



**СЪВЕТ НА
ЕВРОПЕЙСКИЯ СЪЮЗ**

**Брюксел, 19 април 2011 г. (03.05)
(OR. en)**

9324/11

**DAPIX 38
TELECOM 47
COPEN 85**

ПРИДРУЖИТЕЛНО ПИСМО

От: Генералния секретар на Европейската комисия,
подписано от г-н Jordi AYET PUIGARNAU, директор

Дата на получаване: 18 април 2011 г.

До: Г-н Pierre de BOISSIEU, генерален секретар на Съвета на
Европейския съюз

№ док. Ком.: COM(2011) 225 окончателен

Относно: Доклад на Комисията до Съвета и Европейския парламент
— Доклад за оценка на директивата за запазване на данни
(Директива 2006/24/ЕО)

Приложено се изпраща на делегациите документ на Комисията COM(2011) 225 окончателен.

Приложение: COM(2011) 225 окончателен



ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 18.4.2011
COM(2011) 225 окончателен

ДОКЛАД НА КОМИСИЯТА ДО СЪВЕТА И ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

Доклад за оценка на директивата за запазване на данни (Директива 2006/24/ЕО)

ДОКЛАД НА КОМИСИЯТА ДО СЪВЕТА И ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

Доклад за оценка на директивата за запазване на данни (Директива 2006/24/ЕО)

1. ВЪВЕДЕНИЕ

Съгласно директивата за запазване на данни¹ (наричана по-долу „директивата“) от държавите-членки се изисква да задължат доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи (наричани по-долу „оператори“) да запазват данни за трафика и за местоположението за периоди от шест месеца до две години за целите на разследването, разкриването и преследването на сериозни престъпления.

В съответствие с член 14 от директивата в настоящия доклад на Комисията се оценява прилагането на директивата от държавите-членки и нейното въздействие върху икономическите оператори и потребителите, като се взема предвид по-нататъшното развитие на технологиите в електронните съобщения и статистиката, предоставена на Комисията, с оглед да се определи дали е необходимо изменение на разпоредбите на директивата, в частност по отношение на обхвата на данните и периодите на запазване. В настоящия доклад се проучват и последиците от директивата за основните права с оглед на критиките, които бяха изразени срещу запазването на данни като цяло, и се проучва дали е необходимо предприемане на мерки във връзка с опасенията, свързани с използването на анонимни SIM карти за престъпни цели².

Като цяло оценката показва, че запазването на данни е ценен инструмент за системите на наказателно правосъдие и за правоприлагането в ЕС. Приносът на директивата за хармонизиране на запазването на данни е ограничен по отношение например на ограничението на целите и периодите на запазване, както и в областта на възстановяването на разходи, направени от операторите, което е извън обхвата на директивата. Предвид последиците и рисковете за вътрешния пазар и за зачитането на правото на неприкосновеност на личния живот и защитата на личните данни, ЕС следва да продължи да гарантира чрез общи правила постоянно поддържане на високи стандарти за съхранението, извличането и използването на данни за трафика и за местоположението. В контекста на тези заключения Комисията възнамерява да предложи изменения на директивата въз основа на оценката на въздействието.

¹ Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 13.4.2006 г., стр. 54—63).

² Заключения на Съвета относно борбата с престъпната злоупотреба и анонимното използване на електронни съобщения, 2908-о заседание на Съвета по правосъдие и вътрешни работи — Брюксел, 27—28 ноември 2008 г.

2. КОНТЕКСТ НА НАСТОЯЩАТА ОЦЕНКА

Настоящият доклад за оценка се основава на пространни обсъждания с държавите-членки, експерти и заинтересовани страни и информация от тяхна страна.

През май 2009 г. Комисията организира конференция под надслов „Към оценяване на директивата за запазване на данни“, на която присъстваха представители на органи за защита на данните, частния сектор, гражданското общество и академичните среди. През септември 2009 г. Комисията изпрати въпросник на заинтересовани страни от тези групи, на който получи около 70 отговора³. Комисията организира втора конференция през декември 2010 г. на тема „Прилагане на директивата за запазване на данни“, на която присъстваха подобни категории от заинтересовани страни, с цел споделяне на предварителните оценки във връзка с директивата и обсъждане на бъдещи предизвикателства в тази сфера.

Между октомври 2009 г. и март 2010 г. Комисията се среща с представители на всяка държава-членка и асоциирана към Европейското икономическо пространство държава, за да обсъди по-подробно въпросите, свързани с прилагането на директивата. Държавите-членки започнаха да прилагат директивата по-късно от очакваното, по-специално по отношение на свързаните с интернет данни. В резултат на забавяне при транспонирането девет държави-членки бяха в състояние да предоставят на Комисията пълни статистически данни за 2008 г. или 2009 г., както се изисква съгласно член 10 от директивата, а общо 19 държави-членки предоставиха непълни данни (вж. раздел 4.7). През юли 2010 г. Комисията изпрати искания до държавите-членки за допълнителна количествена и качествена информация, свързана с необходимостта от запазване на данни с цел постигане на резултати в правоприлагането. Десет държави-членки отговориха с подробни данни относно специфични случаи, в които данните са се оказали необходими⁴.

Настоящият доклад се основава на становищата, приети от „Платформата за запазване на електронни данни за целите на разследването, разкриването и съдебното преследване на тежки престъпления“⁵ от нейното създаване през 2008 г. насам. Комисията взе под внимание докладите на Работната група за защита на данните по член 29⁶, и по-специално доклада относно второто действие по принудително

³ Отговорите са публикувани на уебсайта на Комисията http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm.

⁴ Белгия, Чешката република, Кипър, Литва, Унгария, Нидерландия, Полша, Словения и Обединеното кралство. Швеция също така посочи няколко случая на конкретни сериозни престъпления, при които данни за трафика за предишни периоди, които са били налични въпреки липсата на задължение за запазване на данните, е било от решаващо значение за издаването на осъдителни присъди.

⁵ Тази експертна група беше създадена съгласно Решение 2008/324/ЕО на Комисията (ОВ L 111, 23.4.2008 г., стр. 11—14). Комисията редовно провежда срещи с групата. Нейните становища са публикувани на http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm.

⁶ Работната група за защита на лицата при обработването на лични данни беше създадена съгласно член 29 от директивата за защита на данните (Директива 95/46/ЕО на Европейския парламент и на Съвета от 24.10.1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., стр. 31).

изпълнение, т.е. нейната оценка на спазването на изискванията на директивата⁷ за защита на данните и сигурност на данните от страна на държавите-членки.

