Mercuriale september 2022

Dataretentie: de zoektocht naar een veilige haven

Tekst werd voorbereid door de heer Robrecht De Keersmaecker, substituut-procureur-generaal bij het hof van beroep en mevrouw Catherine Van den Heyning, substituut procureur des Konings bij de rechtbank van eerste aanleg en uitgesproken door de heer procureur-generaal Patrick Vandenbruwaene op de openingszitting van het hof van beroep en het arbeidshof op 1 september 2022.

Inhoud

Mijnheer de Eerste Voorzitter,
Geachte leden van het Hof,
Waarde dames en heren,
Stafhouders,
Geachte genodigden,
Beste collega's,

De inspiratie voor een mercuriale wordt veelal gevonden in de besognes van het voorgaande gerechtelijk jaar, of waarschuwingen voor de toekomst, in academisch onderzoek, of nog de actualiteit in de media. De inspiratie voor de huidige mercuriale start nederiger, namelijk in de verslagen die de collega's maken over hun wachtdiensten 's nachts en in het weekend.

Men durft wel eens te vergeten dat elke nacht, elk weekend en elke vakantiedag collega's waken over de veiligheid van dit land en zijn burgers en nadien loyaal rapporteren welke feiten hen door de politie werden gemeld en welke opdrachten ze hebben gegeven.

Niet elke nacht brengt de grote criminaliteit met zich mee – gelukkig maar – maar uit de verslagen van de substituten blijkt één zekerheid: nagenoeg elke nacht is er een onrustwekkende verdwijning. Het gaat dan meestal over kinderen en jongeren, maar evengoed personen met psychische problemen of ouderen wiens geheugen hen in de steek laat.

Elke onderzoeker zal u vertellen dat tijdens een verdwijning elk uur dat verstrijkt, de kans op een slechte afloop vergroot. Op dat moment kan een telefoon of smartphone op zak levens redden. Via de signalen die deze telefoons sturen of op basis van het laatste verzonden bericht is het mogelijk de verdwenen persoon te lokaliseren en terug in veiligheid te brengen.

De onrustwekkende verdwijningen zijn een waarschijnlijk weinig dramatisch voorbeeld van het belang van het bewaren van gegevens. Maar het is nochtans een heel belangrijk voorbeeld dat bevattelijk maakt waarom Justitie zich ernstige zorgen maakt over de beslissingen van het Europese Hof van Justitie om het bewaren van deze telefoongegevens te beperken tot een minimum. Zonder deze gegevens zouden immers verschillende verdwijningen slecht aflopen omdat we de persoon niet of te laat terugvinden.

Ik had met een greep van meer spectaculaire voorbeelden kunnen beginnen zoals de zoektocht naar Jurgen Conings, het lokaliseren van terroristen, of nog een moord zonder opsporingsindicaties die werd opgelost naar aanleiding van de telefoniegegevens, of nog het opsporen van kindermisbruik online dat onmogelijk is zonder deze gegevens.

Die voorbeelden zijn in het verleden regelmatig aangehaald door politie en justitie om de bewaring van communicatiegegevens te verdedigen. Maar ze werden door zelf uitgeroepen privacy-experten en actiegroepen vaak afgedaan als anekdotisch of

voorbeelden waar de grote meerderheid van de bevolking nooit mee te maken krijgt. Er wordt geargumenteerd dat telecombedrijven en technologiebedrijven verplicht worden om de communicatiegegevens van elk en ieder van ons bij te houden en dit terwijl slechts een heel kleine fractie onder de burgers crimineel gedrag zal vertonen.

Het is daarom dat de inspiratie voor deze mercuriale over het belang van dataretentie gevonden wordt in de niet-anekdotische angst van de ouder wiens kind onvindbaar is, de man die thuiskomt en merkt dat zijn zwaar depressieve vrouw de woning in een verontrustende context heeft verlaten, of van kinderen die de politie bellen omdat hun demente vader in de winternacht ronddoolt met niets meer dan een dunne kamerjas en nood GSM om de hals.

Sta mij daarom toe om in deze mercuriale uit te leggen waarom de Belgische Justitie blijft hameren op een regeling om telecommunicatie en digitale communicatiegegevens te bewaren, hoe we in een situatie zijn gekomen dat die bewaring van gegevens vandaag onder druk staat, en hoe we vooruit kunnen om een evenwicht te bereiken in de bescherming van enerzijds onze privacy en anderzijds onze veiligheid.

1. De vraag is wat dataretentie is.

Misschien moet in eerste instantie nog even verduidelijkt worden waar dataretentie betrekking op heeft.

Vaak werd dit in de media omschreven als afluisteren, alsof de nieuwe wet de operatoren zou verplichten om elk telefoongesprek, elke sms of WhatsApp bericht bij te houden.

Dit is het voor alle duidelijkheid niet. Als operatoren op vraag van Justitie kennis geven van de inhoud van de communicatie, dan kan dat enkel na een bevel hiertoe van de onderzoeksrechter overeenkomstig artikel 90ter Sv.

Ik kan me uiteraard niet uitspreken over de inhoud waarvan operatoren kennisnemen op basis van hun algemene voorwaarden. Dat is vaak minder duidelijk.

Waar gaat het dan wel over, wanneer we over dataretentie spreken? Telkens wij gebruik maken van een elektronische communicatiedienst, via onze smartphone, of via een tablet of computer, worden er tal van gegevens gegenereerd. Wij delen die gegevens meestal op in drie categorieën:

- Identificatiegegevens: op wiens naam staat dat GSM nummer? Op wiens naam staat het internetabonnement dat het specifieke IP-adres op dat moment gebruikte om die website te consulteren?

- Verkeers- en locatiegegevens: met welk nummer had een GSM-nummer contact? Wanneer? Hoelang? In welk GSM toestel was dat nummer actief? Was er ook dataverkeer? Onder welke zendmast bevond dat toestel zich? Deze gegevens noemt men ook wel eens metagegevens of transactiegegevens.

- Inhoud: welke berichten of foto's verstuurt u ? Wat wordt er gezegd tijdens een WhatsApp videocall? Dit zijn de meest gevoelige gegevens, zodat hiervoor dan ook de grootste waarborgen gelden. Zij worden niet bijgehouden op vraag van Justitie tenzij er een onderzoeksrechter een tapmachtiging aflevert in een concreet gerechtelijk onderzoek, met alle bijhorende wettelijke waarborgen.

2. Waarom zijn deze gegevens zo belangrijk?

Als u kijkt naar de grootste bedrijven ter wereld, zal u merken dat het gros van de toppers tegenwoordig actief is in de technologiesector. Sommigen met een omzet die het BNP van kleinere Europese lidstaten ruim overstijgt.

Sommige van deze bedrijven leveren zelf geen producten of noemenswaardige diensten zoals bijvoorbeeld Meta, het voormalige Facebook. Waar halen zij hun economische waarde dan?

Het antwoord is eenvoudig: uw data, het nieuwe goud. Het gebruik van hun sociale media diensten en de cookies die zij achterlaten op uw systeem, stellen hen in staat om uw online gedrag grotendeels te monitoren, te analyseren en vervolgens zelfs in hoge mate te voorspellen.

