Nieuwe Dataretentiewet pakt end-to-end-encryptie aan

Om het hoofd te bieden aan de stijgende criminaliteit online wil de Belgische regering end-to-end-encryptie van chatdiensten zoals Signal en WhatApp aanpakken[1] De VVJ betwist de proportionaliteit van de maatregel en wijst op het mogelijke *chilling effect* op journalistieke bronnen.

De bewogen geschiedenis van de Dataretentiewet

Op 22 april 2021 oordeelde het Grondwettelijk Hof dat de verplichting tot bewaring van e-communicatiegegevens door operatoren de uitzondering moet blijven. De overheid kan zoiets slechts opleggen wanneer het 'strikt noodzakelijk' is en 'gestoeld op objectieve criteria'.[2] Aanleiding voor de uitspraak[3] is rechtspraak van het Europees Hof van Justitie dat veralgemeende en ongedifferentieerde bewaring van metadata te allen tijde door operatoren voor rechtshandhavingsdoeleinden niet langer toelaatbaar acht.[4] Beide hoven spraken zich overigens eerder uit in deze discussie: zo vernietigde het Grondwettelijk Hof de wet die de Dataretentierichtlijn[5] moest omzetten[6] nadat het Europees Hof van Justitie de bewuste richtlijn ongeldig had verklaard.[7] Dataretentie en grondrechten, het is een moeilijk huwelijk.

Daar staat tegenover dat we leven in een wereld die steeds digitaler wordt. Ook criminelen verleggen hun werkterrein naar het internet. Om pak te krijgen op de groeiende online criminaliteit is het aangewezen dat strafrechtelijke autoriteiten toegang krijgen tot bepaalde data waarover operatoren beschikken.

Het nieuwe Voorontwerp onderzoekt hoe efficiënte dataretentie kan worden verzoend met de in de rechtspraak geschetste krijtlijnen.

Welke data?

Het Voorontwerp viseert twee categorieën van gegevens, identificatiegegevens plus verkeers- en locatiegegevens. Identificatiegegevens zijn onder meer het oproepnummer van het eindapparaat, de naam van de abonnee en de plaats waar het eindtoestel zich bevindt op het moment van de oproep.[8]

[1] Concreet gaat het om het Wetsontwerp van 17 maart 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (hierna: Voorontwerp Dataretentiewet of Voorontwerp).
[2] GwH 22 april 2021, nr. 57/2021, punten 132 en 133.
[3] Concreet gaat het om de artikelen 2, b), 3 tot 11 en 14.
[4] HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, La Quadrature du Net, ECLI:EU:C:2020:791 (hierna: La Quadrature du Net-arrest).
[5] Richtlijn nr. 2006/24/EC van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn nr. 2002/58/EG (Pb. L. 105, 13 april 2006, pp. 54-63).
[6] GwH 11 juni 2015, nr. 84/2015.
[7] HvJ, gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland, CLI:EU:C:2014:238.
[8] Artikel 2, 57 van de Wet betreffende de elektronische communicatie.

Cruciaal is dat identificatiegegevens géén betrekking hebben op de communicatie-inhoud of de geadresseerde van de communicatie (denk aan het IP-adres van de geadresseerde of de locatie van de eindapparatuur). De notie 'verkeersgegevens' slaat op de datum, het tijdstip, de aard of de duur van de communicatie[9]; 'locatiegegevens' verwijzen naar de plaats van de eindapparatuur van de eindgebruiker[10].

Dataretentie binnen de grenzen van Europese rechtspraak

Algemene en ongedifferentieerde databewaring te allen tijde mag dan niet langer toelaatbaar zijn, het Europees Hof van Justitie laat ruimte voor nuance. Zo is algemene en ongedifferentieerde databewaring wel nog mogelijk in geval van een 'werkelijke en actuele of voorzienbare ernstige bedreiging van de nationale veiligheid'.[11] Gaat het daarentegen om het voorkomen van een ernstige bedreiging van de nationale veiligheid of om het bestrijden van zware criminaliteit dan is enkel gerichte gegevensbewaring mogelijk, bijvoorbeeld in bepaalde zones of voor bepaalde categorieën personen waarvan vooraf is vastgesteld dat ze een bijzonder risico vormen.[12]

Over naar het Voorontwerp

Je kan er niet omheen dat de wetgever bijzonder voluntaristisch is omgesprongen met de Europese rechtspraak. In een poging zich te conformeren naar Europa zet België de deur net open naar meer datarententie. Nog meer actoren krijgen toegang tot gegevens (Centrum voor Cybersecurity België, de inspectiedienst consumentenproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, …), er is heel wat beoordelingsmarge voor operatoren – privé-entiteiten tenslotte –, de criteria voor gerichte dataretentie krijgen een maximale invulling, en ga zo maar door. Dit Voorontwerp stelt weinig gerust: het trekt volop de kaart van de rechtshandhaver.

Quid encryptiesystemen?

Encryptie maakt ongewenst meelezen moeilijk. Dat maakt berichten-apps met versleuteling, waaronder Signal, populair, ook bij journalisten. Het Voorontwerp juicht beveiliging via encryptiesystemen toe[13] maar waarschuwt voor het ongewenste gevolg waardoor een operator het verzoek van de strafrechtelijke autoriteiten niet kan beantwoorden.[14] Identificatie- en metagegevens, zo luidt het verdict, mogen dus nooit ingekapseld zitten in end-to-end encryptie.

[9] Artikel 2, 6 van de Wet betreffende de elektronische communicatie.
[10] Artikel 2, 7 van de Wet betreffende de elektronische communicatie.
[11] La Quadrature du Net-arrest, punt 229, 1), eerste streepje.
[12] La Quadrature du Net-arrest, punt 229, 1), tweede streepje.
[13] Zie artikel 107/5, §1 van het Voorontwerp: 'Ter bevordering van de digitale veiligheid is het gebruik van versleuteling vrij binnen de in de paragrafen 2 tot en met 4 gestelde grenzen.'
[14] Zie artikel 107/5, §3 van het Voorontwerp: 'Het gebruik van versleuteling door een operator, met als doel de veiligheid van de communicatie te waarborgen, mag geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie.'

De VVJ stelt zich ernstige vragen bij de proportionaliteit van een dergelijk verbod dat zonder onderscheid ingrijpt op de privacy van alle eindgebruikers om specifieke inbreuken te kunnen beteugelen. En dan zwijgen we nog over het *chilling effect* van een dergelijke maatregel op journalistieke bronnen.

Charlotte Michils