3. ЗАПАЗВАНЕ НА ДАННИ В ЕВРОПЕЙСКИЯ СЪЮЗ

3.1. Запазване на данни за целите на наказателното правосъдие и правоприлагането

Доставчиците на услуги и на мрежи (наричани по-долу „оператори“) в хода на своята дейност обработват лични данни с цел предаване на съобщения, фактуриране, плащания при взаимна връзка, маркетинг и някои други услуги с добавена стойност. Тази обработка включва данни, които показват източника, местоназначението, датата, времето, продължителността и вида на съобщението, както и съобщителното оборудване на ползвателите, а при мобилната телефония — и данни за местоположението на оборудването. По смисъла на Директива 2002/58/ЕО за правото на неприкосновеност на личния живот в сектора на електронните комуникации (наричана по-долу „директива за правото на неприкосновеност на личния живот и електронни комуникации“) ⁸ такива данни за трафика, създадени при използването на електронни съобщителни услуги, по принцип трябва да се заличават или да се правят анонимни, когато вече не са нужни за предаване на съобщения, освен когато и доколкото са необходими с цел фактуриране или когато е получено съгласието на абоната или ползвателя. Данни за местоположението могат да се обработват само ако се направят анонимни или със съгласието на съответния потребител, до степен и с продължителност, които са необходими за предоставяне на услуга с добавена стойност.

Преди влизането в сила на директивата и при определени условия, националните органи отправяха искане до операторите за достъп до такива данни, например с цел идентифициране на абонати, които използват даден IP адрес, анализ на съобщителни дейности и установяване на местоположението на мобилен телефон.

На равнище ЕС запазването и използването на данни за целите на правоприлагането беше разгледано за първи път в Директива 97/66/ЕО относно обработката на лични данни и защитата на неприкосновеността на личния живот в телекомуникационния сектор. В тази директива за първи път беше предвидена възможност държавите-членки да приемат такива законодателни мерки, когато са необходими за защита на обществената сигурност, отбраната или обществения ред, включително

⁷ Доклад 01/2010 относно второто съвместно действие по принудително изпълнение: Спазване на задълженията на национално ниво от страна на доставчиците на далекосъобщителни услуги и доставчиците на интернет услуги, наложени съгласно националното законодателство за запазване на данни за трафика въз основа на правното основание на членове 6 и 9 от Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации и Директива 2006/24/ЕО за запазване на данни, с която се изменя директивата за правото на неприкосновеност на личния живот и електронни комуникации (WP 172), 13.7.2010 г., (вж. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

⁸ Директива на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37—47).

икономическото благосъстояние на държавата, когато дейностите са свързани с държавната сигурност и прилагането на наказателното законодателство⁹.

Тази разпоредба беше допълнително развита в директивата за правото на неприкосновеност на личния живот и електронни комуникации, в която се предвижда възможност държавите-членки да приемат законодателни мерки, с които се отклоняват от принципа за поверителност на съобщенията, включително при определени условия запазването на, както и достъпа до и използването на данни за целите на правоприлагането. Член 15, параграф 1 позволява на държавите-членки да ограничат правата и задълженията за неприкосновеност на личния живот, включително чрез запазването на данни за ограничен период, когато такова ограничение представлява „необходима, подходяща и пропорционална мярка в рамките на демократичното общество, за да се гарантират националната сигурност (т.е. държавната сигурност), отбраната, обществената безопасност и превенцията, разследването, разкриването и съдебното преследване на престъпленията или на непозволеното използване на електронната комуникационна система“.

Ролята на запазените данни в системите на наказателно правосъдие и в правоприлагането се разглежда допълнително в раздел 5.

3.2. Цел и правно основание на директивата за запазване на данни

В резултат на разпоредбите на Директива 97/66/ЕО и на директивата за правото на неприкосновеност на личния живот и електронни комуникации, които позволяват на държавите-членки да приемат законодателство относно запазването на данни, операторите в някои държави-членки бяха задължени да закупят оборудване за запазване на данни и да наемат персонал, който да извлича данни от името на правоприлагащите органи, докато тези в други държави-членки не бяха задължени, като това доведе до нарушения на вътрешния пазар. Освен това поради тенденциите в бизнес моделите и предлагането на услуги, например ръстът на фиксираните тарифи, предплатените и безплатните електронни съобщителни услуги, операторите постепенно спряха да съхраняват данни за трафика и местоположението за целите на фактурирането и следователно намаля наличността на такива данни за целите на наказателното правосъдие и правоприлагането. Терористичните атаки в Мадрид през 2004 г. и в Лондон през 2005 г. направиха по-неотложни обсъжданията на равнище ЕС на справянето с тези проблеми.

В този контекст чрез директивата за запазване на данни беше наложено задължение на държавите-членки, съгласно което доставчиците на обществено достъпни електронни съобщителни услуги и на обществени съобщителни мрежи трябва да запазват съобщителни данни за целите на разследването, разкриването и преследването на сериозни престъпления, както са определени от всяка държава-членка в националното ѝ законодателство, и беше направен опит за хармонизиране навсякъде в ЕС на някои свързани въпроси.

⁹ Член 14, параграф 1 от Директива 97/66/ЕО на Европейския парламент и на Съвета от 15 декември 1997 г. относно обработката на лични данни и защитата на неприкосновеността на личния живот в телекомуникационния сектор (ОВ L 24, 30.1.1998 г., стр. 1—8).

Директивата измени член 15, параграф 1 от директивата за правото на неприкосновеност на личния живот и електронни комуникации, като добави параграф, в който се посочва, че член 15, параграф 1 не се прилага по отношение на данни, запазени съгласно директивата за запазване на данни¹⁰. Следователно държавите-членки (както е посочено в съображение 12 от директивата) продължават да могат да се отклоняват от принципа за поверителност на съобщенията. Директивата (за запазване на данни) урежда само запазването на данни за по-ограничените цели на разследване, разкриване и преследване на сериозни престъпления.

Тази сложна правна връзка между директивата и директивата за правото на неприкосновеност на личния живот и електронни комуникации, съчетана с липсата на определение на понятието „сериозни престъпления“ и в двете директиви, затруднява разграничаването от една страна на мерки, предприети от държавите-членки за транспониране на задълженията за запазване на данни, определени в директивата, и от друга страна по-общата практика на държавите-членки да запазват данни, разрешена съгласно член 15, параграф 1 от директивата за правото на неприкосновеност на личния живот и електронни комуникации¹¹. Това се разглежда допълнително в раздел 4.