Die inzichten veilen ze aan de hoogste bieders, teneinde u toch maar te overtuigen om dit of dat product aan te kopen bij een welbepaalde webwinkel, of zelfs uw stemgedrag te beïnvloeden door het nieuws dat u online te zien krijgt in een bepaalde richting te censureren. Het is voor de operatoren dus van levensbelang deze gegevens bij te houden, ongeacht of Justitie dit vraagt. Het zit ingebakken in hun businessmodel en is de reden dat u dergelijke diensten doorgaans gratis kunt gebruiken. Zij het dat de zon niet voor niets opkomt en deze diensten eigenlijk betaald worden met persoonlijke data.

Dit alles gebeurt uiteraard overeenkomstig de GDPR regelgeving, door de band genomen met uw toestemming, zoals beschreven in die kleine lettertjes, die nagenoeg niemand leest bij het installeren van een nieuwe app.

Voor politie en Justitie zit de meerwaarde van die gegevens in de mogelijkheden die ze bieden om verdachten te identificeren, of net uit te sluiten, en om feitelijke gegevens aan elkaar te linken en zo tot betere inzichten te komen.

Vaak zijn die gegevens zelfs de enige onderzoekselementen die beschikbaar zijn nu ons leven zich steeds meer geheel digitaal afspeelt.

Criminaliteit volgt die maatschappelijke evolutie op de voet en de sporen van sommige misdrijven blijven geheel digitaal wat zeer ingrijpend is voor het verzamelen van het bewijs.

Dit zijn niet alleen de *high profile cases* waar we recent over hoorden in de SKY dossiers.

Het gaat vooral over zaken waar iedere gewone burger vroeg of laat mee te maken krijgt zoals het volledig leeghalen van de bankrekening bij phishing of het afpersen van seksuele beelden bij *sextortion*.

Enkele andere concretere voorbeelden waarbij de communicatiegegevens ter hulp kwamen van politie en justitie:

- Recent kon een bende gevat worden die in tal van supermarkten luxeproducten ging stelen. Op basis van de locatiegegevens van hun GSM-toestellen, bevestigd door de ANPR registraties, werden de verdachten gelinkt aan nog tientallen openstaande dossiers.

- Een jongeman werd geïdentificeerd die online met een vals profiel minderjarige meisjes contacteerde en hen kon overtuigen om seksuele beelden te delen met hem. Eens dit gebeurd was, dreigde hij er echter mee dit openbaar te maken en moesten de slachtoffers steeds verregaandere beelden overmaken. Pas bij analyse van diens computersysteem, kon de politie nog tientallen gelokte meisjes identificeren aan de hand van de IP-adressen. Het bijkomend oplossen van deze feiten zal wellicht velen van hen wat gemoedsrust schenken en vertrouwen in de toekomst.

- Maandelijks krijgen politie en Justitie van internationale partners ook honderden meldingen van Belgische IP-adressen die gezien werden op zogenaamde *peer-to-peer* platformen waar video's en foto's van kindermisbruik gedeeld worden tussen de gebruikers. De politie probeert deze IP-adressen dan te koppelen aan identiteiten, zodat er vervolgens met een huiszoekingsmandaat nagegaan kan worden of deze informatie klopt en desgevallend het materiaal verwijderd kan worden en de verdachten vervolgd.

De vraag kan gesteld worden of deze gevallen zoals beweerd wordt inderdaad zo anekdotisch en uitzonderlijk zijn. De dossiers zoals hierboven beschreven zijn jammer genoeg dertien in een dozijn zoals blijkt uit de politionele en jurisdictionele cijfers.

Waar schuilt het gevaar?

Elke categorie van gegevens kan meer over het privéleven onthullen. Wanneer iemand weet waar en wanneer welke communicatie gevoerd wordt over welke websites of met welke contactpersonen kan hier zeer veel informatie over het persoonlijk leven en de privacy worden afgeleid. Dit is uiteraard niet zonder gevaar.

3. Dataretentie niet zonder gevaar.

Stel dat iemand zich niet lekker voelt, en zoals zovelen onder ons wel eens doen, een google search doet naar zijn/haar symptomen en vervolgens doorklikt op de verschillende vreselijke ziektebeelden kan dit bijzonder gevoelige informatie over de persoonlijke gezondheidstoestand opleveren. Dit gaat niet alleen op voor

gezondheidsgegevens, maar ook voor andere zeer gevoelige gegevens inzake religieuze ingesteldheid, seksualiteitsbeleving, politieke overtuiging die tot de kern van het privéleven behoren. Bedenk hierbij dat een steeds groter deel van het leven, zowel het publieke als privéleven, zich online afspeelt, zodat ook daarover metagegevens gegenereerd worden bij elke muisklik of swipe.

Deze gegevens elk afzonderlijk zijn misschien onschuldig, maar indien ze bij elkaar gebracht worden voor analyse, zou dit toelaten om een akelig accuraat beeld te krijgen van de persoon tot in de intiemste details.

In een democratische rechtstaat als België met duidelijke *checks and balances* en een waakzame en vrije media ligt het gevaar op misbruik van deze gegevens misschien niet meteen bij de overheidsdiensten, maar eerder in het risico dat deze gegevens het voorwerp zouden worden van een zogenaamd datalek, waarbij andere overheidsdiensten uit bepaalde regimes of malafide derden deze gegevens in handen zouden krijgen en hiermee een verregaand en ongeoorloofd inzicht zouden krijgen in het privéleven van anderen.

Het risico bestaat dat iemand plots geconfronteerd kan worden met een grenscontrole en verhoor omwille van bepaalde posts of likes die hij online deed op Facebook of Twitter. Overheden zouden de toegang tot een land kunnen ontzeggen en geen visum verstrekken, omdat de persoonlijke seksuele identiteit niet spoort met de officiële staatsideologie.

Een toekomstige werkgever zou bij een sollicitatie iemand kunnen weren op basis van bepaalde indicaties dat hij of zij een verhoogd risico loopt op hoger ziekteverzuim, louter op basis van de metagegevens die laten uitschijnen dat een bepaalde aandoening opgezocht werd.

Een cybercrimineel zou bepaalde gegevens over het surfgedrag kunnen misbruiken om niets vermoedende personen met zeer persoonlijke phishingmail te benaderen – dit is een *spearphishing* – waardoor deze niet herkend wordt als een crimineel en argeloos meegegaan wordt in een verhaal waarna de bankrekening leeggehaald wordt.

Indien een crimineel weet dat iemand elke week op woensdagavond in de padelclub op de wifi aangemeld wordt van 19u30 tot 22u00, dan biedt dat mogelijkheden om die tijd te gebruiken om het huis leeg te halen tijdens de afwezigheid van de bewoner.

Deze gevaren hebben ertoe geleid dat dataretentie, vooral als deze algemeen is, steeds omzichtiger benaderd wordt en dit vooral onder impuls van Europa.

