op zware criminaliteit inhouden, zoals luchthavens, treinstations, enz. waar personen die zich daar bevinden, systematisch zouden onderworpen worden aan dataretentie. In de tekst staat dat "de regering van mening is dat het niet onmogelijk is dat het gehele nationale grondgebied onder de gegevensbewaring valt (...) Indien aan deze hypothese wordt voldaan, dan is er sprake van bewaring die doelgericht is in haar aanpak maar veralgemeend in haar gevolgen."⁴ Dit zou indruisen tegen de definitie van "gericht": de strafbaarheidsdrempel moet dus worden aangepast. Ten slotte zou de nieuwe wetgeving van toepassing zijn op aanbieders van over-the-top-diensten (OTT)⁵ (zoals WhatsApp, Skype, Signal of Facebook Messenger). Deze diensten kunnen hun gebruikers niet geografisch gericht benaderen en zullen waarschijnlijk gegevens bewaren over het hele Belgische grondgebied. Bovendien zijn zij meestal buiten België gevestigd, en het opleggen van deze vereisten in de Belgische nationale wetgeving zou in strijd kunnen zijn met het oorsprongslandbeginsel in de EU-wetgeving.
- **Gerichte gegevensbewaring moet gebaseerd zijn op objectieve criteria en geverifieerde gegevens:** De gegevens die worden gebruikt om de criminaliteitscijfers per geografisch gebied op te stellen, zouden afkomstig zijn van de Nationale Algemene Gegevensbank (ANG), waarvan bekend is dat zij talrijke fouten, onnauwkeurigheden en onjuiste karakteriseringen bevat. Het gebruik van de ANG als statistische referentie kan derhalve niet worden gebruikt als rechtvaardiging voor de schending van de rechten van een zo groot aantal mensen.
- **De definitie van ernstige strafbare feiten moet worden beperkt:** Het begrip ernstige strafbare feiten zoals gedefinieerd in artikel 90ter van het Wetboek van Strafvordering en dat in het wetsontwerp wordt gebruikt om de criminaliteitscijfers te berekenen, is te ruim. Het omvat delicten van gemeen recht zoals computervervalsing, computerfraude, diefstal met geweld, bezit van verdovende middelen en voegt delicten samen die tot strafdrempels kunnen leiden, zodat het ernstige karakter ervan niet lijkt te worden geobjectiveerd. Voorts verplicht het wetsontwerp de exploitanten om systematisch de gegevens in het gespreksgegevensbestand (call detail record of CDR), de locatiegegevens van verdachten van fraude of misbruik van een elektronisch communicatienetwerk, en de verkeersgegevens die nodig zijn om dergelijke fraude of dergelijk misbruik op te sporen, op te slaan. Fraude is echter geen ernstig misdrijf en deze bewaarplicht zou dus in strijd zijn met het EU-recht. Bovendien bieden mobiele exploitanten hun abonnees

³ RTBF, Lutte contre le terrorisme : la conservation des métadonnées doit être exceptionnelle, selon le Comité T, 18.03.2022, <https://www.rtbef.be/article/lutte-contre-le-terrorisme-la-conservation-des-metadonnees-doit-etre-exceptionnelle-selon-le-comite-t-10958051>.

⁴ Memorie van Toelichting, p 12, <https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf>.

⁵ OTTs zijn mediadiensten die via het internet rechtstreeks aan de kijkers worden aangeboden. OTT gaat voorbij aan kabel-, omroep- en satelliettelevisieplatforms, de soorten bedrijven die traditioneel optreden als controleurs of distributeurs van dergelijke inhoud. De term is ook gebruikt om mobiele telefoons zonder telefoonmaatschappij aan te duiden, waarmee alle communicatie als data wordt aangerekend, en die andere gespreksmethoden vervangen.

steeds vaker forfaitaire factureringsplannen aan waardoor het bewaren van CDR's om commerciële redenen totaal overbodig wordt.

