Rechtbank Den Haag
Zitting van 18 februari 2015
Nr. 480009 KG ZA 14/1575

Conclusie van antwoord

inzake

Staat der Nederlanden (ministerie van Economische Zaken en ministerie van Veiligheid en Justitie)
gevestigd te Den Haag

gedaagde
advocaten: mr. C.M. Bitter en
mr. R.J.M. van den Tweel

tegen

Stichting Privacy First
gevestigd te Amsterdam
Nederlands Juristen Comité voor de Mensenrechten
gevestigd te Leiden
Nederlandse Vereniging van Strafrechtadvocaten
gevestigd te Goirle
Nederlandse Vereniging van Journalisten
gevestigd te Amsterdam
BIT B.V.
gevestigd te Ede
SpeakUP B.V.
gevestigd te Enschede
Voys B.V.
gevestigd te Groningen

eisers
advocaten: mr. F.F. Blokhuis en
mr. O.M.B.J. Volgenant

1 Inleiding

1.1 Op 8 april 2014 heeft het Hof van Justitie van de Europese Unie (hierna: het Hof) de Dataretentierichtlijn[1] ongeldig verklaard.[2] Het Hof heeft geoordeeld dat de Dataretentierichtlijn in strijd is met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest). Deze artikelen omvatten het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens.

1.2 De Dataretentierichtlijn is in Nederland geïmplementeerd door middel van de Wet bewaarplicht telecommunicatiegegevens (hierna: Wbt).[3] Volgens eisers vloeit uit het feit dat de Dataretentierichtlijn in strijd is met de artikelen 7 en 8 van het Handvest voort, dat ook de daarop gebaseerde Wbt in strijd is met de artikelen 7 en 8 van het Handvest. De Wbt zou daarom volgens eisers buiten werking moeten worden gesteld.

1.3 De Staat ziet voor buitenwerkingstelling echter geen aanleiding. Aan het criterium dat de Wbt 'onmiskenbaar onverbindend' is, is niet voldaan.[4] De Staat zal dat toelichten op de zitting van 18 februari 2015. Omdat het juridisch kader van de Dataretentierichtlijn en de relevante nationale wetgeving complex is, wordt het juridisch kader in deze conclusie van antwoord alvast uiteengezet. Ook worden met deze conclusie enkele producties in het geding gebracht. De Staat zal in zijn pleidooi naar deze producties verwijzen en zijn verweer nader uiteen zetten.

2 Vooraf

2.1 De op basis van dit juridisch kader uitgeoefende bevoegdheden moeten niet worden verward met andere bevoegdheden.

2.2 Op grond van het Wetboek van Strafvordering (hierna: Sv) kan de officier van justitie in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan, in het belang van het onderzoek verkeers- en gebruikersgegevens vorderen van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot deze gegevens.

2.3 De Wbt stelt zeker dat telecommunicatiegegevens tot een half jaar respectievelijk een jaar na datum van de communicatie bewaard blijven, zodat deze gegevens beschikbaar zijn voor de opsporing. De gegevens worden bewaard door de aanbieders

[1] Richtlijn 2006/24/EG 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 2002/58/EG (*Pb* 2006, L 105/54).
[2] HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238.
[3] *Stb.* 2009, 333.
[4] HR 1 juli 1983, *NJ* 1984, 360, r.o. 3.4.

van telecommunicatiediensten zelf; zij zijn dus niet bij politie/justitie opgeslagen. De Wbt heeft geen betrekking op de inhoud van de communicatie, en ziet ook niet op de onderschepping en analyse van actuele informatie (tappen, data mining, data freeze, etc.). Met 'mass surveillance' heeft de Wbt al helemaal niets van doen.

3 Juridisch kader

3.1 De Dataretentierichtlijn

3.1.1 De Dataretentierichtlijn is in werking getreden op 3 mei 2006.[5] De richtlijn had tot doel de nationale wetgeving van de lidstaten met betrekking tot het bewaren en verwerken van telecommunicatiegegevens door de aanbieders van telecommunicatiediensten en -netwerken te harmoniseren, zodat deze gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[6]

3.1.2 Artikel 3 van de richtlijn legde de lidstaten de verplichting op om ervoor te zorgen dat telecommunicatiegegevens worden bewaard. Welke gegevens bewaard moeten worden, volgde uit artikel 5 van de richtlijn. Het ging om telefoongegevens en om internetgegevens.

3.1.3 Bij beide soorten gegevens ging het om 'verkeersgegevens' en 'locatiegegevens'.[7] Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie of voor de facturering ervan, zoals gegevens over de datum, het tijdstip en de duur van de communicatie.[8] Locatiegegevens zijn gegevens waarmee de geografische positie van de communicatieapparatuur kan worden bepaald.[9] Daarnaast moesten gegevens worden bewaard die nodig zijn om de abonnee of gebruiker van de communicatiedienst te identificeren,[10] zoals naam en adres van de telefoon- of internetabonnee. Deze gegevens worden ook wel aangeduid als 'gebruikersgegevens'. Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mochten op grond van de richtlijn niet worden bewaard.[11]

3.1.4 Artikel 6 van de richtlijn bevatte de bewaartermijn van de gegevens. Het artikel bepaalde dat de lidstaten ervoor moeten zorgen dat de gegevens gedurende ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie werden bewaard. De verdere invulling hiervan werd aan de lidstaten overgelaten.

[5] Zie artikel 16 Dataretentierichtlijn. Nederland heeft gebruikgemaakt van de mogelijkheid tot uitstel.
[6] Artikel 1 Dataretentierichtlijn.
[7] Zie ook artikel 2 lid 2 aanhef en onder a Dataretentierichtlijn.
[8] Artikel 2 lid 1 Dataretentierichtlijn jo. artikel 2 aanhef en onder b Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*Pb* 2002, L 201/37) (hierna: e-Privacyrichtlijn).
[9] Artikel 2 lid 1 Dataretentierichtlijn jo. artikel 2 aanhef en onder c e-Privacyrichtlijn.
[10] Zie ook artikel 2 lid 2 aanhef en onder a Dataretentierichtlijn.
[11] Artikel 5 lid 2 Dataretentierichtlijn.

3.1.5 Artikel 4 van de richtlijn regelde de toegang tot de bewaarde gegevens. Het artikel bepaalde dat de lidstaten moeten waarborgen dat de bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde nationale autoriteiten werden verstrekt. Aspecten van toegang tot de gegevens die door de aanbieders werden bewaard ten behoeve van de opsporing en vervolging van strafbare feiten, vielen niet onder de Europese wetgeving.[12] Het was aan de lidstaten daar verder invulling aan te geven. De lidstaten moesten daarbij rekening houden met de relevante bepalingen van het recht van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM).

3.1.6 Artikel 7 van de richtlijn bepaalde dat de lidstaten ervoor moeten zorgen dat aanbieders van elektronische telecommunicatiediensten en aanbieders van publieke telecommunicatienetwerken met betrekking tot de bewaarde gegevens ten minste de volgende beginselen van gegevensbeveiliging respecteerden:

- de bewaarde gegevens hebben dezelfde kwaliteit en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;
- de gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
- de gegevens worden onderworpen aan passende technische en organisatorische maatregelen om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen; en
- de gegevens worden aan het einde van de bewaarperiode vernietigd, met uitzondering van de geraadpleegde en vastgelegde gegevens.

3.1.7 Artikel 9 van de richtlijn bepaalde dat elke lidstaat ervoor zorgt dat één of meer overheidsinstanties verantwoordelijk worden gesteld voor het toezicht op de beveiliging van de bewaarde gegevens.

3.2 De implementatie van de Dataretentierichtlijn in Nederland

Inleiding

3.2.1 De Dataretentierichtlijn is in Nederland geïmplementeerd door middel van de Wbt, die op 1 september 2009 in werking is getreden.[13] De Wbt bevat bepalingen tot wijziging van de Telecommunicatiewet (hierna: Tw) en de Wet op de economische delicten, in

[12] Overweging 25 van de Dataretentierichtlijn.
[13] *Stb.* 2009, 360

verband met de bewaring van de gegevens door de aanbieders ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De Tw bevat regels over de telecommunicatie-infrastructuur en telecommunicatiediensten. Dit omvat regels voor de aanbieders van telecommunicatiediensten over de bescherming van de persoonlijke levenssfeer (hoofdstuk 11) en verplichtingen op het gebied van het aftappen (hoofdstuk 13). Deze regels zijn verder uitgewerkt in het Besluit beveiliging gegevens telecommunicatie.[14]

3.2.2 De bepalingen over toegang en de waarborgen voor het gebruik daarbij staan in het Wetboek van Strafvordering (Sv), het daarop gebaseerde Besluit vorderen gegevens telecommunicatie[15] en de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (WIV 2002). Genoemde bepalingen bestonden al vóór de inwerkingtreding van de Dataretentierichtlijn.

De bewaarplicht

3.2.3 De Wbt legt aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten de verplichting op om telecommunicatiegegevens te bewaren ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.[16] De bijlage bij de Wbt bepaalt welke gegevens bewaard moeten worden. Het gaat om dezelfde gegevens als de gegevens die op grond van de Dataretentierichtlijn bewaard moeten worden.

3.2.4 Op grond van de Wbt is de bewaartermijn voor de gegevens twaalf maanden.[17] Aanvankelijk voorzag het wetsvoorstel in een bewaartermijn van 18 maanden voor telecomgegevens. Overeenkomstig het advies van de Raad van State is die termijn teruggebracht tot twaalf maanden. De Tw is na de inwerkingtreding van de Wbt aangepast,[18] waardoor er vanaf 16 juli 2011 een onderscheid wordt gemaakt tussen telefoongegevens en internetgegevens. De bewaartermijn voor telefoongegevens is twaalf maanden.[19] De bewaartermijn voor internetgegevens is zes maanden.[20]

De toegang tot bewaarde gegevens

3.2.5 De Wbt bevat geen bepalingen over de toegang tot de bewaarde gegevens ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven, omdat de nationale wetgeving daarover ten tijde van de inwerkingtreding van de Wbt reeds gedetailleerde bepalingen kende.[21] De bepalingen over de toegang tot de bewaarde gegevens zijn opgenomen in Sv en de WIV 2002. De wetgever zag geen aanleiding om

[14] *Stb.* 2003, 472 (nadien gewijzigd).
[15] *Stb.* 2004, 394 (nadien gewijizgd).
[16] Artikel 13.2a lid 2 Tw.
[17] Artikel 1 aanhef en onder c Wbt.
[18] *Stb.* 2011, 350.
[19] Artikel 13.2a lid 3 aanhef en onder a Tw.
[20] Artikel 13.2a lid 3 aanhef en onder b Tw.
[21] *Kamerstukken II* 2006/07, 31 145, nr. 3, p. 19.

deze bepalingen aan te passen. Blijkens zijn advies zag ook de Raad van State die aanleiding destijds niet.[22]

3.2.6 Op grond van de artikelen 126n en 126u Sv kan de officier van justitie in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan of een redelijk vermoeden dat in georganiseerd verband dergelijke misdrijven worden geraamd of gepleegd,[23] in het belang van het onderzoek verkeers- en gebruikersgegevens vorderen. Op grond van artikel 126zh Sv kan de officier van justitie van deze bevoegdheid ook gebruikmaken in geval van aanwijzingen van een terroristisch misdrijf.

3.2.7 Op grond van de artikelen 126na, 126ua en 126zi Sv zijn ook opsporingsambtenaren bevoegd om in het belang van het onderzoek bepaalde telecommunicatiegegevens te vorderen. Zij kunnen in geval van verdenking van een misdrijf of in geval van aanwijzingen van een terroristisch misdrijf alleen gebruikersgegevens[24] vorderen.

3.2.8 Tot slot kan nog worden vermeld dat de officier van justitie op grond van artikel 126hh Sv de bevoegdheid heeft om gegevensbestanden te vorderen.[25] Van deze bevoegdheid wordt in de praktijk (thans) echter nauwelijks gebruikgemaakt.[26]

3.2.9 Uit de wettelijke regeling vloeit voort dat de bewaarde verkeersgegevens slechts beschikbaar kunnen komen ten behoeve van een concreet opsporingsonderzoek naar een ernstig strafbaar feit, op basis van concrete vermoedens van betrokkenheid van personen bij het beramen of plegen van dat misdrijf.

3.2.10 Op grond van artikel 28 WIV 2002 zijn de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) bevoegd zich te wenden tot aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten met het verzoek gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker.

3.2.11 Op grond van artikel 29 WIV 2002 zijn de AIVD en de MIVD bovendien bevoegd zich te wenden tot aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten met het verzoek gegevens te verstrekken over naam, adres,

[22] *Kamerstukken II* 2006/07, 31 145, nr. 5.

[23] Artikel 67 Sv bepaalt voor welke misdrijven voorlopige hechtenis is toegestaan. Het gaat bijvoorbeeld om misdrijven waarop een gevangenisstraf van vier jaar of meer is gesteld.

[24] Naw-gegevens

[25] Onder gegevensbestand wordt verstaan: een gestructureerd geheel van persoonsgegevens, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (artikel 1 aanhef en onder c Wbp).

[26] De officier van justitie kan van deze bevoegdheid gebruikmaken in geval van een verkennend onderzoek naar terroristische misdrijven. Voor gebruikmaking van de bevoegdheid is een schriftelijke machtiging van de rechter-commissaris vereist.

postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie.

3.2.12 De Wbt bevestigt dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten aan een vordering op grond van Sv of een verzoek op grond van de WIV 2002 moeten voldoen.[27]

De bescherming en beveiliging van bewaarde gegevens

3.2.13 Hoofdstuk 13 van de Tw bevat algemene regels over de bescherming en beveiliging van persoonsgegevens door de aanbieders, in aanvulling op de Wet bescherming persoonsgegevens (hierna: Wbp). Meer specifiek voor de bescherming en beveiliging van de bewaarde telecommunicatiegegevens bepaalt de Wbt dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten passende technische en organisatorische maatregelen nemen teneinde:

- de gegevens te beveiligen tegen vernietiging, tegen verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking;
- te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen;
- de gegevens te kunnen vernietigen na afloop van de bewaartermijn.[28]

3.2.14 Ook bepaalt de Wbt dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten ervoor zorgen dat de bewaarde gegevens:

- dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;
- onverwijld worden vernietigd na afloop van de periode, bedoeld in artikel 13.2a, derde lid.[29]

3.2.15 Deze regels zijn verder uitgewerkt in het Besluit beveiliging gegevens telecommunicatie, dat regels bevat over de beveiliging van de gegevens door de aanbieders.[30] Zo bepaalt artikel 2 van het Besluit dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zorg dragen voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming van de gegevens door onbevoegden te voorkomen. Artikel 3 van het Besluit bepaalt dat de aanbieders zorg dragen voor een beveiligingsplan, waarin is aangegeven op welke wijze uitvoering wordt gegeven aan de beveiligingsplicht. Artikel 4 van het Besluit bepaalt dat uitsluitend personen die een verklaring omtrent het gedrag hebben overgelegd, medewerking kunnen verlenen aan een vordering van gegevens. Artikel 5

[27] Artikelen 13.2b en 13.4 Tw.
[28] Artikel 13.5 lid 2 Tw.
[29] Artikel 13.5 lid 3 Tw.
[30] *Stb.* 2003, 472 (nadien gewijzigd).

bepaalt dat de aanbieders ervoor zorgen dat de bewaarde gegevens na afloop van de bewaartermijn 'onverwijld doch uiterlijk binnen acht dagen' worden vernietigd.

Het toezicht op bewaarde gegevens

3.2.16 Het toezicht op de naleving van de Wbt wordt uitgeoefend door het Agentschap Telecom van het ministerie van Economische Zaken.[31] Het toezicht betreft:

- het naleven van de verplichting tot het bewaren van gegevens;
- de bij nadere regels gestelde eisen aan de wijze waarop de gegevens bewaard worden;
- de waarborgen tegen misbruik van de bewaarde gegevens; en
- tijdige vernietiging van de gegevens na afloop van de bewaartermijn.[32]

Daarnaast houdt het College bescherming persoonsgegevens toezicht op de verwerking van gegevens die zijn aan te merken als persoonsgegevens.[33]

3.3 Het arrest van het Hof van Justitie

3.3.1 In een arrest van 8 april 2014 heeft het Hof de Dataretentierichtlijn ongeldig verklaard. Het Hof stelt in zijn arrest vast dat de door de richtlijn opgelegde bewaarplicht een inmenging vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten.[34] Daarbij stelt het Hof voorop dat de inhoud van de communicatie niet wordt bewaard, hetgeen aard en ernst van de inmenging nuanceert.

3.3.2 De inmenging voldoet volgens het Hof aan een doel van algemeen belang, namelijk de bestrijding van ernstige criminaliteit ter waarborging van de openbare veiligheid.[35] De inmenging is volgens het Hof bovendien geschikt om dit doel te bereiken.[36] Het Hof is echter van oordeel dat de inmenging niet beperkt is tot het strikt noodzakelijke. Het Hof komt tot dat oordeel op basis van een samenstel van omstandigheden.

3.3.3 In de eerste plaats stelt het Hof vast dat de richtlijn algemeen van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens.[37] Het Hof merkt op dat de richtlijn dus ook van toepassing is op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag een verband toont met zware

[31] Artikel 15 lid 1 aanhef en onder i Tw jo. artikel 2 lid 1 Besluit aanwijzing toezichthouders Telecommunicatiewet.
[32] *Kamerstukken II* 2006/07, 31 145, nr. 3, p. 13.
[33] Artikel 51 lid 1 Wbp.
[34] Punt 32 tot en met 37 van het arrest.
[35] Punt 41 tot en met 44 van het arrest.
[36] Punt 49 en 50 van het arrest.
[37] Punt 57 tot en met 59 van het arrest.

criminaliteit. Ook vereist de richtlijn geen verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid.

3.3.4 In de tweede plaats overweegt het Hof dat de richtlijn geen objectieve criteria ter begrenzing van de toegang tot de gegevens bevat.[38] Volgens het Hof wordt in de richtlijn niet precies genoeg gedefinieerd in geval van welke strafbare feiten toegang tot de gegevens gerechtvaardigd is. Bovendien bevat de richtlijn geen materiële en procedurele voorwaarden betreffende de toegang tot de gegevens.

3.3.5 In de derde plaats acht het Hof van belang dat voor wat betreft de bewaartermijn geen onderscheid wordt gemaakt tussen de verschillende categorieën gegevens.[39] Ook merkt het Hof op dat de bewaartermijn varieert van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.[40]

3.3.6 Uit het samenstel van deze omstandigheden leidt het Hof af dat de bepalingen in de richtlijn onvoldoende duidelijk en precies zijn om te kunnen waarborgen dat de inmenging in de artikelen 7 en 8 Handvest beperkt blijft tot het strikt noodzakelijke.[41] Er is daarom volgens het Hof sprake van een schending van deze artikelen.

3.3.7 Ten overvloede merkt het Hof op dat de richtlijn onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan.[42] In de eerste plaats bevat de richtlijn geen specifieke regels die aangepast zijn aan de hoeveelheid gegevens die volgens de richtlijn moeten worden bewaard en aan het gevoelige karakter van de gegevens. In het bijzonder waarborgt de richtlijn volgens het Hof niet dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd. In de tweede plaats schrijft de richtlijn niet voor dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard, zodat niet gewaarborgd is dat een onafhankelijke autoriteit toezicht houdt op de eisen op het gebied van bescherming en beveiliging.

[38] Punt 60 tot en met 62 van het arrest.
[39] Punt 63 van het arrest.
[40] Punt 64 van het arrest.
[41] Punt 65 van het arrest.
[42] Punten 66 tot en met 68 van het arrest.

3.4 *Het conceptwetsvoorstel*

Inleiding

3.4.1 Naar aanleiding van de ongeldigverklaring van de Dataretentierichtlijn heeft de Raad van State een voorlichting uitgebracht aan de minister van Veiligheid en Justitie.[43] De Raad van State heeft vastgesteld dat de ongeldigverklaring van de richtlijn niet in de weg staat aan het opnemen van een bewaarplicht in de nationale wetgeving. De Raad van State heeft geoordeeld dat het in de eerste plaats de wetgever en uiteindelijk de Nederlandse rechter is die het definitieve oordeel dient te geven over de vraag in hoeverre de Wbt in overeenstemming is met de artikelen 7 en 8 van het Handvest.

3.4.2 Naar aanleiding van de voorlichting van de Raad van State is een conceptwetsvoorstel tot wijziging van de Tw en Sv opgesteld.[44] Zoals de minister heeft toegelicht in de beantwoording van Kamervragen,[45] heeft het conceptwetsvoorstel tot doel om 'extra waarborgen in te bouwen', zodat buiten twijfel is dat de nationale wetgeving in overeenstemming is met het Handvest. De belangrijkste aanpassingen in het conceptwetsvoorstel zijn de volgende.

De bewaarplicht

3.4.3 Het conceptwetsvoorstel voorziet in een aanpassing van de lijst met te bewaren gegevens.[46] Voor wat betreft telefoongegevens vervalt de verplichting om gegevens over 'enhanced media services' (EMS) en 'multimedia services' (MMS) op te slaan.[47] Voor wat betreft internetgegevens vervalt de verplichting om gegevens met betrekking tot e-mail over internet op te slaan. Ook wordt voorgesteld om het inbellende nummer voor een inbelverbinding en de 'digital subscriber line' (DSL) te schrappen.[48]

3.4.4 Het conceptwetsvoorstel brengt geen wijzigingen aan in de bewaartermijn. De bewaartermijn voor telefoongegevens blijft dus, conform het advies van de Raad van State van destijds en met een uitvoerige motivering, twaalf maanden en de bewaartermijn voor internetgegevens zes maanden.

3.4.5 Evenmin wordt een wijziging van de regeling voor vernietiging voorzien. In de Dataretentierichtlijn ontbrak een regeling voor de vernietiging van de gegevens na het verstrijken van de bewaartermijn. De Tw voorziet echter reeds in een dergelijke verplichting.[49]

[43] Bijlage bij *Kamerstukken II* 2014/15, 33 542, nr. 16.
[44] Bijlage bij *Kamerstukken II* 2014/15, 33 542, nr. 16.
[45] *Aanhangsel Handelingen II* 2014/15, 1186.
[46] Artikel I, onderdeel F van het wetsvoorstel.
[47] EMS-berichten zijn SMS-berichten met videoboodschap. MMS-berichten zijn SMS-berichten met afbeelding.
[48] De DSL is een type internetverbinding.
[49] Artikel 5 Besluit beveiliging gegevens telecommunicatie.

3.4.6 Wel legt het conceptwetsvoorstel de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten de verplichting op om de gegevens op te slaan en te verwerken binnen de Europese Unie.[50] Deze verplichting beoogt adequaat toezicht beter te waarborgen. Alle grote telecomaanbieders die in Nederland actief zijn, bewaren hun gegevens op dit moment al binnen de Europese Unie. Slechts enkele kleinere aanbieders die alleen gebruikersgegevens bewaren, bewaren die gegevens buiten de Europese Unie.

De toegang tot bewaarde gegevens

3.4.7 Ook voorziet het conceptwetsvoorstel in een wijziging van de bepalingen met betrekking tot de toegang tot de bewaarde gegevens.[51] Het wetsvoorstel brengt een verdere differentiatie aan in de mate waarin de officier van justitie toegang heeft tot bewaarde telefoongegevens. In geval van verdenking van een misdrijf waarop een gevangenisstraf van acht jaar of meer is gesteld (zeer ernstige misdrijven), kan de officier van justitie telefoongegevens vorderen die gedurende een periode van twaalf maanden voorafgaand aan de vordering zijn vastgelegd. In geval van verdenking van een ander misdrijf waarvoor voorlopige hechtenis is toegestaan (ernstige misdrijven), kan de officier telefoongegevens vorderen die gedurende een periode van zes maanden voorafgaand aan de vordering zijn vastgelegd.

3.4.8 Daarnaast bepaalt het conceptwetsvoorstel dat de officier van justitie verkeersgegevens kan vorderen, nadat hij daartoe een schriftelijke machtiging van de rechter-commissaris heeft ontvangen. Daarmee wordt voorzien in een voorafgaande rechterlijke toetsing van die vordering.

De beveiliging van bewaarde gegevens

3.4.9 Het conceptwetsvoorstel voorziet niet in een verdere aanscherping van de beveiligingsmaatregelen die aanbieders moeten treffen. De gegevens moeten op grond van het Besluit beveiliging gegevens telecommunicatie (Bbgt) reeds worden opgeslagen in een beveiligde omgeving, terwijl de gegevens slechts toegankelijk mogen zijn voor een beperkt aantal medewerkers van de aanbieders. De regering wil onderzoeken of de beveiliging nog verder kan worden aangescherpt door middel van versleuteling van de bewaarde gegevens, waartoe dan nadere regels zullen worden opgenomen in het Bbgt. De nationale regelgeving voorziet dus reeds in strikte waarborgen tegen misbruik en verlies van de bewaarde gegevens als waarop het Hof het oog heeft en waarvan het oordeelde dat die waarborgen in de richtlijn hadden moeten worden opgenomen.

[50] Artikel I, onderdeel C van het wetsvoorstel.
[51] Artikel II van het wetsvoorstel.

Het toezicht op bewaarde gegevens

3.4.10 Het conceptwetsvoorstel stelt voor het Agentschap Telecom de bevoegdheid toe te kennen om bij de uitoefening van zijn toezichttaken de bewaarde gegevens in te zien.[52] Op deze manier kan het Agentschap feitelijk onderzoeken of de verwerking, beveiliging en vernietiging van gegevens plaatsvindt conform de wettelijke voorschriften. Dit biedt extra waarborgen voor de privacy van degenen op wie de gegevens betrekking hebben.

3.5 De wetgeving in andere lidstaten

3.5.1 De Dataretentierichtlijn laat de lidstaten veel vrijheid in de implementatie van de bewaarplicht. Dat is overigens een belangrijk kritiekpunt van het Hof en het vormt een belangrijke overweging voor het Hof om de richtlijn ongeldig te verklaren. Zo laat artikel 6 van de richtlijn de lidstaten de vrijheid om – binnen bepaalde marges – een eigen bewaartermijn te bepalen. Artikel 4 van de richtlijn legt de lidstaten slechts de verplichting op om te waarborgen dat de bewaarde gegevens 'alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde nationale autoriteiten worden verstrekt'. Het is aan de lidstaten om te bepalen hoe zij aan deze verplichting uitvoering geven. Artikel 7 van de richtlijn bevat enkel 'beginselen van gegevensbeveiliging' die moeten worden gerespecteerd. Ook hier is het aan de lidstaten om invulling te geven aan deze beginselen.

3.5.2 Het voorgaande impliceert dat de nationale wetgeving die ter implementatie van de Dataretentierichtlijn tot stand is gekomen, per lidstaat aanzienlijk kan verschillen. Het voorgaande betekent ook dat het feit dat in de ene lidstaat bepaalde consequenties zijn getrokken uit de ongeldigverklaring van de Dataretentierichtlijn (nog daargelaten de motivering hiervoor), niet betekent dat in de andere lidstaat dezelfde consequenties moeten worden getrokken.

3.5.3 Dat de lidstaten ook verschillend zijn omgegaan met de implementatie en toepassing van de richtlijn, blijkt uit de evaluatie van de Dataretentierichtlijn door de Europese Commissie in 2009/2010. Het verslag van de Commissie van 18 april 2011 biedt inzicht in de wijze waarop in de lidstaten met de dataretentie is omgegaan (zie met name hoofdstuk 8: conclusies en aanbevelingen).[53]

3.5.4 Uit deze evaluatie en uit een recentere studie van de Commissie van maart 2013[54] blijkt dat de dataretentie een positieve bijdraagt levert aan het strafrechtelijk onderzoek naar ernstige criminaliteit en dat strafbare feiten konden worden

[52] Artikel I, onderdeel E van het wetsvoorstel.
[53] Verslag van de Commissie aan de Raad en het Europees Parlement, Evaluatie van de richtlijn gegevensbewaring, COM(2011) 225 def. **(productie 1).**
[54] Commissie, DG Home, Evidence for necessity of data retention in the EU, maart 2013, **(productie 2)**.

voorkomen en vervolgd. Deze onderzoeken, alsmede het onderzoek van WODC[55], onderschrijven ook de noodzaak van dataretentie. In de toelichting bij het conceptwetsvoorstel worden enkele van de vele voorbeelden genoemd van ernstige misdrijven waarbij op grond van de Wbt bewaarde gegevens een belangrijke rol hebben gespeeld bij de opsporing cq. veroordeling van de dader van deze misdrijven.[56]

3.5.5 Ondanks het feit dat de implementatie van de Dataretentierichtlijn per lidstaat aanzienlijk kan verschillen, is het interessant om te bekijken hoe in andere lidstaten met de ongeldigverklaring van de Dataretentierichtlijn wordt omgegaan. In randnummer 4.30 van de dagvaarding stellen eisers dat de constitutionele rechtscolleges in Bulgarije, Roemenië, Cyprus, Duitsland, Tsjechië, Oostenrijk, Slowakije en Slovenië hebben geoordeeld dat de nationale wetgeving ter implementatie van de Dataretentierichtlijn onhoudbaar was (zonder daarbij evenwel de concrete redenen daarvoor te benoemen). Daarbij moet worden aangetekend dat de constitutionele rechtscolleges in Bulgarije, Roemenië, Cyprus, Duitsland en Tsjechië dit oordeel al hadden uitgesproken, voordat de Dataretentierichtlijn ongeldig werd verklaard.[57] De uitspraken van de rechtscolleges in deze lidstaten zijn dus niet het gevolg van de ongeldigverklaring van de Dataretentierichtlijn. Bovendien geldt in Bulgarije, Cyprus en Tsjechië inmiddels weer een wettelijke bewaarplicht.

3.5.6 Ook in diverse andere lidstaten wordt de bewaarplicht nog onverkort gehandhaafd. Dat geldt bijvoorbeeld voor Denemarken, Zweden, België, Finland, Frankrijk, Spanje, Ierland, Italië, het Verenigd Koninkrijk, Hongarije en Polen.[58] In Denemarken en Zweden wordt op dit moment – net als in Nederland – onderzocht of de nationale wetgeving met betrekking tot de bewaarplicht aanpassing behoeft. In Finland en Ierland is een voorstel tot wijziging van de nationale wetgeving met betrekking tot de bewaarplicht aanhangig. In het Verenigd Koninkrijk is noodwetgeving van kracht om de bewaarplicht na de ongeldigverklaring van de Dataretentierichtlijn te kunnen handhaven. Het Poolse constitutionele Hof heeft geoordeeld dat de bewaarplicht op zich niet inconstitutioneel is, maar dat de Poolse nationale wetgeving onvoldoende waarborgen biedt met betrekking tot de bewaring. De regering en het parlement hebben nu achttien maanden de tijd om de wetgeving aan te passen.

[55] De Wet bewaarplicht telecommunicatiegegevens, Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing, 2013. De slotbeschouwing uit dit rapport (hoofdstuk 7) is door eisers bij productie 23 in het geding gebracht.
[56] Bijlage bij *Kamerstukken II* 2014/15, 33 542, nr. 16, p. 11 en verder.
[57] Zie het overzicht 'Inventarisatie buitenland' **(productie 3)**.
[58] Zie het overzicht 'Inventarisatie buitenland' **(productie 3)**.

3.6 *De rechtspraak van het EHRM*

Inleiding

3.6.1 Eisers beroepen zich in de dagvaarding niet alleen op de artikelen 7 en 8 van het Handvest, maar ook op artikel 8 EVRM. Artikel 8 EVRM omvat het recht op eerbiediging van privé-, familie- en gezinsleven. In deze paragraaf wordt een toelichting gegeven op de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) over artikel 8 EVRM.

Het toetsingskader van het EHRM

3.6.2 Het EHRM toetst volgens een vast stramien of sprake is van een schending van artikel 8 EVRM. Eerst beoordeelt het EHRM of er sprake is van een inmenging in de privacy van burgers. Vervolgens toetst het EHRM of deze inmenging gerechtvaardigd is. Daartoe toetst het EHRM in de eerste plaats of de inmenging 'bij wet voorzien' is. In de tweede plaats toetst het EHRM of de inmenging een legitiem doel dient. In de derde plaats toetst het EHRM of de inmenging in een democratische samenleving noodzakelijk is om het legitieme doel te bereiken.

3.6.3 De noodzakelijkheidstoets bestaat uit twee onderdelen. Het EHRM toetst in de eerste plaats of de inmenging geschikt is om het legitieme doel te bereiken. In de tweede plaats toetst het EHRM of de inmenging proportioneel is en een balans vindt tussen publieke en individuele belangen.[59]

3.6.4 Bij de noodzakelijkheidstoets komt de nationale autoriteiten een 'margin of appreciation' toe. De reikwijdte van deze 'margin of appreciation' hangt af van verschillende factoren, zoals de aard van het grondrecht, het belang van het grondrecht voor het individu, de aard van de inmenging en het doel van de inmenging. De marge is beperkter als het gaat om een kernaspect van het mensenrecht. Maar als er tussen de verdragsstaten geen overeenstemming bestaat ten aanzien van het belang of de wijze waarop het belang moet worden beschermd, is de 'margin of appreciation' ruimer.[60]

Legitiem doel

3.6.5 Het EHRM overweegt bij de beoordeling van opsporingsmaatregelen die een inmenging vormen op de privacy, vrijwel steevast dat hiermee het legitieme doel van het opsporen en voorkomen van misdrijven gediend is. Zo overwoog het EHRM in de zaak S. en Marper tegen het Verenigd Koninkrijk:

[59] Zie bijvoorbeeld EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper tegen het Verenigd Koninkrijk*), punt 118.
[60] EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper tegen het Verenigd Koninkrijk*), punt 102.

> 'The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection and, therefore, prevention of crime.'[61]

3.6.6 In Brunet tegen Frankrijk merkte het EHRM kort en goed op dat het bewaren van gegevens van individuen in een 'recorded offences database' het legitieme doel dient van het voorkomen van criminaliteit en de bescherming van de rechten en vrijheden van derden.[62]

Noodzakelijk in een democratische samenleving

3.6.7 In het kader van de noodzakelijkheidstoets heeft het EHRM verschillende keren expliciet gewezen op het belang van telecommunicatiegegevens voor de opsporing. Het EHRM heeft dat zowel gedaan in het kader van de toets of de inmenging geschikt is om het legitieme doel te bereiken als in het kader van de toets of de inmenging proportioneel is en een balans vindt tussen publieke en individuele belangen.

3.6.8 In het kader van de geschiktheidstoets is de zaak Malone tegen het Verenigd Koninkrijk illustratief. Het EHRM overwoog in deze zaak:

> 'Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2) (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 23, para. 48). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime".'[63]

3.6.9 In het kader van de noodzakelijkheidstoets heeft het EHRM overwogen dat het van belang is dat de Staat effectieve middelen tot zijn beschikking heeft om strafbare feiten te kunnen opsporen:

> 'While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (...).'[64]

[61] EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper tegen het Verenigd Koninkrijk*), punt 100. Zie ook EHRM 18 april 2013, 19522/09 (*M.K. tegen Frankrijk*), punten 31 en 33.
[62] EHRM 18 september 2014, 21010/10 (*Brunet tegen Frankrijk*), punt 32.
[63] EHRM 2 augustus 1984, 8691/79 (*Malone tegen het Verenigd Koninkrijk*), punt 81.
[64] EHRM 2 december 2008, 2872/02 (*K.U. tegen Finland*), punt 43.

3.6.10 De Staat dient daarbij een afweging te maken tussen de verschillende, strijdende, belangen. Voor het vinden van deze *fair balance* is de uitspraak van het EHRM in de zaak K.U. tegen Finland van groot belang.[65] In deze zaak had een onbekende internetter een seksuele advertentie op internet gezet voor een twaalfjarige jongen, die vervolgens door een pedofiel werd benaderd. Op grond van de Finse wetgeving kwam de opsporingsautoriteiten geen bevoegdheid toe om telecomgegevens te kunnen vorderen. Als gevolg daarvan was het niet mogelijk om de dader te identificeren.

3.6.11 Het EHRM overwoog ten aanzien van de afweging tussen het belang van vertrouwelijke communicatie enerzijds en het belang van opsporing anderzijds:

> 'An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.'[66]

3.6.12 Volgens het EHRM had Finland in deze zaak niet de juiste balans gevonden. Finland werd daarom veroordeeld voor een schending van artikel 8 EVRM. Het belang van het individu om zijn of haar privacy gewaarborgd te zien, is namelijk niet absoluut en kan worden ingeperkt met het oog op het algemene belang, waaronder het belang van burgers om effectief beschermd te worden tegen criminaliteit.[67]

3.6.13 De Finse auditeur-generaal heeft in een artikel opgemerkt dat uit het arrest kan worden afgeleid dat op staten de verplichting rust om te zorgen voor deugdelijke identificatiemethoden:

> 'The judgment in the case of K.U. v Finland can be interpreted to mean that legislation and public authorities have an obligation, following from article 8 of the European Convention, to arrange proper identification and authentication in electronic transactions when elements of personal integrity and identity are in question.'[68]

3.6.14 Volgens de auditeur-generaal kan uit het arrest bovendien worden afgeleid dat op staten de verplichting rust om telecommunicatiegegevens te bewaren:

[65] EHRM 2 december 2008, 2872/02 (*K.U. tegen Finland*).
[66] Punt 49 van het arrest.
[67] Zie punt 49 van het arrest.
[68] T. Pöysti, 'Judgment in the case of K.U. v Finland', *Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, p. 39 **(productie 4)**.