4. Dataretentie onder druk: Europese Unie kiest voor de bescherming van privacy.

De Europese Unie zorgde daarom al twintig jaar geleden, in 2002, voor een richtlijn die de privacy en persoonlijke gegevens online beschermt, de zogenaamde E-privacy richtlijn. De nood aan een goede bescherming van deze gegevens is sindsdien enkel maar gegroeid waardoor de Unie de laatste hand legt aan een opvolger van die

richtlijn. Daarmee gepaard besliste de Europese Unie in 2006 om een richtlijn uit te vaardigen die de lidstaten beperkte in de verplichtingen die ze verstrekkers van digitale communicatie kon opleggen in het bijhouden van onze communicatiegegevens. Het werd lidstaten verboden om digitale bedrijven te verplichten de inhoud van de communicaties bij te houden. Wel mochten lidstaten deze online bedrijven verplichten om bepaalde gegevens over communicatie te bewaren en prijs te geven namelijk die wie we zijn, de zogenaamde identificatiegegevens, waar we zijn, de zogenaamde locatiegegevens, en andere gegevens over met wie we en hoe lang we in interactie komen, de zogenaamde verkeersgegevens.

Na jarenlang talmen en een niet mis te verstane tik op de vingers van de Europese Unie zette België uiteindelijk deze richtlijn in 2013 om in een wet. Voor België betekende die dataretentierichtlijn een verbetering voor de bescherming van de online privacy omdat de richtlijn strenger was dan de toen geldende wetgeving over het bewaren van telefoniegegevens en meer waarborgen voorzag naar de bescherming van deze gegevens. Deze richtlijn was echter ook het startschot van een ongeziene juridische strijd voor de nationale hoogste gerechtshoven en voor het Hof van Justitie van de Europese Unie over de vraag waar nu juist de balans tussen privacy en veiligheid moet liggen.

Het eerste arrest van het Europese Hof van Justitie met betrekking tot de vraag of het algemeen bijhouden van communicatiegegevens wel in overeenstemming is met de privacy, voltrok zich in een bijzondere historische context. Na intense jaren in de strijd tegen het internationaal terrorisme waren vele landen massaal gaan inzetten op digitaal toezicht. Daarbij werden massa's aan data verzameld vanuit de strijd tegen terrorisme. In 2013 brak echter een schandaal uit toen Edward Snowden aantoonde dat de Amerikaanse inlichtingendienst NSA wereldwijd communicatiegegevens bijhield van burgers die geen enkel uitstaans hadden met terrorisme of andere staatsonveilige activiteiten. Deze onthullingen zorgden voor een verhoogd bewustzijn dat landen grote hoeveelheden communicatiegegevens voor lange periodes bijhielden en dit vaak zonder gerechtelijk toezicht of toelating en zonder garanties voor burgers wiens gegevens werden bewaard.

In die tijdsgeest van een aangewakkerd privacy-bewustzijn oordeelde het Hof van Justitie dat de Europese richtlijn over het bewaren van communicatiegegevens in strijd was met het recht op privacy en de bescherming van persoonsgegevens. Op basis van deze gegevens kan een intiem beeld geschetst worden van het doen en laten van personen. Het Hof van Justitie meende dat het buiten elke proportie was om gegevens van iedereen te bewaren, ook van wie geen enkel verband heeft met bedreigingen voor de nationale veiligheid en openbare orde of een band heeft met de criminaliteit.

Bovendien benadrukte het Hof van Justitie dat dit ook de vrije meningsuiting zou kunnen ondermijnen, wanneer je weet dat elke stap online gevolgd en bewaard wordt, zal je immers meer opletten wat je online zoekt en post.

In navolging van de vernietiging van deze richtlijn werd ook de Belgische wet van 30 juli 2013 over het bewaren van communicatiegegevens een eerste keer vernietigd door het Grondwettelijk Hof. De Belgische wetgever kwam al snel met een nieuwe wet over het bewaren van gegevens op 29 mei 2016.

Nog steeds konden telecom- en techbedrijven verplicht worden om de identificatie-, locatie- en verkeersgegevens van iedereen bij te houden voor de strijd tegen criminaliteit en de bescherming van de nationale veiligheid en openbare orde, maar de toegang tot deze gegevens door de vervolgende autoriteiten en inlichtingsdiensten werd beperkt. Zo hoopte de Belgische wetgever een evenwicht te hebben gevonden in een brede bewaring maar een beperkt gebruik en toegang tot die gegevens om ervoor te zorgen dat deze gegevens maar bekeken en gebruikt worden als dat strikt noodzakelijk is om België veilig te houden.

5. De Europese Unie zoekt een evenwicht.

De Belgische wetgever koos er principieel voor om vast te houden aan een algemene bewaring van communicatiegegevens omdat een beperkte bewaring ervoor zou zorgen dat de voor strafrechtelijke onderzoeken communicatiegegevens die nodig zijn om een misdrijf op te lossen veelal niet meer aanwezig zouden zijn bij opstart. Strafrechtelijke onderzoeken zijn namelijk door de band genomen historische onderzoeken: meestal start een onderzoek pas als strafbare feiten aan het licht komen en zoekt Justitie in de maanden en jaren voorafgaand aan de feiten om na te gaan wat er gebeurd is en wie daarvoor verantwoordelijk is.

Justitie heeft hierbij uiteraard geen glazen bol om te zien wie eventueel misdrijven kan plegen.

In latere arresten oordeelde het Hof van Justitie dat ook nationale wetgeving disproportioneel is als het een algemene bewaarplicht invoert voor de communicatiegegevens van burgers in de strijd tegen de criminaliteit. Het Hof besliste dat een lidstaat telecom- en techbedrijven niet kan verplichten om de locatie- en verkeersgegevens van iedereen bij te houden voor de strijd tegen de criminaliteit en voor de beveiliging van de openbare orde. Waar in de eerste arresten van het Hof van Justitie over het bewaren van communicatiegegevens de nadruk vooral lag op de bescherming van privacy en persoonsgegevens in een veranderende wereld waar technologie massa surveillance mogelijk maakte, werden de recente arresten beslist in een context waar lidstaten veel kritiek op de rechtspraak van het Hof van Justitie hadden geuit. Vele lidstaten hadden hun bezorgdheid geuit dat het wegvallen van een bewaarplicht het onderzoek naar misdrijven zou bemoeilijken en bepaalde misdrijven vooral online misdrijven zoals cybercrime en kindermisbruikmateriaal onmogelijk zou maken.

Toen het Hof van Justitie in 2018 in de arresten *Tele2 t. Zweden en Watson t. Verenigd Koninkrijk* een eerste keer duidelijk aangaf dat lidstaten niet op algemene wijze locatie- en verkeersgegevens mochten bijhouden, beslisten vele landen om hun eigen wetgeving niet aan te passen en wachtten af tot ook hun eigen nationale wetgeving door het Hof van Justitie beoordeeld zou worden. Het uitblijven van het aanpassen van hun wetgeving leek dan ook niet meer of niet minder dan een stil protest. Zo ook België. In het arrest *La Quadrature du Net* van 2020 besliste het Hof van Justitie dat de Belgische wet het recht van de Europese Unie schond omdat er nog steeds was voorzien in een algemene bewaarplicht van locatie- en verkeersgegevens voor communicatiegegevens in België. In navolging daarvan vernietigde het Grondwettelijk

Hof opnieuw de Belgische wet over het bewaren van gegevens. België was weer bij af, net zoals vele andere lidstaten.

Dat wil niet zeggen dat het Hof van Justitie blind was voor de nationale bezorgdheden. Het Hof van Justitie gaf namelijk uitdrukkelijk aan dat de afwezigheid van communicatiegegevens de strijd tegen criminaliteit, ernstige criminaliteit, kan bemoeilijken of zelfs onmogelijk maken. Voor het Hof woog dat echter onvoldoende door om een algemene bewaarplicht voor locatie-en verkeersgegevens toe te laten. Daarentegen verduidelijkte het Hof wel wat nog toegelaten was.