Директивата се основава на член 95 от Договора за създаване на Европейската общност (заменен с член 114 от Договора за функционирането на Европейския съюз) относно създаването и функционирането на вътрешния пазар. След приемането на директивата нейното правно основание беше оспорено пред Съда на Европейския съюз на основание, че основната цел е разследване, разкриване и преследване на сериозни престъпления. Съдът постанови, че директивата урежда дейности, които са независими от прилагането на каквато и да е форма на полицейско и съдебно сътрудничество по наказателноправни въпроси и че не хармонизира нито достъпа до данните от страна на компетентните национални органи, нито използването и обмена на тези данни между посочените органи. Поради това Съдът заключи, че директивата се отнася основно до дейността на доставчиците на услуги в съответния сектор от вътрешния пазар. В съответствие с това той потвърди правното основание¹².

3.3. Съхраняване на данни

Запазването на данни е различно от съхраняването на данни (известно още като „quick freeze“), съгласно което операторите, на които се връчва съдебно разпореждане, са длъжни да запазват данни, свързани само с конкретни лица, заподозрени в извършване на престъпна дейност, считано от датата на разпореждането за съхраняване на данни.

¹⁰ Член 11 от директивата гласи: „В член 15 от Директива 2002/58/ЕО се добавя следният параграф: „1а. Параграф 1 не се прилага по отношение на данни, специално изисквани от Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. относно запазването на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи, които се запазват за целите, посочени в член 1, параграф 1 от посочената директива.“

¹¹ Работната група по член 29 поставя въпроса дали „целта на директивата [за запазване на данни] е била дерогация от общото задължение [за] заличаване на данни за трафика при приключване на електронното съобщение или даване на мандат за запазване на всички тези данни, които доставчиците вече са били упълномощени да съхраняват за свои собствени бизнес цели.“

¹² Решение на Съда на ЕС от 10 февруари 2009 г. по дело Ирландия/Европейски парламент и Съвет на Европейския съюз, C-301/6, Сборник, стр. I-00593.

Съхраняването на данни е един от инструментите за разследване, предвидени и използвани от държавите, участващи в Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство¹³. Почти всички участващи държави са създали звено за контакт, чиято роля е да гарантира осигуряване на незабавно съдействие при разследвания или производства във връзка с престъпления в кибернетичното пространство. Изглежда обаче не всички страни по конвенцията са въвели разпоредби за съхраняване на данни и все още няма оценка на това колко ефективен е моделът за справяне с престъпленията в кибернетичното пространство¹⁴. Наскоро беше разработен нов вид съхраняване на данни, наричан „quick freeze plus“. Този модел излиза извън рамките на съхраняването на данни, тъй като съдът може да даде достъп до данни, които все още не са били заличени от операторите. Също така ще има много ограничено законово освобождаване от задължението за заличаване, за кратък период от време, на някои съобщителни данни, които по принцип не се съхраняват, като например данни за местоположението, данни за интернет връзката и динамични IP адреси за ползватели, които имат фиксиран абонамент и при които няма нужда от съхранение на данни с цел фактуриране.

Поддръжниците на съхраняването на данни го считат за по-лека форма на нарушаване на неприкосновеността на личния живот от запазването на данни. Повечето държави-членки обаче смятат, че никой вид съхраняване на данни не би могъл адекватно да замести запазването на данни, като посочват, че докато запазването на данни води до наличност на данни за предишни периоди, съхраняването на данни не гарантира възможност за установяване на доказателствени следи преди издаването на разпореждане за съхраняване на данни, не дава възможност за извършване на разследване, когато обектът му е неизвестен, и не дава възможност за събиране на доказателства например за движението на жертви или свидетели на престъпление¹⁵.

4. ТРАНСПОНИРАНЕ НА ДИРЕКТИВАТА ЗА ЗАПАЗВАНЕ НА ДАННИ

Държавите-членки бяха длъжни да транспонират директивата преди 15 септември 2007 г. с възможност прилагането на задълженията за запазване на данни по отношение на интернет достъп, електронна поща по интернет и интернет телефония да бъде отложено до 15 март 2009 г.

Анализът, който следва по-долу, се основава на уведомленията за транспониране, които Комисията получи от 25 държави-членки, включително от Белгия, която е транспонирала директивата само частично¹⁶. В Австрия и Швеция проектозаконите

¹³ Член 16 от Конвенцията за престъпления в кибернетичното пространство (<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>)

¹⁴ Източник: Съвет на Европа.

¹⁵ Това беше също така потвърдено от Конституционния съд на Германия в решението му за отмяна на германския закон за транспониране на директивата (вж. раздел 4.9) (Федерален конституционен съд (Bundesverfassungsgericht), 1 BvR 256/08 от 2 март 2010 г., параграф 208).

¹⁶ Двадесет и петте държави-членки, които уведомиха Комисията за транспонирането на директивата, са Белгия, България, Чешката република, Дания, Германия, Гърция, Естония, Ирландия, Испания, Франция, Италия, Кипър, Латвия, Литва, Люксембург, Унгария, Малта, Нидерландия, Полша, Португалия, Румъния, Словения, Словакия, Финландия и Обединеното кралство. Белгия уведоми Комисията, че проектозаконът, който ще завърши транспонирането, все още се разглежда в парламента.

понастоящем се обсъждат. В тези две държави-членки няма задължение за запазване на данните, но правоприлагащите органи могат и в действителност отправят искания и получават данни за трафика от операторите, доколкото тези данни са налични. След първоначалното уведомление за транспониране от страна на Чешката република, Германия и Румъния, конституционните им съдилища отмениха националните закони, с които се транспонира директивата¹⁷, и сега те обмислят как отново да транспонират директивата.

В настоящия раздел се анализира как държавите-членки са транспонирали съответните разпоредби на директивата. Освен това в него се проучва дали държавите-членки са избрали да възстановяват разходите, направени от операторите за запазване и даване на възможност за извличане на данни, за което няма разпоредба в директивата, и се разглежда съотносимостта към директивата на решенията на конституционните съдилища на Германия, Румъния и Чешката република.