> 'The court indicated that it is a requirement for the protection of fundamental rights and freedoms to store and retain electronic evidence, including communications data, and to provide for access to it in police investigations when essential aspects and values of private life are at issue, and the concern is about the protection of children or other persons with particular vulnerabilities.'[69]

4 Samenvatting

4.1.1 Uit het voorgaande volgt al dat uit het enkele feit dat het Hof de Dataretentierichtlijn in strijd heeft geoordeeld met de artikelen 7 en 8 van het Handvest, niet zonder meer voortvloeit dat ook de Wbt in strijd is met deze artikelen. De Wbt kan in dit kader niet los worden gezien van de voorschriften in Sv en de voorschriften bij en krachtens de Tw. Dit geheel aan nationale (implementatie)maatregelen bevat veel meer waarborgen voor de privacy van de burger dan de Dataretentierichtlijn.

4.1.2 Sv bevat gedetailleerde regels met betrekking tot de toegang tot bewaarde gegevens. De officier van justitie kan alleen gegevens vorderen in geval van:

- verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan;
- een redelijk vermoeden dat in georganiseerd verband dergelijke misdrijven worden geraamd of gepleegd; of
- aanwijzingen van een terroristisch misdrijf.

Het krachtens de Tw vastgestelde Besluit beveiliging gegevens telecommunicatie bevat gedetailleerde regels over gegevensbescherming en -beveiliging. Op grond van de Wbt bedraagt de bewaartermijn in Nederland zes maanden voor internetgegevens en twaalf maanden voor telefoongegevens, conform het advies van de Raad van State van destijds, terwijl de richtlijn ruimte bood voor een bewaartermijn van 24 maanden.

4.1.3 Waar het Hof van Justitie er in zijn beoordeling zwaar gewicht aan heeft toegekend dat relevante normen in de richtlijn niet nader waren ingevuld en die invulling aan de lidstaten was overgelaten, heeft Nederland die normen in de Wbt wel ingevuld en zijn bovendien in Sv normen en waarborgen met betrekking tot de toegang uitgewerkt, hetgeen ook blijkens het advies van de Raad van State destijds over het wetsvoorstel als afdoende werd beoordeeld.

4.1.4 Het enkele feit dat er een conceptwetsvoorstel tot wijziging van de Wbt is opgesteld, betekent niet dat de huidige waarborgen onvoldoende zijn en dat de bewaarplicht onrechtmatig zou zijn. Zoals hiervoor is toegelicht,[70] heeft het conceptwetsvoorstel tot

[69] T. Pöysti, 'Judgment in the case of K.U. v Finland', *Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, p. 44 **(productie 4)**.
[70] Zie randnummer 3.4.1 van deze conclusie.

doel om – mede in het licht van de naar aanleiding van het arrest van het Hof gevoerde maatschappelijke discussie – extra waarborgen in te bouwen, zodat buiten twijfel is dat de nationale wetgeving in overeenstemming is met het Handvest.

4.1.5 Van een schending van de artikelen 7 en 8 van het Handvest is geen sprake. Door (het handhaven van) de Wbt wordt evenmin artikel 8 EVRM geschonden. Uit de rechtspraak van het EHRM volgt dat op staten de plicht rust om een juiste afweging te maken tussen het algemene belang van opsporing en voorkoming van misdrijven en het individuele belang bij privacy. De Wbt voorziet in deze afweging.

4.1.6 Gelet op het voorgaande is de Wbt niet onmiskenbaar onverbindend.

5 Conclusie

5.1 De Staat concludeert:

(i) tot niet-ontvankelijkverklaring van eisers in hun vorderingen, althans tot afwijzing van het gevorderde;

(ii) met veroordeling van eisers in de kosten van het geding, zulks met bepaling dat over die proceskostenveroordeling de wettelijke rente verschuldigd zal zijn met ingang van de vijftiende dag na de datum van het te dezen te wijzen vonnis;

(iii) en met veroordeling van eisers in de nakosten, conform het liquidatietarief begroot op € 131 dan wel in het geval van betekening € 199;

(iv) met verklaring dat deze proceskostenveroordelingen uitvoerbaar bij voorraad zijn.

Den Haag, 13 februari 2015

Advocaat

b.a.

behandeld door	R.J.M. van den Tweel
correspondentie	Postbus 11756, 2502 AT Den Haag
telefoon	(070) 515 38 01
fax	(070) 515 31 45
e-mail	rjm.vandentweel@pelsrijcken.nl
zaaknr	10044271

Productie 1

EUROPESE COMMISSIE

Brussel, 18.4.2011
COM(2011) 225 definitief

VERSLAG VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG)

VERSLAG VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG)

1. INLEIDING

Volgens de richtlijn gegevensbewaring[1] (hierna "de richtlijn" genoemd) moeten de lidstaten aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken (hierna "exploitanten" genoemd) verplichten verkeers- en locatiegegevens tussen de zes maanden en twee jaar te bewaren voor het onderzoeken, opsporen en vervolgen van zware criminaliteit.

In dit verslag evalueert de Commissie, overeenkomstig artikel 14 van de richtlijn, de toepassing van deze richtlijn door de lidstaten en de weerslag ervan op de marktdeelnemers en de consumenten, rekening houdend met verdere ontwikkelingen in elektronische communicatietechnologie en de statistische informatie die aan de Commissie is verstrekt. Doel is na te gaan of het nodig is de bepalingen van de richtlijn aan te passen, in het bijzonder wat betreft de gegevens die onder de richtlijn vallen en de bewaringstermijnen. In dit verslag wordt ook gekeken naar het effect van de richtlijn op de grondrechten, vanwege de algemene kritiek op het bewaren van gegevens, en wordt nagegaan of er maatregelen moeten worden genomen om de bezorgdheid over het anonieme gebruik van simkaarten voor criminele doeleinden weg te nemen[2].

Over het geheel genomen heeft de evaluatie aangetoond dat het bewaren van gegevens een waardevol instrument is voor de strafrechtsystemen en de rechtshandhaving in de EU. De richtlijn heeft slechts in beperkte mate bijgedragen tot de harmonisatie van de gegevensbewaring als het gaat om bijvoorbeeld doelbinding of bewaringstermijnen, alsook wat betreft de vergoeding van kosten van exploitanten, een onderwerp dat buiten het bestek van de richtlijn valt. In verband met de gevolgen en de risico's voor de interne markt en voor de naleving van het recht op privacy en bescherming van persoonsgegevens dient de EU er door middel van gemeenschappelijke regels voor te blijven zorgen dat er hoge normen voor het opslaan, opzoeken en gebruiken van verkeers- en locatiegegevens worden toegepast. Gezien deze conclusies is de Commissie voornemens wijzigingen van de richtlijn voor te stellen, op basis van een effectbeoordeling.

---

1 Richtlijn 2006/24/EG 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 2002/58/EG (PB L 105 van 13.4.2006, blz. 54).

2 Conclusies van de Raad betreffende de bestrijding van het anoniem en voor criminele doeleinden gebruiken van elektronische communicatie, 2908e vergadering van de Raad Justitie en Binnenlandse Zaken – Brussel, 27-28 november 2008.

2. ACHTERGROND VAN DEZE EVALUATIE

Dit evaluatieverslag is gebaseerd op uitvoerige gesprekken met en bijdragen van de lidstaten, deskundigen en belanghebbenden.

In mei 2009 heeft de Commissie de conferentie "Towards the Evaluation of the Data Rentention Directive" georganiseerd, waaraan werd deelgenomen door gegevensbeschermingsautoriteiten, de particuliere sector, het maatschappelijk middenveld en academici. In september 2009 heeft de Commissie belanghebbenden uit die groepen een vragenlijst gestuurd, waarop 70 reacties zijn gekomen[3]. In december 2010 werd een tweede conferentie gehouden, "Taking on the Data Retention Directive", waar door ongeveer dezelfde betrokken partijen de voorlopige evaluatie van de richtlijn en toekomstige problemen op dit werkterrein werden besproken.

Tussen oktober 2009 en maart 2010 heeft de Commissie met vertegenwoordigers van alle lidstaten en geassocieerde EER-landen bepaalde punten betreffende de toepassing van de richtlijn nader besproken. De lidstaten zijn later dan verwacht begonnen met de toepassing van de richtlijn, vooral ten aanzien van internetgegevens. Als gevolg van de late omzetting konden slechts negen lidstaten de Commissie voor 2008 of voor 2009 alle in artikel 10 van de richtlijn bedoelde statistieken verstrekken, hoewel in totaal 19 lidstaten wel enkele statistieken verstrekten (zie punt 4.7). De Commissie heeft in juli 2010 de lidstaten verzocht verdere kwantitatieve en kwalitatieve gegevens te verstrekken over de mate waarin de bewaarde gegevens van betekenis zijn geweest voor de rechtshandhaving. Tien lidstaten hebben daarop gereageerd door nadere gegevens te verstrekken over specifieke gevallen waarin de gegevens van doorslaggevende betekenis zijn geweest[4].

Dit verslag is ook gebaseerd op de nota's die de deskundigengroep "Platform voor elektronische bewaring van gegevens voor het voorkomen, onderzoeken, opsporen en vervolgen van ernstige criminaliteit" sinds haar oprichting in 2008[5] heeft goedgekeurd. De Commissie heeft tevens rekening gehouden met de verslagen van de groep Gegevensbescherming van artikel 29[6], en in het bijzonder met het verslag over de tweede handhavingsactie, d.w.z. de toetsing van de naleving van de gegevensbeschermings- en gegevensbeveiligingsvoorschriften van de richtlijn[7].

---

3 De reacties staan op de website van de Commissie: (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm).

4 België, Tsjechië, Cyprus, Litouwen, Hongarije, Nederland, Polen, Slovenië, Verenigd Koninkrijk. Zweden heeft eveneens verschillende gevallen gemeld van ernstige strafbare feiten waarbij historische verkeersgegevens, die beschikbaar waren hoewel er geen verplichting tot het bewaren van die gegevens geldt, cruciaal waren bij het verkrijgen van een veroordeling.

5 Deze deskundigengroep is opgericht bij Besluit 2008/324/EG van de Commissie (PB L 111 van 23.4.2008, blz 11). De Commissie heeft regelmatig met deze groep vergaderd. De nota's zijn te vinden op: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens is opgericht bij artikel 29 van de richtlijn gegevensbescherming (Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24.101995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31)).

7 Verslag 01/2010 over de tweede gezamenlijke handhavingsmaatregel: Compliance at national level of Telecom Providers and internet service providers with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the

3. GEGEVENSBEWARING IN DE EUROPESE UNIE

3.1. Gegevensbewaring voor strafrechtelijke en rechtshandhavingsdoeleinden

Aanbieders van diensten en netwerken (hierna "exploitanten" genoemd) verwerken, als onderdeel van hun activiteiten, persoonsgegevens bij de transmissie van communicatie, de facturering, interconnectiebetalingen, marketing en bepaalde andere diensten met een toegevoegde waarde. Bij deze verwerking gaat het onder meer om gegevens waaruit de bron, de bestemming, de datum, het tijdstip, de duur en de aard van de communicatie is af te leiden, alsook de communicatieapparatuur van de gebruiker en, in het geval van mobiele telefonie, gegevens betreffende de locatie van de apparatuur. Op grond van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (hierna "e-privacyrichtlijn" genoemd[8]) moeten dergelijke verkeersgegevens die worden gegenereerd bij het gebruik van elektronische communicatiediensten in principe worden gewist of anoniem gemaakt wanneer ze niet langer nodig zijn voor de transmissie van communicatie, behalve wanneer, en dan alleen zolang deze gegevens noodzakelijk zijn voor de facturering, of wanneer de abonnee of de gebruiker toestemming heeft gegeven. Locatiegegevens mogen alleen worden verwerkt als ze anoniem zijn gemaakt of als de betrokken gebruiker toestemming heeft gegeven, voor zover en voor zolang dit nodig is voor het leveren van een dienst met een toegevoegde waarde.

Voordat de richtlijn in werking trad, vroegen de nationale autoriteiten, onder bepaalde voorwaarden, de exploitanten om toegang tot dergelijke gegevens, bijvoorbeeld om na te gaan welke abonnees een bepaald IP-adres gebruikten, eerdere communicatieactiviteiten te analyseren en vast te stellen waar een mobiele telefoon zich bevond.

Het bewaren en gebruiken van gegevens voor rechtshandhavingsdoeleinden werd voor het eerst op EU-niveau geregeld in Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector. Die richtlijn bood de lidstaten voor het eerst de mogelijkheid om wettelijke maatregelen te treffen met het oog op de bescherming van de openbare veiligheid, de landsverdediging of de staatsveiligheid, met inbegrip van het economische welzijn van de staat wanneer de activiteit verband hield met de staatsveiligheid, en met het oog op de wetshandhaving op strafrechtelijk gebied[9].

Die bepaling is verder uitgewerkt in de e-privacyrichtlijn, die de lidstaten de mogelijkheid biedt wetgevende maatregelen te nemen waarin wordt afgeweken van het beginsel dat communicatie vertrouwelijk is en waarin onder bepaalde voorwaarden het bewaren van, de toegang tot en het gebruik van gegevens voor rechtshandhavingsdoeleinden wordt toegestaan. Op grond van artikel 15, lid 1, kunnen de lidstaten privacyrechten en –plichten beperken, bijvoorbeeld door gegevens voor een bepaalde periode te bewaren, "indien dat in een

---

Data Retention Directive 2006/24/EC amending the e-Privacy Directive' (WP 172), 13.7.2010 (zie: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

8 Richtlijn van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37)).

9 Artikel 14, lid 1, van Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (PB L 24 van 30.1.1998, blz. 1).

democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem".

De rol van bewaarde gegevens in strafrechtsystemen en in de rechtshandhaving wordt verder besproken in punt 5.

3.2. Doel en rechtsgrond van de richtlijn gegevensbewaring

Op grond van Richtlijn 97/66/EG en de e-privacyrichtlijn mogen de lidstaten wetgeving vaststellen inzake de bewaring van gegevens. Als gevolg daarvan moesten exploitanten in sommige lidstaten apparatuur voor gegevensbewaring aanschaffen en personeel in dienst nemen om gegevens op te zoeken namens de rechtshandhavingsautoriteiten, terwijl dat in andere lidstaten niet het geval was, waardoor de interne markt verstoord raakte. Bovendien hadden bepaalde veranderingen in bedrijfsmodellen en aangeboden diensten, zoals het toenemend gebruik van vaste tarieven, vooraf betaalde en gratis elektronische communicatiediensten, tot gevolg dat exploitanten steeds minder verkeers- en locatiegegevens opsloegen voor de facturatie, waardoor steeds minder van dergelijke gegevens beschikbaar waren voor strafrechtelijke en rechtshandhavingsdoeleinden. De terroristische aanslagen in Madrid in 2004 en in Londen in 2005 maakten de discussie op EU-niveau over deze problemen nog urgenter.

Tegen deze achtergrond werden de lidstaten door de richtlijn gegevensbewaring verplicht te regelen dat aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk communicatiegegevens moeten bewaren, zodat deze kunnen worden gebruikt voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten; daarnaast werden bepaalde hiermee verband houdende zaken op EU-niveau geharmoniseerd.

De richtlijn wijzigde artikel 15, lid 1, van de e-privacyrichtlijn door middel van een nieuwe bepaling die inhoudt dat artikel 15, lid 1, niet van toepassing is op gegevens die worden bewaard uit hoofde van de richtlijn gegevensbewaring[10]. Daardoor blijft het voor de lidstaten (zoals in overweging 12 wordt verklaard) mogelijk af te wijken van het beginsel dat communicatie vertrouwelijk is. De richtlijn gegevensbewaring regelt alleen de bewaring van gegevens voor een beperkter doel: het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

Dit ingewikkelde juridische verband tussen de richtlijn gegevensbewaring en de e-privacyrichtlijn maakt het, mede vanwege het ontbreken van een definitie in beide richtlijnen van het begrip "ernstige criminaliteit", moeilijk om maatregelen die de lidstaten nemen om de gegevensbewaringsverplichtingen van de richtlijn om te zetten, te onderscheiden van de meer

---

[10] Artikel 11 van de richtlijn luidt: In artikel 15 van Richtlijn 2002/58/EG wordt het volgende lid ingevoegd: "1 bis. Lid 1 is niet van toepassing op de uit hoofde van Richtlijn 2006/24/EG 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 te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden."

algemene praktijk in de lidstaten om gegevens te bewaren op grond van artikel 15, lid 1, van de e-privacyrichtlijn[11]. In punt 4 wordt hier verder op ingegaan.

De richtlijn is gebaseerd op artikel 95 van het Verdrag tot oprichting van de Europese Gemeenschap (vervangen door artikel 114 van het Verdrag betreffende de werking van de Europese Unie), dat betrekking heeft op de totstandbrenging en de werking van de interne markt. Nadat de richtlijn was vastgesteld, werd de rechtsgrond aangevochten voor het Europese Hof van Justitie, met het argument dat het hoofddoel van de richtlijn het onderzoeken, opsporen en vervolgen van ernstige criminaliteit is. Het Hof was van oordeel dat de richtlijn handelingen regelt die losstaan van de uitvoering van enige eventuele vorm van politiële en justitiële samenwerking in strafzaken, en dat zij noch de toegang tot gegevens door de bevoegde nationale autoriteiten, noch het gebruik van die gegevens door en de uitwisseling ervan tussen die autoriteiten harmoniseert. Het Hof concludeerde daarom dat de richtlijn in wezen de activiteiten van aanbieders van diensten in de betrokken sector van de interne markt betreft. De rechtsgrond werd dan ook gehandhaafd[12].

3.3. Bevriezing van gegevens

Het bewaren van gegevens is iets anders dan het bevriezen van gegevens (ook wel "quick freeze" genoemd), waarbij exploitanten een gerechtelijk bevel krijgen om gegevens betreffende specifieke verdachten van criminele activiteiten te bewaren vanaf de datum van het gerechtelijk bevel. Het bevriezen van gegevens is een van onderzoeksinstrumenten die worden gebruikt door de partijen bij het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken[13]. Vrijwel alle landen die partij zijn bij het verdrag hebben een contactpunt aangewezen dat onmiddellijke bijstand moet verlenen bij onderzoeken of procedures die betrekking hebben op cybercriminaliteit. Niet alle partijen bij het verdrag hebben echter de mogelijkheid tot het bevriezen van gegevens ingevoerd, en tot nu toe is nog niet onderzocht hoe effectief deze methode is bij het aanpakken van cybercriminaliteit[14]. Onlangs is een vorm van gegevensbevriezing ontwikkeld die bekend staat als "quick freeze plus". Dit gaat verder dan het bevriezen van gegevens: de rechter kan ook toegang verlenen tot gegevens die nog niet door de exploitant zijn gewist. Hier zou dus ook een zeer beperkte wettelijke uitzondering van korte duur gelden op de verplichte vernietiging van bepaalde verkeersgegevens die normaal gesproken niet worden opgeslagen, zoals locatiegegevens, gegevens over de internetverbinding en dynamische IP-adressen van gebruikers met een vast abonnement waarvoor geen gegevens hoeven te worden opgeslagen ten behoeve van de facturering.

Voorstanders van gegevensbevriezing vinden dat bevriezing minder inbreuk maakt op de privacy dan gegevensbewaring. Maar de meeste lidstaten vinden dat bevriezing in welke vorm dan ook geen goede vervanging is voor gegevensbewaring, omdat gegevensbewaring historische gegevens oplevert, terwijl er bij het bevriezen van gegevens geen garantie is dat er

---

11 De Groep van artikel 29 stelt de vraag of de richtlijn gegevensbewaring was bedoeld om af te wijken van de algemene verplichting om verkeersgegevens te wissen zodra de elektronische communicatie is afgerond, of om het mogelijk te maken alle gegevens te bewaren die exploitanten al mochten opslaan voor hun eigen zakelijke doeleinden.

12 EhvJ, zaak C-301/06 Ierland tegen Europees Parlement en Raad, Jurispr. [2009] I-00593.

13 Artikel 16 van het Cybercrimeverdrag (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) .

14 Bron: Raad van Europa.

bewijzen kunnen worden teruggevonden die dateren van voor het gerechtelijk bevel, er geen onderzoek kan worden gericht als het doel onbekend is, en er geen bewijzen kunnen worden verzameld met betrekking tot verplaatsingen van bijvoorbeeld slachtoffers of getuigen van criminaliteit[15].

4. OMZETTING VAN DE RICHTLIJN GEGEVENSBEWARING

De lidstaten moesten de richtlijn vóór 15 september 2007 hebben omgezet, maar hadden de mogelijkheid om de toepassing van de bewaringsverplichting met betrekking tot internettoegang, internettelefonie en e-mail via internet uit te stellen tot 15 maart 2009.

De onderstaande analyse is gebaseerd op de omzettingskennisgevingen die de Commissie heeft ontvangen van 25 lidstaten, België meegerekend, dat de richtlijn slechts ten dele heeft omgezet[16]. In Oostenrijk en Zweden is de ontwerpwetgeving in behandeling. Deze twee landen kennen geen verplichting tot het bewaren van gegevens, maar de rechtshandhavingsinstanties kunnen er verkeersgegevens opvragen van exploitanten en voor zover de gegevens beschikbaar zijn, ontvangen zij deze ook. Nadat Duitsland, Roemenië en Tsjechië hun omzettingsmaatregelen hadden meegedeeld aan de Commissie, hebben hun respectieve constitutionele hoven de nationale wetgeving ter omzetting van de richtlijn nietig verklaard[17]; deze lidstaten buigen zich nu over een nieuwe manier om de richtlijn om te zetten.

In dit punt wordt geanalyseerd hoe de lidstaten de bepalingen van de richtlijn hebben omgezet. Tevens wordt nagegaan of de lidstaten ervoor hebben gekozen de kosten van de exploitanten voor het bewaren en opzoeken van gegevens te vergoeden, hoewel dit niet in de richtlijn wordt geregeld, en wordt ingegaan op de betekenis van de uitspraken van de constitutionele hoven van Duitsland, Roemenië en Tsjechië voor de richtlijn.

4.1. Doel van de bewaring van gegevens (artikel 1)

De richtlijn verplicht de lidstaten maatregelen vast te stellen om ervoor te zorgen dat gegevens worden bewaard en beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten. Het doel van de bewaring van en/of de toegang tot gegevens wordt in de nationale wetgevingen echter nog steeds op uiteenlopende wijze geformuleerd. Tien lidstaten (Bulgarije, Estland,

---

15 Ook het Duitse constitutionele hof was deze mening toegedaan in het arrest waarin de Duitse wet ter omzetting van de richtlijn nietig werd verklaard (zie punt 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010, para. 208).

16 De 25 lidstaten die de Commissie in kennis hebben gesteld van de omzetting van de richtlijn zijn: België, Bulgarije, Tsjechië, Denemarken, Duitsland, Griekenland, Estland, Ierland, Spanje, Frankrijk, Italië, Cyprus, Letland, Litouwen, Luxemburg, Hongarije, Malta, Nederland, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland en het Verenigd Koninkrijk. België heeft de Commissie laten weten dat de ontwerpwetgeving die de omzetting voltooit, nog in behandeling is bij het Parlement.

17 Beslissing nr. 1258 van 8 oktober 2009 van het Roemeense constitutionele hof, Roemeens staatsblad nr. 789 van 23 november 2009; arrest van het Bundesverfassungsgericht 1 BvR 256/08 van 2 maart 2010, staatsblad van 1 april 2011; arrest van het Tsjechische constitutionele hof van 22 maart over de bepalingen van hoofdstuk 97, punt 3 en 4 van wet nr. 127/2005 over elektronische communicatie en tot wijziging van bepaalde daarmee verband houdende besluiten, en decreet nr. 485/2005 over gegevensbewaring en doorgifte aan de bevoegde autoriteiten.

Ierland, Griekenland, Spanje, Litouwen, Luxemburg, Hongarije, Nederland en Finland) hebben een definitie opgesteld van "ernstige criminaliteit", waarbij een minimumgevangenisstraf wordt genoemd, wordt vermeld dat een vrijheidsstraf kan worden opgelegd, of wordt verwezen naar een lijst van strafbare feiten die elders in het nationale recht worden gedefinieerd. In acht lidstaten (België, Denemarken, Frankrijk, Italië, Letland, Polen, Slowakije en Slovenië) moeten gegevens niet alleen worden bewaard voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, maar van alle strafbare feiten, en voor het voorkomen van criminaliteit of om algemene redenen van nationale, openbare of staatsveiligheid. In de wetgeving van vier lidstaten (Cyprus, Malta, Portugal en het Verenigd Koninkrijk) is sprake van "ernstige criminaliteit" of "ernstig strafbaar feit" zonder dat hiervan een nadere definitie wordt gegeven. Deze gegevens zijn weergegeven in tabel 1.

Tabel 1: Doelbinding voor de bewaring van gegevens in de nationale wetgevingen	
België	Voor het onderzoeken en vervolgen van strafbare feiten, het vervolgen van oneigenlijk gebruik van de nooddiensten, het onderzoeken van kwaadwillig gebruik van elektronische communicatienetwerken of –diensten, en voor het verzamelen van inlichtingen door de inlichtingen- en veiligheidsdiensten[18].
Bulgarije	Voor het opsporen en onderzoeken van ernstige strafbare feiten en strafbare feiten in de zin van de artikelen 319a-319f van het wetboek van strafrecht, alsmede voor het opsporen van personen[19].
Tsjechië	Richtlijn niet omgezet.
Denemarken	Voor het onderzoeken en vervolgen van strafbare feiten.[20]
Duitsland	Richtlijn niet omgezet.
Estland	Toegestaan als de bewijsverkrijging op andere procedurele manieren onmogelijk of bijzonder gecompliceerd is en de procedure betrekking heeft op een strafbaar feit [van de eerste graad of een opzettelijk gepleegd strafbaar feit van de tweede graad dat wordt bestraft met een gevangenisstraf van ten minste drie jaar].[21]
Ierland	Voor het voorkomen van ernstige strafbare feiten (d.w.z. feiten die worden bestraft met een gevangenisstraf van ten minste vijf jaar, of een strafbaar feit dat wordt genoemd in de bijlage bij de omzettingswet), het waarborgen van de staatsveiligheid, het redden van mensenlevens[22].
Griekenland	Voor het opsporen van bijzonder ernstige strafbare feiten[23].

18 Artikel 126, lid 1, van de wet van 13 juni 2005 betreffende de elektronische communicatie.
19 Artikel 250a, lid 2, van de wet op de elektronische communicatie (gewijzigd) 2010.
20 Artikel 1, bevel tot gegevensbewaring.
21 Artikel 110, lid 1, van het wetboek van strafvordering.
22 Artikel 6 Communicaties (Wet gegevensbewaring) 2011.
23 Deze strafbare feiten worden gedefinieerd in artikel 4 van wet 2225/1994; artikel 1 van wet 3917/2011.

Tabel 1: Doelbinding voor de bewaring van gegevens in de nationale wetgevingen	
Spanje	Voor het opsporen, onderzoeken en vervolgen van de in het wetboek van strafrecht en in de bijzondere strafwetten bedoelde ernstige strafbare feiten.[24]
Frankrijk	Voor het opsporen, onderzoeken en vervolgen van strafbare feiten, en dit alleen om de gerechtelijke autoriteiten de nodige informatie te verstrekken, en voor het voorkomen van terroristische handelingen en het beschermen van de intellectuele eigendom.[25]
Italië	Voor het opsporen en tegengaan van strafbare feiten.[26]
Cyprus	Voor het onderzoeken van een ernstig strafbaar feit.[27]
Letland	Om de staatsveiligheid en de openbare veiligheid te beschermen of met het oog op het onderzoeken en vervolgen van strafbare feiten en het voeren van strafprocedures.[28]
Litouwen	Voor het onderzoeken, opsporen en vervolgen van ernstige en zeer ernstige strafbare feiten, als gedefinieerd in het Litouwse wetboek van strafrecht.[29]
Luxemburg	Voor het opsporen, onderzoeken en vervolgen van strafbare feiten die worden bestraft met een gevangenisstraf van ten minste een jaar.[30]
Hongarije	Om onderzoeksinstanties, de openbaar aanklager, de rechter en de nationale veiligheidsbureaus in staat te stellen hun taken te vervullen en het de politie en de nationale belasting- en douanedienst mogelijk te maken strafbare feiten te onderzoeken die worden bestraft met een gevangenisstraf van tenminste twee jaar.[31]
Malta	Voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[32]

24 Artikel 1, lid 1, van Wet 25/2007.

25 Het gebruik van bewaarde gegevens voor het opsporen, onderzoeken en vervolgen van strafbare feiten, het voorkomen van terroristische handelingen en het beschermen van de intellectuele eigendom is geregeld bij respectievelijk: artikel L.34-1(II), CPCE, wat nr. 2006-64 van 23 januari 2006 en wet nr. 2009-669 van 12 juni 2009.

26 Artikel 132, lid 1, van het Wetboek gegevensbescherming.

27 Artikel 4, lid 1, van wet 183(I)/2007.

28 Artikel 71, lid 1, van de wet op de elektronische communicatie.

29 Artikel 65 van wet X-1835.

30 Artikel 1, lid 1, van de wet van 24 juli 2010.

31 Voor de algemene doeleinden van gegevensbewaring: artikel 159/A van wet C/2003, gewijzigd bij wet CLXXIV/2007; voor de toegang van de politie: artikel 68 van wet XXXIV/1994; voor de toegang van de nationale belasting- en douanedienst: artikel 59 van wet CXXII/2010.

32 Artikel 20, lid 1, van wettelijk decreet 198/2008.

Tabel 1: Doelbinding voor de bewaring van gegevens in de nationale wetgevingen	
Nederland	Voor het onderzoeken en vervolgen van ernstige strafbare feiten waarvoor een gevangenisstraf kan worden opgelegd.[33]
Oostenrijk	Richtlijn niet omgezet.
Polen	Voor het voorkomen en opsporen van strafbare feiten, voor het voorkomen en opsporen van fiscale misdrijven, voor gebruik door openbaar aanklagers en rechters indien nodig voor een lopende rechtszaak, en om de binnenlandse veiligheidsdienst, de buitenlandse-inlichtingendienst, het centrale corruptiebestrijdingsbureau, de militaire contra-inlichtingendienst en de militaire inlichtingendienst in staat te stellen hun taken te vervullen.[34]
Portugal	Voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[35]
Roemenië	Richtlijn niet omgezet.
Slovenië	Om de nationale veiligheid en de toepassing van de grondwet te waarborgen, de veiligheid en de politieke en economische belangen van de staat te beschermen en de landsverdediging te garanderen.[36]
Slowakije	Voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.[37]
Finland	Voor het onderzoeken, opsporen en vervolgen van ernstige strafbare feiten als bedoeld in hoofdstuk 5a, artikel 3, lid 1, van de Wet Dwangmaatregelen.[38]
Zweden	Richtlijn niet omgezet.
Verenigd Koninkrijk	Voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[39]

De meeste lidstaten die de richtlijn hebben omgezet, gaan, in overeenstemming met hun nationale wetgeving, verder in het toestaan van toegang tot en gebruik van bewaarde gegevens dan de richtlijn zelf, bijvoorbeeld voor het voorkomen en bestrijden van criminaliteit in het algemeen en van gevaar voor lijf en leden. Hoewel dit is toegestaan uit hoofde van de e-privacyrichtlijn, blijft de mate van harmonisatie die met EU-wetgeving tot

33 Artikel 126 van het wetboek van strafvordering.

34 Artikel 180a van de telecommunicatiewet van 16 juli 2004, gewijzigd bij artikel 1 van het besluit van 24 april 2009.

35 Artikel 1 en artikel 3, lid 1, van wet 32/2008.

36 Artikel 170a, lid 1, van de wet op de elektronische communicatie.

37 Artikel 59a, lid 6, van de wet op de elektronische communicatie.

38 Artikel 14a, lid 1, van de wet op de elektronische communicatie.

39 Regeling gegevensbewaring (EG-richtlijn) 2009 (2009 nr. 859).

stand is gekomen op dit gebied beperkt. Verschillen in het doel van de gegevensbewaring hebben gevolgen voor het aantal en de frequentie van de verzoeken en dus ook voor de kosten die moeten worden gemaakt voor het nakomen van de verplichtingen die voortvloeien uit de richtlijn. Bovendien biedt deze situatie wellicht in onvoldoende mate de voorspelbaarheid die vereist is bij elke wetgevende maatregel die het recht op privacy beperkt[40]. De Commissie zal nagaan of en hoe verdere harmonisatie op dit vlak moet worden verwezenlijkt[41].

4.2. Exploitanten die verplicht zijn gegevens te bewaren (artikel 1)

Deze richtlijn is van toepassing op "aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk" (artikel 1, lid 1). Twee lidstaten (Finland en het Verenigd Koninkrijk) verplichten kleine exploitanten niet om gegevens te bewaren, omdat, zo redeneren zij, de kosten hiervan voor de exploitant en de staat niet zouden opwegen tegen de baten voor het strafrechtstelsel en de rechtshandhaving. Vier lidstaten (Letland, Luxemburg, Nederland en Polen) melden dat zij alternatieve administratieve regelingen hebben getroffen. Grote exploitanten die in verschillende lidstaten actief zijn, hebben relatief minder kosten vanwege de schaalvoordelen; kleinere exploitanten zetten soms gezamenlijke ondernemingen op of besteden bewaar- en opzoekactiviteiten uit aan gespecialiseerde ondernemingen om kosten te besparen. Het uitbesteden van dergelijke technische functies ontslaat de exploitant niet van de verplichting om nauwlettend toe te zien op de verwerking en om de vereiste beveiligingsmaatregelen te treffen, wat soms problematisch is voor kleinere exploitanten. De Commissie zal bij eventuele voorstellen voor wijziging van het gegevensbewaringskader rekening houden met de gegevensbeveiliging en de gevolgen voor kleine en middelgrote ondernemingen.

4.3. Toegang tot gegevens: autoriteiten, procedures en voorwaarden (artikel 4)

De lidstaten moeten bepalingen aannemen "om te waarborgen dat (...) bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde nationale autoriteiten worden verstrekt." Zij moeten zelf in hun nationale wetgeving "de procedure en de te vervullen voorwaarden voor toegang tot gegevens die bewaard worden overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid" vaststellen, "rekening houdend met de relevante bepalingen van de wetgeving van de Unie of publiek internationaal recht, met name het EVRM, zoals geïnterpreteerd door het Europees Hof voor de rechten van de mens".

In alle lidstaten hebben de nationale politie en, behalve in op het gewoonterecht gebaseerde rechtsstelsels (Ierland en het Verenigd Koninkrijk), openbaar aanklagers toegang tot bewaarde gegevens. In veertien lidstaten worden de veiligheidsdienst, de inlichtingendienst of het leger

---

40 Arrest van het Europese Hof van Justitie van 20 mei 2003 in gevoegde zaken C-465/00, C-138/01 en C-139/01 (verzoeken om een prejudiciële beslissing van het Verfassungsgerichtshof en het Oberster Gerichtshof : Rechnungshof (C-465/00) tegen Österreichischer Rundfunk en anderen en Christa Neukomm (C-138/01) en Joseph Lauermann (C-139/01) tegen Österreichischer Rundfunk (Bescherming van natuurlijke personen bij de verwerking van persoonsgegevens - Richtlijn 95/46/EG - Bescherming van persoonlijke levenssfeer - Bekendmaking van gegevens over het inkomen van werknemers van rechtspersonen die onder toezicht van het Rechnungshof staan).

41 Bij de goedkeuring van de richtlijn heeft de Commissie een verklaring uitgegeven waarin zij voorstelt de lijst van strafbare feiten in het Europees aanhoudingsbevel in overweging te nemen (Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten).

ook als bevoegde autoriteit beschouwd. In zes lidstaten geldt dat ook voor de belasting- en/of de douanedienst, en in drie lidstaten voor de grensbewakingsautoriteiten. In één lidstaat kunnen andere overheidsinstanties toegang krijgen tot de gegevens met een machtiging voor specifieke doeleinden volgens afgeleid recht. In elf lidstaten is voor elk verzoek om toegang tot bewaarde gegevens toestemming van de rechter nodig. In drie lidstaten is dat in de meeste gevallen zo. In vier andere lidstaten is toestemming van een hoge instantie vereist, maar niet van de rechter. In twee lidstaten geldt kennelijk alleen de voorwaarde dat het verzoek schriftelijk wordt ingediend.