Ten eerste mogen deze communicatiegegevens en dus ook locatie- en verkeersgegevens nog wel bewaard worden voor de nationale veiligheid in het geval er een ernstige en reële dreiging is. Daardoor zouden de inlichtingendiensten nog wel voor langere tijd kunnen beschikken over deze gegevens indien er een hoger risico bestond voor de nationale veiligheid.

Ten tweede laat het Hof van Justitie ook toe dat een land een algemene bewaarplicht oplegt voor identificatiegegevens. Het Hof van Justitie vond dat de gegevens wie communiceert en van elk toestel minder het recht op privacy beperkt dan de gegevens van waar je communiceert of met wie en wanneer. Ook de IP-adressen van wie communiceert mag van iedereen bijgehouden worden.

Ten derde, en niet onbelangrijk, mogen de locatie- en verkeersgegevens nog wel gericht worden bijgehouden voor de strijd tegen de criminaliteit, zij het alleen maar voor ernstige criminaliteit. Deze gegevens mogen worden bijgehouden van bepaalde personen die in verband met ernstige criminaliteit kunnen gebracht worden, maar ook voor bepaalde zones wanneer de lidstaat over aanwijzingen beschikt die aantonen dat op die plek er een verhoogd gevaar voor ernstige criminaliteit is of een ernstige verstoring van de nationale orde. Het is vooral met dat laatste gegeven, namelijk de mogelijkheid om communicatiegegevens van bepaalde geografische zones bij te houden, dat België aan de slag ging voor de wet over de bewaarplicht nummer 3.

6. Welke gevolgen had dit voor de praktijk?

Maar voor ik u spreek over die nieuwe wet en de toekomst, kijk ik graag naar het heden en het afgelopen jaar waar onze politie en Justitie verder moesten werken in een kader waar de nationale wet voor het bewaren van communicatiegegevens vernietigd was. Een eerste vraag die daarbij al snel aan de orde kwam, was wat er moest gebeuren met de bewijzen die waren verzameld op basis van de reeds vernietigde wet. Kon de rechter nog wel de dader van een moord veroordelen indien hij initieel aan de feiten was gekoppeld op basis van zijn telefoniegegevens verzameld op basis van de oudere, intussen vernietigde wet?

Toen de wet over de bewaarplicht een eerste keer werd vernietigd had het Hof van Cassatie al aangegeven dat de al verzamelde gegevens nog gebruikt mochten worden. Ze waren weliswaar onrechtmatig verzameld omdat ze waren vergaard op basis van een wet waarvan het Hof van Justitie en het Grondwettelijk Hof meenden dat deze in strijd was met de privacy, maar deze gegevens mochten nog wel gebruikt worden omdat deze onrechtmatigheid geen impact had op de betrouwbaarheid van

de gegevens of de rechten van verdediging. Anders gezegd, de inbreuk op de privacy van de verdachte betekende niet dat een beklaagde zich niet zou kunnen verweren voor de rechtbank.

Nu de bewaarplicht een tweede keer werd vernietigd kon het Hof van Cassatie niet deze zienswijze automatisch opnieuw toepassen. Het Hof van Justitie had daarover gezegd dat de nationale rechtbanken in principe mochten oordelen over het lot van communicatiegegevens verzameld op basis van een wet in strijd met haar rechtspraak, maar dat ze daarbij wel moesten rekening houden met bepaalde criteria.

Ten eerste moet een verdachte de verzamelde gegevens wel nuttig kunnen beoordelen en tegenspreken. Dat is evident. Het is van groot belang dat als bewijs gebruikt wordt, of het nu communicatiegegevens zijn of andere, dat de betrouwbaarheid van deze gegevens als zodanig beoordeeld kan worden door de rechter.

Ten tweede moet de rechter nagaan of hij deze aangeleverde communicatiegegevens wel kan beoordelen, namelijk handelen deze gegevens over objectieve vaststaande elementen zoals van waar iemand communiceerde en kan de rechter dit beoordelen zonder verder wetenschappelijk onderzoek of expertise.

En tot slot moet de rechter ook mee in rekening brengen of de communicatiegegevens de enige en doorslaggevende elementen in de strafzaak zijn die de beoordeling van schuld of onschuld zullen bepalen.

Het Hof van Cassatie nam in recente arresten deze criteria over naast de criteria die het eerder al ontwikkelde en gaf aan dat niet één van deze criteria doorslaggevend was. De focus ligt op de vraag of de verzamelde communicatiegegevens betrouwbaar zijn, of de rechter deze gegevens kan beoordelen op hun betrouwbaarheid en of een beklaagde ook nuttig commentaar kan geven op deze gegevens, bijvoorbeeld door aan te geven dat er een bepaalde reden was waarom zijn smartphone op een bepaald moment op een bepaald plaats gecapteerd was maar hij desondanks niets met het misdrijf te maken heeft. Het Hof van Cassatie kwam dan ook op deze wijze tot het oordeel dat de communicatiegegevens die verzameld werden op de intussen vernietigde wet alsnog gebruikt mochten worden.

Na de vernietiging van de wet over de bewaarplicht van communicatiegegevens was er echter nog een tweede vraag. Nu er geen wettelijke basis meer was voor het bewaren van gegevens, hoe kon het nu verder met het gebruik van deze gegevens in nieuwe en lopende onderzoeken? De wettelijke basis voor het Openbaar Ministerie om identificatiegegevens op te vragen was nog steeds intact waardoor de telecom- en techbedrijven deze gegevens nog steeds moesten meedelen. Onderzoeksrechters vielen op hun beurt terug op de oudere wetgeving op basis waarvan ze nog wel locatie- en verkeersgegevens konden opvragen, maar daarbij rekening moesten houden met de vereisten van het Hof van Justitie. In het overgrote deel van de onderzoeken konden deze gegevens op basis van deze criteria nog steeds aangereikt worden.

De techbedrijven hielden deze gegevens namelijk niet alleen bij omwille van de wet die hen daartoe verplichtte voor de strijd tegen de criminaliteit, maar zij gebruiken deze voor de facturatie, voor technische redenen en ook voor marketing. Online gegevens

zijn namelijk big business en worden wel zoals reeds gezegd eens het nieuwe goud genoemd. Al die gratis online diensten die gebruikt worden, houden in ruil deze gegevens bij en verkopen deze aan allerhande derden. Deze derden gebruiken ze dan weer voor reclame en marketing. Bovendien werden vele gegevens uit het verleden bewaard op basis van de intussen vernietigde regelgeving. Waar dus op korte termijn in veel gevallen gegevens nog wel beschikbaar waren, dreigden deze op langere termijn niet meer beschikbaar te zijn omdat enkel nog die gegevens bewaard zouden worden die nuttig zijn voor de techbedrijven zelf. Daarbij komt dat die techbedrijven niet transparant zijn welke gegevens ze wel nog hebben en welke niet meer of nooit gehad. Op die manier zou Justitie afhankelijk zijn van de willekeur van techbedrijven voor het gebruik van deze gegevens in onderzoeken naar ernstige criminaliteit.

