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**