- **Alleen IP-adressen aan de bron mogen in bulk worden bewaard voor de bestrijding van ernstige strafbare feiten:** Het Hof van Justitie stelt dat alleen de algemene en ongedifferentieerde bewaring van "IP-adressen" aan de bron van een elektronische communicatie moet worden toegestaan als uitzondering op het algemene verbod van massale gegevensbewaring. De voorgestelde tekst staat de massale bewaring toe van categorieën gegevens die verder gaan dan de strikt omschreven uitzondering van het Hof, namelijk de identificatiecode die voor elk gesprek wordt gecreëerd, de begindatum van het abonnement of de registratie bij de dienst, gegevens met betrekking tot het type betaling of het identificatienummer van de eindgebruiker-eindapparatuur (International Mobile Equipment Identity, IMEI, Media Access Control, MAC of Permanent Equipment Identifier, PEI). De lijst moet worden beperkt tot wat het Hof van Justitie voorschrijft en de wetgever moet een grens stellen aan de bewaartermijn van IP-adressen, overeenkomstig de eisen van het Hof van Justitie. Wij stellen ook voor voorzichtig te zijn met het bewaren van IP-gegevens, aangezien met de nieuwe IPv6-norm veel gedetailleerdere conclusies over het leven van een persoon kunnen worden getrokken dan met vroegere verbindinggegevens.⁶ In een recente rechtszaak heeft de advocaat-generaal van het Hof van Justitie bevestigd dat de problemen die voortvloeien uit het gebruik van het IPv6-protocol in een toekomstige zaak moeten worden behandeld.⁷
- **De Belgische dataretentiewet mag encryptie niet ondermijnen:** Het wetsontwerp bevestigt dat het "een encryptiesysteem verbiedt dat het voor operatoren onmogelijk maakt om identificatie-, verkeers- of locatiegegevens te bewaren".⁸ Dit gaat verder dan de vorige dataretentieverplichting, waarbij een aanbieder alleen verplicht was gegevens te bewaren die door hem waren gegenereerd of verwerkt. Gegevens die de aanbieder niet heeft verzameld, konden niet worden bewaard. De nieuwe wetgeving zou aanbieders dwingen die gegevens namens de overheid vast te leggen, ook als de aanbieder daar zelf geen noodzaak toe ziet. De gevolgen kunnen verstrekkend zijn. Het betekent dat chatdiensten zoals Signal illegaal worden. Signal is een veilig versleuteld communicatiesysteem, waarop veel mensen (waaronder journalisten en politici) vertrouwen voor de veiligheid en vertrouwelijkheid van hun communicatie. Het verzamelt niet meer gegevens dan nodig is om zijn diensten te verlenen: het wetsontwerp zou de beschikbaarheid van Signal in België en dus het gebruik ervan door Belgische burgers in gevaar brengen.⁹

Wij danken u voor uw aandacht en blijven tot uw beschikking indien u vragen heeft.

Hoogachtend,

Chloé Berthélémy
Beleidsadviseur
chloe.berthelemy@edri.org

⁶ IPv6 maakt het mogelijk een uniek IP-adres toe te wijzen aan bijna elk apparaat in ons leven, met name slimme apparaten zoals horloges, deuren, speelgoed en auto's.

⁷ CJEU, Advocate General Opinion, Joined Cases C-793/19 and C-794/19, para. 83.

⁸ Memorie van Toelichting, p 19, <https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf>.

⁹ Recente plannen in Nederland om chat-apps, zoals WhatsApp, te verplichten achterdeurtjes in hun systeem te maken om toegang tot gegevens te krijgen, werden geschrapt nadat het bedrijf aankondigde zijn diensten niet langer aan te bieden in het land. Zie Marc Hijink en Rik Wassens, 'WhatsApp dreigde uit Nederland te vertrekken om aftapplicht', nrc, 03.06.22, [https://www.nrc.nl/nieuws/2022/06/03/whatsapp-dreigde-te-vertrekken-om-aftaplicht-a4132175](https://www.nrc.nl/nieuws/2022/06/03/whatsapp-dreigde-te-vertrekken-om-aftapplicht-a4132175)