De wetgever oordeelde dat die situatie niet houdbaar was en dokterde dus een nieuwe wet uit.

7. Drie keer is scheepsrecht: de wet inzake dataretentie.

Anderhalf jaar na het arrest nr. 57/2021 van 22 april 2021 van het Grondwettelijk Hof heeft de regering in samenspraak met alle partners – magistratuur, politie, operatoren, inspectiediensten – een nieuw en coherent kader voor dataretentie voorgelegd aan de wetgever dat een evenwicht biedt tussen enerzijds de bekommernissen voor het privéleven, en anderzijds de maatschappelijke belangen van veiligheid en rechtsbescherming.

De wet van 20 juli 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 stapt af van een algemene ongedifferentieerde dataretentie en voert een nieuw perspectief in, in alle transparantie en in lijn met de Europese rechtspraak.

Zonder in detail in te gaan op deze omvangrijke wet, volgen hieronder alvast enkele hoofdlijnen.

De wet gaat vooreerst in op de realiteit zoals reeds uiteengezet dat communicatieverstrekkers reeds zeer veel metagegevens verwerken en bijhouden voor eigen doelstellingen, gegevens die zij nodig hebben om hun diensten überhaupt aan de klant te kunnen verstrekken. Denk aan de locatiegegevens noodzakelijk om de GPS aan te sturen of om een restaurant te kunnen voorstellen bij een citytrip.

Ook houden zij gegevens bij voor de goede werking en de veiligheid van het netwerk of van de dienst of om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, namelijk om ervoor te zorgen dat hun diensten veilig aangeboden kunnen worden.

Ook gebruikt men gegevens om ervoor te zorgen dat hun facturatie correct is en dat deze kan nagekeken worden wanneer de klant plots een gepeperde rekening krijgt voor buitenlands dataverkeer.

Dit alles onder de vereisten en persoonlijke instemming inzake de GDPR.

Belangrijk uitgangspunt is dat enkel voor zover dienstverstrekkers gegevens verwerken, zij verplicht zullen zijn deze gegevens voor bepaalde minimumtermijnen bij te houden.

Dit gaat dus enkel voor gegevens die de dienstverstrekkers zelf al verwerkten en omvat dus geen verplichting om deze gegevens nu plots wel te verwerken waar dit eerder niet gebeurde.

Elke dienstverstrekker hanteert echter thans eigen termijnen gedurende de welke deze gegevens bijgehouden worden.

De nieuwe wet wil hierin transparantie brengen en rechtszekerheid. Die minimumtermijn kan van 4 maanden gaan tot 12 maanden, voor de meest rudimentaire gegevens. Zo creëert de wetgever ook een gelijk speelveld voor al deze dienstverstrekkers.

Daarnaast verplicht de wetgever ook dat bepaalde gegevens bijgehouden worden, los van voormelde eigen doelstellingen, doch opnieuw enkel voor zover die verwerkt of gegenereerd worden in het kader van de verstrekking van die netwerken of diensten.

Het doel van deze bewaringsplicht is het verzekeren van de nationale veiligheid en de strijd tegen de zware criminaliteit.

De eerste soort gegevens zijn de identificatiegegevens[1], zoals reeds eerder vermeld werd. Dit zijn de antwoorden op volgende vragen: “Wie is de gebruiker van een bepaald GSM-nummer, diens naam, adres, wanneer werd deze klant aangemeld, vanop welk IP-adres werd de account aangemaakt, op welk adres wordt de modem geïnstalleerd, welk abonnement heeft deze klant, welk IMSI nummer krijgt de klant”. Deze gegevens moeten worden bijgehouden tot zolang de elektronische communicatiedienst gebruikt wordt en tot twaalf maanden na het einde van de dienst of het einde van de sessie. Telkens het internet betreden wordt, krijgt de gebruiker immers van Telenet, Proximus, etc. (de internet access provider) een nieuw IP-adres geldig voor die sessie. Dynamische IP-adressen wisselen dus tussen gebruikers en sessies. Bij het opsporen van criminelen is het derhalve zeer belangrijk te weten wanneer precies de relevante communicaties gebeurden.

Deze verplichting geldt algemeen en ongedifferentieerd voor alle gebruikers in België, geheel in lijn met de Europese rechtspraak en verschilt niet zoveel van het oude regime. Het verschil ligt erin dat de verschillende identificatiegegevens die moeten worden bewaard indien ze verwerkt worden, nu letterlijk in de wet zelf worden opgesomd en niet langer in een Koninklijk besluit worden opgelijst. Dit komt de transparantie en rechtszekerheid ten goede.

Er zal uiteraard moeten over gewaakt worden dat deze gegevens actueel blijven. Hiertoe is een mechanisme voorzien dat bij Koninklijk besluit andere

[1] Nieuw artikel 126 WEC.

identificatiegegevens (zogenaamde *identifiers*) kunnen worden toegevoegd, maar dat dit binnen een termijn van 6 maanden moet worden bekrachtigd bij wet.

De tweede soort gegevens betreffen de metagegevens, verkeers- en locatiegegevens. Waar en wanneer werd er gecommuniceerd? Hoe lang werd er gebeld?

Deze gegevens mochten niet algemeen en ongedifferentieerd bijgehouden worden. Men moest differentiëren. Zowel naar de doelstelling die de bewaring zou rechtvaardigen, namelijk dat deze gegevens enkel worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijk persoon.

Maar er moest ook gedifferentieerd worden naar het voorwerp van de bewaring, namelijk dat men bv. persoonlijke of geografische criteria zou gebruiken om deze retentie te beperken tot hetgeen noodzakelijk en derhalve gerechtvaardigd is.

Hier voert de wetgever een geheel nieuw kader[2] in.

Ook hier worden de verschillende soorten van metagegevens opgelijst in de wet[3] zelf.

Ook hier betreft het enkel gegevens die reeds door de dienstverstrekker gegenereerd of verwerkt zijn in het kader van zijn dienstverlening.

Er wordt niet met persoonlijke criteria gewerkt. Niet elke veroordeelde of bepaalde bevolkingsgroepen die bovenmatig in de criminaliteitscijfers opduiken worden preventief op een dataretentielijst gezet. Dit zou al snel de deur open zetten voor profiling en discriminatie. Zolang er geen sluitend systeem is om SIM-kaarten aan de effectieve identiteiten te koppelen, zou dergelijk systeem bovendien al te vatbaar zijn voor omzeiling.

Voor de eerste keer worden er geografische zones ingevoerd, zones waarbinnen op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico voor de nationale veiligheid of op het voorbereiden of plegen van feiten van zware criminaliteit. De verschillende types van zones worden opgelijst in de wet, maar de juiste vertaling ervan in exacte locaties zal bij Koninklijk besluit gebeuren op basis van een nauwkeurig omschreven procedure, die elke 3 jaar opnieuw gevolgd moet worden opdat de zones nog actueel relevant zouden zijn.