Tabel 2: Toegang tot bewaarde telecommunicatiegegevens		
	Bevoegde nationale autoriteiten	*Procedures en voorwaarden*
België	Dienst voor gerechtelijke coördinatie, onderzoeksrechters, openbaar aanklager, recherche.	Toestemming nodig van de rechter of openbaar aanklager; op verzoek moeten exploitanten abonneegegevens en verkeers- en locatiegegevens in real-time verstrekken voor oproepen die in de maand daarvoor hebben plaatsgevonden; gegevens over oproepen van langer geleden moeten zo snel mogelijk worden verstrekt.
Bulgarije[42]	Bepaalde directoraten en afdelingen van de rijksdienst voor nationale veiligheid, het ministerie van Binnenlandse Zaken, de militaire inlichtingendienst, de militaire politiedienst, de minster van Defensie, het nationaal onderzoeksbureau; de rechter en autoriteiten die zich bezighouden met het vooronderzoek, onder bepaalde voorwaarden.	Toegang alleen mogelijk op bevel van de voorzitter van een regionale rechtbank.
Tsjechië	Richtlijn niet omgezet.	
Denemarken[43]	Politie	Toestemming van de rechter nodig; rechterlijk bevel wordt afgegeven als het verzoek voldoet aan strikte criteria inzake verdenking, noodzaak en evenredigheid.
Duitsland	Richtlijn niet omgezet.	
Estland[44]	Politie, grenswacht, veiligheidspolitie en, voor goederen en elektronische communicatie, de belasting- en douanedienst.	Toestemming nodig van een onderzoeksrechter; exploitanten moeten bewaarde gegevens in dringende gevallen binnen 10 uur en in andere gevallen binnen 10 werkdagen na ontvangst van het verzoek verstrekken.
Ierland[45]	Leden van de Garda Síochána (politie) met de rang van hoofdcommissaris of hoger, officieren van de strijdkrachten met de rang van kolonel of hoger, ambtenaren van de belastingdienst met de rang van "principal officer" of hoger.	Verzoeken moeten schriftelijk worden ingediend.
Griekenland[46]	Gerechtelijke, militaire en politieautoriteiten.	Beslissing van de rechter nodig waarin

42 Artikel 250b, lid 1, van de wet op de elektronische communicatie (gewijzigd) 2010 (autoriteiten); Artikel 250b, lid 2, en 250c, lid 1, van de wet op de elektronische communicatie (gewijzigd) 2010 (toegang).

43 Artikel 71 van de wet op het procesrecht.

44 Onderafdeling 112, punten 2 en 3, van het Wetboek van strafvordering (over autoriteiten en procedures); artikel 111, lid 9 (voorwaarden) van de wet op de elektronische communicatie.

45 Artikel 6 van de communicatiewet (gegevensbewaring) van 2009.

Tabel 2: Toegang tot bewaarde telecommunicatiegegevens		
	Bevoegde nationale autoriteiten	*Procedures en voorwaarden*
		staat dat onderzoek op een andere manier onmogelijk of buitengewoon moeilijk is.
Spanje[47]	Politiediensten die belast zijn met opsporing, onderzoek en vervolging van ernstige strafbare feiten, nationale inlichtingendienst en de douane.	Toestemming nodig van de rechter.
Frankrijk[48]	Openbaar aanklager, speciaal aangewezen ambtenaren van politie en marechaussee.	Politie moet elk verzoek om toegang tot bewaarde gegevens motiveren en toestemming vragen van de persoon bij het ministerie van Binnenlandse Zaken die daartoe is aangewezen door de Commission nationale de contrôle des interceptions de sécurité; verzoeken om toegang worden behandeld door een speciaal aangewezen ambtenaar die voor de exploitant werkt.
Italië[49]	Openbaar aanklager, politie, raadsman van de verdachte of van de persoon naar wie een onderzoek is ingesteld.	Gemotiveerd bevel van de openbaar aanklager nodig.
Cyprus[50]	Rechters, openbaar aanklagers, politie.	Goedkeuring van openbaar aanklager nodig, wordt verleend als deze van mening is dat gegevens bewijs kunnen opleveren voor het plegen van een ernstig strafbaar feit; de rechter kan een dergelijk bevel uitvaardigen indien er een redelijk vermoeden bestaat dat er een ernstig strafbaar feit is gepleegd en de gegevens daar waarschijnlijk verband mee houden.
Letland[51]	Gemachtigde ambtenaren van instanties die zich bezighouden met het vooronderzoek, personen die het onderzoek verrichten, gemachtigde ambtenaren van de staatsveiligheidsdiensten, het openbaar ministerie, rechters.	Gemachtigde ambtenaren, het openbaar ministerie en rechters moeten de gepastheid en de relevantie van het verzoek toetsen, het verzoek registreren en de bescherming van de verkregen gegevens waarborgen; bevoegde organen kunnen een overeenkomst met een exploitant sluiten over bijvoorbeeld de versleuteling van de verstrekte gegevens.
Litouwen[52]	Organen die zich bezighouden met het vooronderzoek, de openbaar aanklager, de rechter en ambtenaren van de inlichtingendienst.	Bevoegde instanties moeten bewaarde gegevens schriftelijk opvragen; voor toegang voor het vooronderzoek is toestemming van de rechter nodig.
Luxemburg[53]	Gerechtelijke autoriteiten (onderzoeksrechters, aanklagers), autoriteiten die belast zijn met de staatsveiligheid, defensie, openbare veiligheid en het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.	Toestemming van de rechter nodig.

46 Artikelen 3 en 4 van wet 2225/94

47 Artikelen 6 en 7 van wet 25/2007.

48 Artikel 60, leden 1 en 2, van het Wetboek van strafvordering (autoriteiten); artikel L 31-1-1 (voorwaarden).

49 Artikel 132, lid 3, van het Wetboek gegevensbescherming.

50 Artikel 4, leden 2 en 4, van wet 183(I)/2007.

51 Artikel 71, lid 1, van de wet op de elektronische communicatie (autoriteiten); ministerieel besluit nr. 820 (procedures).

52 Artikel 77, leden 1 en 2 van wet X—1835; mondeling verslag aan de Commissie.

Tabel 2: Toegang tot bewaarde telecommunicatiegegevens		
	Bevoegde nationale autoriteiten	*Procedures en voorwaarden*
Hongarije[54]	Politie, nationale belasting- en douanedienst, nationale veiligheidsdiensten, openbaar aanklager, rechters.	Politie en de nationale belasting- en douanedienst hebben toestemming van de openbaar aanklager nodig; openbaar aanklager en nationale veiligheidsdiensten hebben zonder rechterlijk bevel toegang tot de gegevens.
Malta[55]	Maltese politiedienst, veiligheidsdienst.	Verzoeken moeten schriftelijk worden ingediend.
Nederland[56]	De onderzoekende politieambtenaar.	Toegang door middel van een vordering van de officier van justitie of een rechter-commissaris.
Oostenrijk	Richtlijn niet omgezet.	
Polen[57]	Politie, grenswachters, belastinginspecteurs, binnenlandse veiligheidsdienst, buitenlandse-inlichtingendienst, het centrale corruptiebestrijdingsbureau, de militaire contra-inlichtingendienst, militaire inlichtingendienst, rechters en openbaar aanklager.	Verzoeken moeten schriftelijk worden ingediend, en in geval van politie, grenswachters en belastinginspecteurs, met toestemming van de hoogste ambtenaar in de organisatie.
Portugal[58]	Recherche, nationale republikeinse garde, rijksveiligheidsdienst, marechaussee, immigratie- en grensbewakingsdienst, maritieme politie.	Toestemming van de rechter nodig, en alleen indien toegang cruciaal is om de waarheid te achterhalen of dat bewijs op een andere manier onmogelijk of buitengewoon moeilijk te verkrijgen is; voor rechterlijke toestemming moet worden beantwoord aan vereisten inzake noodzakelijkheid en evenredigheid.
Roemenië	Richtlijn niet omgezet.	
Slovenië[59]	Politie, inlichtingen- en veiligheidsdiensten, defensieafdelingen belast met inlichtingen, contra-inlichtingen en veiligheidsopdrachten.	Toestemming van de rechter nodig.
Slowakije[60]	Rechtshandhavingsautoriteiten, rechters.	Verzoeken moeten schriftelijk worden ingediend.
Finland[61]	Politie, grenswachters, douaneautoriteiten (voor bewaarde abonnee-, verkeers- en locatiegegevens); rampencentrum, reddingsdienst voor noodgevallen op zee, subcentrum van de reddingsdienst (voor identificatie- en locatiegegevens in noodgevallen).	Abonneegegevens zijn voor alle bevoegde autoriteiten toegankelijk zonder toestemming van de rechter; voor andere gegevens is een rechterlijk bevel nodig.
Zweden	Richtlijn niet omgezet.	

53 Artikel 5-2, lid 1, en artikel 9, lid 2, van de wet van 24 juli 2010 (autoriteiten); artikel 67-1 van het wetboek van strafvordering (voorwaarden).

54 Artikel 68, lid 1, en artikel 69, lid 1, onder c) en d), van wet XXXIV 1994; artikel 9/A, lid 1, van wet V 1972; artikel 71, leden 1, 3, en 4, artikel 178/A, lid 4, artikel 200, artikel 201, artikel 268, lid 2, van wet XIX 1998; artikel 40, leden 1 en 2, artikel 53, lid 1, artikel 54, lid 1, onder j), van wet CXXV 1995.

55 Artikel 20, leden 1 en 3, van wettelijk decreet 198/2008.

56 Artikel 126 ni van het wetboek van strafvordering.

57 Artikel 179, lid 3, van de telecommunicatiewet van 16 juli 2004, gewijzigd bij artikel 1 van het besluit van 24 april 2009.

58 Artikel 2, lid 1, artikel 3, lid 2, en artikel 9 van wet 32/2008.

59 Artikel 107c van de wet op de elektronische communicatie, Artikel 149b van het wetboek van strafvordering., artikel 24b van de wet op het inlichtingen- en veiligheidsbureau, artikel 32 van de defensiewet.

60 Artikel 59a, lid 8, van de wet op de elektronische communicatie.

61 Artikelen 35, lid 1, en artikel 36 van de wet op de elektronische communicatie, artikelen 31-33 van de politiewet, artikel 41 van de grensbewakingswet.

Tabel 2: Toegang tot bewaarde telecommunicatiegegevens		
	Bevoegde nationale autoriteiten	*Procedures en voorwaarden*
Verenigd Koninkrijk[62]	Politie, inlichtingendiensten, belasting- en douaneautoriteiten, andere bij afgeleid recht aangewezen overheidsinstanties.	Toegang toegestaan, met toestemming van een bevoegd persoon en na een noodzakelijkheids- en evenredigheidstoets, in bepaalde gevallen en in omstandigheden waarin het vrijgeven van de gegevens wettelijk verplicht of toegestaan is; er zijn specifieke procedures afgesproken met exploitanten.

De Commissie zal nagaan of en hoe verdere harmonisatie ten aanzien van de autoriteiten die toegang hebben tot bewaarde gegevens en de procedure voor het verkrijgen van die toegang, tot stand moet worden gebracht. Dit zou kunnen gebeuren aan de hand van lijsten met duidelijker omschreven bevoegde autoriteiten, onafhankelijk en/of rechterlijk toezicht op verzoeken om toegang tot de gegevens, en minimumnormen voor de procedures die exploitanten moeten volgen bij het verlenen van toegang aan de bevoegde autoriteiten.

4.4. Werkingssfeer en categorieën te bewaren gegevens (artikel 1, lid 2, artikel 3, lid 2, en artikel 5)

De richtlijn is van toepassing op telefonie over een vast netwerk, mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie. In artikel 5 worden de te bewaren categorieën gegevens genoemd, namelijk de gegevens die nodig zijn voor het identificeren of bepalen van:

(a) de bron van een communicatie;

(b) de bestemming van een communicatie;

(c) de datum, het tijdstip en de duur van een communicatie;

(d) het type communicatie;

(e) de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers; en

(f) de locatie van mobiele communicatieapparatuur.

De richtlijn heeft ook (artikel 3, lid 2) betrekking op oproeppogingen zonder resultaat, d.w.z. een communicatie waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord, en waarbij gegevens worden gegenereerd, verwerkt en opgeslagen of gelogd door exploitanten. Er mogen op grond van deze richtlijn geen gegevens worden bewaard waaruit de inhoud van de communicatie kan worden opgemaakt. Later is ook verduidelijkt dat zoekopdrachten, d.w.z. serverlogs die

---

62 Artikel 25, schema 1 van de wet inzake de regeling van onderzoeksbevoegdheden 2000, artikel 7 van de regeling gegevensbewaring; artikel 22, lid 2, van de wet tot regeling van de onderzoeksbevoegdheden bepaalt voor welke doeleinden deze autoriteiten toegang tot de gegevens kunnen krijgen.

zijn gegenereerd door het aanbieden van een zoekmachinedienst, buiten de werkingssfeer van de richtlijn vallen, omdat zij niet als verkeersgegevens, maar als inhoud moeten worden beschouwd[63].

In eenentwintig lidstaten voorziet de omzettingswetgeving in de bewaring van elk van deze categorieën gegevens. België heeft niet bepaald welke categorieën telefoniegegevens moeten worden bewaard en heeft ook geen bepalingen inzake internetgegevens vastgesteld. De respondenten van de vragenlijst van de Commissie vonden het niet nodig de categorieën te bewaren gegevens te wijzigen, hoewel het Europees Parlement de Commissie in een schriftelijk verzoek vraagt de werkingssfeer van Richtlijn 2006/24/EG uit te breiden tot zoekmachines, "zodat snel en doeltreffend kan worden opgetreden tegen kinderporno en seksueel geweld online"[64]. In haar verslag over de tweede handhavingsactie heeft de Groep gegevensbescherming van artikel 29 gesteld dat de categorieën gegevens die in de richtlijn worden genoemd, als volledig moeten worden beschouwd en dat geen bijkomende bewaringsverplichtingen aan exploitanten moeten worden opgelegd. De Commissie zal nagaan in hoeverre al deze categorieën gegevens noodzakelijk zijn.

4.5. Bewaringstermijnen (artikelen 6 en 12)

De lidstaten moeten ervoor zorgen dat de in artikel 5 genoemde categorieën gegevens gedurende ten minste zes maanden en ten hoogste twee jaar worden bewaard. Lidstaten "met specifieke omstandigheden die een in tijd beperkte verlenging (...) rechtvaardigen", kunnen de maximale bewaringstermijn verlengen. De lidstaten melden een dergelijke verlenging aan de Commissie, die uiterlijk zes maanden na die kennisgeving de verlenging bekrachtigt of verwerpt. De maximale bewaringstermijn kan dus worden verlengd, maar er is geen bepaling over de verkorting van de bewaring tot minder dan zes maanden. Op één na passen alle lidstaten die de richtlijn hebben omgezet, bewaringstermijnen toe die binnen de gestelde grenzen vallen en er zijn geen verlengingen bij de Commissie gemeld. De termijnen zijn echter verre van uniform.

In vijftien lidstaten geldt een enkele bewaringstermijn voor alle categorieën gegevens: in één lidstaat (Polen) is dat tweeënhalfjaar, in één lidstaat (Letland) anderhalf jaar, in tien lidstaten (Bulgarije, Denemarken, Estland, Griekenland, Spanje, Frankrijk, Nederland, Portugal, Finland en het Verenigd Koninkrijk) één jaar, en in drie lidstaten (Cyprus, Luxemburg en Litouwen) zes maanden. In vijf lidstaten gelden verschillende bewaringstermijnen voor verschillende categorieën gegevens: in twee lidstaten (Ierland en Italië) geldt twee jaar voor vaste- en mobiele-telefoniegegevens en één jaar voor gegevens over internettoegang, e-mail via internet en internettelefonie; in één lidstaat (Slovenië) geldt veertien maanden voor telefoniegegevens en acht maanden voor internetgegevens; in één lidstaat (Slowakije) geldt één jaar voor vaste- en mobiele-telefoniegegevens en zes maanden voor internetgegevens; in één lidstaat (Malta) geldt één jaar voor vaste-, mobiele- en internet-telefoniegegevens en zes maanden voor internettoegang en e-mail via internet. In één lidstaat (Hongarije) worden alle gegevens één jaar bewaard behalve de gegevens over oproeppogingen zonder resultaat, die

---

63 Advies van de Groep gegevensbescherming artikel 29 over gegevensbescherming en zoekmachines, 4 april 2008.

64 Schriftelijke verklaring, ingediend overeenkomstig artikel 123 van het Reglement, over het opzetten van een Europees alarmsysteem (EAS) tegen pedofielen en plegers van seksueel geweld, van 19.4.2010 (0029/2010).

slechts zes maanden worden bewaard. Eén lidstaat (België) heeft geen bewaringstermijnen vastgesteld voor de categorieën gegevens die in de richtlijn worden genoemd. Tabel 3 geeft een gedetailleerd overzicht.

Tabel 3: Bewaringstermijnen in de nationale wetgevingen	
België[65]	Tussen 1 jaar en 36 maanden voor openbaar beschikbare telefoniediensten; geen bepalingen met betrekking tot internetgegevens.
Bulgarije	1 jaar; gegevens waartoe al toegang is verleend mogen op verzoek nog eens 6 maanden worden bewaard.
Tsjechië	Richtlijn niet omgezet.
Denemarken	1 jaar
Duitsland	Richtlijn niet omgezet.
Estland	1 jaar
Ierland	2 jaar voor vaste- en mobiele-telefoniegegevens en 1 jaar voor gegevens over internettoegang, e-mail via internet en internettelefonie.
Griekenland	1 jaar
Spanje	1 jaar
Frankrijk	1 jaar
Italië	2 jaar voor vaste- en mobiele-telefoniegegevens en 1 jaar voor gegevens over internettoegang, e-mail via internet en internettelefonie.
Cyprus	6 maanden
Letland	18 maanden
Litouwen	6 maanden
Luxemburg	6 maanden
Hongarije	6 maanden voor oproeppogingen zonder resultaat en 1 jaar voor alle andere gegevens.
Malta	1 jaar voor vaste-, mobiele- en internet-telefoniegegevens, 6 maanden voor internettoegang en e-mail via internet.
Nederland	1 jaar
Oostenrijk	Richtlijn niet omgezet.
Polen	2 jaar
Portugal	1 jaar
Roemenië	Richtlijn niet omgezet (6 maanden in de nietig verklaarde omzettingswet).
Slovenië	14 maanden voor telefoniegegevens, 8 maanden voor internetgegevens.
Slowakije	1 jaar voor vaste- en mobiele-telefoniegegevens, 6 maanden voor gegevens over internettoegang, e-mail via internet en internettelefonie.
Finland	1 jaar
Zweden	Richtlijn niet omgezet.
Verenigd Koninkrijk	1 jaar

De richtlijn biedt weliswaar ruimte voor deze diversiteit, maar daardoor genieten exploitanten die in meer dan een lidstaat actief zijn en burgers van wie de communicatiegegevens in verschillende lidstaten opgeslagen kunnen zijn, slechts een beperkte rechtszekerheid en voorspelbaarheid. Gezien de toenemende internationalisering van de gegevensverwerking en de uitbesteding van gegevensopslag moet worden nagegaan hoe de bewaringstermijnen in de EU verder kunnen worden geharmoniseerd. Met het oog op het evenredigheidsbeginsel en in het licht van de kwantitatieve en kwalitatieve bewijzen van de waarde van bewaarde gegevens in de lidstaten, en de ontwikkelingen op het gebied van communicatie en technologie en van criminaliteit en terrorisme, zal de Commissie zich buigen over de vraag of er verschillende

[65] Artikel 126, lid 2, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

bewaringstermijnen moeten gelden voor verschillende categorieën gegevens, verschillende categorieën ernstige strafbare feiten, of een combinatie van beide[66]. Uit de kwantitatieve informatie die de lidstaten tot nu hebben verstrekt over de ouderdom van de bewaarde gegevens, blijkt dat het (eerste) verzoek om toegang door rechtshandhavingsautoriteiten bij ongeveer negentig procent van de gegevens na zes maanden of eerder en bij ongeveer zeventig procent na drie maanden of eerder wordt gedaan (zie punt 5.2).

4.6. Gegevensbescherming, gegevensbeveiliging en toezichthoudende autoriteiten (artikelen 7 en 9)

Volgens de richtlijn moeten de lidstaten ervoor zorgen dat de exploitanten ten minste vier beginselen van gegevensbeveiliging respecteren, namelijk dat de bewaarde gegevens:

(a) dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het publieke communicatienetwerk;

(b) worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

(c) worden onderworpen aan passende technische en organisatorische maatregelen om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen; en

(d) aan het einde van de bewaarperiode worden vernietigd, met uitzondering van de [voor het in de richtlijn bepaalde doel] geraadpleegde en bevroren gegevens.

Volgens de gegevensbeschermingsrichtlijn en de e-privacyrichtlijn mogen exploitanten gegevens die in het kader van de richtlijn worden bewaard, niet voor andere doeleinden verwerken, vooropgesteld dat de gegevens anders niet zouden zijn bewaard[67]. De lidstaten moeten een autoriteit aanwijzen die op volledig onafhankelijke wijze toezicht houdt op de toepassing van deze beginselen; dit kunnen dezelfde autoriteiten zijn als die welke op grond van de gegevensbeschermingsrichtlijn moeten worden aangewezen[68].

Vijftien lidstaten hebben al deze beginselen omgezet in hun wetgeving. Vier lidstaten (België, Estland, Spanje en Letland) hebben twee of drie van de beginselen omgezet maar kennen geen specifieke bepalingen voor de vernietiging van gegevens aan het einde van de bewaringstermijn. Twee lidstaten (Italië en Finland) hebben bepaald dat de gegevens moeten worden vernietigd. Het is niet duidelijk welke technische en organisatorische beveiligingsmaatregelen er precies worden toegepast, zoals versterkte authenticatie en nauwkeurige toegangsregistratie[69]. Tweeëntwintig lidstaten hebben een toezichthoudende

---

66 In haar voorstel voor een richtlijn over gegevensbewaring van 2005 ging de Commissie uit van een bewaringstermijn van een jaar voor telefoniegegevens en zes maanden voor internetgegevens.

67 Artikel 13, lid 1, van Richtlijn 95/46/EG.

68 Artikel 28 van Richtlijn 95/46/EG.

69 Bij versterkte authenticatie gaat het om dubbele authenticatiemechanismen, zoals een wachtwoord en biometrische kenmerken, of een wachtwoord en een token, als garantie dat degene die belast is met de

autoriteit die toeziet op de toepassing van de beginselen. In de meeste gevallen is dat de gegevensbeschermingsautoriteit. Tabel 4 geeft een gedetailleerd overzicht.

Tabel 4: Gegevensbescherming, gegevensbeveiliging en toezichthoudende autoriteiten		
Lidstaat	*Gegevensbeschermings- en gegevensbeveiligingsbepalingen in het nationale recht*	*Toezichthoudende autoriteit*
België	Exploitanten moeten ervoor zorgen dat bij het doorsturen de gegevens niet door derden kunnen worden onderschept; zij moeten voldoen aan de ETSI-normen voor de beveiliging en rechtmatige interceptie van telecommunicatie[70]. Verplichte vernietiging van gegevens aan het einde van de bewaringstermijn kennelijk niet geregeld.	Instituut voor Postdiensten en Telecommunicatie.
Bulgarije	Omzettingswet vereist toepassing van de vier beginselen[71].	Commissie Bescherming persoonsgegevens ziet toe op verwerking en opslag van gegevens om ervoor te zorgen dat de verplichtingen worden nagekomen; Parlementaire commissie in de nationale vergadering ziet toe op de procedures voor machtiging en toegang tot de gegevens.
Tsjechië[72]	Richtlijn niet omgezet.	
Denemarken	Vier beginselen omgezet. [73].	Nationaal IT- en telecombureau ziet toe op de verplichting voor aanbieders van elektronische communicatienetwerken en -diensten om ervoor te zorgen dat de apparatuur en systemen het technisch mogelijk maken dat de politie toegang heeft tot informatie over telecommunicatieverkeer.
Duitsland	Richtlijn niet omgezet.	
Estland	Drie van de vier beginselen omgezet in nationaal recht. Geen expliciete bepaling voor het vierde beginsel, maar eenieder die vindt dat zijn privacy is geschonden door toezichtactiviteiten kan op basis van een rechterlijke beslissing verzoeken om vernietiging van de gegevens[74].	Technische toezichthoudende autoriteit.
Ierland[75]	Omzettingswet vereist toepassing van de vier beginselen.	Aangewezen rechter is bevoegd om te onderzoeken of bevoegde nationale autoriteiten de omzettingswet naleven en om hierover verslag uit te brengen.

verwerking van de verkeersgegevens, persoonlijk aanwezig is. Nauwkeurige toegangsregistratie houdt in dat de toegangs- en verwerkingshandelingen nauwkeurig worden bijgehouden, waarbij de gegevens over de identiteit van de gebruiker, de toegangstijd en de dossiers die zijn geraadpleegd, worden bewaard.

70 Artikel 6 van het Koninklijk Besluit van 9 januari 2003.

71 Artikel 4, lid 1, van de wet op de elektronische communicatie (gewijzigd) 2010.

72 Artikel 87, lid 3, en artikel 88 van besluit 127/2005 als gewijzigd bij besluit 247/2008; artikel 2 van besluit 336/2005; artikel 3, lid 4, van besluit 4/2005; artikel 28, lid 1, van besluit 101/2000.

73 Besluit over de verwerking van persoonsgegevens, Uitvoeringsbesluit nr. 714 van 26 juni 2008 over het aanbieden van elektronische communicatienetwerken en -diensten.

74 Artikel 111, lid 9, van de wet op de elektronische communicatie; Artikel 122, lid 2, van het wetboek van strafvordering.

75 Artikelen 4, 11 en 12 van de communicatiewet (gegevensbewaring) 2009.

Tabel 4: Gegevensbescherming, gegevensbeveiliging en toezichthoudende autoriteiten		
Lidstaat	*Gegevensbeschermings- en gegevensbeveiligingsbepalingen in het nationale recht*	*Toezichthoudende autoriteit*
Griekenland[76]	Omzettingswet vereist toepassing van de vier beginselen en verplicht exploitanten een plan op te stellen en uit te voeren om de regels na te leven onder toezicht van een manager gegevensbeveiliging.	Autoriteit Bescherming persoonsgegevens en autoriteit communicatieprivacy.
Spanje[77]	Gegevensbeveiligingsbepalingen hebben betrekking op drie van de vier beginselen (kwaliteit en beveiliging van bewaarde gegevens, toegang door gemachtigde personen en bescherming tegen ongeoorloofde verwerking).	Bureau voor gegevensbescherming.
Frankrijk[78]	Omzettingswet vereist toepassing van de vier beginselen.	Nationale commissie voor informatietechnologie en vrijheid ziet toe op naleving van de regels.
Italië	Geen specifieke bepalingen over beveiliging van bewaarde gegevens, maar er geldt een algemene verplichting om verkeersgegevens te vernietigen of anoniem te maken en toestemming te vragen om locatiegegevens te verwerken[79].	Gegevensbeschermingsautoriteit ziet toe op naleving van de richtlijn.
Cyprus[80]	Elk van de vier beginselen omgezet in nationaal recht.	Commissaris voor bescherming van persoonsgegevens ziet toe op toepassing van omzettingswet.
Letland[81]	Twee beginselen omgezet in nationaal recht: vertrouwelijkheid van en toegang met machtiging tot bewaarde gegevens, en vernietiging van gegevens aan het einde van de bewaringstermijn.	De rijksdienst voor gegevensinspectie ziet toe op de bescherming van persoonsgegevens in de sector elektronische communicatie, maar niet op de toegang tot en de verwerking van bewaarde gegevens.
Litouwen[82]	Elk van de vier beginselen omgezet in nationaal recht.	Rijksdienst voor gegevensbescherming ziet toe op de toepassing van de omzettingswetgeving en moet de Europese Commissie statistieken verstrekken.
Luxemburg[83]	Elk van de vier beginselen omgezet in nationaal recht.	Gegevensbeschermingsautoriteit.
Hongarije[84]	Elk van de vier beginselen omgezet in nationaal recht.	Parlementair commissaris voor gegevensbescherming en vrijheid van informatie.
Malta[85]	Elk van de vier beginselen omgezet in nationaal recht.	Commissaris voor gegevensbescherming.

76 Artikel 6 van Wet 3917/2011.

77 Artikel 8 van wet 25/2007, artikel 38, lid 3, van de algemene telecommunicatiewet; de wet (art 9) verwijst naar de uitzonderingen op toegang en het recht op schrapping in wet 15/1999 inzake de bescherming van persoonsgegevens (art 22 en 23).

78 Artikel D.98-5, CPCE; artikel L-34-1(V), CPCE; artikel 34 van wet nr. 78-17; artikel 34-1, CPCE; artikel 11 van wet nr. 78-17 van 6 januari 1978.

79 Artikelen 123 en 126 van het wetboek gegevensbescherming.

80 Artikelen 14 en 15 van wet 183(I)/2007.

81 Artikel 4, lid 4, en artikel 71, leden 6-8 van de wet op de elektronische communicatie.

82 Artikel 12, lid 5, artikel 66, leden 8 en 9, van de wet op de elektronische communicatie, gewijzigd op 14 november 2009.

83 Artikel 1, lid 5, van de wet van 24 juli 2010.

84 Artikel 157 van wet C/2003, gewijzigd bij wet CLXXIV/2007; Artikel 2 van decreet nr. 226/2003, en wet LXII/1992 inzake gegevensbescherming.

Tabel 4: Gegevensbescherming, gegevensbeveiliging en toezichthoudende autoriteiten		
Lidstaat	*Gegevensbeschermings- en gegevensbeveiligingsbepalingen in het nationale recht*	*Toezichthoudende autoriteit*
Nederland[86]	Elk van de vier beginselen omgezet in nationaal recht.	Agentschap Telecom ziet toe op naleving van de verplichtingen door internet- en telecomaanbieders; College bescherming persoonsgegevens ziet toe op algemene verwerking van persoonsgegevens; de samenwerking tussen beide instanties is geregeld in een overeenkomst.
Oostenrijk	Richtlijn niet omgezet.	
Polen	Elk van de vier beginselen omgezet in nationaal recht[87].	Gegevensbeschermingsautoriteit.
Portugal	Elk van de vier beginselen omgezet in nationaal recht[88].	Portugese gegevensbeschermingsautoriteit.
Roemenië	Richtlijn niet omgezet.	
Slovenië[89]	Elk van de vier beginselen omgezet in nationaal recht.	Commissaris voor informatie.
Slowakije[90]	Elk van de vier beginselen omgezet in nationaal recht.	De nationale autoriteit voor regels en tarieven op het gebied van elektronische communicatie ziet toe op de bescherming van persoonsgegevens.
Finland	Alleen de verplichting om gegevens aan het einde van de bewaringstermijn te vernietigen is expliciet omgezet in nationaal recht[91].	Finse autoriteit voor regelgeving op het gebied van communicatie ziet toe op de naleving van de bewaarvoorschriften door de exploitanten; ombudsman voor gegevensbescherming ziet toe op algemene rechtmatigheid van de verwerking van persoonsgegevens.
Zweden	Richtlijn niet omgezet.	
Verenigd Koninkrijk	Elk van de vier beginselen omgezet in nationaal recht[92].	Commissaris voor informatie ziet toe op de bewaring en/of verwerking van communicatiegegevens (en andere persoonsgegevens) en op de controle op de gegevensbescherming. Commissaris voor interceptie (een hogere, nog actieve of gepensioneerde rechter) houdt toezicht op de verkrijging van communicatiegegevens door de autoriteiten volgens de RIPA. Tribunaal voor onderzoeksbevoegdheden onderzoekt klachten over misbruik van gegevens die zijn verkregen op grond van de omzettingswet (RIPA).

85 Artikelen 24 en 25 van wettelijk decreet 198/2008; artikel 40b van de gegevensbeschermingswet (Cap.440)

86 Artikel 135, lid 5, van de wet op de telecommunicatie; de volledige titel van de samenwerkingsovereenkomst luidt: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens*.

87 Artikelen 180a en 180e van de telecommunicatiewet.

88 Artikel 7, leden 1 en 5, en artikel 11, van wet 32/2008; artikelen 53 en 54 van de wet inzake de bescherming van persoonsgegevens.

89 Artikel 107a, lid 6, en artikel 107c, van de wet op de elektronische communicatie.

90 Artikel 59a van de wet op de elektronische communicatie; artikel S33 van wet nr. 428/2002 inzake de bescherming van persoonsgegevens.

91 Artikel 16, lid 3, van de wet op de elektronische communicatie.

92 Artikel 6 van de regeling gegevensbewaring,

Artikel 7 is op uiteenlopende manieren omgezet. Bewaarde gegevens kunnen van zeer persoonlijke en gevoelige aard zijn. Daarom moeten bij het opslaan, opzoeken en gebruiken van deze gegevens consequent en zichtbaar hoge gegevensbeschermings- en -beveiligingsnormen worden toegepast om het risico van privacyschending tot een minimum te beperken en het vertrouwen van burgers te behouden. De Commissie zal zich buigen over mogelijkheden om de gegevensbeveiligings- en -beschermingsnormen aan te scherpen, bijvoorbeeld door middel van ingebouwde privacy, om ervoor te zorgen dat deze normen worden nageleefd bij de opslag en doorgifte van gegevens. Zij zal ook rekening houden met de aanbevelingen voor minimumwaarborgen en voor technische en organisatorische maatregelen die de Groep gegevensbescherming van artikel 29 heeft gedaan in haar verslag over de tweede handhavingsactie[93].

4.7. Statistieken (artikel 10)

De lidstaten moeten jaarlijks statistische informatie aan de Commissie verstrekken over de bewaring van gegevens, met name over:

- gevallen waarin overeenkomstig de toepasselijke nationale wetgeving gegevens zijn verstrekt aan de bevoegde autoriteiten;
- de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten ze hebben opgevraagd (i.e. de ouderdom van de gegevens); en
- de gevallen waarin verzoeken niet konden worden ingewilligd.

De Commissie heeft de lidstaten verzocht om bij de statistieken details te verstrekken over individuele verzoeken om gegevens. Niettemin verschilden de verstrekte statistieken zowel inhoudelijk als wat de details betreft: sommige lidstaten maakten een onderscheid tussen verschillende soorten communicatie, sommige vermeldden hoe lang de gegevens waren bewaard voordat ze werden opgevraagd, en sommige verstrekten alleen jaarlijkse statistieken zonder verdere indeling. Negentien lidstaten[94] hebben statistieken verstrekt over het aantal verzoeken om gegevens in 2009 en/of 2008. Daaronder waren ook Ierland, Griekenland en Oostenrijk, waar gegevens werden opgevraagd hoewel de richtlijn op dat moment nog niet was omgezet, alsook Tsjechië en Duitsland, waar de wetgeving inzake gegevensbewaring nietig is verklaard. Zeven lidstaten die de richtlijn hebben omgezet hebben geen statistieken verstrekt, hoewel België een raming heeft gegeven van het aantal verzoeken om telefoniegegevens per jaar (300 000).

Betrouwbare kwantitatieve en kwalitatieve gegevens zijn cruciaal om de noodzaak en de waarde van veiligheidsmaatregelen als gegevensbewaring aan te tonen. Dit werd erkend in het actieplan uit 2006 voor het meten van de omvang van de criminaliteit en het strafrecht[95], waarin als doelstelling was opgenomen methoden te ontwikkelen voor het regelmatig

---

93 Advies 3/2006 van de Groep gegevensbescherming van artikel 29 (WP119); verslag 01/2010.

94 Tsjechië, Denemarken, Duitsland, Estland, Ierland, Griekenland, Spanje, Frankrijk, Cyprus, Letland, Litouwen, Malta, Nederland, Oostenrijk, Polen, Slovenië, Slowakije, Finland, Verenigd Koninkrijk,

95 Mededeling van de Commissie COM82006) 437 "Ontwikkeling van een algemene en coherente EU-strategie voor het meten van de omvang van de criminaliteit en het strafrecht: een EU-actieplan 2006 – 2010".

verzamelen van gegevens overeenkomstig de richtlijn en de statistische informatie op te nemen in de database van Eurostat (mits de gegevens beantwoorden aan de kwaliteitsnormen). Deze doelstelling kon niet worden verwezenlijkt, omdat de meeste lidstaten pas in de afgelopen twee jaar de richtlijn volledig hebben omgezet en op verschillende manieren interpreteren wat de bron van de statistieken moet zijn. De Commissie zal zich er in haar toekomstige voorstel tot wijziging van het gegevensbewaringskader en bij de herziening van het hierboven bedoelde actieplan op toeleggen bruikbare meetmethoden en verslagleggingsprocedures te ontwikkelen, die leiden tot een transparant en zinvol toezicht op gegevensbewaring en geen onnodige belasting vormen voor het strafrechtstelsel en de rechtshandhavingsautoriteiten.

4.8. Omzetting in de EER-landen

IJsland, Liechtenstein en Noorwegen hebben wetgeving op het gebied van gegevensbewaring vastgesteld[96].

4.9. Beslissingen van constitutionele hoven over omzettingswetten

Het Roemeense constitutionele hof heeft in oktober 2009 de wet tot omzetting van de richtlijn nietig verklaard op grond van het feit dat de wet ongrondwettig was; het Duitse constitutionele hof deed hetzelfde in maart 2010 en het Tsjechische constitutionele hof in maart 2011. Het Roemeense hof[97] achtte inperking van de grondrechten aanvaardbaar mits aan bepaalde regels wordt voldaan en goede en voldoende waarborgen zijn ingebouwd om bescherming te bieden tegen willekeurige overheidsmaatregelen. Op basis van de jurisprudentie van het Europese Hof voor de rechten van de mens[98] was het hof echter van oordeel dat de omzettingswet ten aanzien van de werkingssfeer en het doel onduidelijk was en onvoldoende waarborgen bood. Het hof oordeelde dat een permanente wettelijke verplichting om alle verkeersgegevens zes maanden te bewaren onverenigbaar was met het recht op privacy en het recht op vrijheid van meningsuiting van artikel 8 van het Europees Verdrag voor de rechten van de mens.