4.1. Цел на запазването на данни (член 1)

Директивата задължава държавите-членки да приемат мерки, с които да гарантират, че се запазват данни и те са достъпни за целите на разследването, разкриването и преследването на сериозни престъпления, както те са определени в националното право на всяка държава-членка. Въпреки това целите, посочени за запазването и/или достъпа до данни в националните законодателства, продължават да се различават в рамките на ЕС. Десет държави-членки (България, Естония, Ирландия, Гърция, Испания, Литва, Люксембург, Унгария, Нидерландия, Финландия) са определили „сериозни престъпления“ във връзка с налагането на наказание лишаване от свобода за определен минимален срок, във връзка с възможността за налагане на наказание лишаване от свобода или във връзка със списък от престъпления, определени на друго място в националното законодателство. Осем държави-членки (Белгия, Дания, Франция, Италия, Латвия, Полша, Словакия, Словения) изискват запазване на данни не само за разследване, разкриване и преследване на сериозни престъпления, но и във връзка с всички престъпления и с цел наказателна превенция или на общи основания, свързани с националната, държавната и/или обществената сигурност. В законодателството на четири държави-членки (Кипър, Малта, Португалия, Обединеното кралство) има позоваване на „сериозно престъпление“ или „сериозно нарушение“, без то да се определя. Подробеностите са изложени в таблица 1.

¹⁷ Решение № 1258 от 8 октомври 2009 г. на Конституционния съд на Румъния, Държавен вестник на Румъния № 789 от 23 ноември 2009 г.; Решение на Конституционния съд на Германия (Bundesverfassungsgericht) 1 BvR 256/08 от 2 март 2010 г.; Държавен вестник от 1 април 2011 г., Решение на Конституционния съд от 22 март относно разпоредбите на член 97, алинеи 3 и 4 от Закон № 127/2005 Сб. за електронните съобщения и за изменение на някои свързани закони, изменен, и Указ № 485/2005 Сб. за запазването на данни и предаването им на компетентните органи.

Таблица 1: Ограничение на целите на запазването на данни в националните законодателства	
Белгия	За разследване и преследване на престъпления, преследване на злоупотреби с телефонните номера за спешно повикване, разследване на квалифицирани злоупотреби с електронни съобщителни мрежи или услуги, за целите на разузнавателни мисии, извършвани от разузнавателните служби и службите за сигурност ¹⁸ .
България	„За нуждите на разкриването и разследването на тежки престъпления и престъпления по чл. 319а—319е от Наказателния кодекс, както и за издирване на лица.“ ¹⁹
Чешката република	Директивата не е транспонирана.
Дания	За разследване и преследване на престъпни деяния ²⁰ .
Германия	Директивата не е транспонирана.
Естония	Може да се използва, ако събирането на доказателства чрез други процесуални действия е преклудирано или твърде усложнено и предметът на наказателното производство е престъпление [от първа степен или умишлено извършено престъпление от втора степен с наказание лишаване от свобода най-малко три години] ²¹ .
Ирландия	За предотвратяване на сериозни престъпления [т.е. престъпления, които се наказват с лишаване от свобода за срок от 5 години или повече, или престъпления, изброени в приложението към Закона за транспониране], защита на сигурността на държавата и спасяването на човешки живот ²² .
Гърция	За целите на разкриването на особено сериозни престъпления ²³ .
Испания	За разкриване, разследване и преследване на сериозните престъпления, посочени в Наказателния кодекс или в специалните наказателни закони ²⁴ .
Франция	За разкриване, разследване и преследване на престъпления и единствено с цел предоставяне на необходимата информация на съдебните органи, както и за предотвратяване на терористични актове и защита на интелектуалната собственост ²⁵ .
Италия	За разкриване на и борба с престъпленията ²⁶ .
Кипър	За разследване на сериозни престъпления ²⁷ .

¹⁸ Член 126, алинея 1 от Закона от 13 юни 2005 г. за електронните съобщения. .

¹⁹ Член 250а, алинея 2 от Закона за електронните съобщения (изменен) от 2010 г.

²⁰ Член 1 от Наредбата за запазване на данните.

²¹ Член 110, алинея 1 от Наказателно-процесуалния кодекс.

²² Член 6 от Закона за съобщенията (Закон за запазването на данни) от 2011 г.

²³ Такива престъпления са определени в член 4 от Закон 2225/1994 и в член 1 от Закон 3917/2011.

²⁴ Член 1, алинея 1 от Закон 25/2007.

²⁵ Законите, които уреждат използването на запазени данни съответно за престъпления, за предотвратяване на терористични актове и за защита на интелектуалната собственост, са както следва: Член L.34-1, параграф II от Кодекса за пощите и електронните съобщения (CPCE), Закон № 2006-64 от 23 януари 2006 г. и Закон № 2009-669 от 12 юни 2009 г.

²⁶ Член 132, алинея 1 от Кодекс за защита на данните.

²⁷ Член 4, алинея 1 от Закон 183(1)/2007.

Таблица 1: Ограничение на целите на запазването на данни в националните законодателства	
Латвия	За защита на държавната и обществената сигурност или за осигуряване на разследването на престъпления, наказателното преследване и съдебните наказателни производства ²⁸ .
Литва	За разследване, разкриване и преследване на сериозни и много сериозни престъпления, определени в Наказателния кодекс на Литва ²⁹ .
Люксембург	За разкриване, разследване и преследване на престъпления, които се наказват с лишаване от свобода за срок от една година или повече ³⁰ .
Унгария	За да се даде възможност на разследващите органи, прокуратурата, съдилищата и националните агенции за сигурност да изпълняват своите задължения и да се даде възможност на полицията и на Националната данъчна и митническа служба да разследват умишлени престъпления, които се наказват с две или повече години лишаване от свобода ³¹ .
Малта	За разследване, разкриване или преследване на сериозни престъпления ³² .
Нидерландия	<i>За разследване и преследване на сериозни престъпления, за които може да бъде наложено наказание лишаване от свобода³³.</i>
Австрия	Директивата не е транспонирана.
Полша	За предотвратяване или разкриване на престъпления, за предотвратяване и разкриване на данъчни престъпления, за използване от прокурори и съдилища, ако данните са подходящи за провежданото съдебно производство, с цел изпълнение на задачите на Агенцията за вътрешна сигурност, Агенцията за чуждестранно разузнаване, Централното антикорупционно бюро, службите за военно контраразузнаване и службите за военно разузнаване ³⁴ .
Португалия	За разследване, разкриване и преследване на сериозни престъпления ³⁵ .
Румъния	Директивата не е транспонирана.
Словения	За гарантиране на националната сигурност, конституционното управление и сигурността, политическите и икономическите интереси на държавата ... и за целите на националната отбрана ³⁶ .
Словакия	За предотвратяване, разследване, разкриване и преследване на престъпления ³⁷ .
Финландия	За разследване, разкриване и преследване на сериозни престъпления, определени в глава 5а, член 3, алинея 1 от Закона за принудителните мерки ³⁸ .