Over welke zones gaat het nu concreet? Voor de bedreiging van de nationale veiligheid, terrorisme met andere woorden, zal er ook met zones gewerkt worden waarbinnen er een bewaarplicht geldt zolang het dreigingsniveau 3 of hoger is. Denk hierbij aan bv. kerncentrales of andere kritieke infrastructuren. Indien het dreigingsniveau 3 of hoger is voor het gehele grondgebied, zal de bewaarplicht voor het gehele grondgebied gelden. De wet voorziet ook in waarborgen om dergelijke beslissing zo snel mogelijk door het politieke niveau te laten bevestigen. Het is logisch

[2] Nieuw artikel 126/1 WEC.
[3] Nieuw artikel 126/2 WEC.

dat we inzake terrorismebestrijding zo veel mogelijk garanties willen dat er geen informatie verloren gaat.

Maar wat met de bestrijding van de criminaliteit? De wet voorziet ook een bewaarplicht voor zones waar veel criminaliteit gepleegd wordt. Niet zomaar kleine overlast, maar misdrijven die ernstig genoeg geacht worden om opgenomen te worden in de taplijst van artikel 90ter Sv. Zo worden er concreet gerechtelijke arrondissementen en politiezones aangeduid waar afhankelijk van het aantal van dergelijke feiten een bewaartermijn van 6, 9 of 12 maanden zal gelden. De statistieken die hiervoor moeten dienen, zullen uit de Algemene Nationale Gegevensbank (ANG) komen en zullen moeten worden gevalideerd door het Controleorgaan op de politionele informatie.

Daarnaast zijn er gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of aan zware criminaliteit, met name havens, spoorwegstations, luchthavens, gevangenissen, wapenhandel.

De wetgever vermeldt ook zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, zoals de gebouwen waarin de staatsmachten huizen, maar ook politieburelen, grensgemeenten, internationale instellingen, etc. Ook hier is voorzien in een procedure om deze lijsten actueel en relevant te houden met een belangrijke rol voor het Controleorgaan op de politionele informatie en het Vast Comité I.

Teneinde te vermijden dat deze zones openbaar gekend zouden zijn en de mogelijke risico's voor de dataretentie, stelt de wetgever een geheimhoudingsplicht in. Het is immers niet wenselijk dat criminelen of terroristen aan de hand van een eenvoudig appje zouden kunnen vaststellen of ze al dan niet in een zone van bewaarplicht bevinden.

Elke operator moet ook een Coördinatiecel oprichten belast met het verstrekken van de elektronische-communicatiegegevens op verzoek van de wettelijk bevoegde autoriteiten. De wet biedt ook de mogelijkheid om een gemeenschappelijke Coördinatiecel op te richten. Dit zal ervoor zorgen dat er bij elke operator, dus ook de nieuwe OTT's, een *single point of contact* zal zijn waar politie en justitie terecht kunnen met hun vorderingen.

Naast dit nieuwe kader voor gerichte dataretentie, brengt de wet ook een duidelijk kader aan voor gebeurlijke bewaring van gegevens en het gebruik ervan door andere diensten dan politie en justitie, denk aan de administratieve inspectiediensten. De uiteindelijk praktische uitwerking ervan zal moeten gebeuren in de diverse respectievelijke organieke wetten van deze diensten en valt verder buiten bestek van deze mercuriale. Het is echter een goede zaak dat deze wet ook hieraan gedacht heeft en zo tot een algemeen kader komt, zodat Justitie niet als doorgeefluik overladen wordt met aanvragen van dergelijke diensten in het kader van hun eigen bevoegdheden. Een bijzondere vermelding verdient het Centrum voor Cybersecurity Belgium, dat met deze nieuwe wetgeving zelf de bevoegdheid zal krijgen om o.a. IP-adressen te identificeren in het kader van hun bevoegdheden, hetgeen zal toelaten om sneller te schakelen en meer cybercriminaliteit te voorkomen.

Er wordt ook nog een nieuw instrument ingevoerd in het kader van het strafrechtelijk onderzoek.

In het wetboek van strafvordering wordt in artikel 39quinquies Sv. namelijk een *future freeze* ingevoerd. Dit houdt een bevel in gericht aan operatoren om verkeers- en locatiegegevens die ze verwerken vanaf het moment van de vordering die ook mondeling gegeven kan worden, te bewaren en niet meer te verwijderen, in afwachting van een vordering om toegang te krijgen tot deze gegevens. Dergelijk bevel geldt voor 2 maanden en kan verlengd worden, met een maximale looptijd van 6 maanden. Dit precisie-instrument zal toelaten om in individuele strafrechtelijke onderzoeken tegemoet te komen aan gebeurlijke lacunes in de dataretentie. Zo kan een welbepaald toestel geviseerd worden, ongeacht in welke zones dit zich zou begeven. Men zou ook bepaalde locaties kunnen bevragen, die misschien onder het algemene kader geen retentie toelaten voor de bestrijding van zware criminaliteit. Dit nieuwe kader zal wellicht leiden tot een verschuiving in de manier waarop vandaag de dag de onderzoeken gevoerd worden. Men zal er niet meer van kunnen uitgaan dat gegevens sowieso bewaard worden of beschikbaar zijn, maar in elk dossier zal moeten nagegaan worden wat er mogelijk, voorradig en proportioneel is, welke toestellen of locaties interessant zijn en dan vervolgens zo snel mogelijk het nodige te doen om te verzekeren dat deze gegevens niet verloren gaan. Daarmee zal het bewaren in grote mate de logica volgen die nu al gehanteerd wordt voor het opvragen van gegevens, namelijk dat steeds wordt nagegaan of de gegevens nodig zijn voor het onderzoek, het opvragen van de gegevens proportioneel is voor het op te sporen of op te lossen misdrijf, en of ze voorradig zijn.

Dit alles zal uiteraard niet van vandaag op morgen mogelijk zijn, maar zal een proces worden waarover een ieder betrokken bij de wet zich zal moeten buigen. De wet voorziet dan ook in een ruime overgangsbepaling en stelt de inwerkingtreding van dit nieuwe kader uit tot uiterlijk 1 september 2027. Dit geeft niet alleen de ruimte om de werkprocessen bij te werken, maar werd vooral ingegeven in het belang van de operatoren.

Die operatoren zullen immers hun handen vol hebben aan het technisch vertalen van dit wettelijk kader. Sommige verplichtingen zullen echter al sneller gelden voor de dienstenverstrekkers binnen de 24 maanden na bekendmaking van de wet. Wat echter nu al zeker lijkt, is dat het een waar huzarenstuk zal worden om voor al deze verschillende soorten gegevens de verschillende dataretentieregimes technisch te vertalen in een robuuste en werkbare architectuur die zal toelaten om in real-time op mondelinge vorderingen te schakelen en gegevens veilig te stellen.

8. De toekomst – veiligheid & privacy geen zero sum game.

Het Hof van Justitie zette strenge lijnen uit om een evenwicht te vinden tussen enerzijds de bescherming van privacy en anderzijds de strijd tegen criminaliteit en de bescherming van de openbare en nationale veiligheid. Het bewaren van gegevens is zeker niet het enige punt van discussie in de zoektocht naar dit evenwicht. Het zal u niet ontgaan zijn dat eenzelfde debat wordt gevoerd over het versleutelen van communicatiegegevens. Digitale technologie maakt het mogelijk om alle gegevens en communicatie die we versturen onleesbaar te maken voor derden, wat we versleutelen

of encryptie noemen. Dit heeft grote voordelen naar privacy en veiligheid. Zo kunnen we ons beschermen tegen cybercriminelen of buitenlandse mogendheden die graag zouden meelezen. Denk maar aan al de verrichtingen via bankapplicaties. Zonder het versleutelen zouden deze transacties bijzonder onveilig zijn.