Het Duitse constitutionele hof[99] was van oordeel dat gegevensbewaring burgers het gevoel geeft dat ze worden gecontroleerd, wat een belemmering kan vormen voor de vrije uitoefening van de grondrechten. Het hof erkende uitdrukkelijk dat gegevensbewaring voor strikt beperkte doeleinden en met afdoende gegevensbeveiliging niet noodzakelijkerwijs een schending van de Duitse grondwet hoeft te zijn. Het hof beklemtoonde echter dat de bewaring van dergelijke gegevens een ernstige inperking van het recht op privacy vormde en daarom alleen kon worden toegestaan in zeer specifieke omstandigheden, en dat een bewaringstermijn van zes maanden op de grens ("*an der Obergrenze*") was van wat nog als evenredig kon worden beschouwd (punt 215). Gegevens zouden alleen mogen worden opgevraagd wanneer er al een vermoeden van een ernstig strafbaar feit of een bewijs van een bedreiging van de openbare veiligheid bestaat, en er zou een verbod moeten gelden op het terugzoeken van gegevens betreffende bepaalde vormen van communicatie (zoals die welke verband houden

---

96 In Ierland bij de telecommunicatiewet 81/2003 (gewijzigd in april 2005), in Liechtenstein bij de telecommunicatiewet 2006. In Noorwegen werd de omzettingswetgeving op 5 april 2011 aangenomen en moet nog worden bekrachtigd door de Kroon.

97 Beslissing nr. 1258 van 8 oktober 2009 van het Roemeense constitutionele hof.

98 EHRM, Rotaru tegen Roemenië 2000, Sunday Times tegen Verenigd Koninkrijk 1979 en Prins Hans-Adam van Liechtenstein tegen Roemenië 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, punt 1 – 345.

met emotionele of sociale nood) die zijn gebaseerd op vertrouwelijkheid. Ook zouden gegevens moeten worden gecodeerd en zou er transparant toezicht moeten zijn op het gebruik ervan.

Het Tsjechische constitutionele hof[100] heeft de omzettingswetgeving nietig verklaard omdat deze, als maatregel die inbreuk maakt op de grondrechten, niet nauwkeurig en helder genoeg was geformuleerd. Het hof vond de doelbinding te breed, gezien de schaal en de werkingssfeer van de verplichte gegevensbewaring. Het was van oordeel dat in de omzettingswetgeving niet duidelijk genoeg was gedefinieerd welke autoriteiten toegang hebben tot en gebruik mogen maken van bewaarde gegevens, noch welke procedures daarvoor gelden en dat daardoor de integriteit en de vertrouwelijkheid van de gegevens niet waren gewaarborgd. Naar het oordeel van het hof genoot de individuele burger onvoldoende waarborgen tegen mogelijk machtsmisbruik door de overheid. Het hof had geen kritiek op de richtlijn zelf, die volgens het hof voldoende ruimte bood om te worden omgezet in overeenstemming met de Tsjechische grondwet. Het hof uitte in een *obiter dictum* echter twijfels over de noodzaak, de doeltreffendheid en het nut van het bewaren van verkeersgegevens, nu zich nieuwe vormen van criminaliteit voordoen waarbij bijvoorbeeld gebruikgemaakt wordt van anonieme simkaarten.

Deze drie lidstaten bekijken nu hoe zij de richtlijn alsnog kunnen omzetten. Ook andere constitutionele hoven hebben zich gebogen over gegevensbewaring, zoals in Bulgarije, waar de omzettingswet vervolgens werd herzien, in Cyprus, waar rechterlijke bevelen die waren uitgevaardigd op grond van de omzettingswet ongrondwettig werden bevonden, en in Hongarije, waar een zaak betreffende het ontbreken van de wettelijke doeleinden van gegevensverwerking in de omzettingwet nog hangende is[101].

De Commissie zal de kwesties die in de nationale rechtspraak aan de orde zijn gesteld, meewegen in haar toekomstige voorstel tot herziening van het kader voor gegevensbewaring.

4.10. Verdere handhaving van de richtlijn

De Commissie verwacht van de lidstaten die de richtlijn nog niet volledig hebben omgezet of die nog geen wetgeving hebben vastgesteld in plaats van de omzettingswetgeving die door de nationale rechter nietig is verklaard, dat zij dit zo snel mogelijk doen. Indien dit niet gebeurt, behoudt de Commissie zich het recht voor gebruik te maken van de bevoegdheden die haar bij de Verdragen zijn toegekend. Tot nu toe zijn twee lidstaten die de richtlijn nog niet hebben omgezet (Oostenrijk en Zweden) volgens het Hof van Justitie in gebreke gebleven omdat zij hun verplichtingen op grond van het EU recht niet zijn nagekomen[102]. In april 2011 heeft de Commissie besloten Zweden opnieuw voor het Hof te dagen wegens het niet uitvoeren van het arrest in zaak C-185/09, waarbij zij op grond van artikel 260 van het Verdrag betreffende de werking van de Europese Unie financiële sancties eist, omdat het Zweedse parlement heeft besloten de goedkeuring van de omzettingswetgeving met twaalf maanden uit te stellen. De

---

100 Arrest van het Tsjechische constitutionele hof van 22 maart over wet nr. 127/2005 en decreet nr. 485/2005, zie met name de punten 45-48, 50-51 en 56.

101 Beslissing nr. 13627 van het hoogste Bulgaarse administratieve hof van 11 december 2008; zaken nrs. 65/2009, 78/2009, 82/2009 en 15/2010-22/2010 van het hoogste hof van Cyprus, 1 februari 2011; de constitutionele klacht werd op 2 juni 2008 ingediend door de Hongaarse unie voor burgerlijke vrijheden.

102 Respectievelijk zaak C-189/09 en C-185/09.

Commissie blijft de situatie in Oostenrijk, dat een tijdschema heeft ingediend voor de goedkeuring van de omzettingswetgeving, nauwlettend volgen.

5. DE ROL VAN BEWAARDE GEGEVENS IN HET STRAFRECHT EN DE RECHTSHANDHAVING

In dit punt wordt beschreven welke functie bewaarde gegevens hebben volgens de bijdragen van de lidstaten aan de evaluatie.

5.1. Hoeveelheid bewaarde gegevens waartoe de bevoegde nationale autoriteiten toegang hebben gehad

Zowel de omvang van het telecommunicatieverkeer als het aantal verzoeken om toegang tot verkeersgegevens neemt toe. Uit de statistieken die 19 lidstaten hebben verstrekt over 2008 en/of 2009 blijkt dat in de EU als geheel ruim twee miljoen toegangsverzoeken per jaar werden ingediend, waarbij de aantallen tussen de lidstaten variëren van minder dan 100 per jaar (Cyprus) tot ruim één miljoen (Polen). Volgens de informatie die twaalf lidstaten over 2008 en/of 2009 hebben verstrekt over het soort gegevens dat werd opgevraagd, werden het vaakst gegevens over mobiele telefonie opgevraagd (zie de tabellen 5, 8 en 12). Uit de statistieken kan niet worden afgeleid voor welk doel de gegevens precies werden opgevraagd. Tsjechië, Letland en Polen hebben verklaard dat de bevoegde autoriteiten in het geval van mobieletelefoniegegevens bij elke grote exploitant hetzelfde verzoek moesten indienen, en dat het werkelijke aantal verzoeken dus aanzienlijk lager lag dan de statistieken deden vermoeden.

Er is geen duidelijke verklaring voor het verschil in cijfers, hoewel bevolkingsomvang, criminaliteitstrends, doelbinding, toegangsvoorwaarden en kosten van het verkrijgen van gegevens allemaal factoren zijn die een rol spelen.

5.2. Ouderdom van de bewaarde gegevens waartoe toegang is verleend

Uit de statistische indeling die negen lidstaten[103] hebben verstrekt voor 2008 (zie overzicht in tabel 5 en verdere uitwerking in de bijlage) blijkt dat de rechtshandhavingsautoriteiten bij ongeveer negentig procent van de opgevraagde gegevens na zes maanden of eerder en bij ongeveer zeventig procent na drie maanden of eerder (voor het eerst) om toegang hebben verzocht.

Tabel 5: Ouderdom van de bewaarde gegevens waartoe toegang is verleend in de negen lidstaten die een indeling naar soort gegevens hebben verstrekt voor 2008

Ouderdom	*Vaste telefonie*	*Mobiele telefonie*	*Internetgegevens*	*Totaal*
Minder dan 3 maanden	61%	70%	56%	67%
3 - 6 maanden	28%	18%	19%	19%
6 - 12 maanden	8%	11%	18%	12%
Meer dan 1 jaar	3%	1%	7%	2%

[103] Tsjechië, Denemarken, Estland, Ierland, Spanje, Cyprus, Letland, Malta, Verenigd Koninkrijk.

Volgens de meeste lidstaten worden gegevens die langer dan drie of zes maanden zijn bewaard, minder vaak gebruikt maar kunnen zij wel cruciaal zijn, en is het gebruik ervan in drie categorieën onder te brengen. Ten eerste worden internetgegevens in een strafrechtelijk onderzoek doorgaans later opgevraagd dan andere vormen van bewijs. De analyse van vaste- en mobieletelefoniegegevens levert vaak aanwijzingen op die ertoe leiden dat ook oudere gegevens worden opgevraagd. Zo kan het voorkomen dat onderzoekers een naam hebben gevonden op basis van vaste- of mobieletelefoniegegevens en vervolgens willen nagaan welk IP-adres de betrokkene heeft gebruikt en met wie hij gedurende een bepaalde periode via dat IP-adres contact heeft gehad. In een dergelijk geval ligt het voor de hand dat onderzoekers gegevens opvragen waarmee zij ook kunnen nagaan met welke andere IP-adressen er contact is geweest en de identiteit van de betrokken gebruikers kunnen vaststellen.

Ten tweede wordt bij onderzoeken naar bijzonder ernstige strafbare feiten, een reeks strafbare feiten, georganiseerde criminaliteit en terroristische incidenten vaak gebruikgemaakt van oudere gegevens waaruit kan worden afgeleid hoeveel tijd is besteed aan de voorbereiding van de feiten, zodat criminele gedragspatronen en relaties tussen medeplichtigen in kaart kunnen worden gebracht en opzet kan worden vastgesteld. Activiteiten die verband houden met gecompliceerde financiële strafbare feiten worden vaak pas na een aantal maanden ontdekt. Ten derde vragen de lidstaten bij hoge uitzondering verkeersgegevens op die in een andere lidstaat worden bewaard, waar deze gegevens pas kunnen worden vrijgegeven nadat de rechter daarvoor toestemming heeft gegeven in antwoord op een rogatoire commissie van de rechter in de verzoekende lidstaat. Deze vorm van wederzijdse rechtshulp kan veel tijd in beslag nemen, wat verklaart waarom sommige van de opgevraagde gegevens in deze gevallen ouder zijn dan zes maanden.

5.3. Grensoverschrijdende verzoeken om bewaarde gegevens

Onderzoek en vervolging van strafbare feiten kunnen betrekking hebben op bewijzen of getuigen uit of gebeurtenissen in meer dan één lidstaat. De statistieken die de lidstaten hebben verstrekt, wijzen uit dat minder dan 1% van de verzoeken om toegang betrekking had op gegevens die in een andere lidstaat werden bewaard. Rechtshandhavingsautoriteiten vragen liever gegevens op bij binnenlandse exploitanten, die de relevante gegevens misschien hebben opgeslagen, dan dat zij een tijdrovende procedure voor wederzijdse rechtshulp beginnen die geen enkele garantie biedt dat de gevraagde toegang wordt verleend. Kaderbesluit 2006/960/JBZ van de Raad betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten[104], waarin termijnen zijn vastgesteld voor het verstrekken van informatie na een verzoek van een andere lidstaat, is niet van toepassing, omdat bewaarde gegevens worden beschouwd als informatie die is verkregen met dwangmaatregelen, en die valt buiten de werkingssfeer van het instrument. Toch heeft geen enkele lidstaat of rechtshandhavingsautoriteit erop aangedrongen de grensoverschrijdende uitwisseling van deze gegevens verder te vereenvoudigen.

---

104 Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie (PB L 386 van 29.12.2006, blz. 89 en PB L 200 van 1.8.2007, blz. 637).

5.4. Waarde van bewaarde gegevens voor het onderzoek en de vervolging van strafbare feiten

Weliswaar zegt het aantal verzoeken om toegang tot gegevens op zichzelf niets over de waarde van die gegevens in de afzonderlijke strafrechtelijke onderzoeken, maar de lidstaten vinden gegevensbewaring in het algemeen op zijn minst waardevol en in sommige gevallen onmisbaar[105] voor het voorkomen en bestrijden van criminaliteit, de bescherming van slachtoffers en de vrijspraak van onschuldige personen in strafprocedures. Voor veroordelingen zijn bekentenissen, getuigenverklaringen of forensisch bewijs nodig. Met behulp van bewaarde gegevens konden getuigen worden opgespoord die anders onbekend zouden zijn gebleven, en konden bewijzen van of aanwijzingen voor medeplichtigheid aan een strafbaar feit worden geleverd. Sommige lidstaten[106] beweerden ook dat dankzij bewaarde gegevens de onschuld van verdachten van strafbare feiten kon worden bewezen zonder dat gebruik hoefde te worden gemaakt van andere methoden, zoals interceptie en huiszoeking, die als een grotere inbreuk zouden kunnen worden ervaren.

Er bestaat geen algemene definitie van "ernstige criminaliteit" in de EU en er zijn dus ook geen EU-statistieken over de mate waarin ernstige criminaliteit voorkomt of over onderzoeken of vervolgingen van ernstige strafbare feiten, hoewel er regelmatig gegevens over criminaliteit en justitie worden gepubliceerd. In totaal werden door de 19 lidstaten die gegevens over 2009 en/of 2008 hebben verstrekt, 2,6 miljoen verzoeken om toegang tot bewaarde gegevens gemeld. Afgezet tegen de meest recente criminaliteits- en strafrechtstatistieken voor deze 19 lidstaten – die betrekking hebben op alle vormen van criminaliteit, niet alleen de ernstige – blijken er iets meer dan twee verzoeken per politieagent per jaar te zijn geweest, of ongeveer elf verzoeken per 100 geregistreerde strafbare feiten[107].

Op basis van de statistieken en voorbeelden van de lidstaten waarin een verband wordt gelegd tussen het gebruik van bewaarde communicatiegegevens en het aantal veroordelingen, vrijspraken, geseponeerde zaken en voorkomen strafbare feiten, kunnen een paar conclusies worden getrokken over de rol en de waarde van bewaarde gegevens in strafrechtelijk onderzoek.

Sporen van bewijs volgen

In de eerste plaats kunnen aan de hand van bewaarde gegevens sporen van bewijs worden gevolgd die naar een strafbaar feit leiden. De gegevens worden gebruikt om de activiteiten en verbanden tussen verdachten in kaart te brengen of andere vormen van bewijs daarvan te bevestigen. Met name locatiegegevens zijn zowel door rechtshandhavingsautoriteiten als door

---

105 Tsjechië vond gegevensbewaring "absoluut onmisbaar in veel gevallen", Hongarije omschreef het als "onmisbaar voor de activiteiten van rechtshandhavingsautoriteiten", Slovenië stelde dat het ontbreken van bewaarde gegevens "de werking van rechtshandhavinginstanties zou verlammen", en een politiedienst uit het Verenigd Koninkrijk beschreef de beschikbaarheid van verkeersgegevens als "absoluut cruciaal voor het onderzoek naar de dreiging van terrorisme en ernstige criminaliteit".

106 Duitsland, Polen, Slovenië, Verenigd Koninkrijk.

107 In 2007 waren er in de EU-27 1,7 miljoen politieagenten, onder wie 1,2 miljoen uit de 19 lidstaten die statistieken hebben verstrekt over verzoeken om bewaarde gegevens; In 2007 werden door de politie 29,2 miljoen strafbare feiten geregistreerd, waarvan 24 miljoen in de 19 lidstaten die statistieken hebben verstrekt (bron: Eurostat 2009).

verdachten gebruikt om aan te tonen dat verdachten niet op de plaats delict aanwezig waren en om alibi's te controleren. Met dit soort bewijs kunnen mensen dus verder buiten een strafrechtelijk onderzoek worden gehouden, zonder dat andere, meer ingrijpende onderzoeksmethoden hoeven te worden gebruikt, of kunnen zij in een rechtszaak worden vrijgesproken. België noemt de veroordeling in 2008 van de daders van de tigerkidnapping van een ambtenaar van de correctionele rechtbank in Antwerpen, waarbij de locatiegegevens die een verband lieten zien tussen de activiteiten van de daders in drie verschillende steden, doorslaggevend waren voor het oordeel van de jury. In een ander geval, een moord in 2007 waarbij een motorbende was betrokken, bewezen de locatiegegevens van de mobiele telefoons van de daders dat zij in de buurt waren toen de moord werd gepleegd, wat tot een gedeeltelijke bekentenis leidde[108]. België, Ierland en het Verenigd Koninkrijk zijn van mening dat bepaalde strafbare feiten, waarbij wordt gecommuniceerd via internet, *uitsluitend* met behulp van gegevensbewaring kunnen worden onderzocht: een bedreiging met geweld die in een chatroom wordt geuit, laat bijvoorbeeld geen enkel ander spoor na dan de verkeersgegevens in cyberspace. Hetzelfde geldt voor strafbare feiten die per telefoon worden gepleegd. Hongarije en Polen beschrijven een geval van telefonische oplichting van ouderen, eind 2009/begin 2010, waarbij de daders zich voordeden als familieleden die geld nodig hadden en alleen konden worden geïdentificeerd aan de hand van de bewaarde telefoongegevens.

Een strafrechtelijk onderzoek instellen

In de tweede plaats hebben zich gevallen voorgedaan waarin, bij gebrek aan forensisch bewijs of ooggetuigen, alleen op basis van bewaarde gegevens een strafrechtelijk onderzoek kon worden ingesteld. Duitsland noemde de moord op een politieagent, waarbij de aanvaller was ontkomen in de auto van het slachtoffer en die later ergens had achtergelaten. Er kon worden vastgesteld dat hij vervolgens telefonisch een ander vervoermiddel had gezocht. Er waren geen ooggetuigen en er was geen forensisch bewijs van de identiteit van de moordenaar, dus de autoriteiten waren afhankelijk van de beschikbaarheid van deze verkeersgegevens om het onderzoek uit te voeren. In gevallen van seksueel misbruik van kinderen met behulp van internet zijn bewaarde gegevens onmisbaar gebleken voor succesvol onderzoek. Samen met andere onderzoekstechnieken maken bewaarde gegevens het mogelijk om de identiteit vast te stellen van afnemers van kinderpornografie[109], en slachtoffers te identificeren en te redden. Tsjechië meldt dat het in het kader van "operatie Vilma" zonder toegang tot bewaarde internetgegevens geen onderzoek zou kunnen hebben ingesteld naar een netwerk van gebruikers en verspreiders van kinderporno. Op EU-niveau konden in het kader van "Operation Rescue" (waarbij werd samengewerkt met Europol) kinderen soms niet goed worden beschermd tegen misbruik, omdat sommige lidstaten wegens het ontbreken van gegevensbewaringswetgeving geen onderzoek konden doen naar leden van een groot internationaal pedofielennetwerk door gebruik te maken van bepaalde IP-adressen, die soms een jaar oud waren.

---

108 National Policing Improvement Agency (Verenigd Koninkrijk), *The Journal of Homicide and Major Incident Investigation*, deel 5, nr. 1, voorjaar 2009, blz. 39-51.

109 Het project "Measurement and analysis of p2p activity against paedophile content", dat werd gefinancierd in het kader van het programma Veiliger internet, heeft nauwkeurige informatie opgeleverd over pedofiele activiteiten in het eDonkey peer-to-peer systeem, waardoor 178 000 gebruikers konden worden geïdentificeerd die kinderporno vroegen (van de 89 miljoen gebruikers die werden gescreend).

In onderzoeken naar cybercriminaliteit is een IP-adres vaak het eerste aanknopingspunt. Aan de hand van verkeersgegevens kan de identiteit van de abonnee van het IP-adres worden vastgesteld voordat wordt besloten of er een strafrechtelijk onderzoek kan worden ingesteld. Ook biedt het de politie de mogelijkheid potentiële slachtoffers van een cyberaanval te waarschuwen: wanneer de politie erin slaagt een command-and-control server in beslag te nemen die door botnet-operators wordt gebruikt, kan zij alleen zien welke IP-adressen bij die server horen, terwijl zij aan de hand van bewaarde gegevens ook de potentiële slachtoffers kan identificeren en waarschuwen die zich van de betrokken IP-adressen bedienen.

Bewaarde gegevens zijn een vast onderdeel van strafrechtelijk onderzoek

Ten derde is het zo dat, hoewel rechtshandhavingsautoriteiten en rechterlijke instanties in de meeste lidstaten geen statistieken bijhouden over welk soort bewijs doorslaggevend is bij veroordelingen of gevallen van vrijspraak, het gebruik van bewaarde gegevens een vast onderdeel is van strafrechtelijk onderzoek en strafrechtelijke vervolging in de EU. Sommige lidstaten verklaarden dat zij niet altijd het belang van de bewaarde gegevens voor het onderzoek en de vervolging konden vaststellen, omdat rechterlijke instanties al het ingediende bewijsmateriaal meewegen en slechts zelden van oordeel zijn dat één bepaald bewijsstuk de doorslag heeft gegeven[110]. Nederland heeft meegedeeld dat historische verkeersgegevens tussen januari en juli 2010 een beslissende rol hebben gespeeld in 24 vonnissen. In Finland bleken de bewaarde gegevens in 56% van de 3405 verzoeken "belangrijk" of "essentieel" te zijn voor de opsporing en/of vervolging van strafbare feiten. Het Verenigd Koninkrijk heeft gegevens verstrekt die het effect van gegevensbewaring op strafvervolging kwantificeren: voor drie van zijn rechtshandhavingsinstanties waren bewaarde gegevens nodig in de meeste, zo niet alle onderzoeken die leidden tot strafvervolging of een veroordeling.

5.5. Technologische ontwikkelingen en het gebruik van vooruitbetaalde simkaarten

Rechtshandhavingsautoriteiten moeten de technologische ontwikkelingen volgen die worden gebruikt voor het plegen van strafbare feiten of het helpen daarbij. Gegevensbewaring is een van de onderzoeksinstrumenten die de rechtshandhavingsautoriteiten nodig hebben om de hedendaagse diverse, grootschalige en snelle vormen van criminaliteit op een beheersbare en doelmatige manier aan te pakken. Een aantal steeds vaker gebruikte vormen van communicatie vallen buiten de werkingssfeer van de richtlijn. Via virtuele particuliere netwerken (VPN) van bijvoorbeeld universiteiten of grote ondernemingen hebben verschillende gebruikers toegang tot internet via een enkel toegangspunt met een enkel IP-adres. Nieuwe technologische ontwikkelingen maken het nu echter mogelijk adressen aan afzonderlijke VPN-gebruikers te koppelen.

Het percentage gebruikers van mobiele telefoons dat gebruikmaakt van vooruitbetaalde diensten verschilt per lidstaat. Sommige lidstaten stellen dat anonieme vooruitbetaalde simkaarten, vooral wanneer die in een andere lidstaat worden gekocht, ook door criminelen kunnen worden gebruikt om identificatie in een strafrechtelijk onderzoek te voorkomen[111]. Zes lidstaten (Denemarken, Spanje, Italië, Griekenland, Slowakije en Bulgarije) hebben de registratie van vooruitbetaalde simkaarten verplicht gesteld. Deze en andere lidstaten (Polen,

---

110 België, Tsjechië, Litouwen.

111 Conclusies van de Raad betreffende de bestrijding van het anoniem en voor criminele doeleinden gebruiken van elektronische communicatie.

Cyprus, Litouwen) hebben gepleit voor een EU-maatregel voor de verplichte registratie van de identiteit van gebruikers van vooruitbetaalde diensten. De efficiëntie van deze nationale maatregelen is niet aangetoond. Er is gewezen op mogelijke beperkingen, zoals bij identiteitsdiefstal of wanneer een simkaart door een derde wordt gekocht of een gebruiker roamt met een kaart die in een derde land is gekocht. Al met al is de Commissie er niet van overtuigd dat er in dit stadium maatregelen op EU-niveau moeten worden genomen op dit gebied.

6. GEVOLGEN VAN GEGEVENSBEWARING VOOR EXPLOITANTEN EN CONSUMENTEN

6.1. Exploitanten en consumenten

In een gezamenlijke verklaring aan de Commissie hebben vijf grote bedrijfsorganisaties de economische gevolgen van de richtlijn "substantieel" of "enorm" genoemd voor "kleinere aanbieders van diensten", omdat de richtlijn "veel speelruimte" biedt[112]. Acht exploitanten hebben zeer uiteenlopende ramingen opgesteld van de operationele en kapitaaluitgaven die moeten worden gedaan om aan de richtlijn te voldoen. Deze ramingen worden wellicht bevestigd door de vergoedingen van kosten van exploitanten die vier van de lidstaten hebben meegedeeld (zie tabel 6).

In een studie die werd verricht voordat de richtlijn in de meeste lidstaten was omgezet, werden de kosten van het opzetten van een systeem voor het bewaren van gegevens voor een internetaanbieder met een half miljoen klanten geraamd op ongeveer 375 240 euro in het eerste jaar en vervolgens 9 870 euro aan operationele kosten per maand[113]; de kosten van het opzetten van een systeem voor het opzoeken van gegevens werden geraamd op 131 190 euro, met operationele kosten van 28 960 euro per maand. Het Duitse constitutionele hof achtte in zijn arrest van 2 maart 2010 echter de verplichting om gegevens op te slaan geen buitensporige belasting voor de dienstenaanbieders en ook niet onevenredig wat betreft de financiële lasten die voor de ondernemingen voortvloeien uit de opslagverplichting[114]. De kosten per eenheid van gegevensbewaring zijn omgekeerd evenredig met de omvang van de exploitant en de mate waarin de interactie met exploitanten in een lidstaat is gestandaardiseerd[115].

De meeste exploitanten konden in hun antwoord op de vragenlijst van de Commissie de gevolgen van de richtlijn voor de concurrentie, de prijzen voor de consument of de investeringen in nieuwe infrastructuur en diensten niet kwantificeren.

Er zijn geen bewijzen van een kwantificeerbaar of substantieel effect van de richtlijn op de consumentenprijzen van elektronische communicatiediensten; er waren geen bijdragen van consumentenorganisaties aan de openbare raadpleging van 2009. Een enquête die in Duitsland is gehouden namens een maatschappelijke organisatie heeft uitgewezen dat consumenten voornemens waren hun communicatiegedrag te wijzigen en het gebruik van elektronische communicatiediensten in sommige omstandigheden vermijden, hoewel er geen ondersteunend

---

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 Wilfried Gansterer & Michael Ilger, Data Retention – The EU Directive 2006/24/EC from a Technological Perspective, Wenen, Verlag Medien und Recht, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 van 2 maart 2010, punt 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

bewijs is dat er in een van de lidstaten of in de EU als geheel een gedragsverandering heeft plaatsgevonden[116].

De Commissie is voornemens na te gaan wat het effect van toekomstige wijzigingen van de richtlijn op de sector en consumenten zal zijn. Zo zou onder meer door middel van een specifieke Eurobarometer-enquête kunnen worden geïnventariseerd hoe het publiek tegenover de wijzigingen staat.

6.2. Vergoeding van kosten

De vergoeding van de kosten die exploitanten moeten maken als gevolg van de verplichting om gegevens te bewaren, wordt niet door de richtlijn geregeld. Het gaat om de volgende kosten:

(e) *operationele uitgaven*, d.w.z. werkingskosten of vaste uitgaven die verband houden met de werking van de onderneming, een apparaat, een component, een onderdeel van de apparatuur of de inrichting; en

(f) *kapitaaluitgaven*, d.w.z. uitgaven die in de toekomst winst opleveren, of de kosten van het ontwikkelen of aanbieden van niet-consumeerbare delen van het product of systeem, zoals de kosten van personeel en uitgaven voor gebouwen, zoals huur en nutsvoorzieningen.

Alle lidstaten kennen een of andere vorm van vergoeding indien de gegevens worden opgevraagd in het kader van een strafprocedure. Twee lidstaten melden dat zij zowel operationele als kapitaaluitgaven vergoeden. Zes lidstaten vergoeden alleen operationele uitgaven. Andere vergoedingsregelingen zijn niet aan de Commissie meegedeeld. Tabel 6 geeft een gedetailleerd overzicht.

Tabel 6: Lidstaten die kosten vergoeden

Lidstaat	Operationele uitgaven	Kapitaaluitgaven	Jaarlijks vergoede kosten (in miljoen euro)
België	Ja	Nee	22 (2008)
Bulgarije	Nee	Nee	-
Tsjechië	Richtlijn niet omgezet[117]		
Denemarken	Ja	Nee	-
Duitsland	Richtlijn niet omgezet		
Estland	Ja	Nee	-
Ierland	Nee	Nee	-
Griekenland	Nee	Nee	-
Spanje	Nee	Nee	-
Frankrijk	Ja	Nee	-
Italië	-	-	-
Cyprus	Nee	Nee	-

[116] De enquête werd verricht door Forsa in opdracht van AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

[117] Voordat de omzettingswetgeving nietig werd verklaard, werden in Tsjechië zowel operationele als kapitaaluitgaven vergoed. In 2009 ging het om 6,8 miljoen euro.

Letland	Nee	Nee	-
Litouwen	Ja, na gemotiveerd verzoek	Nee	-
Luxemburg	Nee	Nee	-
Hongarije	Nee	Nee	-
Malta	Nee	Nee	-
Nederland	Ja	Nee	-
Oostenrijk	Richtlijn niet omgezet		
Polen	Nee	Nee	-
Portugal	Nee	Nee	-
Roemenië	Richtlijn niet omgezet		
Slovenië	Nee	Nee	-
Slowakije	Nee	Nee	-
Finland	Ja	Ja	1
Zweden	Richtlijn niet omgezet		
Verenigd Koninkrijk	Ja	Ja	55 (totaal over drie jaar)

Uit het bovenstaande kan worden geconcludeerd dat het doel van de richtlijn om gelijke voorwaarden te scheppen voor alle exploitanten in de EU, niet volledig is verwezenlijkt. De Commissie zal nagaan welke mogelijkheden er zijn om de belemmeringen voor de werking van de interne markt tot een minimum te beperken door ervoor te zorgen dat exploitanten de kosten die zij maken om aan de gegevensbewaringsverplichting te voldoen, overal op dezelfde manier vergoed krijgen; zij zal daarbij in het bijzonder aandacht besteden aan kleine en middelgrote exploitanten.

7. GEVOLGEN VAN GEGEVENSBEWARING VOOR DE GRONDRECHTEN

7.1. Het fundamentele recht op privacy en bescherming van persoonsgegevens

Gegevensbewaring is een inperking van het recht op de eerbiediging van het privéleven en de bescherming van persoonsgegevens, twee grondrechten in de EU[118]. Overeenkomstig artikel 52, lid 1, van het Handvest van de grondrechten moeten dergelijke beperkingen bij wet worden geregeld en de wezenlijke inhoud van die rechten eerbiedigen, stroken met het evenredigheidsbeginsel, noodzakelijk zijn en beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen. In de praktijk betekent dit dat elke beperking[119]:

(g) nauwkeurig en voorspelbaar moet worden geformuleerd;

(h) noodzakelijk zijn om een doelstelling van algemeen belang te bereiken of om de rechten en vrijheden van anderen te beschermen;

---

118 Artikel 7 en artikel 8 van het Handvest van de grondrechten van de Europese Unie (PB C 83 van 30.3.2010, blz. 389) garanderen eenieder het recht op "bescherming van zijn persoonsgegevens". Artikel 16 van het Verdrag betreffende de werking van de Europese Unie (PB C 83 van 30.3.2010, blz. 1) garandeert eveneens eenieder het recht op "bescherming van zijn persoonsgegevens".

119 Zie de checklist in verband met de grondrechten die de Commissie hanteert voor alle wetgevingsvoorstellen in de mededeling COM(2010) 573 "Strategie voor een doeltreffende tenuitvoerlegging van het Handvest van de grondrechten door de Europese Unie".

(i) evenredig moet zijn met de beoogde doelstelling; en

(j) de wezenlijke inhoud van de betrokken grondrechten moet eerbiedigen.

Artikel 8, lid 2, van het Europees Verdrag voor de rechten van de mens bepaalt ook dat inmenging van het openbaar gezag in het recht op eerbiediging van het privéleven is toegestaan indien dit noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het voorkomen van strafbare feiten[120]. In artikel 15, lid 1, van de e-privacyrichtlijn en de overwegingen van de gegevensbewaringsrichtlijn worden deze beginselen herhaald als uitgangspunten van het EU-beleid op het gebied van gegevensbewaring.

In de jurisprudentie van het Europese Hof van Justitie en het Europees Hof voor de rechten van de mens zijn de voorwaarden voor elke vorm van beperking van het recht op eerbiediging van het privéleven nader uitgewerkt. Deze arresten bepalen mede of de richtlijn moet worden aangepast, met name als het gaat om de voorwaarden voor toegang en gebruik van bewaarde gegevens.

Elke beperking van het recht op eerbiediging van het privéleven moet nauwkeurig worden geformuleerd en een voorspelbare uitwerking hebben

In zaak van de Österreichischer Rundfunk oordeelde het Europese Hof van Justitie dat elke wettelijke inmenging in het recht op eerbiediging van het privéleven, om te voldoen aan het vereiste van voorzienbaarheid, voldoende nauwkeurig moet zijn geformuleerd, opdat de burger zijn gedrag kan bepalen.

Elke beperking van het recht op eerbiediging van het privéleven moet noodzakelijk zijn en bepaalde minimumwaarborgen bieden

In de zaak Copland tegen het Verenigd Koninkrijk, die betrekking had op het toezicht van de overheid op privételefoongesprekken, –e-mails en –internetgebruik, bepaalde het Europese Hof voor de rechten van de mens dat een dergelijke beperking van het recht op eerbiediging van het privéleven alleen als noodzakelijk kon worden beschouwd als zij was gebaseerd op de nationale wetgeving ter zake[121]. In S. en Marper tegen het Verenigd Koninkrijk, een zaak die betrekking had op het bewaren van DNA-profielen of vingerafdrukken van personen die zijn vrijgesproken van een strafbaar feit of wier zaak is geseponeerd voordat het tot een veroordeling kwam, oordeelde het Hof dat een dergelijke beperking van het recht op eerbiediging van het privéleven alleen is toegestaan als zij beantwoordt aan een dwingende maatschappelijke behoefte, als zij evenredig is aan het beoogde doel, en als het openbaar gezag er relevante en voldoende redenen voor aanvoert[122]. De kernbeginselen van gegevensbescherming vereisen dat het bewaren van gegevens evenredig is met het doel waarvoor de gegevens worden verzameld, en dat de bewaringstermijn beperkt is[123]. Voor het afluisteren van telefoongesprekken, onopvallend toezicht en het heimelijk verzamelen van

---

120 Artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (ETS nr. 5) van de Raad van Europa van 4.11.1950.

121 Copland tegen het Verenigd Koninkrijk, arrest van het Europees Hof voor de rechten van de mens, Straatsburg, 3.4.2007, blz. 9.

122 Marper tegen het Verenigd Koninkrijk, arrest van het Europees Hof voor de rechten van de mens, Straatsburg, 4.12.200, blz. 31.

123 Marper, blz. 30.

inlichtingen moeten duidelijke, gedetailleerde regels voor de werkingssfeer en de toepassing van de maatregelen gelden, met minimumwaarborgen voor onder andere de duur, de opslag, het gebruik, de toegang van derden, de procedures voor het bewaken van de integriteit en de vertrouwelijkheid van de gegevens en de procedures voor het vernietigen ervan, zodat er voldoende waarborgen zijn tegen misbruik en willekeurigheid.

Elke beperking van het recht op eerbiediging van het privéleven moet evenredig zijn met het algemeen belang

Het Europese Hof van Justitie heeft eveneens in zijn arrest in de zaak Schecke & Eiffert over de bekendmaking van de begunstigden van landbouwsubsidies op internet[124] geoordeeld dat de EU-wetgever kennelijk onvoldoende maatregelen had genomen om een goed evenwicht tot stand te brengen tussen de eerbiediging van de wezenlijke aspecten van het recht op privacy enerzijds en het algemeen belang (transparantie) anderzijds. Het Hof vond met name dat de wetgevers geen andere vormen van bekendmaking hadden overwogen die in overeenstemming zouden zijn geweest met de doelstelling, maar tegelijkertijd het recht van de begunstigden op eerbiediging van hun privéleven en op de bescherming van hun persoonsgegevens minder aantastten. Dientengevolge oordeelde het Hof dat de wetgevers de door het evenredigheidsbeginsel gestelde grenzen hadden overschreden, omdat "beperkingen van de bescherming van persoonsgegevens binnen de grenzen van het strikt noodzakelijke moeten blijven".