²⁸ Член 71, алинея 1 от Закона за електронните съобщения.

²⁹ Член 65 от Закон X-1835.

³⁰ Член 1, алинея 1 от Закона от 24 юли 2010 г.

³¹ За общите цели на запазването на данни член 159/А от Закон С/2003, изменен със Закон CLXXIV/2007; за целите на достъп на полицията член 68 от Закон XXXIV/1994; за целите на достъп на Националната данъчна и митническа служба член 59 от Закон СXXII/2010.

³² Член 20, алинея 1 от Законово известие 198/2008.

³³ Член 126 от Наказателно-процесуалния кодекс.

³⁴ Член 180а от Закона за далекосъобщенията от 16 юли 2004 г., изменен с член 1 от Закона от 24 април 2009 г.

³⁵ Член 1, алинея 3, точка 1 от Закон 32/2008.

³⁶ Член 170а, алинея 1 от Закона за електронните съобщения.

³⁷ Член 59а, алинея 6 от Закона за електронните съобщения.

Таблица 1: Ограничение на целите на запазването на данни в националните законодателства	
Швеция	Директивата не е транспонирана.
Обединеното кралство	За разследване, разкриване и преследване на сериозни престъпления ³⁹ .

Съгласно своето законодателство повечето от държавите-членки, които транспонираха директивата, позволяват достъпа до и използването на запазени данни за цели, които надхвърлят определените в директивата цели, включително предотвратяване и борба с престъпността като цяло и риска за живота и здравето. Макар това да се допуска съгласно директивата за правото на неприкосновеност на личния живот и електронни комуникации, степента на хармонизиране, постигната от законодателството на ЕС в тази област, остава ограничена. Целите на запазването на данни се различават в отделните държави, което вероятно ще се отрази на обема и честотата на исканията, а това на свой ред — на разходите, направени за спазване на задълженията, предвидените в директивата. Освен това тази ситуация може да не гарантира в достатъчна степен предвидимостта, което е условие на всяка законодателна мярка, ограничаваща правото на неприкосновеност на личния живот⁴⁰. Комисията ще направи оценка на необходимостта и вариантите за постигане на по-голяма степен на хармонизиране в тази област⁴¹.

4.2. Оператори, които са длъжни да спазват изискването за запазване на данни (член 1)

Директивата се прилага по отношение на „доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи“ (член 1, параграф 1). Две държави-членки (Финландия и Обединеното кралство) не изискват от малките оператори да запазват данни, защото, както твърдят те, разходите за доставчика и за държавата от това действие са по-големи от ползите за системите на наказателно правосъдие и за правоприлагането. Четири държави-членки (Латвия, Люксембург, Нидерландия и Полша) докладват, че са въвели алтернативни административни договорености. Докато големите оператори, които извършват дейност в няколко държави-членки, се възползват от икономии от мащаба от гледна точка на разходите, по-малките оператори в някои държави-членки с цел намаляване на разходите си са склонни да създават съвместни предприятия или да възлагат част от своите дейности на външни изпълнители, специализирани в запазването и извличането

³⁸ Член 14а, алинея 1 от Закона за електронните съобщения.

³⁹ Наредбите за запазване на данните (директива на ЕО) от 2009 г. (2009 № 859).

⁴⁰ Решение на Съда на Европейския съюз от 20 май 2003 г. по съединени дела C-465/00, C-138/01 и C-139/01 (преюдициално запитване от Verfassungsgerichtshof и Oberster Gerichtshof): Rechnungshof (C-465/00)/Österreichischer Rundfunk и други, и Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01)/Österreichischer Rundfunk (защита на физическите лица при обработването на лични данни — Директива 95/46/ЕО — защита на личния живот — разкриване на данни за дохода на служителите на органи, подлежащи на контрол от Rechnungshof).

⁴¹ При приемането на директивата Комисията публикува декларация, в която се предлага да бъде използван списъкът с престъпления от европейската заповед за арест. (Рамково решение 2002/584/ПВР на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите-членки.)

на данни. По този начин възлагането на технически дейности на външни изпълнители не се отразява върху задължението на доставчиците да извършват надлежен контрол на операциите по обработка и да гарантират, че изискуемите мерки за сигурност са налице, което може да бъде проблематично, особено за по-малките оператори. Комисията ще разгледа въпросите за сигурността на данните и въздействието им върху малките и средните предприятия във връзка с възможните варианти за изменение на правната рамка на запазването на данни.

4.3. Достъп до данни: органи, процедури и условия (член 4)

Държавите-членки са длъжни „да гарантират, че [запазените данни] се предоставят само на компетентните национални органи в специфични случаи и в съответствие с националното право“. Държавите-членки сами определят в своето национално право „процедурите, които трябва да бъдат следвани, и условията, които трябва да бъдат изпълнени, за да се получи достъп до запазените данни, в съответствие с изискванията за необходимост и съразмерност, [...] при условията на съответните разпоредби на правото на Европейския съюз или на публичното международно право, и в частност на Европейската конвенция за правата на човека, така както тя се тълкува от Европейския съд за правата на човека“.

Във всички държави-членки националните полицейски служби и, с изключение на юрисдикциите по общото право (Ирландия и Обединеното кралство), прокурорите имат достъп до запазените данни. Четиринадесет държави-членки посочват службите за сигурност или разузнаване или въоръжените сили сред компетентните органи. Шест държави-членки посочват данъчни и/или митнически органи, а три посочват гранични органи. Една държава-членка допуска други публични органи да имат достъп до данните, ако са упълномощени във връзка със специфични цели съгласно вторичното законодателство. Единадесет държави-членки изискват съдебно разрешение за всяко искане за достъп до запазени данни. В три държави-членки съдебно разрешение се изисква в повечето случаи. Четири други държави-членки изискват разрешение от по-висш орган, но не от съдия. В две държави-членки изглежда единственото условие е искането да е в писмен вид.