Maar zoals het in de digitale wereld gaat, heeft elk voordeel zijn nadeel. Ook criminelen maken gretig gebruik van versleuteling om te voorkomen dat hun misdrijven worden ontdekt, dat zij geïdentificeerd worden en bewijs wordt verzameld. Justitie botst hierbij steeds meer op de ondoordringbare barrières van versleuteling. Wanneer gegevens gevraagd worden aan internetdienstverleners wordt vaak geantwoord dat de gegevens niet in een leesbare vorm gegeven kunnen worden omdat deze versleuteld zijn. Opnieuw een uitdaging om het evenwicht te zoeken tussen privacy en veiligheid: moet encryptie beperkt worden om onze veiligheid te garanderen, of is dit, zoals privacy-experten voorhouden, een verkeerde afweging omdat encryptie ook onze veiligheid beschermt?

Opnieuw een blik naar Europa. De Europese Unie nam initiatieven in de strijd tegen online netwerken waar kindermisbruikmateriaal versleuteld wordt uitgewisseld door digitale dienstverleners om te verhinderen dat versleuteling het onmogelijk zou maken om nog automatisch kindermisbruikmateriaal te detecteren.

Ook de nieuwe bewaarwet stelt grenzen aan versleuteling. Ze verhindert dat digitale dienstverleners zich achter versleuteling verschuilen doordat de wet eist dat de gegevens in een leesbare vorm worden gegeven. Het gaat hier dus om de zogenaamde metagegevens waar we het over hadden, wie wanneer waar communiceerde of online aanwezig was, en niet om inhoud van de communicatie.

De toekomst zal uitwijzen waar hier het evenwicht moet komen te liggen. Maar een evenwicht moet er zijn en het debat moet gevoerd worden. Een kader waarbij privacy per definitie als ondergeschikt aan de bestrijding van criminaliteit wordt beschouwd en er anderzijds geen beperkingen zijn in het bijhouden en gebruik van communicatiegegevens, past niet binnen een democratische rechtsstaat. Een democratie moet scherp waken over welke gegevens bewaard worden en op welke manier onafhankelijke rechters streng toekijken op het gebruik.

Maar ook privacy-experten moeten het debat ernstig aangaan in de zoektocht naar een digitale wereld waarin de privacy zo goed mogelijk beschermd wordt terwijl voorkomen wordt dat het internet constant misbruikt wordt om strafbare feiten te plegen.

Het is hierbij niet ernstig om te starten vanuit het uitgangspunt dat het Openbaar Ministerie binnen het kader van een democratische rechtsstaat eropuit is om elke burger te controleren en buitensporig datahongerig is.

Het zal u niet ontgaan zijn dat bepaalde overheden of onderzoekers, zij het politieagenten, Openbaar Ministerie of onderzoeksrechters wel eens sterk uit de hoek komen in reactie op dergelijke argumenten. Ook bij mij knaagt het. Politie en Justitie kunnen deze gegevens maar opvragen binnen een sterk gereglementeerd kader, waarbij rechters steeds een controle uitvoeren, zowel tijdens het onderzoek als erna. Er mag ook niet vergeten worden dat zowel de techbedrijven meekijken of de

verzoeken wel wetsconform zijn en dat tot slot ook de verdediging inzage neemt van het ganse proces. Het kader is dus streng, evenals de controle ervan.

Toch komen deze verwijten vooral de kant uit van Justitie en is er een ernstige beperking voor het gebruik van locatie- en verkeersgegevens voor vervolgende autoriteiten. Nochtans zijn de grote privacy-schandalen in de media niet het gevolg van het gebruik door justitie in concrete strafonderzoeken in democratische staten, maar wel door veiligheidsdiensten of door techbedrijven zoals Cambridge Analytica. Die grote techbedrijven verzamelen massaal veel gegevens die bijzonder gevoelig zijn en met nagenoeg geen controle over het bijhouden en het gebruik ervan.

Techbedrijven moeten zich weliswaar conformeren met Europese regelgeving zoals de verordening gegevensbescherming, de zogenaamde GDPR, en de nieuwe digitale diensten- en marktenwet, maar er is nauwelijks controle en transparantie.

Dat vervolgende autoriteiten binnen zo'n kader als niet te vertrouwen data-vampieren worden weggezet door sommigen, is geen ernstige basis voor een goed debat.

Het staat buiten kijf dat Justitie moet opereren binnen een strikt wettelijk kader waarbij proportionaliteit en subsidiariteit bij het gebruik van communicatiegegevens de leidraad zijn. Dat sommige gegevens zelfs helemaal buiten het bereik zijn en moeten zijn van Justitie of slechts onder strenge voorwaarden kunnen worden ter kennis gebracht zoals de vertrouwelijke communicatie tussen een arts en patiënt in het kader van het medisch beroepsgeheim of advocaat en cliënt in het kader van de vertrouwelijke communicatie, zijn basisprincipes van het strafrecht en strafprocesrecht.

Hierbij mag niet uit het oog verloren worden dat de wet geen bewaring van de inhoud van de communicatie verplicht en die kan dus niet zomaar opgevraagd worden. Dit laatste is een belangrijke waarborg voor de privacy en bescherming van de vrijemeningsuiting. Anderzijds zijn veel cybercriminelen erop uit om privacy te gijzelen voor het groot financieel gewin. Denk maar aan de trend van dubbele afpersing bij ransomware. Dit is software waarbij computers worden versleuteld door criminelen en maar weer worden vrijgegeven tegen de betaling van een fikse som aan cryptocurrency. Om de druk op het gegijzelde bedrijf op te drijven, hacken de criminelen veelal voorafgaand in het netwerk van het bedrijf en stelen alle gegevens die het bijhoudt. Als een bedrijf dan toch weigert om het losgeld voor de ontsleuteling van hun software te betalen, dreigen ze ermee om alle gegevens online prijs te geven, waaronder zeer gevoelige persoonlijke gegevens van werknemers, klanten en gebruikers. Stel dat een abortuskliniek in de VS hiermee geconfronteerd wordt.

Is dat evenwicht tussen veiligheid en privacy gevonden in de nieuwe bewaarwet? Drie keer is scheepsrecht, wordt in deze havenstad gezegd, maar het is nog maar af te wachten of dit ook zo zal zijn voor de wet.

Nog voor de wet in het parlement werd besproken en gestemd, kondigden belangengroepen al op sociale media aan dat ze deze wet voor het grondwettelijk hof zouden aanvechten. Bovendien hangen ook nog tal van andere zaken voor het Hof van Justitie en het Europees Hof voor de Rechten van de Mens, die hier een directe impact op zullen hebben.

De logica wil dat ook deze wet op termijn dus opnieuw op het bord van het Hof van Justitie zal belanden met alle onzekerheid tot gevolg. Het is eenieders recht om dit te doen en deze afweging vraagt ook om een scherp juridisch en democratisch toezicht.