7.2. Kritiek op het beginsel van gegevensbewaring

Een aantal maatschappelijke organisaties heeft de Commissie geschreven omdat zij van mening zijn dat gegevensbewaring in principe een ongerechtvaardigde en onnodige beperking is van het recht op eerbiediging van het privéleven. Zij vinden het ongevraagd, algemeen en ongedifferentieerd bewaren van verkeers-, locatie- en abonneegegevens van personen een onwettige beperking van de grondrechten. Naar aanleiding van een beroep dat door burgerrechtenactivisten in een van de lidstaten (Ierland) is ingesteld voor de nationale rechter, wordt de vraag betreffende de wettigheid van de richtlijn waarschijnlijk naar het Europese Hof van Justitie verwezen[125]. Ook de Europese Toezichthouder voor gegevensbescherming heeft twijfels geuit over de noodzaak van de maatregel.

7.3. De roep om striktere regels voor gegevensbeveiliging en gegevensbescherming

In haar verslag over de tweede handhavingsmaatregel stelde de Groep van artikel 29 dat mogelijke inbreuken op de vertrouwelijkheid van communicatie en op de vrijheid van meningsuiting inherent zijn aan het opslaan van verkeersgegevens. De Groep bekritiseerde sommige aspecten van de toepassing door de lidstaten, zoals gegevensregistratie, bewaringstermijn, de aard van de bewaarde gegevens en de gegevensbeveiligingsmaatregelen. De Groep maakte melding van gevallen waarin informatie over de *inhoud* van internetcommunicatie, een aspect dat geheel buiten de werkingssfeer van de richtlijn valt, werd bewaard, met inbegrip van IP-adressen van bestemming en URL's van websites, de titel

---

124 Zaak C-92/09 Volker en Markus Schecke GbR tegen Land Hessen en zaak C-93/09 Eifert tegen Land Hessen en Bundesanstalt für Landwirtschaft und Ernährung, 9.11.2010.

125 Op 5 mei 2010 heeft het Irish High Court ingestemd met het verzoek van Digital Rights Ireland Limited om het Europese Hof van Justitie om een prejudiciële beslissing te vragen op grond van artikel 267 van het Verdrag betreffende de werking van de Europese Unie.

van e-mails en de lijst van geadresseerden in het "Cc"-vak. De Groep drong er daarom op aan te verduidelijken dat de categorieën gegevens volledig zijn, en dat geen bijkomende bewaringsverplichtingen aan exploitanten mogen worden opgelegd.

De Europese Toezichthouder voor gegevensbescherming heeft verklaard dat de richtlijn niet heeft geleid tot een harmonisatie van de nationale wetgevingen en dat het gebruik van bewaarde gegevens niet strikt beperkt blijft tot de bestrijding van ernstige criminaliteit[126]. Hij was van mening dat een EU-instrument met regels voor verplichte gegevensbewaring, voor het geval de noodzaak ervan is aangetoond, ook regels moet bevatten voor de toegang en het verdere gebruik door rechtshandhavingsautoriteiten. Hij heeft er bij de EU op aangedrongen een algemeen rechtskader vast te stellen dat niet alleen de exploitanten er toe verplicht gegevens te bewaren, maar ook regelt hoe de lidstaten de gegevens voor rechtshandhavingsdoeleinden kunnen gebruiken, zodat de burgers meer rechtszekerheid krijgen.

Gegevensbeschermingsautoriteiten vinden in het algemeen dat gegevensbewaring altijd een gevaar van privacyschending in zich bergt, maar in plaats van dit op EU-niveau te ondervangen, verplicht de richtlijn de lidstaten ervoor te zorgen dat de nationale gegevensbeschermingsregels worden nageleefd. Hoewel er geen concrete gevallen bekend zijn van ernstige privacyschendingen, blijft het gevaar van een tekortschietende gegevensbeveiliging bestaan, en kan dit zelfs toenemen, gezien de technologische ontwikkelingen en de trends in communicatievormen, ongeacht of gegevens worden opgeslagen om commerciële of veiligheidsredenen, binnen of buiten de EU, tenzij verdere waarborgen worden ingebouwd.

8. CONCLUSIES EN AANBEVELINGEN

In dit verslag zijn een aantal sterke en zwakkere punten van de huidige EU-regels voor gegevensbewaring belicht. De EU heeft de richtlijn vastgesteld in een tijd van verhoogde waakzaamheid voor dreigende terreuraanvallen. De effectbeoordeling die de Commissie voornemens is te verrichten biedt de gelegenheid om de gegevensbewaring in de EU te onderwerpen aan een noodzakelijkheids- en evenredigheidstoets, uitgaande van de interne veiligheid, de soepele werking van de interne markt en een betere eerbiediging van de privacy en het fundamentele recht op bescherming van persoonsgegevens. In haar voorstel tot wijziging van het gegevensbewaringskader moet de Commissie rekening houden met de volgende conclusies en aanbevelingen.

8.1. De EU dient gegevensbewaring als veiligheidsmaatregel te bepleiten en er regels voor op te stellen

De meeste lidstaten stellen zich op het standpunt dat EU-regels op het gebied van gegevensbewaring noodzakelijk blijven als instrument voor rechtshandhaving, de bescherming van slachtoffers en de werking van het strafrechtstelsel. De bewijzen die de lidstaten aandragen in de vorm van statistieken en voorbeelden zijn in sommige opzichten beperkt, maar laten niettemin zien hoe belangrijk bewaarde gegevens zijn bij strafrechtelijk onderzoek. Deze gegevens leveren waardevolle aanwijzingen en bewijzen op die ertoe leiden

---

126 Toespraak van Peter Hustinx op de conferentie "Taking on the Data Retention Directive" van 3 december 2010.

dat strafbare feiten kunnen worden voorkomen en vervolgd en dat het strafrecht zijn beloop kan hebben. Dankzij de bewaarde gegevens zijn veroordelingen uitgesproken voor strafbare feiten die zonder deze gegevens misschien nooit zouden zijn opgelost. Ook zijn onschuldige personen vrijgesproken op basis van bewaarde gegevens. Met geharmoniseerde regels op dit gebied wordt gegevensbewaring een doeltreffend instrument voor de bestrijding van criminaliteit, krijgt de sector rechtszekerheid binnen een soepel werkende interne markt en worden de hoge normen voor de eerbiediging van het privéleven en de bescherming van persoonsgegevens overal en altijd toegepast in de EU.

8.2. De richtlijn is op verschillende manieren omgezet

In 22 lidstaten is de richtlijn omgezet in nationaal recht. De grote speelruimte die de lidstaten krachtens artikel 15, lid 1, van de e-privacyrichtlijn genieten bij het vaststellen van maatregelen op het gebied van gegevensbewaring, maakt het bijzonder problematisch om de richtlijn gegevensbewaring te evalueren. Er zijn grote verschillen in de omzettingswetgeving op het gebied van doelbinding, toegang tot gegevens, bewaringstermijnen, gegevensbescherming en gegevensbeveiliging, en statistieken. Drie lidstaten maken inbreuk op de richtlijn sinds hun respectieve constitutionele hoven de nationale wetgeving ter omzetting van de richtlijn nietig hebben verklaard. Twee andere lidstaten moeten de richtlijn nog omzetten. De Commissie zal met alle lidstaten blijven samenwerken om ervoor te zorgen dat de richtlijn goed wordt toegepast. Zij zal tevens blijven toezien op de naleving van het EU-recht en in het uiterste geval zo nodig inbreukprocedures inleiden.

8.3. De richtlijn heeft niet gezorgd voor een volledige harmonisatie van de gegevensbewaringsvoorschriften en niet geleid tot gelijke voorwaarden voor alle exploitanten

De richtlijn heeft ervoor gezorgd dat nu in de meeste lidstaten gegevens worden bewaard. De richtlijn biedt zelf geen garantie dat bij het opslaan, opvragen en gebruiken van de gegevens het recht op eerbiediging van het privéleven en bescherming van persoonsgegevens volledig wordt nageleefd. De verantwoordelijkheid voor het naleven van deze rechten ligt bij de lidstaten. Met de richtlijn werd slechts een gedeeltelijke harmonisatie van de gegevensbewaringsvoorschriften beoogd; het is dan ook niet verwonderlijk dat er geen gemeenschappelijk aanpak is ontstaan, noch ten aanzien van specifieke bepalingen van de lidstaten zoals de doelbinding of bewaringstermijnen, noch ten aanzien van aspecten die buiten de werkingssfeer van de richtlijn vallen, zoals de vergoeding van kosten. Maar buiten de variatie die expliciet door de richtlijn mogelijk wordt gemaakt, hebben de verschillen in de nationale gegevensbewaringsvoorschriften de exploitanten voor grote problemen gesteld.

8.4. Exploitanten dienen overal op dezelfde manier hun kosten vergoed te krijgen

Er is nog steeds een gebrek aan rechtszekerheid in de sector. De verplichting om gegevens te bewaren en terug te zoeken brengt aanzienlijke kosten met zich mee, vooral voor kleinere exploitanten, en de mate waarin exploitanten hun kosten vergoed krijgen, verschilt per lidstaat; er zijn echter geen aanwijzingen dat de telecommunicatiesector als geheel nadelige gevolgen heeft ondervonden van de richtlijn. De Commissie zal zich buigen over een uniforme vergoeding van de kosten voor exploitanten.

8.5. Zorgen voor evenredigheid in het totale traject van opslag, retrieval en gebruik

De Commissie zal ervoor zorgen dat toekomstige voorstellen op het gebied van gegevensbewaring beantwoorden aan het evenredigheidsbeginsel, geschikt zijn voor het verwezenlijken van de doelstelling om ernstige criminaliteit en terrorisme te bestrijden, en niet verder gaan dan nodig is om dat te bereiken. Zij zal uitgaan van het principe dat uitzonderingen of beperkingen ten aanzien van de bescherming van persoonsgegevens alleen van toepassing mogen zijn, indien dat nodig is. Zij zal grondig onderzoeken wat de gevolgen van strengere regels voor de opslag, de toegang het gebruik van verkeersgegevens zullen zijn voor de effectiviteit en de efficiëntie van het strafrechtsysteem en de rechtshandhaving, voor de eerbiediging van het privéleven en voor de kosten voor de overheid en exploitanten. Bij de effectbeoordeling dient in het bijzonder aandacht te worden besteed aan de volgende punten:

(1)consistentie in de afbakening van het doel van gegevensbewaring en de soorten strafbare feiten waarvoor bewaarde gegevens mogen worden opgevraagd en gebruikt;

(2)meer harmonisatie en eventueel verkorting van de termijnen voor verplichte gegevensbewaring;

(3)onafhankelijk toezicht op verzoeken om toegang en op de bewarings- en toegangsvoorschriften in het algemeen die in de lidstaten worden toegepast;

(4)beperking van de autoriteiten die toegang hebben tot de gegevens;

(5)beperking van de categorieën gegevens die moeten worden bewaard;

(6)richtsnoeren voor technische en organisatorische beveiligingsmaatregelen voor de toegang tot gegevens, zoals overdrachtsprocedures;

(7)richtsnoeren voor het gebruik van gegevens, bijvoorbeeld ter voorkoming van datamining; en

(8)ontwikkeling van bruikbare meetmethoden en verslagleggingsprocedures om bij een toekomstig instrument de verschillende toepassingen te kunnen vergelijken en evalueren.

De Commissie zal ook nagaan of en zo ja, hoe, EU-regels voor de bevriezing van gegevens een aanvulling zouden kunnen vormen op de bewaring van gegevens.

Uitgaande van de grondrechtenchecklist en het informatiebeheersbeleid op het gebied van vrijheid, veiligheid en recht[127], zal de Commissie zich over elk van deze punten buigen met inachtneming van het evenredigheidsbeginsel en het voorzienbaarheidsvereiste. Zij zal daarbij ook de consistentie met de lopende herziening van het EU-gegevensbeschermingskader in het oog houden[128].

---

127 Zie verwijzing naar de mededeling over de toepassing van het Handvest van de grondrechten, "Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht (COM(2010) 385) van 20.7.2010.

128 COM(2010) 609 van 4.11.2010.

8.6. Volgende stappen

Op basis van deze evaluatie zal de Commissie een herziening van de huidige regels voor gegevensbewaring voorstellen. Zij zal in overleg met rechtshandhavingsautoriteiten, justitie, de telecommunicatiesector en consumentenorganisaties, gegevensbeschermingsautoriteiten en maatschappelijke organisaties een aantal opties formuleren. Zij zal verder onderzoek doen naar de publieke perceptie van gegevensbewaring en de weerslag ervan op het gedrag van de burgers. Deze bevindingen zullen worden verwerkt in een effectbeoordeling van de diverse beleidsopties, die als basis zal dienen voor het voorstel van de Commissie.

Bijlage: Bijkomende statistieken over het bewaren van verkeersgegevens

Opmerkingen betreffende de bijlage:

1. Met "ouderdom van gegevens" wordt de tijd bedoeld die is verstreken tussen de datum waarop de gegevens zijn opgeslagen en de datum waarop de bevoegde autoriteiten de gegevens hebben opgevraagd.

2. Internetgegevens zijn gegevens betreffende de toegang tot internet, e-mail via internet en internettelefonie.

3. Statistieken voor Tsjechië, Letland en Polen onder voorbehoud (zie punt 5.1).

Door de lidstaten verstrekte statistieken over 2008

Tabel 7: Verzoeken om bewaarde verkeersgegevens naar ouderdom in 2008									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	102691	18440	10110	319	0	0	0	0	131560
Denemarken	2669	672	185	37	23	2	7	4	3599
Duitsland	9363	2336	985	0	0	0	0	0	12684
Estland	2773	733	157	827	0	0	0	0	4490
Ierland	8981	2016	936	1855	90	85	78	54	14095
Griekenland	Geen indeling naar ouderdom verstrekt								584
Spanje	22629	15868	10298	4783	0	0	0	0	53578
Frankrijk	Geen indeling naar ouderdom verstrekt								503437
Italië	Geen gegevens verstrekt								
Cyprus	30	4	0	0	0	0	0	0	34
Letland	10539	2739	1368	1211	597	438	0	0	16892
Litouwen	55735	23817	5251	512	0	0	0	0	85315
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	810	59	0	0	0	0	0	0	869
Nederland	Geen indeling naar ouderdom verstrekt								85000
Oostenrijk	Geen indeling naar ouderdom verstrekt								3093
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen indeling naar ouderdom verstrekt								2821
Slowakije	Geen gegevens verstrekt								
Finland	9134	1144	448	214	268				4008
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	315350	88339	34665	19398	6385	2973	1536	1576	470222
Total	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Exclusief Finland

Tabel 8: Verzoeken om bewaarde verkeersgegevens naar soort gegeven in 2008 (tussen haakjes het aantal gevallen waarin niet kon worden ingegaan op het verzoek – indien verstrekt)				
Soort gegevens/ lidstaat	**Telefonie via vast netwerk**	**Mobiele telefonie**	**Internetgegevens**	**Totaal**
België	Geen gegevens verstrekt			
Bulgarije	Geen gegevens verstrekt			
Tsjechië	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Denemarken	192 (0)	3273 (5)	134 (0)	3599 (5)
Duitsland	Geen indeling naar soort gegeven verstrekt			12684 (931)
Estland	4114 (1519)	376 (7)	Geen gegevens verstrekt	4490 (1526)
Ierland	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Griekenland	Geen indeling naar soort gegeven verstrekt			584
Spanje	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Frankrijk	Geen indeling naar soort gegeven verstrekt			503437
Italië	Geen gegevens verstrekt			
Cyprus	3 (0)	31 (5)	0 (0)	34 (5)
Letland	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Litouwen	765 (72)	84550 (5657)	Geen gegevens verstrekt	85315 (5729)
Luxemburg	Geen gegevens verstrekt			
Hongarije	Geen gegevens verstrekt			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Nederland	Geen indeling naar soort gegeven verstrekt			85000
Oostenrijk	Geen indeling naar soort gegeven verstrekt			3093
Polen	Geen gegevens verstrekt			
Portugal	Geen gegevens verstrekt			
Roemenië	Geen gegevens verstrekt			
Slovenië	Geen indeling naar soort gegeven verstrekt			2821
Slowakije	Geen gegevens verstrekt			
Finland	Geen indeling naar soort gegeven verstrekt			4008
Zweden	Geen gegevens verstrekt			
Verenigd Koninkrijk	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Totaal				1392281

Tabel 9: Verzoeken om bewaarde verkeersgegevens betreffende *telefonie via een vast netwerk*, naar ouderdom, 2008									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	3669	916	143	124	0	0	0	0	4852
Denemarken	133	28	31	0	0	0	0	0	192
Duitsland	Geen gegevens verstrekt								
Estland	1876	161	74	484	0	0	0	0	2595
Ierland	4118	712	197	182	32	21	23	16	5301
Griekenland	Geen gegevens verstrekt								
Spanje	1948	1431	741	328	0	0	0	0	4448
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	3	0	0	0	0	0	0	0	3
Letland	698	213	167	193	104	137	0	0	1512
Litouwen	251	442	0	0	0	0	0	0	693
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	28	1	0	0	0	0	0	0	29
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	54805	27052	5340	753	1135	437	1050	175	90747
Totaal	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Tabel 10: Verzoeken om bewaarde verkeersgegevens betreffende *mobiele telefonie*, naar ouderdom, 2008									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	98232	17013	7518	1	0	0	0	0	122764
Denemarken	2433	628	143	33	20	1	7	3	3268
Duitsland	Geen gegevens verstrekt								
Estland	248	58	35	28	0	0	0	0	369
Ierland	4326	820	230	240	57	63	52	37	5825
Griekenland	Geen gegevens verstrekt								
Spanje	17403	12114	7444	3052	0	0	0	0	40013
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	23	3	0	0	0	0	0	0	26
Letland	8928	2298	1085	746	394	257	0	0	13708
Litouwen	55484	23375	14	20	0	0	0	0	78893
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	575	53	0	0	0	0	0	0	628
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	229375	52241	26228	16040	3333	521	339	1344	329421
Total	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Tabel 11: Verzoeken om bewaarde *internetverkeersgegevens*, naar ouderdom, 2008									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	737	412	137	168	0	0	0	0	1454
Denemarken	102	14	11	2	3	1	0	1	134
Duitsland	Geen gegevens verstrekt								
Estland	Geen gegevens verstrekt								
Ierland	492	460	498	1422	0	0	0	0	2872
Griekenland	Geen gegevens verstrekt								
Spanje	3278	2323	2113	1403	0	0	0	0	9117
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	0	0	0	0	0	0	0	0	0
Letland	424	150	75	219	74	34	0	0	976
Litouwen	Geen gegevens verstrekt								
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	76	3	0	0	0	0	0	0	79
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	31170	9046	3097	2605	1917	2015	147	57	50054
Totaal	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Door de lidstaten verstrekte statistieken over 2009

Tabel 12: Verzoeken om bewaarde gegevens naar ouderdom in 2009									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	210975	56623	11620	1053	0	0	0	0	280271
Denemarken	2980	685	179	104	54	38	12	14	4066
Duitsland	Not provided								
Estland	4299	1836	1210	1065	0	0	0	0	8410
Ierland	8117	1652	805	297	168	134	69	41	11283
Griekenland	Geen gegevens verstrekt								
Spanje	29775	19346	13999	6970	0	0	0	0	70090
Frankrijk	Geen indeling naar ouderdom verstrekt								514813
Italië	Geen gegevens verstrekt								
Cyprus	31	8	1	0	0	0	0	0	40
Letland	20758	2414	1088	796	565	475	0	0	26096
Litouwen	30247	35456	5886	884	0	0	0	0	72473
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	3336	362	151	174	0	0	0	0	4023
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Polen	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovenië	Geen indeling naar ouderdom verstrekt								1918
Slowakije	Geen indeling naar ouderdom verstrekt								5214
Finland	2000	1310	532	152	76	0	0	0	4070
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	Geen gegevens verstrekt								
Totaal	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Tabel 13: Verzoeken om bewaarde verkeersgegevens naar soort gegeven in 2009 (tussen haakjes het aantal gevallen waarin niet kon worden ingegaan op het verzoek – indien verstrekt)				
Soort gegevens/ lidstaat	**Telefonie via vast netwerk**	**Mobiele telefonie**	**Internetgegevens**	**Totaal**
België	Geen gegevens verstrekt			
Bulgarije	Geen gegevens verstrekt			
Tsjechië	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Denemarken	133 (0)	3771 (10)	162 (1)	4066 (11)
Duitsland	Geen gegevens verstrekt			
Estland	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Ierland	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Griekenland	Geen gegevens verstrekt			
Spanje	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Frankrijk	Geen indeling naar soort gegeven verstrekt			514813
Italië	Geen gegevens verstrekt			
Cyprus	0 (0)	23 (3)	14 (0)	40 (3)
Letland	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Litouwen	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxemburg	Geen gegevens verstrekt			
Hongarije	Geen gegevens verstrekt			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Nederland	Geen gegevens verstrekt			
Oostenrijk	Geen gegevens verstrekt			
Polen	Geen indeling naar soort gegeven verstrekt			1048318
Portugal	Geen gegevens verstrekt			
Roemenië	Geen gegevens verstrekt			
Slovenië	Geen indeling naar soort gegeven verstrekt			1918 (48)
Slowakije	Geen indeling naar soort gegeven verstrekt			5214 (157)
Finland	Geen indeling naar soort gegeven verstrekt			4070
Zweden	Geen gegevens verstrekt			
Verenigd Koninkrijk	Geen gegevens verstrekt			
Totaal				2051082 (1069885)

Tabel 14: Verzoeken om bewaarde gegevens betreffende *telefonie via een vast netwerk*, naar ouderdom, 2009									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	9919	2907	47	36	0	0	0	0	12909
Denemarken	105	19	7	2	0	0	0	0	133
Duitsland	Geen gegevens verstrekt								
Estland	2254	866	599	424	0	0	0	0	4143
Ierland	3934	337	69	70	50	39	16	11	4526
Griekenland	Geen gegevens verstrekt								
Spanje	2371	1492	844	348	0	0	0	0	5055
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	0	0	0	0	0	0	0	0	0
Letland	744	253	157	143	68	89	0	0	1454
Litouwen	469	773	73	6	0	0	0	0	1321
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	83	25	18	20	0	0	0	0	146
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	Geen gegevens verstrekt								
Totaal	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Tabel 15: Verzoeken om bewaarde gegevens betreffende *mobiele telefonie*, naar ouderdom, 2009									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	197620	48841	472	0	0	0	0	0	246933
Denemarken	2777	639	162	98	47	19	12	7	3761
Duitsland	Geen gegevens verstrekt								
Estland	318	397	96	70	0	0	0	0	881
Ierland	3669	835	220	210	115	92	50	28	5219
Griekenland	Geen gegevens verstrekt								
Spanje	24065	15648	11147	5273	0	0	0	0	56133
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	17	16	0	0	0	0	0	0	23
Letland	18832	1912	778	515	394	263	0	0	22694
Litouwen	25713	19595	28	0	0	0	0	0	45336
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	2332	246	111	122	0	0	0	0	2811
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	Geen gegevens verstrekt								
Totaal	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Tabel 16: Verzoeken om bewaarde *internetgegevens*, naar ouderdom, 2009									
Ouderdom opgevraagde gegevens (maanden)/lidstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totaal**
België	Geen gegevens verstrekt								
Bulgarije	Geen gegevens verstrekt								
Tsjechië	3369	4811	861	942	0	0	0	0	9983
Denemarken	98	27	10	4	4	7	0	1	151
Duitsland	Geen gegevens verstrekt								
Estland	315	145	56	102	0	0	0	0	618
Ierland	489	455	502	0	0	0	0	0	1446
Griekenland	Geen gegevens verstrekt								
Spanje	3339	2206	2008	1349	0	0	0	0	8902
Frankrijk	Geen gegevens verstrekt								
Italië	Geen gegevens verstrekt								
Cyprus	12	2	0	0	0	0	0	0	14
Letland	852	198	74	90	88	86	0	0	1388
Litouwen	4060	15087	1	88	0	0	0	0	19236
Luxemburg	Geen gegevens verstrekt								
Hongarije	Geen gegevens verstrekt								
Malta	150	14	0	0	0	0	0	0	164
Nederland	Geen gegevens verstrekt								
Oostenrijk	Geen gegevens verstrekt								
Polen	Geen gegevens verstrekt								
Portugal	Geen gegevens verstrekt								
Roemenië	Geen gegevens verstrekt								
Slovenië	Geen gegevens verstrekt								
Slowakije	Geen gegevens verstrekt								
Finland	Geen gegevens verstrekt								
Zweden	Geen gegevens verstrekt								
Verenigd Koninkrijk	Geen gegevens verstrekt								
Totaal	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**

Productie 2

Evidence for necessity of data retention in the EU

Table of Contents

1. Introduction 2
2. Context 2
3. How communications data are used 3
4. Overview of types of cases in which data are important 4
5. Consequences of absence of data retention 5
6. Cross-border aspects of data retention 6
7. Statistics and quantitative data 7

Article 10 7

Available statistics 7

Limitations of quantitative data 8

Conceptual and methodological issues 8

8. Qualitative data 9

Terrorism 9

Murder and manslaughter 11

Serious sexual offences and child abuse 15

Buying or offering online child pornography 18

Drugs trafficking 19

Armed robbery 21

Burglary, theft and organised trafficking 22

Cybercrime 26

Fraud 27

1. Introduction

This document draws together evidence which has been supplied by Member States and Europol in order to demonstrate the value to criminal investigation and prosecution of communications data retained under the Directive 2006/24/EC (the Data Retention Directive or 'DRD'). It contains some general context on the role of historical data in various types of investigations, some observations on the available statistics, and a selection of individual case studies which have been provided by Member States. It is intended to provide further information on the question of the necessity of data retention; readers should also consult the evaluation report for the Commission's general evaluation of the DRD,[1] which included (section 5.4) a number of the arguments which are developed in this document, along with a few illustrative examples, and other statements including replies to questions from the European Parliament[2] concerning the role of communications data in the investigation and prosecution of the most serious crimes.

2. Context

Crime in the EU[3] is increasingly characterised by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by widespread illicit use of the internet. These groups focus their activities where they perceive the risks of detection to be low, like credit fraud and counterfeiting, which along with trafficking in weapons, drugs and human beings are also extensively used to finance terrorist activities. The EU furthermore is a key target for cybercrime, and the prevalence of internet technology has created a market for child abuse material.

Criminal exploitation of communications technologies mirrors general trends in consumer behaviour. In the 1990s a typical user might make 10-20 fixed line or mobile calls a day and send two or three SMS over a few networks; in the 2000s with increased volume and network coverage, a typical user might make 15-25 calls and send 5-15 emails and SMS, and also use online chat, browsing and 'voice over the internet' services.[4] Internet protocol (IP) traffic volumes were estimated to have more than trebled between 2007 and 2010,[5] and in the current decade the internet is the primary source of communication.

Criminals attempt to evade detection through the use of false identities or anonymous communications services. Investigators therefore need not only to be able to access traffic and location data and associated identification details, but also to be confident that these data cannot be fabricated or falsified. The access by and exchange between law enforcement authorities of these communications data is essential to the successful disruption of organised criminal networks.

---

[1] COM(2011)225, 'Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)' http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

[2] E.g. E-004636/2012

[3] See Commission Communication 'First Annual Report on the implementation of the EU Internal Security Strategy', COM(2011) 790 Internal Security Report; Europol: Organised Crime Threat Assessment (OCTA) 2011.

[4] Analysys Mason, Europe's Digital Deficit: Revitalising the Market in Electronic Communications, 3 March 2010.

[5] Source: Cisco Visual Networking Index.

Communications data which do not concern the 'content' (e.g. the conversation during the telephone call, the message in the email) but rather the 'envelope' or 'metadata', consist of information on the identity of subscribers or clients (i.e. service-associated information e.g. IP addresses), traffic data (i.e. communication-associated information e.g. logs of calls received and made), and data on the location of the user at the time of the communication.[6] Such non-content data were used before the adoption of the DRD in high-profile investigations including the murder of Irish journalist Veronica Guerin in 1996, the uncovering of a massive international drug trafficking ring centred around the 'Ndrangheta mafia organisation (known as operation IBISCO), the murder in 1998 of Corsican police prefect Claude Erignac, and the 2004 Madrid bombings.

The DRD was adopted on 15 March 2006 with the aim of ensuring that such data be retained for between six months and two years and be available for the purpose of the investigation, detection and prosecution of serious crime. It is in force in most Member States.[7] The Commission's evaluation report, published in April 2011,[8] concluded that, given the objectives of the Internal Security Strategy[9] and the Digital Agenda,[10] the EU should continue to support and regulate the storage of, access to and use of communications data, but should improve EU rules to prevent the different types of operators facing unfair obstacles in the Internal Market and to ensure that high levels of respect for privacy and the protection of personal data are applied consistently.

3. How communications data are used

During criminal investigations requests for communications data usually proceed - and often result in – the arrest of suspects, bringing of charges or the exclusion of people from investigation. Fewer data are used during prosecution proceedings in court. This may be because prosecuting authorities are unlikely to use information about individuals who have been investigated and then deemed to be of no further interest to the investigation, or because accused parties when confronted with evidence provided through communications data decide to enter guilty pleas which thus remove the need for the communications evidence to be adduced in court. Communications data are used to corroborate other evidence like witness statements and evidence of the association of suspects and location and chronology of event. Some crimes may be dealt with through administrative means (e.g. a caution), and certain investigations may be unable to progress for various reasons. Consequently, more data tend to be acquired initially by the investigator than is later relied on in court. Defence counsel also obtain access to these data: one UK authority reported that there had been 204 such requests between April 2009 and March 2010.

---

[6] These types of data are reflected in Article 5(1) of the DRD i.e. from whom (sub-article a)) and to whom (b) the communication was sent, when it was sent and how long it lasted (c), what sort of communication (d), how the communication was sent i.e. what equipment was used (e) and where the communication was sent (f). For definitions see ETSI Technical Standard 101 331.

[7] The deadline for transposition was September 2007, with the option of postponing the implementation of retention of internet data until March 2009. Twenty-six Member States have transposed it, two (Belgium and Germany) have partially transposed it.

[8] COM(2011)225, 'Evaluation Report on the data retention directive (Directive 2006/24/EC)'

[9] Commission Communication, 'The Internal security strategy in action: Five steps towards a more secure Europe,' COM(2010) 673.

[10] Digital Agenda, COM(2010) 245 final/2.

4. Overview of types of cases in which data are important

The importance of subscriber, traffic and location data is demonstrated by research and the practical experience in the EU. Since the adoption of data retention measures, Member States as well as Europol have provided a considerable number of case studies in which data have proven important or crucial in solving some of the most serious crimes. These data can be the only lead to identify a suspect or to identify his/her accomplices at the start of an investigation where eye witness accounts or confessions and other forensic evidence are unavailable, and to decide whether it is justified to use more intrusive surveillance tools like interception. They can help establish whether an offence was planned in advance. They are particularly valuable for cases where internet/communication services are used to commit a crime, such as grooming and uploading/downloading child pornography and identity theft: for example, where someone is detected in an internet chat room attempting to sell child pornography, investigators need first to find the IP address used to connect to the chat room, and then ask the internet service provider (ISP) to identify which individual user has been assigned that particular IP address. Similarly, where threats to commit suicide or attack others are placed on the internet (e.g. Sweden claims to have investigated 15 such threats to carry out massacres in schools over 12 months in 2009-10), police can only begin investigation through identifying the user of a particular IP address based on data held by the ISP.

While most data tends to be requested within a few months or even weeks of the communication taking place, there are four categories of criminal investigation for which **older data** tend to be needed.[11]

a. **Terrorism and organised crime** including severe types of financial crime which are often characterised by repetition or by a long period of preparation. Investigations often require time in order to establish a clear pattern and relationships between multiple events and so to expose not just individual suspects but whole criminal networks, especially where associates repeatedly exchange SIM cards to avoid detection. The gap between the moment the criminal offence is committed and the moment of its detection by law enforcement authorities, through the identification and seizure of servers containing evidence, can be several months or even years. Such delays occur in cases of:

    i. trafficking in human beings and drugs trafficking, where there is a complex division of labour among accomplices;[12]

    ii. repeated extortion where victims are in a relationship with the offender and where the victim may only seek help months or even years after the exploitation started;

    iii. tax fraud, serious cases of financial crime and corruption of public officials which may span several years. Such offences may only be detected after the end of a financial year, after audits have been carried out or on the basis of annual reports. Authorities may therefore need to examine data which are at

[11] See the Commission's evaluation report.

[12] Prosecutors in Poland study traffic data in 70% of preparatory proceedings in drugs possession cases. E.Kuźmicz, Z. Mielecka-Kubień, D. Wiszejko-Wierzicka (red.) Karanie za posiadanie. Artykuł 62 ustawy o przeciwdziałaniu narkomanii – koszty, czas, opinio. Raport z badań, Instytut Spraw Publicznych, Warsaw 2009, s.58.

least a year old, or several years old to investigate 'triangulation' structures involving false invoices or transactions which appear at first to be legal, especially across jurisdictions;

iv. repeat burglaries, where proof of involvement of the same gang often depends on mobile telephone location data which shows connected individuals to have been in the same area at suspicious times of day.

b. **Serious sexual offences** where the victim may not report the crime for months after the event. UK report that over half of communications data used in such investigations were six months old or over.

c. **Substantiating previous intent to commit illegal activities**, which is important within criminal and pre-criminal proceedings and to determine whether a homicide is a case of premeditated murder;

d. **Large cross-border cases** which may involve mutual legal assistance procedures, such as offences committed by travelling gangs or where several requests for data from different operators are often necessary. It is often only after months of investigation that all relevant facts are collated. Where servers are located in a foreign country data logs held on servers must be analysed to extract the IP addresses of computers used by persons suspected of accessing the child abuse images. Shorter data retention periods often make it impossible to obtain effective results. Rogatory letters take time to execute, and as a result IP addresses and telephone numbers may be identified for which subscriber data can no longer be requested.

5. Consequences of absence of data retention

The crucial value of mandatory communications data retention as a measure, as distinct from communications data *per se*, is the *guarantee* that potentially valuable data will be available for a given amount of time. Other measures, such as rules on data preservation (or 'quick freeze'), whilst valuable in many ways, signally fail to provide such a guarantee, and as such rely wholly on the need or willingness of operators to store these data for their own commercial purposes, and to do so in such a way as to render these data accessible in time to be valuable to investigations and prosecution. Before the DRD entered into force, operators may have stored some data but not in an easily retrievable way: mobile telephony data might have been stored in a street-side cabinet or mobile telephone tower, while ISPs may not have logged IP addresses in many cases where they are switched frequently (in processes known as dynamic address allocation and load-balancing). However, according to data protection authorities and operators, certain data have minimal business value and are only stored in a retrievable form because of mandatory data retention. Such data include: (a) fixed/ mobile traffic data for flat-rate unlimited use contracts and pre-paid services;[13] (b) source ID (i.e. telephone number) for incoming calls; (c) unsuccessful call attempts; (d) IP addresses[14]; (e) cell ID (i.e. location) data; and (f) email data. The absence of a guarantee of the availability of

[13] In Germany, the proportion of private internet users with such flat-rate plans rose from 18% in 2005 to 87% in 2009. The proportion of users of prepaid services varies, from about 20% in Finland to about 80% in Portugal. Some Member States (Bulgaria, Denmark, Greece, Italy, Slovakia and Spain) require registration of all pre-paid SIM cards, though there is no evidence of the efficacy of this as a law enforcement measure.

[14] This will change with when the Internet Protocol version 6 is deployed, that is the so-called 'internet of things' where virtually any object could be integrated into the information network with a unique IP address.

these data is deemed to constitute an unacceptably high risk to the ability of police and judicial authorities to investigate and prosecute serious crime, particularly in cross border cases.

If certain traffic data were not stored, detecting and investigating certain crimes would be practically impossible. The experience of Germany since the constitutional court judgment annulling data retention measures in March 2010 may illustrate the consequences of the absence of mandatory data retention. According to the German federal police (*Bundeskriminalamt*) and state police (*Landeskriminalämter*),[15] for 44.5% of the cases involving requests for historical data traffic data, there was no other means of conducting the investigation. They reported that 30% of criminal cases have collapsed since the judgment of the Constitutional Court.[16] According to the Lower Saxony *Landeskriminalamt*, between the judgement of the Constitutional Court and summer 2011, traffic data would have been requested had they been available; in 257 cases (or 75% of all cases) investigations could not be solved, while for 32 cases (9%) investigations were only solved by investing significant additional resources. These claims should be considered in the light of a report completed in July 2011 and published in January 2012 by the Federal Minister of Justice, which concludes that the present situation is characterised by very limited statistical and empirical data.[17] Meanwhile, according to the statistics provided by Czech Republic, the number of unsuccessful requests for data increased from 3% in 2009 to 14% in 2011, the year in which the constitutional court annulled the legislation transposing data retention.