Таблица 2: Достъп до запазени далекосъобщителни данни		
	<i>Компетентни национални органи</i>	<i>Процедури и условия</i>
Белгия	Звеното за съдебна координация, разследващите магистрати, прокуратурата и криминалната полиция.	Достъпът трябва да се разреши от магистрат или прокурор. При поискване операторите трябва да предоставят в „реално време“ данни за абонатите и данни за трафика и местоположението за обаждания, направени в рамките на последния месец. Данни за по-стари обаждания трябва да се

Таблица 2: Достъп до запазени далекосъобщителни данни		
	Компетентни национални органи	Процедури и условия
		предоставят във възможно най-кратък срок.
България ⁴²	Определени дирекции и отдели на Държавна агенция „Национална сигурност“ и на Министерството на вътрешните работи, службите „Военна информация“ и „Военна полиция“ към министъра на отбраната, Националната разузнавателна служба, както и съда и органите на досъдебното производство при определени условия.	Достъпът е възможен само с разпореждане от председателя на районния съд.
Чешката република	Директивата не е транспонирана.	
Дания ⁴³	Полицията.	За достъпа се изисква съдебно разрешение; съдебни разпореждания се издават, ако искането отговаря на строги критерии относно подозрение, необходимост и пропорционалност.
Германия	Директивата не е транспонирана.	
Естония ⁴⁴	Национален съвет „Полиция и гранична охрана“, Национален съвет „Охранителна полиция“ и, за предмети и електронни съобщения — Съвет „Данъчни и митнически въпроси“.	За достъпа се изисква разрешение от съдията, който провежда предварителното разследване. Операторите трябва „да предоставят [запазените данни] в спешни случаи не по-късно от 10 часа, а в другите случаи в срок от 10 работни дни [от получаване на искането]“.
Ирландия ⁴⁵	Членовете на Garda Síochána (полицията) с ранг на старши полицейски служител или по-висок; служителите на редовните въоръжени сили (<i>Permanent Defence Force</i>) с ранг полковник или по-висок; служителите на данъчната администрация (<i>Revenue Commissioners</i>) на длъжност ръководител или по-висока.	Исканията трябва да са в писмен вид.
Гърция ⁴⁶	Съдебните, военните или полицейските публични органи.	За достъпа се изисква съдебно решение, в което се посочва, че разследването чрез други средства е невъзможно или изключително трудно.
Испания ⁴⁷	Полицейските органи, компетентни за разкриването, разследването и преследването на сериозни престъпления, Центъра за национално разузнаване и Агенция „Митници“.	За достъпа до тези данни от компетентните национални органи се изисква предварително съдебно разрешение.
Франция ⁴⁸	Прокуратурата и определени служители на полицията и жандармерията.	Полицията трябва да представи обосновка за всяко искане за достъп до запазени данни

⁴² Член 250б, алинея 1 от Закона за електронните съобщения (изменен) от 2010 г. (органи); Член 250б, алинея 1 и член 250в, алинея 1 от Закона за електронните съобщения (изменен) от 2010 г. (достъп).

⁴³ Член 71 от Закона за съдебната власт.

⁴⁴ Член 112, алинеи 2 и 3 от Наказателно-процесуалния кодекс (относно органите и процедурата); Член 111, алинея 9 от Закона за електронните съобщения (относно условията).

⁴⁵ Член 6 от Проектозакона за съобщенията (запазване на данни) от 2009 г.

⁴⁶ Членове 3 и 4 от Закон 2225/94.

⁴⁷ Членове 6—7 от Закон 25/2007.

Таблица 2: Достъп до запазени далекосъобщителни данни		
	Компетентни национални органи	Процедури и условия
		и трябва да поиска разрешение от съответния служител в Министерство на вътрешните работи, определен от Националната комисия за контрол на електронните прихващания за целите на националната сигурност (<i>Commission nationale de contrôle des interceptions de sécurité</i>). Исканията за достъп се обработват от определен служител, работещ за оператора.
Италия ⁴⁹	Прокуратурата, полицията и защитника на ответника или на разследваното лице.	За достъпа се изисква „мотивирано разпореждане“, издадено от прокурора.
Кипър ⁵⁰	Съдилищата, прокуратурата и полицията.	Достъпът трябва да бъде одобрен от прокурор, ако същият счита, че така може да се осигурят доказателства за извършено сериозно престъпление. Съдия може да издаде такова разпореждане, ако е налице основателно подозрение за извършено сериозно престъпление и ако е вероятно данните да бъдат свързани с него.
Латвия ⁵¹	Упълномощените служители на институциите за досъдебно разследване, лицата, които извършват действия по разследване, упълномощените служители на институциите за държавна сигурност, прокуратурата и съдилища.	Упълномощените служители, прокуратурата и съдилищата са длъжни да оценят „адекватността и уместността“ на искането, да го запишат и да гарантират защитата на получените данни. Упълномощените органи могат да подпишат споразумение с оператор, например за криптиране на предоставените данни.
Литва ⁵²	Органите за досъдебно разследване, прокуратурата, съдилищата (съдиите) и служителите от разузнаването.	Упълномощените публични органи трябва да отправят писмено искане за запазените данни. За достъпа за досъдебни разследвания е необходимо съдебно разпореждане.
Люксембург ⁵³	Съдебните органи (разследващите магистрати, прокурорите), органите, отговорни за защита на държавната сигурност, за отбраната, за обществената сигурност и за предотвратяване, разследване, разкриване и преследване на престъпления.	За достъпа се изисква съдебно разрешение.
Унгария ⁵⁴	Полицията, Националната данъчна и митническа служба, службите за национална сигурност, прокуратурата и съдилищата.	Полицията и Националната данъчна и митническа служба изискват разрешение от прокурор. Прокуратурата и агенциите за национална сигурност имат достъп до такива данни без

⁴⁸ Членове 60-1 и 60-2 от Наказателно-процесуалния кодекс (органи); член L.31-1-1 (условия).

⁴⁹ Член 132, алинея 3 от Кодекса за защита на данните.

⁵⁰ Член 4, алинея 2 и член 4, алинея 4 от Закон 183(I)/2007.

⁵¹ Член 71, алинея 1 от Закона за електронните съобщения (органи); Постановление на Министерски съвет № 820 (процедури).

⁵² Член 77, алинеи 1 и 2 от Закон X-1835; устен доклад до Комисията.

⁵³ Член 5-2, алинея 1 и член 9, алинея 2 от Закона от 24 юли 2010 г. (органи); член 67-1 от Кодекса за наказателно разследване (условия).