Er zijn veel redenen om de wet te verdedigen. De wet hanteerde de handvaten die het Europese hof heeft aangereikt in de arresten, namelijk dat de algemene bewaring van gegevens alleen maar wordt toegelaten voor identificatiegegevens en voor de bescherming van de nationale veiligheid bij een ernstige dreiging. De wet stapt af van een algemene bewaring van locatie- en verkeersgegevens voor de strijd tegen ernstige criminaliteit en een ernstige verstoring van de openbare orde. Deze mogen in lijn met de Europese rechtspraak enkel gericht bewaard worden, namelijk op basis van een gericht bevel ofwel voor bepaalde personen ofwel voor bepaalde zones.

Daarmee is echter niet alles gezegd. De vraag die vandaag al wordt gesteld is of die zones niet te breed gedefinieerd zijn waardoor het erop neer zou komen dat het hele Belgische grondgebied wordt gedekt. De Gegevensbeschermingsautoriteit bekritiseerde de overheid omdat deze concrete toetsing nog niet gebeurde, namelijk wat de criteria nu concreet betekenen voor het bewaren van gegevens in België.

Bovendien zal het Hof van Justitie zich nog moeten buigen over de vraag of de Belgische wetgeving deze gerichte bewaring van locatie- en verkeersgegevens en de toegang ertoe voor de onderzoeksrechter wel alleen toelaat voor ernstige misdrijven. In vorige rechtspraak weigerde het Hof van Justitie al eens te bepalen wat nu juist een ernstig misdrijf is. Het Hof gaf aan dat het aan de nationale rechters is om de ernst van het misdrijf af te wegen tegen de ernst van de beperking van de privacy.

Daar lijkt m.i. aan voldaan door de wet. Deze gegevens kunnen alleen maar opgevraagd worden voor misdrijven die ook aanleiding kunnen geven tot de vrijheidsbeneming, namelijk waar een hoofdgevangenisstraf van 1 jaar op staat. Als het misdrijf voldoende ernstig is om de vrijheid van iemand te ontnemen, lijkt dit ook de drempel van de ernst voor het bewaren en opvragen van locatie- en verkeersgegevens te halen.

De nieuwe wet is niet het eindpunt. Dataretentie zal ongetwijfeld nog genoeg voer leveren voor de komende mercuriales. Daarom is het noodzakelijk om de werking van deze nieuwe wetgeving en de gevolgen ervan op het terrein duidelijk in kaart te brengen. Meten is weten.

9. Een call to action: proefproject dataretentie.

Transparantie is een belangrijk element in het debat. En dat was ongetwijfeld het zwakste element over de afweging privacy versus veiligheid. Verschillende overheden voerden voor het Hof van Justitie aan dat deze communicatiegegevens essentieel zijn voor het oplossen van misdrijven, terwijl privacy-experten dit ontkrachtten en aangaven dat misdrijven evengoed zonder deze gegevens konden opgelost worden. Ook in België werd tijdens de parlementaire debatten bij de totstandkoming van deze wet aangevoerd dat in deze of gene studie uit het buitenland zou blijken dat dataretentie niet voor meer opheldering zou zorgen. Nochtans zijn de adviezen van

de bevraagde experten inzake strafrechtelijk onderzoek, te weten de politiediensten, vereniging van onderzoeksrechters en het College van procureurs-generaal, unaniem in de overtuiging dat het bevragen van metagegevens absoluut noodzakelijk is om in nagenoeg elk onderzoek de waarheid aan het licht te brengen en dat andere onderzoeksmethoden niet dezelfde resultaten hebben, tenzij ze een nog verregaandere inbreuk op het privéleven van betrokkenen teweegbrengen.

Denk daarbij aan de telefoontap of het hacken van een toestel op afstand, waarbij meteen ongefilterd zicht gekregen wordt op elke communicatie, elk verzonden bericht of persoonlijke foto.

Door het gebrek aan duidelijke cijfers werd zowel op het federale als Europese niveau een debat gevoerd op basis van principes en assumpties, maar al te vaak zonder dat dit gestaafd werd door betrouwbare cijfers. Niet omdat de cijfers niet mededeelbaar waren maar simpelweg omdat ze niet systematisch werden bijgehouden. Transparantie over cijfers kan dan ook een belangrijke bijdrage leveren aan het debat in de toekomst.

Het is dan ook positief dat in de nieuwe wetgeving wordt voorzien in het opvolgen van de toepassing van de wet. Het BIPT zal jaarlijks aan de bevoegde ministers statistieken moeten overmaken over de verstrekking aan de autoriteiten van gegevens die bewaard worden krachtens de nieuwe artikelen 122, 123, 126, 126/1, 126/3 en 127. Deze ministers sturen op hun beurt die statistieken jaarlijks door naar de Kamer van volksvertegenwoordigers[4]. Deze statistieken geven een beeld van de gegevens die bevraagd worden, de tijd verstreken tussen de datum van bewaring van de gegevens en het opvragen ervan en of er al dan niet gegevens verstrekt konden worden. Dit zal duidelijkheid bieden welke informatie het meest bevraagd wordt en hoe oud deze informatie is. Bovendien zullen de cijfers kunnen aantonen of onze bewaarverplichting al dan niet een te ruime periode beslaat dan wel te krap is in de praktijk.

Deze cijfers laten echter niet toe om na te gaan of de meegedeelde informatie überhaupt nuttig was voor het onderzoek, dan wel of het geen relevante elementen voor het strafrechtelijk onderzoek bevatte. Bovendien moeten die cijfers aantonen op welke wijze deze gegevens een rol spelen in het strafonderzoek: om beter zicht te krijgen op de feiten, om een verdachte te identificeren dan wel om slachtoffers te vinden. Die analyse kan enkel gebeuren op een case-by-case manier en op basis van het concrete strafdossier en de verkregen gegevens. Dergelijke informatie is essentieel om eindelijk een antwoord te bieden op de vraag wat nu het belang is van deze gegevens binnen een strafrechtelijk onderzoek.

Hierbij wordt dan ook het Openbaar Ministerie opgeroepen om de impact van deze nieuwe wet in het werkveld van nabij op te volgen. Niet alleen de hoeveelheid vorderingen inzake telefoniegegevens zijn relevant, maar bovenal de vraag naar de resultaten van die vorderingen. Wat is de impact ervan in het onderzoek ? Zodoende zal in alle transparantie in kaart kunnen gebracht worden welke rol deze gegevens spelen, los van anekdoten. Deze steekproef zal dan ook van wezenlijk belang zijn bij de toekomstige betwistingen over de verenigbaarheid van deze nieuwe wetgeving met

[4] Nieuw artikel 127/1 § 7.

de fundamentele rechten zoals voorzien in de Europese verdragen en in de rechtspraak van de hoogste rechtsinstanties.

Op die manier wordt alvast tegemoet te komen aan de verwachtingen van het Hof van Justitie in het bijzonder en de maatschappij in het algemeen en hoeft niet gevreesd te worden dat persoonlijke gegevens zomaar te grabbel worden gegooid. In elk onderzoek zal aldus een proportionele en subsidiaire afweging gemaakt worden tussen de talrijke belangen die spelen, privacy, recht op een efficiënt rechtsmiddel, recht op bescherming van leven, veiligheid en eigendom met deze nieuwe wetgeving als duidelijk kader.

Willen we het schip op koers houden op die fijne doch essentiële lijn tussen privacy en veiligheid, behoeft de kapitein duidelijke coördinaten. Laten we daarvoor zorgen.