6. Cross-border aspects of data retention

Member States regularly exchange requests, with a copy sent to Europol, for investigations of serious crime, with an estimated 50% (or 40 000) of these requests involving communications data.[18] The exchange of traffic or location data requires mutual legal assistance procedures which, according to law enforcement authorities, can be slow and result in delays in investigations and the loss of associated data if the target of an investigation switches SIM cards or IP addresses while the request is being processed. Where there is a good level of trust (e.g. Franco-Spanish cooperation against the ETA terrorist threat) it seems that data are exchanged more easily. One UK law enforcement authority over a six month period in 2009-10 reported five operations which required communications data and which resulted 14 cases brought before courts in another Member State or outside the EU, each of which resulted in a conviction. Lithuania in its statistics for 2010 reported that, of the total of around 136 000 cases in which data were requested in 2010, 23 000 concerned requests for legal assistance from other Member States in relation to high-volume and high-value mobile telephone theft.

---

[15] Sachstandsbericht Nr. 8: Stand der statistischen Datenerhebung im BKA, 23 June 2011, at 13.

[16] http://www.faz.net/artikel/C30833/straftaten-im-internet-lka-direktor-jeder-muss-identifizierbar-sein-30334057.html

[17] Max-Planck-Institut für ausländisches und internationales Strafrecht: *Schützlücken durch Wegfall der Vorratdatenspeicherung: Eine Untersuchen zu Problemen der Gefahrenabwehr und Strafverfolgen bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, July 2011.

[18] Source: Workshop with police on future options for data retention in the EU, 17 June 2011. 'Serious crime' is defined in Council Decision 2009/371/JHA establishing the European Police Office (Europol).

7. Statistics and quantitative data

Article 10

Article 10 of the DRD requires Member States to provide the Commission with statistics on a yearly basis which should include:

- the cases in which information was provided to the competent authorities in accordance with national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

In November 2008 the Commission expert group on data retention[19] adopted a template for submitting these statistics, which was presented to Member States delegations at a meeting in January 2009. The delegations undertook to provide annual statistics on the basis of that template.

Available statistics

Twenty-three Member States have provided some statistics since 2008. While most Member States have used the 2009 template, they interpret in different ways terms from the DRD such as 'case' and 'request', and statistics vary in format which limits their comparability. (Poland's statistics alone account for around half of requests reported overall, partly because competent authorities submit identical requests to each of the main mobile telephone operators.) It appears that there are over two million requests per year for retained data, equivalent to about two requests for every police officer in the EU or 11 requests for every 100 recorded crimes. The number of requests varies greatly between Member States. Certain Member States (France, Poland and UK) claim that communications data are needed for most criminal investigations. UK claims that for an 'average' murder investigation, there may be between 500 and 1000 communications data requests.[20] Finland stated that 56% of all requests for data proved important or essential to the outcome of criminal investigation or prosecution. Each investigation into a serious crime is likely to require multiple items of data. UK reported that for a certain investigation 120 applications were made, including 17 for traffic data, 45 for 'service use data' and 58 for subscriber data, resulting in nine convictions.

Most requests concern mobile telephony data (approximately 75%). Approximately 67% of data is requested within three months and 89% within six months, but a sizeable minority of requests – 11% - concern data 6-12 months old. Ensuring that data are retained for more than six months helps prevent investigators from asking for excessive amounts of untargeted data earlier on in the inquiry.

---

[19] See http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/index_en.htm

[20] Home Office in oral evidence to Joint Committee on Draft Communications Data Bill, UK Parliament, 10 July 2012.

Limitations of quantitative data

The Commission considers statistics on crime and criminal justice to be indispensable tools for developing evidence-based policy at EU level, and continues to work to address the general lack of comparable statistical information.[21] Certain NGOs have attempted, using selected crime statistics, to draw negative conclusions about the value of data retention.[22] These claims fail to acknowledge that crime statistics – including the number of crimes and the number of crimes which are solved ('clearances') - are determined by multiple socio-economic factors, and success in tackling crime cannot be attributed to a specific security measure, such as data retention.[23] Police use different methods for measuring crime clearance rates and, moreover, it may be argued that an undue focus on such statistics can be counterproductive to the effectiveness of law enforcement.[24] In any case, it would not be possible to identify meaningful statistical trends only a few years after the DRD entered into force.

Conceptual and methodological issues

A number of areas of confusion regarding Article 10 remain.

a. There are different interpretations of the term 'cases' – which could mean (i) each and every item of data that was or was not provided, (ii) each request which may be for one or multiple sets of data, or (iii) each investigation in which there might be multiple requests for multiple items of data.

b. Where the request to a service provider is for more than one item of data, the data may be of different ages. Recording the age of individual data records could be unduly onerous for operators and/or competent authorities.

c. Statistics submitted from some Member States only refer to requests for traffic and location data and not to subscriber information acquired from operators.

d. The phrase 'Cases where requests for data could not be met' has been interpreted variously as cases where i) the service provider was unable to provide data that should have been retained under the DRD but were not retained; ii) data that were needed but which do not fall within the scope of the DRD, or iii) data that had been retained but were no longer available because the request was made after the expiry of the retention period.

---

[21] See COM(2012) 713, 'Measuring Crime in the EU: Statistics Action Plan 2011- 2015'.

[22] See, for example, http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[23] See K. von Lampe, 'Measuring organised crime: A Critique of current approaches', in *Threats and Phantoms and Organised Crime, Corruption and Terrorism,* eds. P.C. van Duyne, M. Jager, K. von Lampe and J. L. Newell, 2004, pp. 85-110.

[24] See for example J.H. Skolnick and D. Bailey, *The New Blue Line: Police Innovation in Six American Cities*, New York, 1986: 'Variations in crime and clearance rates are best predicted by social conditions such as income, unemployment, population, income distribution and social heterogeneity'.

The expert group addressed this issue and in November 2012 adopted updated and more comprehensive guidance on provision of statistics under Article 10, which the Commission encourages all Member States to follow.[25]

Furthermore, Member States law enforcement authorities and data protection authorities are generally not in a position to know whether the precise data used in investigations and prosecutions was stored by the operators solely in order to comply with the data retention obligation. There is no obligation to store separately those data needed for (a) business purposes), (b) purposes of combating 'serious crime', as referred to in the DRD, and (c) for public order purposes other than combating serious crime, which may be permitted under Directive 2002/58/EC. Supervisory authorities do not have enforcement powers to ascertain which data is kept for which purposes, although, according to a report by the Article 29 Working Party, separation seems to be the norm in most Member States.[26]

8. Qualitative data

Member States are under no obligation to provide evidence of the value to serious criminal investigation and prosecution of *retained data* (i.e. data kept only because of mandatory retention). The Commission nevertheless wrote to each Member State in February 2012 with some specific guidance – consistent with the deliberations of the expert group - on qualitative and quantitative evidence to be provided. The evidence in this document includes responses to this request, as well as other examples provided before and since the publication of the evaluation report. Below are case studies provided by Member States in order to illustrate the importance of historical data; some of these cases predate transposition of the DRD in the Member State in question. Some cases may be understood as 'negative' examples – that is, examples of where investigations have stalled because of the absence of a data retention requirement. Some examples are more elaborated than others.

Terrorism

Case 1 (Germany)

Individuals were suspected of supporting Al-Qaida and the Uzbekistan Islamist Movement by distributing propaganda material on the internet and trying to attract supporters for their cause. The internet access provider had not retained the IP address of one user who had logged in to establish an internet video channel for those purposes, and investigators were unable to pursue that part of the inquiry.

---

[25] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf

[26] Article 15(1) of Directive 2002/58/EC on 'e-Privacy' allows Member States to restrict privacy rights and obligations, including through the retention of data for a limited period, to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. See EDPS opinion on evaluation report on the DRD, May 2011 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf and Article 29 Working Party Report 01/2010 'Report 01/2010 on the second joint enforcement action: compliance at national level of telecom providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of article 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/E amending the e-Privacy Directive' http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf. Recital 12 of the DRD acknowledges that data may be retained beyond the categories in the scope of the DRD and for purposes other than those set down in DRD.

Case 2 (Germany)

In an internet forum on 12 April 2010 a video of a terrorist organisation was made available through various internet links. One of these links had been created by an unknown person registered under a certain e-mail address. An inquiry concerning the e-mail address with the responsible email service provider revealed that it had been registered only a day before the release of the video. The IP address had been allocated by a major ISP, but as seven days had already elapsed the ISP said they it did not hold the IP address details. The person could not be identified and the case remains open.

Case 3 (Germany)

Following the murder of Hamas official Mahmoud al-Mabhouh in Dubai 2010, an investigation was conducted into a person suspected of acting an agent for an intelligence service and of misleading another to make false official entries. Financial investigations revealed that calls made via one of the suspect's mobile telephone were billed retrospectively over a period of four to six months. It is likely that analysis of communications data contacts would have enabled the identification of further leads and collaborators in Germany. However the communications data were no longer stored. Consequently, it has not been possible to date to progress the investigation.

Case 4 (Germany)

Information was received by US and Lebanese authorities on attacks in Germany in 2010 planned by members of Fatah al-Islam. This led to preventive measures with the aim of identifying possible cell members in Germany and communication among them. In the end, only one of the persons mentioned was identified in Germany. This person, who had been staying in Germany under a false identity, was also the subject of an arrest warrant issued by the Lebanese authorities for general offences. This person has been arrested and is being detained pending extradition. The suspicion that this person posed a terrorist threat has been eliminated. All additional measures taken against the group were fruitless since the historical communications data were not fully made available by the providers.

Case 5 (UK)

Operation Vivace, an investigation into four attempted bombings in the London area on 21 July 2005 which mirrored those carried out a fortnight earlier on 7 July, made extensive use of historical communications data. These data identified regular contact between the main five offenders and assisted in identifying further offenders who were arrested and charged with offences relating to the attacks. The data placed some the offenders close to the attack scenes prior to and after the attempted attacks on 21 July, and routinely placed four of the offenders in the vicinity of the bomb factory, showing that three of the defendants were there the night before the attacks. The data also implicated two suspects who provided material assistance to offenders during their escape after the attacks from London to the south of England and then abroad. These investigations lasted between several months and several years, with fresh information coming to light throughout the process. As more information was gathered, so further fresh target communications were identified. Equally, as each day passed, historical communications data was lost as it was deleted from operators' storage databases in line with data retention policy along with potentially valuable leads.

Murder and manslaughter

Case 1 (Czech Republic)

Czech investigators suspected that prior to a murder committed in the Kroměříž region in June 2011 the victim and accomplice had been close acquaintances. Communications data were requested immediately but operators stated that in order to comply with the national constitutional court judgment the data had been deleted. Authorities needed over a week to assemble other biological evidence and witness statements before they were able to secure the suspects arrest, whereas communications data could have been expected to provide grounds for arrest on the day of the murder and so avoid risk of further danger to the public.[27]

Case 2(Czech Republic)

During investigation into a murder committed in September 2011 police were unable to assemble sufficient evidence due to the unreliability of witness statements. Police were aware of the mobile telephone numbers that were used by these persons and whose devices were probably switched on at the time of murder. However service providers were no longer keeping the data necessary to identify the location of mobile communication equipment. A lot of interrogation has been carried out by police along with other operations but without any results. Police consider that had they been able to access these data they would have identified the perpetrator.

Case 3 (Czech Republic)

A Roma dwelling in Vítkov was subject to an arson attack in 2009. The court classified the conduct as an attempted multiple racially-motivated homicide. At the scene of crime there was no clear evidence leading to the perpetrators. Police investigation led to the information that an individual, 'J.L.', had been heard telling people in a nightclub about plans to 'go after gypsies'. J.L. was known to be a right-wing extremist who had taken part in a number of public gatherings. Analysis of his mobile telephone revealed connections to one suspect who shortly after the attack was known to have burns on his arms, and data related to his mobile telephone in turn enabled police to identify further perpetrators.

Case 4 (Denmark)

An elderly woman was discovered dead in her home. Subsequently 6000 DKK (800 EUR) worth of transactions were made using her bank card. Police studied CCTV footage from locations where the card was used, and images were released to the press but there were no positive identifications of any suspect. Communications data obtained following a court order enabled investigators to identify mobile phones which were within the vicinity of the credit card transactions and at the estimated time of death of the woman. A young male was at first suspected but later was excluded as he had not been in the areas where the card was used. Investigators then identified two brothers using the call data, leading to their arrest.

---

[27] http://www.novinky.cz/krimi/236446-muz-obvineny-z-brutalni-vrazdy-studentky-v-huline-tvrdi-ze-se-zabila-sama.html

Case 5 (Denmark)

A 33-year-old man was shot dead in a rural area where he regularly went fishing with his partner. His female partner who was near the scene at the time was suspected by investigators of involvement in the murder, which she denied. Police obtained a warrant to carry out wiretap and obtain historical communications data concerning the partner. These data revealed that the partner had been in contact with a male by telephone calls and text messages during the hour leading up to the murder. Police then obtained communications data associated with this person, leading to the arrest of both individuals. Location data was used to refute the man's alibi that he had been at his home 25 miles away from the murder scene, and he subsequently confessed to murder and implicated the woman in the conspiracy. Each of them was sentenced to 13 years' imprisonment for manslaughter.

Case 6 (Denmark)

An investigation into six attempted murders, assault and the possession of a stash of weapons in connection with wars between biker gangs involved analysis of over 730 000 items of historical call data associated with around 85 telephone numbers. These data supplied evidence which corroborated the statements of key witnesses and culminated in the conviction in September 2011 of 15 gang members and sentences of a total of 135 years' imprisonment.

Case 7 (Germany)

Polish authorities were searching for a murder suspect, believed to be in Germany, who was known to log on regularly to a Polish social network. Polish authorities sent to German authorities a list of the login data including the IP addresses, which were their only lead. All these data had been deleted by the ISP in Germany, and the case remains open.

Case 8 (Germany)

After the murder of a police officer the offender escaped in the car of the victim. The examination of the scene of crime did not yield any additional information on the identity of the offender. No eye-witnesses were known. Investigators had reason to believe that the offender had abandoned his vehicle and had made a call to a taxi firm using a mobile telephone. The network provider had deleted all traffic data, which might have enabled police to identify the offender.

Case 9 (Germany)

A body found in a street in Cologne was identified several days later as a 43-year-old Italian national. The Italian authorities advised that the victim was believed to have been connected with the mafia. It took three months of investigation to identify the possible scene of the murder and three suspects. By this time historical data relating to the suspects' communications and location were not available, and the investigation is still unresolved.

Case 10 (Estonia)

Sergey Kulešov was convicted in 2009 for murdering his female business partner in 2006 on the basis of traffic and location data of mobile telephone communications which connected him with the victim and the scene of the murder. There was no other clear evidence other than suspected motivation which emerged during the investigation.

Case 11 (Hungary)

An investigation in 2009 was opened into a homicide involving an unidentified individual who was believed to have unlawfully entered a privately-owned farm with the intention of committing burglary. The suspect killed the victim by striking him several times on the head with an axe found at the scene of the crime. He stole cash and valuables worth about 270 000 Forints (1000 EUR). He hid the victim's corpse in a cesspit in the grounds of the farm. Location data retained by the service provider enabled investigators to connect the suspect with the scene and time of the homicide and then to a location 200 kilometres away from the farm where the suspect was tracked down and arrested.

Case 12 (Luxembourg)

In 2011 a body was discovered in a forest hanging from tree. There were no identification documents and the state of decomposition of the corpse suggested it had been left for several weeks if not months. Investigators had been unable to identify the body. Around 10 months after the unidentified person's death, contacts outside Luxembourg led to a suspicion that the death may have been the result of a criminal offence rather than suicide. By this point, however, it communications data which may have enabled a reconstruction of last movements and communications of the person were unavailable.

Case 13 (Luxembourg)

A man was suspected of conspiring with his partner of murdering his adoptive parent. The investigating judge ordered disclosure of traffic data dating back over three months concerning these persons' telephone activities. These data enabled investigators to link the suspects to the contract killer and to refute the stories of several credible witness statements to the contrary.

Case 14 (Luxembourg)

In August 2008 a man's body was discovered abandoned in a forest. The investigating judge ordered disclosure of communications data relating to telephone calls made by the victim's wife several months prior to the murder. These data enabled investigators to identify a suspect who confessed to the murder and to the fact that it had been contracted by the wife since early 2007.

Case 15 (Netherlands)

A man was shot dead in the basement of his electronics stop in Rotterdam in September 1999. His wife was suspected of complicity in the murder but the prosecution initially failed due to lack of evidence. Subsequently, using traffic and location data investigators were able to link the woman to the man who carried out the murder, and Rotterdam District Court sentenced her to 12 years imprisonment in July 2010.

Case 16 (Poland)

In February 2007 in Myślenice two owners of a currency exchange office were shot dead with machine guns. The perpetrators stole 150 000 PLN (37 000 EUR). Investigators obtained communications data which enabled police to arrest the suspects three weeks after the murders had taken place. Analysis of the calls made using the suspect's SIM card which had been seized enabled investigators to implicate the suspects of the February 2007 murders in

separate similar murder case. Further investigation led to three individuals being charged and in July 2010 convicted by the District Court in Kraków on three counts of murder and two of attempted murder between 2005 and 2007 in Kraśnik, Tarnów and Sosnowiec. Tadeusz G and Wojciech W were sentenced to life imprisonment and Jacek P to 15 years imprisonment.

Case 17 (Slovakia)

On 22 June 2011 a man was lured from a 'casino-café' in Bratislava to nearby Vráble and killed with eight gunshot wounds in his own vehicle, before being driven and his body disposed of in Jabloňovce. Communications data provided investigators with evidence that the murder had been premeditated. The accused was believed to have telephoned an accomplice the day prior to the murder to arrange transport. Location and call data implicated the accused at the murder scene, corroborating the statements of witnesses that he had made telephone calls on arrival at and departure from the location. Together with the conclusions of the forensic autopsy, the data helped establish that the victim was dead by the time the perpetrator left the scene of the crime. During the court proceedings, these data made it possible to refute the perpetrator's defence as to the sequence of events, and contributed significantly in establishing that the perpetrator had planned and prepared the murder of the victim in advance. (To this end, he had already dug a hole, in which he subsequently buried the victim's body within 30 minutes of inflicting the fatal stab wounds.) These findings ultimately resulted in a change in the legal classification of the crime to a more serious offence with the prospect of a more stringent penalty.

Case 18 (Slovenia)

Italian police alerted authorities in Slovenia, Croatia and Bosnia and Herzegovina following the disappearance of Roberto Menicali in June 2011 who was believed to have crossed the Italy-Slovenia border with the intention of selling his car to a man and a woman. Authorities were able to connect movements of the missing person's car, use of his bank card and traffic data from mobile phones and thereby to establish that the suspects were citizens of Bosnia and Herzegovina. Analysis of data from Menicali's mobile led police to the discovery of a man's body in woods near Nova Gorica, later established to be that of Menicali's, and subsequent cross-border cooperation with authorities of Serbia and Montenegro resulted in an international search warrant and the arrest of both suspects in Montenegro.

Case 19 (Sweden)

In July 2010 police began an investigation into a series of shootings, the first of which occurred in October 2009 and involved the death of a young woman and the serious injury of a young man. Investigators obtained traffic data from the crime scene to identify possible suspects. Analysis of these data along with a psychological profile led to the suspicion of a single individual using a legally-obtained weapon. The police received a tip-off and the person was arrested. Ballistic evidence connected him to some of the shootings. In order to connect him to all the shootings and to rule out other possible suspects the investigators used traffic data, some of which was over 10 months old, from mobile telephone operators as well as information from banks and other sources which revealed the suspect's movements.

Case 20 (Sweden)

Anders Eklund was convicted in 2008 for the murder of 10-year-old Engla Hoglund. There was a reasonable assumption that Eklund could have committed other crimes that were not

known to the police, and these suspicions were substantiated by location data generated by his mobile telephone along with other evidence such as DNA analysis, leading to the conviction of Eklund for the murder of Pernilla Hellgren in Falun in 2000.

Case 21 (UK)

In September 2009 the body of taxi driver Stuart Ludlam was discovered with two gunshot wounds to the head in the boot of his taxi outside the train station in Derbyshire. Police carried out checks on the mobiles Ludlam was carrying at the time of his murder in order to help identify his killer. His work telephone had been stolen but data on communications using that device were identified through subscriber checks which revealed that Ludlam had received diverted calls from the main taxi office number. Incoming and outgoing call data with cell site locations were requested to trace Ludlam's movements on that day. Call data was of no use at this time as it only showed the taxi number on divert calling. Police then applied for call data for the taxi landline number to identify the last number to have contacted Ludlam and any other numbers that might be of interest to the investigation, in order to establish how he might have been lured to the murder scene. The last number to have called the taxi company was attributed to a pre-paid SIM card for which there were no subscriber details. Using the telephone data police were able to identify the place where the telephone had been purchased and where the last top-up before the murder had been purchased, which was at a supermarket petrol station a few days beforehand. The petrol station did not have in-store CCTV but police requested the till records which revealed another transaction of 20 GBP of petrol at the same time as the purchasing of the mobile telephone top-up. Officers now knew the time the top-up was purchased, and so examined all CCTV tapes from locations in the vicinity of the supermarket, which showed a male purchasing a mobile telephone in a nearby shop. This male was identified as Colin Cheetham, who after further investigation was convicted of Ludlam's murder and jailed for 30 years. Without access to relevant traffic data Cheetham might never have been identified.

Serious sexual offences and child abuse

Case 1 (Belgium)

A Belgian lifestyle and relationships website (zoetie.be) hosts a forum in which teenagers exchange questions and answers. An 11-year-old girl was groomed by someone pretending to be a 17-year-old male who attempted to persuade her to have sexual intercourse with an older man in exchange for money and designer clothes. The girl's father discovered these exchanges and informed the police just before the girl and the boy had arranged to meet. Following three-months of investigation, including the use of IP addresses and assistance from communications service providers which had set up the e-mail addresses used to contact the girl, police identified their suspect as a 35-year-old man. Investigators needed to build up evidence from computers seized from at the man's house, from data obtained via letters rogatory from a communications service provider based in the US. Ten months later the offender was given a suspended sentence and ordered to pay substantial damages.

Case 2 (Czech Republic)

In Olomouc region, a girl under the age of 15 was coerced into prostitution by a man through a social media channel. The man arranged for her to have sex with 10 men over nine days in January 2012. He was identified by traffic data generated by his interaction with the girl and subsequently charged with trafficking in human beings and sexual abuse.

Case 3 (Czech Republic)

In 2011 police investigated the operator of a pornography website which announced the availability of child pornographic images. Internet data enabled investigators to locate the computer from which images had been uploaded, and led to the charging of two persons for sexual abuse of a seven-year-old girl and production of child pornography.

Case 4 (Europol/UK)

In 2007 UK and Australian authorities independently discovered boylover.net, a covert forum for adults to discuss their sexual interest in young boys. Subscribers to the forum once they had made contact with one another would then move to more private means such as email to exchange and share images of children being abused. Police detected 70 000 such subscribers across the UK, US, New Zealand, Australia and Thailand.

As a result Operation Rescue was launched, in which Member States authorities monitored the internet and obtained relevant data (often terabytes in volume) from ISPs which was then transmitted in plain text format log files to Europol. Europol used these data to produce 3 378 intelligence reports and send requests on suspicious IP addresses to EU Member States as well as seven third countries with which Europol had an operational cooperation agreement.

In the UK investigators posed as members of the discussion forum and were able to identify a server which was seized, handed over to Europol for forensic examination and which revealed the personal details of all members, including date of birth, occupation and country of residence. Those Member States which had not yet transposed - Austria, Germany (which received packages of IP data related to 377 suspects), Sweden, Czech Republic and Norway, and others which lacked specific legal measures against child pornography, were unable to meet these requests because data were not available from service providers could not be or do not defined legislation or definition of written child pornography.

Of the eight EU Member States and six third countries which were able to take action, the operation identified overall 230 victims of child abuse and 670 suspects leading to 184 arrests. Two-hundred and forty of these suspects were UK residents and included police officers, teachers and youth leaders, and there have been 33 convictions. One man was sentenced in March 2010 to six years' imprisonment for sexual abuse of two minors after police discovered more than 60 000 indecent images on his computer.

Case 5 (France)

In April 2007 French Police National were charged with investigating 'MGJ-P' who had been on the run since his conviction in absentia in December 1997 when he was sentenced to 20 years' imprisonment for rape of a minor. Police took a close interest in the fugitive's family circle and in particular his mother, Mme GJ. Detailed call records for the number of Mme GJ for the previous 12 months were requested from her telephone service provider. Examination of the call records enabled the identification of a telephone number in another country ('P'). Investigations also showed that Mme GJ was sending cash through Western Union to a person who was resident in P. The interception of the telephone line of Mme GJ confirmed that she was making regular calls to her son who was living in country P. With the help of the liaison officer and local authorities in P, MGJ-P was arrested in September 2007 pending extradition to France.

Case 6 (Poland)

A major suspect in a series of incidents of sexual abuse of minors in Wrocław had managed to evade detection. After 15 months involving interviews with 40 people the police obtained the e-mail address of the offender. A list of system logs for this account was obtained that allowed to determine the IP address. Subsequently the perpetrator was identified. Police consider that without this period of retention identification would not have been possible.

Case 7 (Spain)

Spanish investigators following a report in October 2007 uncovered a string of grooming incidents between January 2007 and August 2008 in which a man pretending to be a woman or minor on various internet for a persuaded young girls to take photographs and videos of themselves of a sexual nature. He then used a software tool to send these images and videos to various email addresses using the name 'Rafael'. Traffic data were obtained from the service provider on basis of a court order in May 2008 which enabled offender to be identified, as was acknowledged explicitly by the judge in the trial in which the man was convicted of six counts of corruption of a minor.

Case 8 (Sweden)

In 2010 an eight-year-old girl was kidnapped not far from her school. She was driven away in a car and sexually assaulted before being released. At the police station the girl described the make and colour of the car, and recalled that during the assault the man had received but not answered two telephone calls. As there were too many cars fitting the description to enable accurate identification, the police requested the log of active mobile phones in the area, and identified two numbers to which there had been two unanswered calls. This led to the identification, arrest and confession of the offender who was sentenced to six-year imprisonment.

Case 9 (UK)

A 14-year old female from the Fife area was reported missing in November 2009. She had a history of self-harm and multiple suicide attempts. She had left a note for her parents in which she claimed to have been 'hearing voices'. A trace to find the live location of the victim's telephone was carried out but it had been switched off. Historical call data was examined to ascertain with whom she had been in contact prior to her going missing. The call data identified a mobile telephone whose subscription was attached to an individual unknown to the girl's parents. Checks at the registered address of the subscriber revealed that the missing girl was in the company of a 36-year-old man whom she had met in an internet chat room. The man was charged with sexual offences.

Case 10 (UK)

UK authorities received intelligence from US authorities that an individual using internet email had sent a movie file of a woman sexually abusing a four-month-old girl. The log-on IP address for this account was found to be registered to a male from Northampton. Further enquiries established that a girlfriend of the individual had three children all less than four years old. After investigation both were convicted of the serious sexual abuse of the children. The children had been found in conditions of neglect, described by an officer as filthy, unsanitary and unfit for human residence.

Case 11 (UK)

Internet data were used in an investigation into the grooming of a 13-year-old girl on an internet chat service. Examination of the victim's computer by the authorities revealed the email address of a man who had coerced the girl into sending naked photographs of herself and exposing herself during webcam chat. Police officers made enquiries about the e-mail address which revealed the IP address belonged to an address in Wales. Further investigation resulted in the man being charged preventing potentially more serious sexual offences taking place.

Buying or offering online child pornography

Case 1 (Czech Republic)

An e-mail box was suspected to be connected to child pornography and investigation (known as Operation VILMA) began through requests for access logs and e-mail addresses related to particular suspicious e-mail traffic. This revealed a network of holders and disseminators of child zoophile pornography, leading to dozens of house searches across the country and to several arrests.

Case 2 (Europol/ Spain)

Operation Atlantic was a joint investigation by the FBI and Europol over the course of a year into users of a forum for exchange and downloading of paedophile content hosted on a private peer-to-peer server. Europol distributed to France, Italy, Netherlands, Spain and UK in December 2010 information gathered by the FBI. Spanish investigators were able to resolve IP addresses which had been retained for over six months, leading to the arrest of two individuals who were subsequently also found to have sexually abused a seven-year-old. Overall, by February 2012, 37 child sex offenders had been identified with 17 arrests for child sexual molestation and production of illegal content.[28]

Case 3 (Germany)

Police in April 2010 launched an investigation into the dissemination of child pornographic images and videos. Internet research uncovered a number of temporary websites from which users could access a portal – in exchange for a payment of $200 to various Russian individuals - for purchasing child pornographic images. Investigators carried out surveillance of email accounts and stored traffic data relating to persons interested in these images over the course of a month but none of the IP addresses used to log onto these email accounts was available.

Case 4 (Luxembourg)

Police discovered a server based in Luxembourg distributing child pornography images. The server was seized for analysis. It took specialists four months to identify with certainty a total of 57890 IP addresses located in 134 different countries around the world which had been used to view or download the images. As part of the subsequent international investigation

[28] https://www.europol.europa.eu/content/press/european-police-and-fbi-dismantle-network-child-sex-offenders-1361; http://www.guardiacivil.es/en/prensa/noticias/4010.html

known as 'Operation Charly', hundreds of arrests on suspicion of child pornography offences have been reported around the EU.

Case 5 (Luxembourg)

Irish authorities obtained information from New Zealand that a child was at risk of sexual abuse by an internet user based in Ireland. Irish investigators discovered him to be exchanging child pornographic images with a user based in Luxembourg by means of instant messaging software. Two Luxembourg based IP addresses were provided to police via Europol, but the six month retention period had already lapsed and the investigation could proceed not further.

Case 6 (Poland)

In 2009, Polish authorities coordinated eight operations targeting persons distributing child pornography over the internet, using data obtained from regional police investigators, Europol and Interpol. Investigators carried out 428 searches in private houses, businesses, workplaces and internet cafes) and arrested 473 persons leading to 62 provisional sentences.

Case 7 (Spain)

Spanish police (Operation Kruna) detected a user in September 2010 distributing 65 child pornography files over a peer-to-peer network. The court order for obtaining the user and traffic data from the ISP was signed in June 2011, which enabled the location of a large volume of child pornography material.

Case 8 (Spain)

Having detected distribution of child pornography files over a peer-to-peer file sharing network to 65 users in January 2010, Spanish investigators (Operation Oslo) requested judicial authorisation to request data held by ISPs to identify the distributer. Authorisation was issued in June 2010 and led to nine arrests.

Case 9 (Spain)

Police were notified in June 2009 by Interpol of a suspected distribution of child pornography via internet servers located in Spain. In October, investigators sought judicial authorisation to access IP data, which led to the identification and arrest of three individuals.

Drugs trafficking

Case 1 (Denmark)

Police arrested a person at the Danish border for possession of 7.5 kilo of amphetamines. The person disclosed the name and telephone number of the supplier of the drugs. Traffic data, along with lawful interception of telephone calls and video surveillance led to the identification and eventual conviction of three individuals involved in an international drugs trafficking ring.

Case 2 (Denmark)

Police investigating the activities of a man suspected of organising the smuggling cocaine from Netherlands to Denmark used evidence acquired through wiretaps to seize 9 kg of cocaine and to make five arrests. Communications data connected to devices in the possession

of the individuals arrested enabled investigators to implicate the man at the centre of the smuggling activities.

Case 3 (Spain)

In 2010 Spanish police in collaboration with Paraguayan authorities carried out an investigation into an organisation dealing in the trafficking of Paraguayan women into Spain for purposes of sexual exploitation in clubs in the province of Albacete. In June 2010 Paraguayan authorities arrested two of the leaders of the organisation at the national airport. In January 2011, Spain received rogatory letters from the Paraguayan public prosecutor requesting subscriber and traffic data concerning two Spanish telephone lines between May and June 2010. The data had been retained and were exchanged in accordance with the request.

Case 4 (UK)

In 2010/ 2011 police used data from thousands of calls over the previous 12 months between more than a dozen mobile phones to dismantle a nationwide cocaine trafficking ring. Two gang members found to be in possession of 3.58 kg of cocaine (valued 165 000 EUR) were arrested and their mobile phones seized. Detectives then spent months examining communications data to identify links between the other members of the group. This resulted in conviction of six gang members who were sentenced for a total of 53 years imprisonment and the confiscation of 61 000 EUR in cash which is being used to fund police operations targeting other drug dealers.

Case 5 (UK)

Operation Frant was a detailed investigation into a number of drug dealers who were flooding London and the UK with high grade heroin from Afghanistan. The aim was to target the individuals who were masterminding this organised crime network, and as they were not 'hands on' the only possible method of detection was detailed investigation of communications data. The first part of the operation targeted the 'runners' with their consignments. In December 2007 Ghaffor Hussein was arrested in possession of a kilogramme of heroin and in January 2008 Christian Bailey was arrested in possession of 8 kilos of heroin. In April 2008 Harminder Chana and Patrick Kuster (a Dutch national) were arrested in possession of 356 kilos of heroin, having been under surveillance when the exchange took place. One of the ringleaders, Atif Khan, was also arrested later that day on the basis of telephone data and additional surveillance evidence linking him and Chana. Upon arrest all suspects' telephones were seized enabling investigators to obtain the cell site data and establish who orchestrated the deals. Mobile telephone call logs revealed that a certain telephone number had been used to call Khan's telephone 26 times, along with several texts, in a 45-minute period after Khan's arrest. This so-called 'dirty telephone' was attributed to one Abdul Rob by cell site analysis which showed two mobile phones always in the same place at the same time. The telephone evidence was crucial in the case against Rob as there was no previous surveillance evidence of association with the other members of the network. Four members of the network were convicted for conspiracy to supply heroin and sentenced for total 81.5 years imprisonment.

Case 6 (UK)

In January 2008 customs officers at Birmingham airport discovered over 16 kilos of heroine concealed with straws which had been threaded through rugs imported from Afghanistan, they

alerted the Serious Organised Crime Agency. SOCA substituted the drugs rugs with dummies, replaced the original packaging, and began a surveillance operation when the gang came to collect them. After the gang's hire car was abandoned for the second time, SOCA investigators decided to switch from traditional surveillance and to focus instead on their other main lead – a single unregistered mobile telephone number used by the gang to contact the courier company. Analysis of telephone data ultimately led to the identification of five men involved in the plot. All five gang members pleaded guilty on the strength of the telephone evidence. The four main players were sentenced at Birmingham Crown Court in June 2009 to between 10 years 8 months and 14 years 8 months and 14 years 5 months for conspiracy to import Class A drugs.

Armed robbery

Case 1 (Belgium)

In the Antwerp area at night over the Easter holidays two men broke into a second-floor apartment. The resident of the apparent was badly beaten and tied up with tape. A little while later, the same apartment block was broken into a second time, this time on the first floor. The attackers used tear gas and the resident was also tied up and blindfolded. Knowing he was an employee in the court in Antwerp in possession of keys and security code for the court registry where the evidence was stored, the attackers obtained security details. The investigation of the crime scene yielded little information on the perpetrators. The only clear DNA profiles found belonged to the victims. Authorities obtained data on mobile telephone mast traffic and compared telephone activity near the apartment building and the court, and detected two telephone numbers present at both locations communicating only with each other by text message. The numbers had been activated a week before the attacks and deactivated soon afterwards. Police established that the same communication method and activation/ deactivation activity had taken place in the same area involving a further eight Dutch mobile telephone numbers. These methods are often used to evade detection. The data were used were used to disprove the suspects' alibis, and to link the mobile phones with the suspects. The court found that the data demonstrated 'with reasonable certainty that the owners of the telephone numbers were involved' in the crime.

Case 2 (Czech Republic)

Two masked men paralysed an employee of a security firm and stole three safe boxes containing over 14 million CZK (582 000 EUR) in cash. The men used a car driven by a third individual to get away before abandoning and setting fire to the vehicle at a remote location. Czech police obtained list of active calls at the place of attack and at the place where the getaway car had been purchased. By comparing the lists some active numbers were found to be the same. This led to further investigation on other numbers that were in contact on both places with the already identified numbers. Investigators would have been severely limited in their ability to pursue the case without access to the data.

Case 3 (Czech Republic)

A gang robbed Raiffeisen Bank in Chomutov and during escape fired guns at the police. Czech police were able to identify the perpetrators through analysis of the telephone calls made before and after the robbery.

Case 4 (Germany)

A taxi was ordered using fixed telephone line. The taxi arrived and was hailed by a woman. The taxi then stopped, and a man jumped out of nearby bushes and pointing a gun at him demanded the taxi driver's money. Both suspects (the man and the woman) escaped with the money. The investigation has proceded no further because the telephone provider said that the traffic data had been deleted and therefore an identification of the subscriber of the calling telephone line would not be possible.

Case 5 (Netherlands)

A group of 12 individuals was suspected of involvement in several cases of armed robbery, extortion and burglary in Netherlands in 2010. Using historical traffic police detected plans by the group to raid a house in Groessen, and the four were arrested in a car while en route to the house.

Case 6 (UK)

Police investigated (Operation Backfill) a series of armed robberies where high value cars were advertised on a website for sale for 'strictly cash only'. Persons interested in buying the cars went to meet the supposed traders and were robbed at gun point. Police examined internet data and identified the laptop and premises from where the suspects had logged onto the internet when posting the advertisements, leading to a number of arrests.