Таблица 2: Достъп до запазени далекосъобщителни данни		
	Компетентни национални органи	Процедури и условия
		съдебно разпореждане.
Малта ⁵⁵	Полицейските служби на Малта; Службата за сигурност.	Исканията трябва да са в писмен вид.
Нидерландия ⁵⁶	Разследващият полицейски служител.	Достъпът се извършва с разпореждане на прокурор или разследващ съдия.
Австрия	Директивата не е транспонирана.	
Полша ⁵⁷	Полицията, граничната охрана, данъчните инспектори, Агенцията за вътрешна сигурност, Агенцията за чуждестранно разузнаване, Централното антикорупционно бюро, службите за военно контраразузнаване, службите за военно разузнаване, съдилищата и прокуратурата.	Исканията трябва да се отправят в писмена форма и по отношение на полицията, граничната охрана и данъчните инспектори трябва да се получи разрешение от старшия служител в организацията.
Португалия ⁵⁸	Криминалната полиция, Националната републиканска гвардия, Службата за обществена сигурност, военната криминална полиция, Службата за имиграция и гранична охрана и морската полиция.	За предаването на данни се изисква съдебно разрешение на основание на факта, че достъпът е от ключово значение за разкриване на истината или че събирането на доказателства по друг начин ще бъде невъзможно или много трудно. Издаването на съдебно разрешение се обуславя от изисквания за необходимост и пропорционалност.
Румъния	Директивата не е транспонирана.	
Словения ⁵⁹	Полицията, агенциите за разузнаване и сигурност и агенциите за отбрана, които отговарят за разузнаването и контраразузнаването и за мисиите във връзка със сигурността.	За достъпа се изисква съдебно разрешение.
Словакия ⁶⁰	Правоприлагащите органи и съдилища.	Исканията трябва да са в писмен вид.
Финландия ⁶¹	Полицията, граничната охрана и митническите органи (за запазени данни за абонатите, трафика и местоположението). Центърът за спешно реагиране, Морската спасителна служба и Морският спасителен подцентър (за данни за идентифициране и местоположение при спешни случаи).	До данни за абонатите имат достъп всички компетентни органи без съдебно разрешение. За други данни се изисква съдебно разпореждане.
Швеция	Директивата не е транспонирана.	

⁵⁴ Член 68, алинея 1 и член 69, алинея 1, букви с) и d) от Закон XXXIV 1994; член 9/A, алинея 1 от Закон V 1972; член 71, алинеи 1, 3 и 4, член 178/A, алинея 4, членове 200 и 201, член 268, алинея 2 от Закон XIX 1998; член 40, алинеи 1 и 2, член 53, алинея 1, член 54, алинея 1, буква j) от Закон CXXV 1995.

⁵⁵ Член 20, алинеи 1 и 3 от Законово известие 198/2008.

⁵⁶ Член 126пi от Наказателно-процесуалния кодекс.

⁵⁷ Член 179, алинея 3 от Закона за далекосъобщенията от 16 юли 2004 г., изменен с член 1 от Закона от 24 април 2009 г.

⁵⁸ Член 2, алинея 1, член 3, алинея 2 и член 9 от Закон 32/2008.

⁵⁹ Член 107с от Закона за електронните съобщения; член 149b от Наказателно-процесуалния кодекс; член 24, буква b) от Закона за агенцията за разузнаване и сигурност; член 32 от Закона за отбраната.

⁶⁰ Член 59а, алинея 8 от Закона за електронните съобщения.

⁶¹ Член 35, алинея 1 и член 36 от Закона за електронните съобщения; членове 31—33 от Закона за полицията; член 41 от Закона за граничната охрана.

Таблица 2: Достъп до запазени далекосъобщителни данни		
Компетентни национални органи		Процедури и условия
Обединеното кралство ⁶²	Полицията, службите за разузнаване, данъчните и митническите органи и други публични органи, определени във вторичното законодателство.	Достъп се дава при разрешение от „упълномощено лице“ и проверка на необходимостта и пропорционалността, в специфични случаи и при обстоятелства, при които разкриването на данните се разрешава или изисква по закон. С операторите са договорени специфични процедури.

Комисията ще оцени необходимостта и вариантите за постигане на по-голяма степен на хармонизиране по отношение на органите, които имат достъп до запазени данни, и процедурите за получаване на достъп до такива данни. Вариантите може да включват по-ясно определени списъци с компетентни органи, независим и/или съдебен надзор върху исканията за данни и минимални изисквания към процедурите за осигуряване на достъп на компетентните органи от страна на операторите.

4.4. Обхват на запазването на данни и обхванати категории данни (член 1, параграф 2, член 3, параграф 2 и член 5)

Директивата се прилага в областите на фиксираната мрежова телефония, мобилната телефония, интернет достъпа, електронната поща по интернет и интернет телефонията. В нея се посочват (в член 5) категориите данни, които следва да се запазят, а именно данни, необходими за установяване на:

- а) източника на съобщението;
- б) местоназначението на съобщението;
- в) датата, времето и продължителността на съобщението;
- г) вида съобщение;
- д) съобщителното оборудване на ползвателите или на това, което се счита, че е тяхно оборудване; както и
- е) местоположението на мобилното съобщително оборудване.

Освен това в нея се обхващат (член 3, параграф 2) неуспешни опити за повикване, тоест съобщение, при което телефонното обаждане е успешно свързано, но на него не е било отговорено или е имало намеса на мрежовото ръководство, когато данни за тези опити са създадени или обработени и съхранени или записани от операторите. За целите на директивата не може да бъде запазвана никаква информация, разкриваща съдържанието на съобщението. По-късно беше изяснено и това, че запитванията за търсене, тоест дневниците на сървърите, генерирани чрез предлагането на услуги на

⁶² Член 25, таблица 1 от Закона за уреждане на правомощията за разследване (RIPA) от 2000 г.; член 7 от Наредбата за запазване на данните. В член 22, алинея 2 от RIPA се уреждат целите, за които тези органи могат да получават данни.

машина за търсене, също така са извън обхвата на директивата, защото те се считат по-скоро за съдържание, отколкото за данни за трафика⁶³.

Двадесет и една държави-членки предвиждат запазването на всяка една от тези категории данни в своето законодателство за транспониране. Белгия не е предвидила кои видове данни за телефония се запазват, нито пък има разпоредби относно свързаните с интернет данни. Респондентите, които отговориха на въпросника на Комисията, не счетоха за необходимо да се изменят категориите данни, които следва да се запазват, макар че Европейският парламент изготви писмена декларация до Комисията, в която призовава обхватът на директивата да бъде разширен, така че да обхване търсачките в интернет „с цел бързо [...] противодействие на детската порнография и сексуалните посегателства по интернет“⁶⁴. В доклада си относно второто действие по принудително изпълнение Работната група за защита на данните по член 29 се обоснова, че списъкът на посочените в директивата категории следва да се счита за изчерпателен, като на операторите не се налагат допълнителни задължения за запазване на данни. Комисията ще оцени необходимостта от всички тези категории данни.