Burglary, theft and organised trafficking

Case 1 (Bulgaria)

In 2012 three mobile telephone operators provided data enabling detection of leaders of an organised group dealing in illegal acquisition and sale of moveable cultural property to Germany, Austria, Spain, Switzerland, Italy and USA.

Case 2 (Czech Republic)

In 2006 there were seven incidents in the Liberec region of the Czech Republic in which three individuals would remove ATMs and take them to another location where they would remove the cash and discard the machine, causing loss and damage of 40 million CRK (1.5 million EUR). Suspecting that mobile phones were used by the gang to coordinate the robberies, police acquired data showing that in four cases the same telephone numbers were involved. Investigators were able to connect suspects to the theft overall of 24 ATMs (totalling 100 million CRK or 4 million EUR).

Case 3 (Czech Republic)

In 2008 and 2009 there were a number of robberies targeting shops in the Vsetin and Zlin regions in which goods and cash to the value of 3 000 000 CRK (120 000 EUR) were stolen. Little evidence was left at the crime scene, so police analysed data from mobile communication which revealed the presence of the same telephone number and IMEI at two of the locations, leading to several arrests.

Case 4 (Denmark)

Investigators intercepted communications using a mobile telephone which had been stolen during a burglary, leading to a police raid on an abandoned property in which a large quantity of stolen goods was discovered. Further analysis of related historical communications data pointed to four members of a family from another European country that was already under suspicion in connection with various other offences, including a homicide. The investigation led to the discovery of a container of stolen goods valued at 2 700 000 DKK (362 000 EUR), and to the extradition and charge of one of the family members.

Case 5 (Denmark)

Four masked men broke into the home of an elderly couple using threatening behaviour to steal their car and obtain the PIN numbers for their credit cards. One of the offenders was soon afterwards arrested, and communications data connected to his mobile telephone revealed those with whom he had been in contact around the time of the robbery. Location data then enabled police to place three further suspects at the scene of the crime and at the ATM machine where the stolen cards had been used.

Cases 6-8 (Germany, Hungary, Poland)

Soray P. headed a criminal group engaged in fraud by pretending to be the granddaughter of hundreds of elderly people in Germany, Austria, Italy and Poland. German police issued a European Arrest Warrant in connection with crimes involving the theft of 400 000 EUR. Polish police were able to identify and arrest in August 2011 the woman through examining data relating to various telephone numbers over the course of several months. The investigation into a similar case involving 38 incidents in the Warmińsko-Mazurskie district and the theft of 48 000 EUR between June 2009 and January 2010 led to the conviction of Adam M. In a third example, Hungarian police began an investigation into telephone fraud in which a number of elderly persons in Budapest, Tolna and other areas regions had in 2009/2010 been tricked into handing over their savings. The perpetrators were identified by telephone service provider data. German police reported a similar set of incidents which could not be investigated because of the absence of telephone data.

Case 9 (Germany)

During three months prior to a burglary, residents noted random test calls made to their landline. Immediately after the burglary was committed a court order to identify the subscriber was obtained to get hold of the subscriber. But data had not been retained by the provider and the investigation has proceeded no further.

Case 10 (Germany)

After a spate of burglaries of residential properties, investigators discovered that over two-three months irregular 'test-calls' had been made to the houses which had been subsequently broken into. Immediately after the next similar burglary, a request was made to the telephone service provider for data on the recent callers to that house, but the data were no longer available.

Case 11 (Germany)

Police investigated a series of thefts of vehicles and expensive construction machines which were dismantled and their parts sold over an internet auction site. Orders for the release of retrograde communications data regarding mobile and fixed-line phones, revealed by the police in separate cases, were issued in connection with an investigation into gang-related trade in stolen property. Historical communications data was not available. Therefore the overall structure of the gang, the individuals and their places of handover, have not been identified. It was not possible to prove the meeting points for making arrangements on the basis of the coordinates.

Case 12 (Latvia)

Latvian police were able to connect a man using an anonymous pre-paid SIM card to a spate of robberies by analysing traffic data which enabled his girlfriend to be identified. The man was convicted on 17 counts of robberies.

Case 13 (Luxembourg)

A bank employee was found to have diverted customers' funds through the use of falsified documents. The accusation was brought before the prosecutor several months after the alleged offence. The plaintiff, one of the bank's customers, cited in evidence a telephone call to the bank, in which the customer expressed a wish to transfer to another bank. Traffic data was requested and obtained two weeks before the expiry of the applicable six month data retention period. On the basis of these data the prosecutor obtained and executed a search warrant on a travel agency for the purpose of locating the suspect who was subsequently arrested. During questioning the suspect implicated two others with whom he had been in contact by telephone. It was not possible to follow up on these leads as the data was no longer available, and investigation could not proceed further.

Case 14 (Luxembourg)

Victims of what is known as 'boiler room' scam, some of them resident outside Luxembourg, were approached by telephone and encouraged to buy shares which were claimed to be rising in value. Meanwhile the criminals perpetuating the scam manipulated the stock market by buying large volumes of shares at low prices thus artificially inflating the price of the shares. Investigators were able to identify and locate the suspects through obtaining telecommunications data. For several of the victims there was a time lag before they realised that they had been defrauded and reported the crime to the police, especially for those victims outside Luxembourg. These delays and the applicable data retention limit of six months have prevented law enforcement authorities from launching an international investigation into the extent of the fraud.

Case 15 (Poland)

Authorities in Białystok investigated cases of fraudulent insurance claims for cars which had been taken abroad and then reported as stolen. Communications data confirmed that contact had been established between the owners of the cars, and the people who crossed the border with them. The prosecutor could also confirm that during the time of the alleged theft of the vehicles, the owners were not in the place that they claimed to be the scene of the crime, but elsewhere where they handed over the vehicle to their accomplices.

Case 16 (Poland)

In an investigation into the theft from the Auschwitz-Birkenau national museum in December 2009 of a part of the main gate bearing the inscription *'Arbeit Macht Frei'*, police examined telephone logs from the area and identified a Swedish telephone number. Through mutual legal assistance agreement investigators obtained from Sweden data on telephone connections and subscribers, which enabled them to arrest and charge a number of suspects.

Case 17 (Spain)

Operation Olmo started in August 2009 and culminated in with the breaking up of an international criminal organisation involved in kidnappings, serious injuries, drugs trafficking, possession of illegal arms, threats, extortion, illegal detention, crimes against moral integrity, misappropriation of public office, violent robbery and intimidation, falsification of public documents, theft and break-in of vehicles, crimes against administration of justice, misappropriation of civil status, fraud and money laundering. Communications data enabled investigators to identify the time, duration and location of crimes committed leading to the trial of 34 individuals.[29]

Case 18 (Spain)

Operación Lentisco dismantled a criminal gang involved in burglaries of town halls and private properties, counterfeiting of currencies, violent robberies of industrial units and petrol stations, and extortion. Mobile telephony subscriber and traffic data were especially relevant as the gang constantly switched pre-paid cards and addresses. Twenty-two crimes were detected and 14 individuals were arrested, seven of whom were given prison sentences.[30]

Case 19 (Spain)

In 2009 a jewellers was robbed of diamonds valued at 10m EUR as result of a 'rip deal' confidence trick. It took Spanish investigators in cooperation with Interpol and police in France, Italy and Belgium six months to gather sufficient information to request court order for communications data, which eventually led to the identification and trial of seven individuals.[31]

Case 20 (Spain)

Operation Cobra dismantled an organised gang involved in burglaries disguised as police and Guardia Civil officers to gain the confidence of the victims and using balaclavas, scarves and gloves as well as signal and GPS jammers to escape detection. The leader of the group used a sawn-off shotgun in case his other intimidation methods were insufficient. Six individuals were arrested in connection with 45 incidents including one attempted homicide. Mobile telephony data were necessary to identify the culprits and their whereabouts.[32]

---

[29] http://www.policia.es/wap/prensa/20110518_1.html; http://www.policia.es/wap/prensa/20120301_1.html

[30] http://www.teleprensa.es/almeria-noticia-334247-desarticulada-una-organizacin-en-almera-especializada-en-robos-y-extorsiones-a-empresarios.html

[31] http://www.policia.es/prensa/20110629_1.html

[32] http://www.elmundo.es/elmundo/2012/02/03/andalucia/1328262438.html

Case 21 (Spain)

A series of incidents of internet fraud, falsification of credit cards and the collection, distribution and sale of stolen goods, took place in December 2007. Following a lead appearing in October 2008, police requested IP addresses which enabled the identification and location and subsequent wiretap of an ASDL, culminating in the arrest of 26 members and collaborators of a criminal gang in connection with around 500 offences.

Case 22 (Germany)

Five persons were suspected of being members of a group of smugglers. Their mobile telephone numbers could be identified but due to the absence of data retention, it was not possible to determine their location at the time of the smuggling or the identities of persons receiving calls from the suspects.

Case 23 (Sweden)

During 2003-2005 a team of at least four individuals drugged and robbed men in the nightclub district of Stockholm. They took the victims to their houses and stole everything of value and also stole money from their bank accounts. Telephone records demonstrated the suspects' presence in a number of different crime scenes throughout the period in question, and this was crucial to the prosecution of two of the perpetrators.

Case 24 (UK)

In October 2004 a large criminal network conspired to steal 229 million GBP (265 million EUR) from a bank in the City of London by transferring funds to bank accounts opened in seven different countries. Landline and mobile telephone communication data was critical to establishing those involved in this crime and understanding how it happened. The network members used landline, mobile, and kiosk phones in the UK and across multiple countries. Three defendants were extradited to the UK for trial. Billing data, call data and cell-site location data were all used as evidence in the trial which took place in March 2009. Three defendants were convicted of conspiracy to steal and two were convicted of money laundering.

Cybercrime

Case 1 (Denmark)

In March 2009 Danish police were notified by an online payment service provider that several customers' accounts had been hacked. Authorities in another state meanwhile reported that information on their credit cards had been disclosed in forums on the internet. Investigators identified three IP addresses belonging to two electronic communications service providers, which enabled the telephone service providers to identify the subscribers. This evidence led in 2009 to the conviction and sentencing to three years' imprisonment of a man for 19 separate offences, including computer fraud and attempted fraud, hacking, forgery and disclosure of stolen credit card information.

Case 2 (France)

In May 2009 a publically-funded regional body noticed a website was hosting a 'phishing' page which fraudulently redirected surfers into providing username and passwords for their

online bank accounts. A representative of the body in June 2009 reported this as an act of piracy to the French National Police. Technical queries run on a copy of the site in question revealed that the fraudulently acquired data were being sent in the form of an email to two active webmail accounts. The owners of these accounts were suspected of complicity with the pirates and a judicial warrant was issued on the webmail service. Details of access to these emails revealed a number of Moroccan IP addresses for the first account and a Paris-based company for the second. It appeared that the company was offering file-sharing services and internet anonymisation services. Interviews with the directors of the company and inspection of their equipment revealed two French IP addresses had been used to access the inbox. Investigators requested details of the user of these IP addresses from the French ISP and the response received in February 2010 identified two French nationals. Further investigation of the activities of these persons led in turn to a resident of Morocco who was profiting from the phishing page.

Case 3 (Germany)

German police received information from Luxemburg following the analysis of a seized Command and Control Server of a botnet which anonymised data and obtained the digital identities of unwitting users. 218 703 German IP addresses which had accessed this server were sent to the police to inform/warn the owners of the computers, but most of the requests for information subsequently submitted by the police authorities because the subscriber details had not been retained.

Case 4 (Poland)

In December 2009 there were a number of attempts to destroy, to damage, to remove or to hinder access to computer data being used to create a government website. The data were located on a servers administered by the Centre of the Prime Minister, the National Hydrological Services and the Geological Institute/ National Research Institute. Police arrested the perpetrator through identification of the computer's IP address.

Case 5 (Spain)

A group of hackers inadvertently installed botnet malware on around 13 million computers in various countries. This enabled between December 2009 and February 2010 the infiltration of denial-of-service actions where huge volumes of credit card data were obtained and a search engine was tricked as to the value of a web advert through the simulation of user click which in reality were automated by the botnet. Spanish police were requested by the authorities of another country to assist in the investigation, which required access to data which were up to one year old. The investigation is ongoing but at time of reporting had resulting in 10 arrests and three charges.[33]

Fraud

Case 1 (Czech Republic)

A person set up an e-shop which required advance payments but then did not deliver the goods which had been purchased. Over a short period customers were defrauded of thousands of CRK. The e-shop was operated for just a few weeks before it was shut down. The

[33] http://tecnologia.elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html

communication between the customers and perpetrator was through e-mails and electronic forms, and payments made by credit card and internet banking. Without data concerning internet access, it would not be possible to investigate this case.

Case 2 (Denmark)

In March 2009 Danish police was alerted by police in another Member State that an anonymous person had passed information on stolen credit cards in closed forums on the internet. The police launched in a background investigation of the case and identified three IP addresses that belonged to two electronic communications service providers. With a court order the North Jutland Police accessed the retained relevant IP addresses. Based on the information gathered the perpetrator was charged and sentenced to three years in prison on a total of 19 counts, including computer fraud and hacking and exchanging stolen goods.

Case 3 (Denmark)

That police were alerted by a Danish on-line payment service provider that several of their customers' accounts had been hacked and subsequently used to deposit money using stolen credit card information. The money was subsequently transferred from customers' accounts to an online poker account located outside Denmark, while a smaller portion of the proceeds were transferred to a Danish bank as winnings from online gambling. One particular IP address was used to log into all of the hacked accounts, so there was a presumption that there was one unidentified individual. It was known that this person had used various addresses in connection with registration with the online payment service provider, and the email providers were able to supply data for identifying the individual who was subsequently charged on further counts of hacking, computer fraud, forgery and the dissemination of credit card information.

Case 3 (France)

In November 2005, French National Police was charged with investigating and locating an individual, known as 'MGB', who was wanted following convictions by various courts on serious charges. The police investigations in 2006 and early 2007 centred on the family circle and close relations of MGB, and relied mainly on telephony. Interception of telephone communication did not provide any evidence of a connection between the fugitive and his family. In February 2007, the fugitive's sister, 'MB', was arrested on charges of organised fraud. The police obtained some information about the fugitive's sister, in particular her aliases and her immediate circle of friends/acquaintances. One of the aliases, 'LA', attracted the attention of the investigators. By cross-checking call records, it was shown that LA was in fact MGB. A detailed invoice for the telephone line of MGB, (registered under an assumed name) provided call data over a one year period. This enabled calls to Senegal in March 2006 to be highlighted and associated with the telephone number assigned to LA. As a result the investigation relating to the fugitive focused on calls to and from Senegal, thus enabling telephone numbers, obtained under assumed identities, to be identified as those of MGB's family. Subsequently, thanks to new judicial interceptions and the help of the in-country liaison officer in the country where he was hiding, MGB was formally identified, located, and arrested by local police in March 2007, and found to be in possession of falsified French identity documents using the alias 'LA'.

Case 4 (France)

In May 2008 police noticed an unusually large invoice caused by the diversion to premium-rate telephone lines of 10 telephone lines belonging to a ministry. These lines were being used intensively to obtain codes allowing pirates to access payable internet sites or to receive gifts. Initial investigations focused on the telephone architecture of the ministry and how it was possible to connect to it, through interviews with technicians and service providers. A large volume of information on incoming calls for these 10 lines indicated that there were 10 separate subscribers. During autumn 2008, these subscribers were identified. The details of their IP accounts were requested and obtained from the ISP in December 2008.

These data gave rise to a suspicion that two IP addresses were using a subscriber's SIP profile without his knowledge in order to connect to the ministerial private automatic branch exchange network (PABX) and to use it to call the premium rate numbers. The alleged offenders were therefore only identified in mid-December – about seven months after the discovery of the suspicious invoice.

Case 5 (Lithuania)

In 2010 a series of instances of telephone fraud were detected in Vilnius. Victims were approached by calls made from mobile telephones and were falsely informed about crimes that their relatives had allegedly committed or about disastrous events which had befallen their relatives. Victims were pressurised into surrendering money or other valuable possessions. A special police task force was set up to investigate the incidents. It took investigators several months to obtain and to analyse communications data, which enabled them to uncover a conspiracy including prisoners in Marijampole and who were involved in similar fraudulent activities in other Lithuanian towns. Eventually 18 individuals were arrested on suspicion of committing 29 counts of fraud totalling about 85 000 LTL (25 000 EUR).

Case 6 (Poland)

Polish citizens involved in the import via Germany into Poland of textiles, footwear and other goods from China and Vietnam were found to have evaded an estimated 100 million PLN (24 million EUR) per year in VAT payments. They used falsified documents and frequent switching of mobile phones and SIM cards to attempt to evade detection. Investigators' analysis of traffic data revealed connections to known members of a criminal group, and location data and IP addresses connected them to the place of delivery of the goods and computers used to send commercial documents.

DG Home

European Commission

March 2013

Productie 3

Inventarisatie Buitenland

Samengesteld op basis van informatie afkomstig uit openbare bronnen

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
Austria	The implementing legislation was annulled in July 2014, as a result of the ECJ ruling.	The Austrian Constitutional Court repealed the data retention law transposing Data Retention Directive. The ruling of the Court was issued on 19th of July and published on x of July, from this date its effects being mandatory. The Constitutional Court of Austria had – together with the High Court in Ireland and others - requested the European Court of Justice to examine the validity of the Data Retention Directive.				
Belgium	The implementing legislation is still in place.	In Belgium, the implementing legislation remains so far unaffected. An action for annulment is however pending before the Belgium Constitutional Court which will assess the legislation in light of the ECJ ruling. The Belgium government is of the opinion that the safeguards provided for in the legislation are in compliance with the requirements of the ECJ and that position will be defended. A decision of the Constitutional Court is expected early				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		2015.				
Bulgaria	The implementing legislation is still in place.	In December 2008, the Bulgarian Constitutional Court annulled the law transposing the Directive. Legislation was amended in February 2010 and in effect in May 2010. On 15 April 2014, the Bulgarian Ombudsman submitted a request to the Bulgarian Constitutional Court on the constitutionality of the Law on Electronic Communications Act. According to the Ombudsman, the national law that transposed the EU Directive is against the principles of the Bulgarian Constitution. The Bulgarian DPA has issued a statement with a similar message				
Croatia						
Cyprus		The Supreme Court of the Republic of Cyprus decided on 1 February 2011 that Arts. 4 and 5 of the Law on the Retention of Telecommunications Data for the Investigation into Criminal Offences (L.183(I)2007) are in breach of the Constitution. The Law on Retention of Telecommunications Data for the Purpose of Investigating Serious Criminal Offences, Law Number				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		183(I)/2007 (the 'POTD Act') is currently in effect.				
Czech Republic	The implementing legislation is still in place.	In March 2011, the Czech Constitutional Court annulled the law transposing the Directive on the basis that, as a measure which interfered with fundamental rights, it was insufficiently precise and clear in its formulation. Legislation was adjusted in November 2012. According to the Czech DPA the current national legislation has sufficient safeguards (put in place after the ruling of Czech constitutional court), although more improvements are possible (f.e. a retention period of 2 months instead of 6 months for some data). The Czech government will not open discussions on national legislation. The Association of Czech Mobile Operators has sent a letter to the Ministry of Industry and Ministry of Justice, asking for an impact assessment of the ECJ ruling. The Association has expressed concerns relating to conditions of access and data protection by relevant authorities.				
Denmark	The implementing	The Danish Ministry of Justice has evaluated the consequences of the ECJ				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
	legislation is still in place.	ruling for the Danish legislation on data retention in a memorandum (legal analysis)which has been sent to the Danish Parliament (only available in Danish- hyperlink xx). In the memorandum it is concluded that that the DK data retention legislation is in line with EU law (and the criteria of the judgment not to be cumulative). There is no reason to assume that the Danish legislation on data retention should be inconsistent with the Charter. However, at the same time DK repealed a provision which requires telecom providers to retain data on what home pages internet users look at (”session logging"). This provision did not fall within the scope of the DRD. However, recent media reports suggest that the Danish government is considering reintroducing session logging. Furthermore, the Danish Ministry of Justice is currently in the process of conducting a general review of the Danish legislation on data retention (which was already scheduled before the ECJ ruling). Following this review, the Danish Ministry of Justice will				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		submit a proposal for new legislation to the Danish Parliament in the next parliamentary session.				
Estonia						
Finland	The implementing legislation was amended for procedural reasons. Legislation for retaining and accessing data is still in place.	In Finland the legislation needed to be amended because it cannot be based anymore on the directive. The Constitutional Committee of Parliament had delivered its opinion on the proposal emphasizing that the ECJ decision had to be taken into account while amending legislation. In its' opinion there are several preconditions that have to be clarified in future legislation. Finnish regulation on information society - the Information Society Code ("the Code") - was approved on Friday 7 November 2014 and took effect on 1 January 2015. The original wording of the Code proposed more extensive retention of such data than previously required and would have enabled retention of data collected in context of browsing websites, for example. The Code's approach to data retention was not considered problematic by the Finnish Parliament in light of the aforementioned ruling of the European				Proposal in Parliament regarding procedural aspect of the ECJ ruling. Proposed amendments on other aspects?

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		Court of Justice, however, certain methods proposed in the original wording of the Code and some current data retention practices were limited in the final version of the Code.				
France	The implementing legislation is still in place.	Bewaart nog steeds (source: Dutch National Police)				
Germany	The implementing legislation was annulled in 2010, before the ECJ ruling.	The German Constitutional Court (Bundesverfassungsgericht) annulled the German Act transposing the DRD directive in 2010. The German Constitutional Court did not consider data retention unconstitutional as such, but found the law transposing the Directive to be unconstitutional since it did not sufficiently limit the circumstances in which law enforcement authorities could access the data, and did not contain sufficient measures to protect retained data against breaches of confidentiality (data security). Since then, no new Act has been adopted by the German Parliament. The German Minister of Justice announced in June 2014 that there won't be any				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		new national initiative for a new Act on DR at least until the COM has not taken any further steps on a European level. Thus, Germany will wait and see what the new COM is planning on that issue. On 15 January, the German Chancellor said in the lower house of parliament (Bundestag) that Germany should insist that the revision of the directive promised by the EU Commission is quickly completed.				
Greece						
Hungary	The implementing legislation is still in place.	The Hungarian DPA drafted an assessment of the national law, which according to the DPA is not in line with the ruling. The national government has not given any feedback to this assessment				
Ireland	The implementing legislation is still in place.	Proposal for amending legislation, specifically the retention period. Currently, the retention period is 24 months for phone and 12 months for internet (source: Dutch National Police). The High Court in Ireland has – together with the Constitutional Court of Austria and others - requested the European Court of Justice to examine the validity of the Data Retention Directive.				Proposal for amending retention period (now 24 months for phone and 12 months for internet)
Italy		The implementing legislation is still in				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		place. The implementing legislation is still in place. (source: Dutch National Police). The ministries of the Interior and Justice have assessed the national legislation. Their preliminary conclusion is that it is ok. There are concerns about the paragraphs of the Court on undifferentiated data (58-59) and on the location of the data (68) and whether this also has consequences for transfer of bulk data. The DPA finds that the Italian legislation is quite strict, as it was implemented under the supervision of the Italian DPA. The problem might however be the issue of indiscriminate retention.				
Latvia						
Lithuania						
Luxembourg						
Malta						
Netherlands	The implementing legislation is still in place.	A proposal to amend the legislation is being prepared. The Dutch data retention law will have its day in court on Feb. 18, when Dutch government is sued by a coalition of organisations to annul the legislation immediately. On Feb. 18, the District Court of the Hague will decide on the case.		Prior review by a prosecutor for traffic data.		Prior review by a court for traffic data.

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
Poland	The implementing legislation is still in place.	On 30 July 2014 the Polish Constitutional Court ruled on data retention legislation. It did not find data retention as such unconstitutional, but considered that there were not sufficient safeguards with regard to independent control, destruction of data etc in the Polish law. The government and parliament now have 18 months to change the law				
Portugal						
Romania	The implementing legislation was repealed in 2012.	Bij Roemenië was sprake van een volledige ongeldig verklaring in oktober 2009 waarna de wet is aangepast in mei 2012 (juni van kracht). The Romanian Court found in 2009 the law transposing the Directive to be ambiguous in its scope and purpose, with insufficient safeguards, and found, against that background, the obligation to retain data for a period of six months to be unconstitutional. In July 2014 the Romanian Constitutional Court repealed the law from 2012 transposing Data Retention Directive. The ruling of the RCC was issued on 8th of July 2014 and published on 3rd of Sept 2014, from this date its effects being mandatory.				
Slovakia	The	The Constitutional court has				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
	implementing legislation was temporarily suspended.	temporarily suspended data retention legislation until review on merits is completed.				
Slovenia	The implementing legislation was annulled in July 2014.	On 3 July 2014, the Constitutional Court ruled the data retention provisions of the Electronic Communications Act unconstitutional. The Court has decided that by introducing mandatory retention for traffic data, the Slovenian legislator has not carefully regulated the circumstances that guarantee that the interference is necessary to achieve the purpose and proportionate with the right of protection of personal data. Specifically, the Court argued that the national legislation: i) did not limit the data retention to a specific time period, geographical area or group of persons who may be in a certain relation with the aim pursued by the measure, ii) does not allow for anonymous use of means of communication for cases in which untraceable use is necessary to reach certain purposes (e.g. telephone services to assist mental distress), iii) did not explain the reasons for setting a retention period of 14 months for data				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		relating to publicly available telephone services and 8 months for other data, iv) did not limit the purpose of storage and processing of data only to the investigation, detection and prosecution of serious crime.				
Spain	The implementing legislation is still in place.	The Ministries of Justice and Interior have done a first analysis (non-binding) and have concluded national DR legislation seems to be ok. Telecommunication operators are retaining data without any further discussion.				
Sweden	The implementing legislation is still in place.	The inquiry has in a preliminary report concluded that Swedish legislation on the storage and disclosure of information keeps within the limits imposed by the European Union law's general principles and the obligation to respect fundamental rights. This conclusion notwithstanding, the inquiry also is of the opinion that given that EU law and European law only sets up certain minimum requirements for the protection of privacy that must be met by national law, there is reason to further consider some rule changes to further strengthen the protection of personal privacy. The Administrative Court of Stockholm			Prior review by a court for traffic data.	

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		has ruled on 13 October stating that there is no need to repeal Swedish legislation. According to the Court there are some weaknesses in the Swedish legislation (some provisions on retention period, access and security). However these weaknesses do not lead to the conclusion that the legislation is not proportionate, as these weaknesses are outweighed by other factors. The Court therefore considers the Swedish legislation to be compatible with the Charter, the ECHR and the e-Privacy Directive. Appeal is still possible at this stage of the proceedings. There has been little attention given to the ruling but the service and network providers have begun to store and provide data in accordance with the law.				
United Kingdom	The implementing legislation was amended for procedural reasons. Legislation for retaining and accessing data is still in place.	On 10 July, the Government announced emergency legislation, the Data Retention and Investigation Power Bill (DRIP), to maintain the capacity to retain and access telecommunications data after the invalidation of DRD. The UK has stated that no new powers or capabilities are introduced, and that at the same time oversight regimes and controls on who can have access are strengthened. The Bill also clarifies the				

			CURRENT LEGISLATION			NEW LEGISLATION
Country	**Status**		**Types of crime in**	**Prior review**	**Other conditions**	**Proposed amendments (if applicable)**
		extra-territorial effect of the interception and communications data provisions in RIPA (Regulation of Investigative Powers Act 2000). Despite critics from several members of both the House of Commons and House of Lords, the emergency legislation was voted on 15 July and was given the Royal Assent from the Queen on 17 July. The Open Rights Group has threatened legal action against the government and underlined that the UK has not adhered to the judgment of the ECJ. A complaint has been sent to the European Commission by various Privacy NGO's. The DRIP expires at the end of 2016.				

Productie 4

ARTICLE:

JUDGMENT IN THE CASE OF *K.U. V FINLAND:*

THE EUROPEAN COURT OF HUMAN RIGHTS REQUIRES ACCESS TO COMMUNICATIONS DATA TO IDENTIFY THE SENDER TO ENABLE EFFECTIVE CRIMINAL PROSECUTION IN SERIOUS VIOLATIONS OF PRIVATE LIFE

By **Tuomas Pöysti**

Introduction

The European Court of Human Rights (ECHR) has developed a system of human rights and fundamental rights and freedoms on the basis of the European Convention for the Protection of Human Rights and Fundamental Rights and Freedoms (Convention). The court's case law has opened new dimensions in the material definition of private life as a right to integrity and identity, and in the ways in which private life has to be protected by the domestic legal orders of the Contracting States of the European Convention. The ECHR case law should be compulsory reading for all lawyers specializing in ICT law (information and communication technology law or computer law) and law on electronic evidence. The judgments of the ECHR do not, however, always enjoy the attention they deserve by the specialised lawyers working in fields other than human rights law itself, and certainly not the attention of ITC experts and systems developers.

The ECHR has, in the 2008 judgment of the case of *K.U. v Finland*, further developed its case law concerning the protection of private life – the right to privacy – and the criminal law protection that the Contracting States to the European Convention should give to the right to private life.[1] *K.U. v Finland* is the second judgment during 2008 in applications brought against Finland concerning the positive obligations of the Contracting States to provide for the efficient and effective protection for the right to privacy, and to assure such protection in the context of information and communication systems. The first of these cases, the case of *I. v Finland* of 17 July 2008, concerns the security arrangements on the access to records of sensitive and confidential health data kept by a public hospital.[2] In this judgment, the ECHR stated that it is necessary to have such information security measures in place that provide practical and effective protection to exclude the possibility of unauthorized access from taking place in accordance with the provisions of article 8 of the European Convention of Human Rights. The second of these cases, the case of *K.U. v Finland*, concerns the use of criminal law in the protection of privacy. The ECHR found that the positive obligations of the Contracting States to ensure the protection of private life entailed an obligation to provide law enforcement agencies with the ability to obtain access to dynamic IP addresses and communication data[3] in order to identify a private person who has violated another individual's right to private life.

The ECHR judgment in *K.U. v Finland* contributes to the definition of the balance between the freedom and confidentiality of communications and anonymity over the internet, and the requirements of privacy and limitations of anonymity and confidentiality of communications. This judgment deserves wide international attention, even though it is not a Grand Chamber decision. It opens a new dimension in the case law, and takes position on an issue of interpretation felt particularly important by the court itself. This judgment is also noteworthy in respect of further developments of

[1] *K.U. v Finland, no. 2872/02, 2 December 2008.*
[2] *I. v Finland, no. 20511/03, 17 July 2008.*
[3] *Where the phrase 'communication or communications data' is used, it refers to data that is capable of identifying the sender and recipient of the communication.*

© Pario Communications Limited, 2009

It was claimed in the advertisement that he was looking for an intimate relationship with a boy of his age or older 'to show him the way'.

the obligations of legislators to follow societal and technical developments and amend legislation so as to provide an effective protection, and also to provide for electronic evidence for investigations of alleged violations.

If the judgment in the case of *K.U. v Finland* is set in the wider perspective of the ECHR case law, these requirements seem to go beyond criminal law. The court requires the provisions of a privacy friendly legal, information and communications infrastructure and architecture, which also provides for effective remedies. According to the judgment, an effective and efficient protection of private life and deterrence against violations of private life must be included in the information and communication architecture. The government and the legislator are required to ensure that legislation is up-to-date, and also to ensure that legislation is applicable and effectively applied in practice.

Factual background and the judgment

Material events and legal procedures in Finland

The events in the case of *K.U. v Finland* began on 15 March 1999. On this day, an unknown person placed an advertisement on a dating site on the internet in the name of a 12 year old boy, K.U. The advertisement mentioned the age and year of birth of the boy. It also gave a detailed description of his physical characteristics and a link to his website. This included his picture, and his telephone number, which was correct save for one digit. It was claimed in the advertisement that he was looking for an intimate relationship with a boy of his age or older 'to show him the way'. K.U. became aware of the advertisement when he received an e-mail from a man who proposed to meet him and 'to see what you want'. K.U.'s father requested the police to identify the person who placed the advertisement on the dating site in order to prefer criminal charges. The internet service provider refused to divulge the identity of the holder of the dynamic IP address in question, regarding itself bound by the confidentiality of communications as defined by law.

The police requested the District Court to issue an order to divulge the dynamic IP address and the identity of the holder of the IP address on the basis of the Criminal Investigations Act, Act no. 449/1987 (Esitutkintalaki 449/1987). On 19 January 2001, the District Court refused the order in the absence of an explicit legal provision authorising the court to order a service provider to disclose telecommunications data. According to the decision of the District Court, the Finnish legislation in force at the time allowed the police the right to obtain telecommunication data only in certain offences. The placing of the advertisement in this case would be categorised as a calumny under the Penal Code. The law in force in Finland at the material time did not refer to calumny in the list of offences in which the police had the right to obtain telecommunications data. On 14 March 2001, the Court of Appeal upheld the decision of the District Court. On 31 August 2001, the Supreme Court refused to leave appeal. The prosecutor in charge of the case decided, on 2 April 2001, that the managing director of the internet service provider could not be charged for the violation of the Personal Data Act no 523/1999 because the alleged offence was time-barred.[4]

The application in the European Court of Human Rights

On 1 January 2002, K.U. lodged an application in the European Court of Human Rights against Finland, alleging that the State had failed in its positive obligations to protect the applicant's right to respect for his private life under article 8 of the Convention.

The European Court of Human Rights exercises the

[4] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.95, p. 31-50 was implemented in Finland by Personal Data Act no 523/1999 (Henkilötietolaki 22.4.1999/523). The Personal Data Act is the general data protection statute in Finnish law and it gives effect to the provisions in section 10 of the Constitution of Finland, which requires that protection for personal data shall be provided by law.*

 © Pario Communications Limited, 2009

A person convicted of committing an act of calumny against another person by a derogatory statement or by another degrading act faced a maximum term of three months imprisonment if convicted.

highest and final instance jurisdiction on the interpretation of the European Convention on Human Rights. The ECHR assesses whether the law of the Contracting States to the Convention provides guarantees for human rights and fundamental freedoms as they are guaranteed in the Convention. The court focuses on the functioning of the legal order of Member States from the point of view of the protection of human rights.[5]

The ECHR, because it is the final court in terms of protection of the human rights and fundamental rights and freedoms, has an excessive case load. This explains, partly, the time it takes for the court to hear a case. In the case of K.U., the judgment was delivered six years after the application and over eight years after the material events took place. For the development of precedents in the context of the internet and ICT, six years is a very long time. The relevant legislation in the Contracting States has often changed in the meantime. This is also the situation in the case of K.U. However, the reasoning of the ECHR and the requirements it set out are valid and topical.

At the time of the events of the case, section 8 of the Finnish Constitution Act provided that everyone's right to private life is guaranteed. Paragraph 2 of section 8 of the Constitution Act provided for the inviolability of correspondence, telephone calls and other forms of confidential communications. The protection of Privacy and Data Security in Telecommunications Act (Act no 565/1999), which was repealed on 1 September 2004, provided for the protection of the confidentiality of data in relation to transmissions to a particular subscriber connection. Pursuant to section 18 of the Act, the police had the right to obtain data relating to the identity of a person for the purpose of investigating an offence referred to in listed sections of the Penal Code. Calumny was not in the list of the crimes referred to in this Act. The investigations by the police are covered by the Criminal Investigations Act (Act no. 449/1987) and Coercive Measures Act (Act no. 450/1987). At the time of the events of the case, chapter 5a, section 3 of the Coercive Measures Act provided that the police could, upon authorisation of a court, monitor the telecommunications connection in the suspect's possession or otherwise presumed to be in his use, if the information obtained by monitoring could be assumed to be very important for the investigation, and the alleged offence was punishable by imprisonment of not less than four months, or the suspected offence is an offence against a computer system using a terminal device, or a narcotics offence.

Telecommunications monitoring was, thus, allowed in some specific computer related crimes or in serious crimes. At the time of the events, calumny was defined in chapter 27, section 3a of the Penal Code (the provision was inserted to the Penal Code by Act no. 908/1974). A person convicted of committing an act of calumny against another person by a derogatory statement or by another degrading act faced a maximum term of three months imprisonment if convicted. The maximum sentence was four months if the calumny was committed in public or in print or disseminated in writing. Further provisions at that time in relation to chapter 27, section 3a were introduced in 1974 to the Finnish Penal Code as a reaction to the infringement of privacy by the mass media. Other offences against the honour of a person and defamation also had fines as minimum penalty and were not listed as offences in which the monitoring of telecommunications would have been possible.

The processing and publishing of sensitive information concerning sexual behaviour on an internet server without the person's consent was criminalised at the material time as a data protection offence in section 43 of the Personal Files Act (Henkilörekisterilaki 471/1987, criminal provisions were amended by act no 630/1995) and in chapter 38, section 9 of the Penal Code or as data protection violation in section 44 of the Personal Files Act. The publishing of information concerning sexual behaviour could also have caused

[5] *K.U. v Finland*, 44.

© Pario Communications Limited, 2009

liability and a claim for damages in accordance with the provisions of the Personal Files Act. At the material time of the events of the case, the legal position in Finland was that the criminal law did not provide very strong penalties or provide for coercive investigation methods in offences related to moral integrity or other immaterial values. This situation had also been criticized in the legal literature; the criminal law seemed to provide stronger and more comprehensive protection in classic crimes against life and physical integrity and property than in offences against moral integrity or other intangible values.

Since the events of the case, the Finnish law has been changed in many respects. The Constitutional provisions on human rights are substantially the same. The protection of private life is found in section 10 of the Constitution. Freedom of expression, which included a right to receive and send communications, is guaranteed in section 12 of the Constitution. The most significant change is that the Exercise of the Freedom of Expression in Mass Media Act no 460/2003 (Laki sananvapauden käyttämisestä joukkoviestinnässä 460/2003), which entered into force on 1 January 2004. This new act is widely applicable to internet activities. This act also provides access to communications data if the content of a message is of such kind that providing it to the public is a criminal offence. The provisions of section 17 of the Act sets out the conditions of the release of information relating to the identity of the person: a court may order the release of information required to identify a sender of a network message provided that there are reasonable grounds to believe that the contents of the message are such that providing it to the public is a criminal offence. The Act also requires the service provider to keep and record data identifying the sender and the contents of the messages for a certain time in order to ensure the practical implementation of both criminal and civil liability for the contents of the messages.

The general Act on the protection of personal data, the Personal Data Act, provides that a service provider is under a criminal liability to verify the identity of the sender before publishing an announcement on the web.[6] The Coercive Measures Act has been amended by Act no. 646/2003 concerning the definition and conditions of telecommunications surveillance. Disclosure of confidential information about the parties to telecommunications and communications data is only possible in respect of listed serious offences. These are generally offences for which the maximum penalty is at least four years of imprisonment, and certain other crimes including crimes against the functioning of computer systems. Defamation, calumny or the data protection offence in the form of failure of the network service provider to identify the sender of the message in accordance with the provisions of Personal Data Act do not belong to the offences in which a court may authorise surveillance. The Penal Code has been reformed concerning offences against confidentiality of communications and privacy. A new chapter 24 contains offences against privacy. Section 17 in the Exercise of Freedom of Expression in Mass Media Act remains the only provision in Finnish law of the disclosure of dynamic IP addresses or other communications data in cases of unauthorised distribution of information violating individual privacy. The sufficiency of these changes was also discussed shortly by the ECHR, since the Finnish government presented the argument that later legislative changes had rectified some of the alleged defects in the legal framework.

The government's arguments

The response of the Finnish government to the application in the case of *K.U. v Finland* rested on two essential arguments. First, a private individual interfered with the applicant's private life; it was not caused by a public authority. Second, the service provider of the dating service had an obligation to verify the identity of the person who had placed the advertisement. This duty was reinforced by provisions in the Penal Code and Personal Data Act, which made the failure to identify a person a criminal offence, and also established civil damages for the failure to respect the provisions on identity. According to the government, these provisions had sufficient deterrent effect and the State had, thus, taken measures required by the Convention to ensure the protection of private life. The government referred to the ECHR judgment in the case of *X and Y v Netherlands*, according to which the liability in damages could provide a sufficient deterrent effect.[7]

The government also drew attention to the fact that the criminal investigation in the case of K.U. was not successful because of the legislation, whose aim was to protect the freedom of expression and the right to anonymous expression that the fundamental right and freedom entails. The extensive protection to the

[6] *Section 48 of the Personal Data Act.*
[7] *ECHR judgment in the case of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91.*

© Pario Communications Limited, 2009

anonymity of internet messaging, which even covered messages interfering with another person's right to private life, was a mere side effect of the broad and vague concept of message. This definition of the concept of message made it, according to the government, impossible to exclude messages interfering with private life from other messages.

The government argued that the legislation concerning the protection of private life should be assessed in the light of the social context of the time, and that at the material time of the events the rapid increase on the use of the internet was only just beginning. Legislative arrangements undertaken after the material events of the case have, according to the government's argument, further strengthened the protection of private life in respect of the freedom of expression. Legislation thus reflects the legislator's reaction to social development and the need for protection.

The judgment of the court

The ECHR cited and reviewed the relevant Finnish legislation and took note of the legal changes since the events of the case. The court went on to cite relevant international materials, and emphasised the Council of Europe Recommendation No R (95) concerning criminal procedure law connected with information technology and the Council of Europe Convention on Cybercrime of 23 November 2004. The court also reviewed the some of the contents of the European Union Directive 2006/24/EC amending Directive 2002/58/EC, the Directive on Privacy and Electronic Communications, and the EC Electronic Communications Data Retention Directive 2006/24/EC which requires the Member States of the European Union to ensure, amongst other things, that data are available for the purpose of investigation, detection and the prosecution of serious crime in relation to the use of the internet and e-mail communications, such as the address of the subscriber or the registered user to whom an Internet Protocol (IP) address is allocated at the time of communication.[8]

The ECHR took particular note of the fact that in the case of K.U., a minor was the subject of an advertisement of a sexual nature. This created a stronger positive obligation on the legislator and other public authorities of a Contracting State to protect fundamental rights and freedoms, even in the relationships between private individuals. The court also pointed out that even though the material events of the case were qualified as calumny under the Finnish law, the case was essentially about the right to private life. The court preferred to assess the events and protection provided by the domestic legal order from that perspective. The situation was aggravated by the vulnerability caused by the relatively young age of K.U. at the time.[9] According to the court, children and other vulnerable individuals are entitled to State protection, in the form of an effective deterrence, from grave types of interference with essential aspects of their private life.[10]

The court reiterated its earlier case law that article 8 of the Convention does not only compel the State to abstain from arbitrary interference by public authorities to private life, but creates positive obligations to ensure the protection of private life.[11] These positive obligations may involve the adoption of measures designed to secure the respect for private life in the sphere of relations of individuals between themselves.[12]

The positive obligations to secure respect for private life extend to the horizontal relations between individuals, and are not only applicable in the vertical relations between individuals and public authorities. The court also recalled its earlier case law, according to which in cases where fundamental values and essential aspects of private life are at stake, efficient criminal law provisions are required.[13]

The court rejected the Finnish government's argument that the mere possibility of a criminal prosecution and the general prevention this possibility was sufficient protection of the right to private life. According to the court, the positive obligations may extend to the effectiveness of a criminal investigation.[14] The court considered that in the case of *K.U. v Finland*, a practical and effective protection required that effective steps be taken to identify and prosecute the perpetrator. In the case of K.U., such protection was not afforded, and

[8] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.*

[9] *K.U. v Finland, 41.*

[10] *K.U. v Finland, 46; the ECHR referred, in respect to this argument, to its judgment on Stubbings and Others v the United Kingdom, 22 October 1996, § 64, Reports 1996-IV.*

[11] *K.U. v Finland, 42. ECHR cited its judgment on the case of Airey v Ireland, judgment of 9 October 1979, Series A no 32, § 32.*

[12] *K.U. v Finland, 43.*

[13] *K. U. v Finland, 43; the ECHR cited its judgments on the case of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91, §§ 23-24 and 27, and the case of August v United Kingdom (dec.), no 36505/02, 21 January 2003 and M.C. v Bulgaria, no 39272/98, § 150, ECHR 2003-XII.*

[14] *K.U. v Finland, 46. The court referred to its earlier case law to judgments on the case of Osman v United Kingdom, judgment of 28 October 1998, Reports 1998-VIII, § 128 and the case of M.C. v Bulgaria, § 153.*

© Pario Communications Limited, 2009

hence there was a violation of right to private life in accordance with the Article 8 of the Convention.[15]

The assessment of the judgment

Substantive and timely topicality of the judgment

Technically, the case concerned conditions of access to the identity of the holder of a dynamic IP address assigned by the internet service provider to a subscriber. The questions concerning preventive surveillance and the storing of communications data is a live issue in many countries. This issue emerges increasingly as a subject in court proceedings. The human rights and fundamental rights and freedoms set limits to the surveillance, storing and use of communications data. The recording and retention of data for the purpose of investigation is, on most occasions, seen as a risk to privacy and other individual rights and freedoms. In difficult cases, the issue is, however, not of only of protecting individual rights against interference by surveillance and data retention, but, rather, of finding a correct balance between various parties and their fundamental rights and freedoms.

The balance between the various rights and liberties based on human rights and fundamental rights and freedoms depends on the context, and the weight given to the various arguments and rights is different depending on each situation. The standards of balancing are created in the legislation. The legislative response, as well as the application of the legislation, is subject to the standards that follow from the protection of human rights and fundamental rights and freedoms and, for the Contracting States of the European Convention, developed mainly by the European Court of Human Rights. The court itself admitted that States and legislators have a margin of appreciation concerning the choice of appropriate ways of ensuring the protection for human rights, but the margin of appreciation is circumscribed by the provisions of the Convention, and the court, in the interpretation of them, must have regard to changing conditions and respond to evolving convergence as to the standards to be achieved.[16]

The ECHR wanted to say that the standards controlling the legislators' use of discretion in ensuring protection are converging and tightening. In Europe, the jurisprudence of the ECHR increasingly determines the limits of the national law and the EC/EU law on electronic evidence. It also acts as a balance between privacy and freedom of expression and anonymity of expression, both in vertical relations between public authorities and individuals, and in horizontal relationships between individuals themselves. For this reason, domestic legislators must have a close look to the evolving jurisprudence of the ECHR.

The content and efficiency of the right to private life

The judgment in the case of *K.U. v Finland* does not bring significant additional elements to the definition of the concept of private life itself. In the judgment, the ECHR rather shortly refers to its already established case law on the matter, particularly to the judgment in the case of *X and Y v the Netherlands*. Private life covers and entails protection of the physical and moral integrity of the person. In the ECHR case law, integrity is also seen as a condition for physical and moral welfare. In the judgment in the case of *K.U. v Finland*, the court underlines the importance for the State to protect the physical and moral welfare of children because of their particular vulnerabilities.[17] The court emphasised the need to protect minors from the inappropriate processing of information concerning sexual behaviour and from approaches of potential sex offenders.[18] In the context of the case of *K.U. v Finland*, it is important also to recall that communications data, traffic data, and the retention of such data falls under the concept of private life in article 8 of the Convention. The ECHR has confirmed this in the judgment in the case of *Copland v the United Kingdom*.[19]

The court sent an important message by recalling that, contrary to the analyses under Finnish domestic law and courts, the issue was not about calumny and criminal investigation within the limits set by the principle of legality, but that the situation in the case should be analysed as concerning the protection of individual integrity and the right to private life. The court analysed the essential issues, and considered the balance between fundamental rights and freedoms from legal technicalities, which the domestic law had been focused upon.[20]

The court's assessment follows its earlier established case law. The ECHR has developed a broad definition of private life, and also underlined the point that the concept is not susceptible to an exhaustive definition. Private life covers, among other things, physical and psychological integrity of a person and several aspects

[15] *K.U. v Finland, 49 – 50.*

[16] *ECHR judgments in the case of K.U. v Finland, 44, and, in the case of Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI.*

[17] *X and Y v the Netherlands, § 22 and K.U. v Finland, 41.*

[18] *K.U. v Finland, 46.*

[19] *ECHR judgment on the case of Copland v the United Kingdom, no. 62617/00, §§ 41 – 44, 3 April 2007.*

[20] *K.U. v Finland, 41.*

© Pario Communications Limited, 2009

of the physical and social identity of a person.[21]

The wide definition of the concept of private life and, consequently, the wide duties of positive protection are also significant with regard to the eventual consequences of the application of the principles laid down in the ECHR case law, including the judgment in the case of *K.U. v Finland*, to the situations likely to arise, for example, in the social media. The social media is one of the environments where violations of privacy and information security similar to the material events in the case of *K.U. v Finland* are likely to arise in the near future for investigation and legal proceedings. The legislation and standard legal interpretations in many countries are not necessarily well adapted to treat with these kinds of problems. The law and the courts sometimes struggle to find a judicial angle from which to approach the violations of individual rights in the context of information and communication networks. In the case of *K.U. v Finland*, the ECHR provides some essential elements concerning legislation and the judicial approach concerning the assessment of the alleged violations of private life and unfair processing of personal information in such contexts of private and social networks.

Private life in the system of the European Convention is a wider concept than the right to informational self-determination, which is at the core of the rights defined by the EC Personal Data Directive 95/46/EC.[22] The wide, integrity-focused approach of the ECHR and the approach emphasising the right to informational self-determination complement each other in defining the elements of protection in the context of electronic communications and ICT systems. Together, these approaches create a powerful legal response to address some of the problems in the current ICT environment.

Non-existent or weak user-identification and authentication of the parties may easily create problems of fundamental rights and freedoms, and particularly the right to the integrity of private life. Personal data legislation can also be used to address these weaknesses. In Finland, identity and authentication have recently been raised as legal problems in the context of the short term, high interest consumer credit available through the mobile telephone, for example by text messaging (SMS). Two problems have become apparent in relation to the use of mobile telephones: loans directed to minors, and the fraudulent use of mobile telephones to purchase goods and services without the consent of the subscriber of the connection. The Data Protection Ombudsman, the national data protection authority, has emphasised the requirements of the EC Personal Data Directive and the Finnish Personal Data Act to properly identify and authenticate such consumer credit transactions.

Under the European Convention, the State has positive duties of protection, which also extend to physical and psychological integrity and the social identity of a person. The judgment in the case of *K.U. v Finland* can be interpreted to mean that legislation and public authorities have an obligation, following from article 8 of the European Convention, to arrange proper identification and authentication in electronic transactions when elements of personal integrity and identity are in question.

A substantial and significant point in the judgment in the case of *K.U. v Finland* is that the ECHR did not accept the wide protection given to the freedom of speech and anonymity of communications in the Finnish law of the time. The court recognised that freedom of expression and the protection of the confidentiality of communication are primary considerations, and that users of the internet must have guarantees for these rights to be respected. At the same time, the ECHR emphasised that the protection of the freedom of expression and anonymity of communications is not absolute, and must yield on occasion to other legitimate interests. The ECHR calls for a balance between various fundamental rights and freedoms and the rights and interests of various parties.

The requirement of a fair balancing between various interests and fundamental rights is strongly present in the case law of the European level constitutional courts in cases concerning access to communication data to establish responsibility and liability in relation to infractions of information-related rights. In the judgment on the case of *K.U. v Finland*, the ECHR clearly underlines that the balance is, in the fist place, for the legislator. The legislator is required to provide the framework for reconciling the various competing claims for protection.[23]

The European Court of Justice recalled the need to balance the various competing claims for the protection of different fundamental rights and freedoms in the judgment in Case C-275/06 *Productores de Música de*

[21] *For a short recollection of the various elements of the concept of private life in the case law of the ECHR, see the ECHR Grand Chamber judgment on case S and Marper v United Kingdom [GC], nos. 30562/04 and 30566/04, § 66.*

[22] *The Directive of the European Parliament and of the Council 95/46/EC of 24 October 1995 on the protection of individuals with regard the processing of personal data and the free movement of such data, OJ L 281, 23.11.1995, p. 31 – 50.*

[23] *K.U. v Finland, 49.*

España (Promusicae) v Telefónica de España SAU, judgment of 29 January 2008.[24] Case C-275/06 concerned, among other things, the interpretation of the EC Directive on Privacy and Electronic Communications 2002/58/EC in relation to the EC Copyright in the Information Society Directive 2001/29/EC and the rules concerning the effectiveness of the protection of copyright and the interpretation of the EU Charter on Fundamental Rights in this context.[25] The ECHR in turn referred to the EC Directive on Privacy and Electronic Communications 2002/58/EC in the arguments in the case of *K.U. v Finland*. The Directive on Privacy and Electronic Communications is, together with the Electronic Communications Data Retention Directive 2006/24/EC, a core part of the EU legislative framework for the protection and access to communications data.

The specific issue in the *Promusicae* case was the access to communications data held by the internet operator in an alleged infringement of copyright. In its judgment, the European Court of Justice underlined the need for the national courts to develop and apply such interpretations of EU Directives and national legislation implementing directives that enable the achievement of a fair and proper balance between various fundamental rights and freedoms. Concerning the interpretation of the EC Directive on Privacy and Electronic Communications, the European Court of Justice stated that neither the Directive on Privacy and Electronic Communications nor the EC Copyright Directives require the Member States to arrange for the retention of communications data in court proceedings that aimed at providing for liability under civil law. Directives do not exclude either form of retention if it is provided in national legislation and leads to a fair balance between various fundamental rights and freedoms, and respects the general principles of law, in particular the principle of proportionality. The European Court of Justice reminded Member States that pursuant to article 15 (1) of the EC Directive on Privacy and Electronic Communications, Member States are allowed to provide for exceptions on the confidentiality of communications data – among other things for the purposes of preventing, investigating and the prosecution of crime.[26]

Both the ECHR and the European Court of Justice, underline the role of the legislator to balance the competing fundamental rights and freedoms in various contexts. Since the context of the judgment of the European Court of Justice in case C-275/06 *Promusicae* was the interpretation of law in pending court proceedings, the ECJ went on to consider further specifications for the method of interpretation and role of the courts. In comparison, the ECHR, in the case of *K.U. v Finland*, considered the appropriateness of the protection given by the legislation at the time. The European Court of Justice went on to explain why EC law, in particular the Directive on Privacy and Electronic Communications, was fairly abstract and provided little direct guidance for a judge in a concrete case, but that this gap has to be filled by the State legislator and the national courts in interpreting the applicable EU and national legislation.[27]

To understand the European law concerning access to communication data, the judgments of the ECHR in the case of *K.U. v Finland*, and the European Court of Justice in Case C-275/06 *Promusicae*, should be read together. Apart from emphasising the role of legislators and the need to balance rights and duties, the European Court of Justice took up the particular role and methods of the interpreting judge and stated that the Union legislator had not provided for the retention of communications data in civil proceedings concerning infringements of copyright. EC Electronic Communications Data Retention Directive 2006/24/EC provides for the storage and retention of data linking a communication to an identity, and traffic data for the purposes of the investigations of crimes. The ECHR considered, in particular, that children, because of their vulnerabilities, require particular protection for the private life and right to physical and moral integrity and right to psychological security. The ECHR stated that sexual abuse of children is unquestionably an abhorrent type of wrongdoing.[28] In the context of sexual abuse, the State legislators should, to enable a fair and proper balance between competing claims for the protection of fundamental rights and freedoms, arrange for access to communication data to allow effective investigation of alleged offences. The assessment in the cases concerning infringement of copyright might be different.

[24] *Judgment of the European Court of Justice (Grand Chamber) of 29 January 2008 in C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU, ECR [2008] I-271.*

[25] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.*

[26] *Judgment of the European Court of Justice in C-275/06 Promusicae, paras 60 - 70.*

[27] *The European Court of Justice has extended this apology for abstract writing style to the EC Personal Data Directive 95/46/EC, see the judgment of the European Court of Justice of 7 May 2009 in Case C-553/07 College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, not yet reported in ECR.*

[28] *ECHR judgment in the case of K.U. v Finland, 49 and also the ECHR judgment in the case of Stubbings and Others v the United Kingdom, 22 October 1996, § 64, Reports 1996-IV.*

 © Pario Communications Limited, 2009

The ECHR and the European Court of Justice are right to emphasise the role of the legislator in balancing freedom of expression and the right to confidentiality of communications against the right to effective protection of private life. Legal certainty is improved when the framework for balancing can be read clearly from the legislation. This enhanced role of the legislator also fits well with the principles of democracy.

In practice, however, the ECHR sets very far-reaching duties and obligations on the State legislator, whereas the European Court of Justice seems to be more realistic about the possibilities the EC legislator has in the provision of guidance through abstract, universal norms to all potential conflicts and competing claims for protection in different circumstances that Member States face.[29]

A fairly detailed and far-reaching specification of the role and responsibilities of the Contracting State legislator by the ECHR in ensuring the protection of private life in the changing social and technological context is a very significant point in the judgment on the case of *K.U. v Finland*. The ECHR said the court was sensitive to the argument of the Finnish government that any legislative shortcoming should be seen in the light of its social context at the time. The court stated that it accepted the view of the difficulties involved in policing modern societies. The positive obligations to protect fundamental rights and freedoms should be interpreted in a way that does not impose an impossible or disproportionate burden on the legislator or authorities. The court recalled that another relevant consideration is to ensure that powers to control, prevent and investigate crime are exercised in a manner that fully respects the due process and other guarantees of the fundamental rights and freedoms, including guarantees on which the accused can rely on.[30]

The ECHR requires the legislator to ensure there are clear and well-defined expressions of the outcomes of the balance that must be taken in legislation. But the court also requires the respect of the principle of proportionality, and applies the principle of reasonableness according to which the positive obligations to ensure the protection of private life or other fundamental rights do not make it necessary to take measures that cause a disproportionate burden to the public authorities. The principle of proportionality applied by the ECHR provides that in the horizontal relations between individuals, the positive duties of protection should not create a disproportionate burden to other concerned private persons. These principles are fairly abstract, albeit they are easy to accept as guiding principles of balancing of the benefits, costs and burdens. A significant point in the judgment in the case of *K.U. v Finland*, is that (concurring with earlier case law) the ECHR defined the standards concerning measures that should be considered, and what counts as a disproportionate burden or difficulty in policing. A significant point is that this is, according to the court, a matter ultimately to be assessed by the ECHR from the perspective of the protection of human rights and fundamental rights and freedoms, albeit the legislator of the Contracting State has a margin of appreciation and is required to define the necessary and appropriate measures for the protection of fundamental rights.

The limitation of the State's margin of appreciation by the Convention and the principles laid down in the case law of the ECHR is not a novelty, but well established case law of the court.[31] Noticeable in the judgment in the case of *K.U. v Finland* is the extent of the control exerted by the ECHR over the choices made in State legislation. The court was sensitive to the Finnish government's argument about noting legislative shortcomings in the social context at the time, but the court considered that in 1999, when the material events of the case of K.U. took place, it was well known that the internet could be used for criminal purposes and that a wide-spread problem of the sexual abuse of children existed. The court went further to state that it could not be said that the government lacked the opportunity to put in place a system to protect children from being exposed via the internet. The court considered, thus, that the government of Finland had, in breaching article 8 of the Convention, failed to take measures that could provide practical and effective protection for the applicant's private life by enabling the authorities to identify and prosecute the person who had placed the offensive advertisement on the internet based dating service.[32]

The judgment can be read so that the ECHR places a particular obligation on the government and legislator of a Contracting State to follow societal and technical developments and risks, and to take such effective and practical action that are necessary to protect the human and fundamental rights and freedoms guaranteed by the Convention. The ECHR seems to require an active and systematic approach to learning about social

[29] *European Court of Justice in C-275/06 Promusicae, para 67, and also the judgment of the European Court of Justice in C-553/07 concerning the abstract writing style of the EC Personal Data Directive.*

[30] *K.U. v Finland, 48.*

[31] *The ECHR cited in the judgment in the case of K.U. v Finland its earlier judgment on the case of Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI, on the margin of appreciation see K.U. v Finland, 43 and 44.*

[32] *K.U. v Finland, 48.*

© Pario Communications Limited, 2009

problems and risks to fundamental rights, and to the management of risks to ensure the effective protection of fundamental rights.

The ECHR is certainly right to require such an approach in order to ensure a good level of protection of fundamental rights. This is a significant point for which all governments and legislatures should pay attention to. In many countries, there remain important caveats and items of out-dated legislation in the face of new models of network society and network based communications. Governments and legislatures can only adequately discharge this duty by combining a systematic information and communication technology assessment with a regular general effectiveness assessment of legislation and a review of legislation. The lack of such analyses may be a weak point for several governments. In a legal science perspective, a skills and analyses of ICT law and legal informatics is required.

Use of criminal law in the protection of private life and the requirement of efficient investigations

A significant point in the judgment in the case of *K.U. v Finland* is how far the positive duties for the protection of private life extended in the domain of criminal law. The deterrence by the mere general threat of sanctions was not considered a sufficient protection of private life. Following case law from the judgment in case of *Airey v Ireland*, the ECHR stated that article 8 of the Convention contains not only the negative obligation to refrain from interference with an individual's private life, but also the positive obligation to secure respect for private life in relations between individuals.[33] The Contracting States have a margin of appreciation on the choice of measures, but this margin of appreciation is controlled by the requirements set out in the Convention and developed in the case law of the court. The general requirement for the measures of protection is that they must be efficient. According to the court, this means that in grave acts against private life there should be practical and efficient criminal law measures available.[34] In *K.U. v Finland*, the scope of the acts in which efficient criminal law protection is required was extended to a situation that, according to the court, was not trivial but did not have the same seriousness as some of the situations cited in the earlier case law of the court.[35]

Criminal law is the instance of ultimate state power. Because of the restrictive and punitive character of the criminal law, the use of it and criminal policy is guided by the principle of the last resort (ultima ratio) of criminal law or, the subsidiarity of criminal law, according to which criminal law shall be used only as the measure of last resort when other, morally more acceptable measures are unable to provide sufficient and efficient protection. In several countries, the last resort of criminal law is recognised as a policy principle or policy guideline and in some, for example in Germany and as an application of the principle of proportionality in Finland, it is even recognised as a principle of constitutional law.[36]

In *K.U. v Finland* and in the earlier case law in which the requirement of the efficient criminal law protection is set, the ECHR does not seem to discuss the application of the last resort principle to the situations in the material events of cases. In the judgment of *K.U. v Finland*, the court explicitly rejected the Finnish government's argument that there were other means and remedies available to K.U., and moved on to require practical and efficient criminal law protection.

The court may be too optimistic about the possibilities of criminal law to provide efficient protection for the protection of identity and other essential aspects of private life. On the other hand, the court is right that essential aspects and values of private life need protection by criminal law and thereby recognised as the core values to be protected by the State. The protection of private life and the provision of secure physical, moral and psychological identities can be achieved by attempting to provide for proof of identity and authentication in ICT systems and information networks. Without dispute, there are the essential elements for the feeling of security for individuals.

The ECHR is right to emphasise this aspect and the duties of the State to provide protection against infractions of these rights related to the right to private life. However, the success rate of investigations in crimes conducted through anonymous messages on the internet is limited. This is the case in general in relation to all computer related crime. Pushing the requirements

[33] *ECHR judgments in the cases of K.U. v Finland, 42 and Airey v Ireland, judgment of 9 October 1979, Series A no. 32, § 32.*

[34] *ECHR judgments in the cases of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91, §§ 23-24 and 27 and M.C. v Bulgaria, no 39272/98, § 150, ECHR 2003-XII.*

[35] *K.U. v Finland, 43 and 44.*

[36] *In Germany the principle of last resort, the subsidiarity of criminal law is recognised as a principle in the judgments of the Federal Constitutional Court, see in particular judgment of the Federal Constitutional Court in BVerfGE 39, p. 1 (p.47) and BVerfGE 88, p. 203 (p. 257-258). Principle of last resort is discussed in legal literature in all Nordic (Scandinavian) Countries and it is recognised as policy guideline in the official policy documents of the government concerning drafting of criminal law in Sweden, Norway and Finland. In Finland, the Constitutional Law Committee of the Parliament, which is the highest interpreter of the abstract constitutionality of the proposed Acts of Parliament, requires an assessment if certain conduct is to be penalised and it is necessary for the attainment of the legal good, and the protection required cannot be achieved by other means.*

 © Pario Communications Limited, 2009

for criminal law protection too far may be problematic in the view of the last resort principle. Realising this approach in practice may require extensive police measures that may also become problematic in view of the balancing that is required between various rights and claims for protection. The ECHR is not beyond the reasonable limits of criminal law. The court emphasised that in the case of *K.U. v Finland*, the essential concern was the need to protect minors from sexual abuse, and here there are no problems with regard to the principle of proportionality and the principle of last resort of criminal law. However, a cautious reading of the ECHR case law will be needed in order not to widen, without proper thought, the scope of protection under the criminal law without considering alternative measures.

Given the international character of the problem of the sexual abuse of children and the internet, efficient solutions must of necessity be international in scope. This is indirectly recognised by the court, which presents in very a positive light the Council of Europe Convention on Cybercrime as the only wide international instrument that deals with computer and internet-related crime, and which also states that in the assessment of the efficiency of the protection of private life, the court has to take into account the evolving convergence of the standards to be achieved.[37]

Another domain in which problems of the practical effectiveness of user identity have emerged recently is the web-casting and publishing possibilities of the internet, such as YouTube. Such services can be used for anonymous connection, and it has not been possible for law enforcement agencies to identify the perpetrators of violent threats on the basis of the dynamic IP addresses that the publication service providers have disclosed. Traces end at a third country server providing anonymous services.[38] The principles laid down in the ECHR judgment on the case of *K.U. v Finland*, and in the EC Electronic Communications Data Retention Directive 2006/24/EC, or the Council of Europe Convention on Cybercrime, are efficient and effective only if the legislative measures to implement these principles are reasonably global and all countries have law enforcement functions with a sufficient level of integrity and rapidity to offer and provide effective international assistance for investigations.[39] A global problem in the global networks requires a global answer. Although the approach taken by the ECHR is sound and correct, the efficiency of the protection required by the ECHR may still be limited.

An important point in the judgment in the case of *K.U. v Finland* is that the ECHR rejected the Finnish government's argument that civil liability and deterrence caused by the general threat of criminal sanction – the general prevention – gave sufficient protection for private life. The court continued, in *K.U. v Finland*, to develop its case law further, that investigations and prosecution of the crime should be effective in practice, and only this practical effectiveness of criminal investigations provides the necessary level of protection when the physical and moral wellbeing of a child is at stake. The court considered, in particular, that the implementation of practical and effective protection required that effective steps should be taken to identify and prosecute the perpetrator. The overriding requirement of the confidentiality of communications data in the Finnish national law in force at the material time of the events of the case prevented the perpetrator from being identified and thus, also an effective investigation.[40]

A significant contribution of the judgment in the case of *K.U. v Finland* is the requirement of the practical effectiveness of investigations of alleged offences as part of the protection of private life in accordance with article 8 of the Convention. Here, the court went beyond the concept of effectiveness of an individual investigation, but sees success of the investigations in a wider perspective of efficiency of legal protection. The legal order and procedures protecting fundamental rights and freedoms have to be efficient as a system, and they must enable success in individual cases.

The idea of the practical effectiveness of rights and the availability of remedies is not a novelty as such. The practical effectiveness of rights and availability of remedies are, rather, part of the very concept of the rights in the system of the European Convention of Human Rights and in case law of the ECHR. This emphasis on the practical effectiveness has also made the European Convention one of the most successful international systems for the protection of human rights and fundamental rights and freedoms. The law does not remain in books, but the law is of practical protection to individuals.

The ECHR considered, in *K.U. v Finland*, that this general principle of practical effectiveness required the

[37] *K. U. v Finland, 24 and 44; see also ECHR judgment in Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI.*

[38] *This problem has emerged in the investigation of the threats of violence presented trough social media. The aliases behind the dynamic IP addresses assigned by a third country anonymous server have proven to be very difficult to investigate.*

[39] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63. The Council of Europe Convention on Cybercrime, opened for signatures on 23 November 2001, and the Additional Protocol to the Cybercrime Convention adopted in 2003.*

[40] *K.U v Finland, 48 and 49.*

© Pario Communications Limited, 2009

availability of appropriate and efficient means and methods of investigations of alleged crimes and a legal framework that provides the availability of such methods. This will have, if taken seriously and generalised, significant consequences for the law on evidence and access to electronic evidence. The court indicated that it is a requirement for the protection of fundamental rights and freedoms to store and retain electronic evidence, including communications data, and to provide for access to it in police investigations when essential aspects and values of private life are at issue, and the concern is about the protection of children or other persons with particular vulnerabilities. In the light of the case law of the ECHR, the police should also be provided with sufficient resources and expertise to carry out such investigations.

These requirements will add an important additional aspect to the legal and legislative debate about obtaining access to communication data and the surveillance of such data. The storing and retention of communications data is not only a threat to individual rights, on some occasions it is required for the protection of fundamental rights. In the case of *Copland v the United Kingdom*, the court set out some general criteria where access to communications data and communications surveillance may be granted under the European Convention of Human Rights.[41] The *K.U. v Finland* judgment complements this approach well.

The requirement set by the ECHR is a fair one, but not without difficulties in practice. In societies based on the rule of law, the criminal law and criminal justice system exist to protect the individual and his fundamental rights and freedoms. In recent developments, the functioning of the criminal law, criminal procedure and investigations, and the activities of the criminal justice system are increasingly analysed and defined from the perspective of their capacity to protect and respect fundamental rights and freedoms. The judgment in *K.U. v Finland* adds to this development. The Contracting States should, as a consequence, evaluate whether the criminal law and procedure and the law concerning access to communication data and other significant sources of electronic evidence correspond to the test of being able to provide effective practical protection – and beyond that, to guarantee the overall efficiency of the protection of fundamental rights and freedoms. But it is necessary to be cautious about not falling into the fallacy of believing that criminal law and criminal investigations alone could provide sufficient protection for the essential aspects and values of private life.

Effect beyond the criminal law: privacy-friendly information and communication infrastructure

In the case of *K.U. v Finland*, the ECHR required an effective means of identifying the person who placed the advertisement. Indirectly, this requirement means that both the legislation and the information and communication infrastructure, including the ICT architecture, should provide for the reliable identification and authentication of the parties to a communication, and access to past communications data. In the other recent case on private life, where Finland was the responding government and where a violation of the right to private life was also found, the case of *I. v Finland*, the ECHR stated, at 47, that: 'What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place. Such protection was not given here.' In this context, it is necessary to provide for the proper security of IT and archive systems, including the requirement of an effective audit. In *I. v Finland*, the ICT system failed to record who had been obtaining access to and consulting confidential files, access to files was not restricted only to those members of the staff who were responsible for the treatment of a particular individual. These failures were considered to constitute a breach of private life.[42] The judgment in *I. v Finland* makes it clear that the obligations of the State are to ensure that confidential data stored in an ICT system must be held securely; only authorized personnel may be given access to the data, and it should be subject to effective audits. Similar obligations also exist concerning the identity and recording of communications data and the traffic data.

A picture emerges from the ECHR judgments by which the court makes it clear that an information and communication infrastructure and ICT architecture, including the software code and functions, should be designed to protect fundamental rights and freedoms. Proper information and communications security is an essential element of this infrastructure and architecture. Keeping logs and transaction records, secure storage and controlled access to communications identification and traffic data, and reliable and secure identification and authentication of the parties of communications are part of this infrastructure and architecture that emerge

[41] *ECHR judgment in Copland v the United Kingdom, 3 April 2007, no. 62617/00, §§ 45 – 48.*

[42] *I. v Finland, judgment of 17 July 2008, no. 20511/03.*

 © Pario Communications Limited, 2009

from the ECHR case law. The court has contributed significantly to providing strong and highly authoritative human rights foundations for the development of the general principles of ICT law, or to the general doctrines and principles of legal informatics, to guide planning and management of information and communication systems and networks. The Contracting State is required to provide a practically effective legal framework for such rights-friendly infrastructure.

The first consequences of this should be that the functioning of the anonymous servers, that is servers providing a system that aims to make the identity of the parties to communications difficult or impossible, should be critically assessed in all countries. On many occasions, anonymity is compatible with the requirements of fundamental rights and freedoms, but not in all cases. The anonymity of the communications over the internet should be put into a wider and more critical perspective. Secondly and even more significantly, the enforcement of the Data Protection laws requiring confirmation of identity and authentication should be assessed and strengthened, and legislative caveats corrected. Thirdly, legislators have the duty to provide an effective response to the risks to secure identity. The last issue is an old theme in the literature in computer and ICT law – in this, the ECHR has not provided any additional arguments and foundations for such an approach.

Conclusions

The judgment in the case of *K.U. v Finland* is significant, because it requires Contracting States to ensure high quality IT systems are in place in order to provide for the positive obligations of the protection of private life in relations between individuals themselves. In addition, the court also requires Contracting States to have practical and effective legal protection in place, including criminal sanctions, to provide for the protection of private life. This judgment requires governments and legislators to follow societal and technological developments, and to ensure that the legislation in force can provide effective protection. The court extended the principle of practical effectiveness of protection and its implication to require practical effectiveness of investigations to cover electronic evidence and information necessary to identify the perpetrator of the alleged offence. Legislators are required to provide for access to communication data, and governments should ensure the conditions for successful criminal investigations in cases where essential values and elements of private life are at risk. The protection of children against sexual abuse through the internet is essential, because values and elements of private life are in danger, and the right to freedom of expression and anonymity of communications must be over-ridden when dealing with such cases for the benefit of effective investigation. The court has also indirectly defined further general requirements based on human rights and fundamental rights and freedoms concerning the principles of ICT law. In particular it is now necessary (although it has always been so) to consider the implications for security surrounding the identity of parties to communications and the retention of communications data. The ECHR addresses actual and difficult issues relating to crimes occurring in the context of the internet and the need to identify the parties to communications, and also the conditions for success in criminal investigations of serious computer and cyber crime. The ECHR has, in the case of *K.U. v Finland*, contributed to the development of European and international law on electronic evidence and the protection of private life through criminal law.

© Tuomas Pöysti, 2009

Dr Tuomas Pöysti is the Auditor-General of Finland, President of the National Audit Office of Finland and Permanent Advisor of the Government Advisory Board for Better Regulation. Dr Pöysti is a Docent of Administrative law at the University of Helsinki, teaches advanced courses on ICT and European criminal law and has an extensive list of scientific publications on information law.

http://www.vtv.fi
tuomas.poysti@vtv.fi