4.5. Периоди на запазване (член 6 и член 12)

Държавите-членки са длъжни да гарантират, че категориите данни, посочени в член 5, се запазват за периоди не по-кратки от шест месеца и не по-дълги от две години. Максималният период на запазване може да бъде удължен от държава-членка, която „е изправена пред особени обстоятелства, които налагат удължаване за един ограничен период“. Комисията трябва да бъде уведомена за това удължаване и в рамките на период от шест месеца от уведомлението тя решава да одобри или да отхвърли удължаването. Максималният период на запазване може да бъде удължен, но няма разпоредба за съкращаване на периода на запазване под шест месеца. Всички държави-членки (с изключение на една), които са транспонирали директивата, прилагат период или периоди на запазване в рамките на тези ограничения и не са уведомявали Комисията за удължавания. Не съществува обаче съгласуван подход в рамките на ЕС.

Петнадесет държави-членки посочват един-единствен период за всички категории данни: една държава-членка (Полша) посочва период на запазване от две години, една (Латвия) посочва период от година и половина, десет посочват една година (България, Дания, Естония, Гърция, Испания, Франция, Нидерландия, Португалия, Финландия и Обединеното кралство) и три посочват шест месеца (Кипър, Люксембург и Литва). Пет държави-членки са определили различни периоди на запазване за различните категории данни: две държави-членки (Ирландия и Италия) посочват две години за данни за фиксирана и мобилна телефония и една година за данни за интернет достъп, електронна поща по интернет и интернет телефония; една държава-членка (Словения) посочва четиринадесет месеца за данни за телефония и осем месеца за свързани с интернет данни; една държава-членка (Словакия) посочва една година за фиксирана и мобилна телефония и шест месеца за свързани с интернет данни; една държава-членка (Малта) посочва една година за данни за фиксирана, мобилна и интернет телефония и шест

⁶³ Становище от 4 април 2008 г. на Работната група по член 29 по въпроси за защита на личните данни, свързани със системите за търсене.

⁶⁴ Писмена декларация, внесена съгласно член 123 от Правилника за дейността, относно създаването на европейска система за ранно предупреждение (ЕСРП) за борба срещу педофилите и лицата, извършващи сексуални посегателства, 19.4.2010 г., 0029/2010.

месеца за интернет достъп и електронна поща по интернет. Една държава-членка (Унгария) запазва всички данни за една година с изключение на данни за неуспешни опити за повикване, които се пазят в продължение на шест месеца. Една държава-членка (Белгия) не е посочила никакъв период на запазване на данни за категориите данни, посочени в директивата. Подробностите са представени в таблица 3.

Таблица 3: Периоди на запазване, посочени в националното законодателство	
Белгия ⁶⁵	Между 1 година и 36 месеца за „обществено достъпни“ телефонни услуги. Няма разпоредби за свързаните с интернет данни.
България	1 година. Данните, до които е получен достъп, могат да бъдат запазени за допълнителни 6 месеца при поискване.
Чешката република	Директивата не е транспонирана.
Дания	1 година
Германия	Директивата не е транспонирана.
Естония	1 година
Ирландия	2 години за данни за фиксирана и мобилна телефония, 1 година за данни за интернет достъп, електронна поща по интернет и интернет телефония
Гърция	1 година
Испания	1 година
Франция	1 година
Италия	2 години за данни за фиксирана и мобилна телефония, 1 година за данни за интернет достъп, електронна поща по интернет и интернет телефония
Кипър	6 месеца
Латвия	18 месеца
Литва	6 месеца
Люксембург	6 месеца
Унгария	6 месеца за неуспешни повиквания и 1 година за всички други данни
Малта	1 година за данни за фиксирана, мобилна и интернет телефония, 6 месеца за данни за интернет достъп и електронна поща по интернет
Нидерландия	1 година
Австрия	Директивата не е транспонирана.
Полша	2 години
Португалия	1 година
Румъния	Директивата не е транспонирана (6 месеца съгласно отменения преди това закон за транспониране).
Словения	14 месеца за данни за телефония и 8 месеца за свързани с интернет данни
Словакия	1 година за данни за фиксирана и мобилна телефония, 6 месеца за данни за интернет достъп, електронна поща по интернет и интернет телефония
Финландия	1 година
Швеция	Директивата не е транспонирана.
Обединеното кралство	1 година

Макар че това разнообразие от подходи се разрешава съгласно директивата, от това следва, че директивата осигурява само ограничена правна сигурност и предвидимост в ЕС за операторите, които извършват дейност в повече от една държава-членка, и за гражданите, чиито съобщителни данни могат да се съхраняват в различни държави-

⁶⁵ Член 126, алинея 2 от Закона от 13 юни 2005 г. за електронните съобщения.

членки. Като се имат предвид нарастващото интернационализиране на обработката на данни и възлагането на съхранението на данни на външни изпълнители, следва да се проучат вариантите за допълнително хармонизиране на периодите на запазване в ЕС. С цел спазване на принципа на пропорционалност и с оглед на количествените и качествените данни за ползата от запазените данни в държавите-членки, както и в контекста на тенденциите в съобщенията и технологиите и в престъпленията и тероризма, Комисията ще обмисли възможността да се прилагат различни периоди за различните категории данни, за различните категории сериозни престъпления или комбинация от двете⁶⁶. Предоставените досега от държавите-членки количествени данни относно актуалността на запазените данни показват, че около 90 % от данните датират отпреди шест месеца или по-малко, а около 70 % — отпреди три месеца или по-малко, когато първоначалното искане за достъп е направено от правоприлагащи органи (вж. раздел 5.2).

4.6. Защита на данните и сигурност на данните и наблюдаващи органи (членове 7 и 9)

Съгласно директивата от държавите-членки се изисква да гарантират, че операторите спазват като минимум четири принципа за сигурност на данните, а именно че запазените данни:

- а) са от същото качество и са предмет на същата сигурност и защита като аналогичните данни в [обществената съобщителна] мрежа;
- б) се подлагат на подходящи технически и организационни мерки, за да бъдат защитени от случайно или незаконно унищожаване, случайна загуба или промяна, или от непозволено или незаконно съхраняване, обработване, достъп или разкриване;
- в) се подлагат на подходящи технически и организационни мерки, за да се осигури, че до тях може да има достъп само специално упълномощен персонал; както и
- г) данните с изключение на онези, до които е имало достъп и са били съхранени, се унищожават в края на периода за запазване [за целта, определена в директивата].

В съответствие с директивата за защита на данните и директивата за правото на неприкосновеност на личния живот и електронни комуникации на операторите се забранява да обработват данни, запазени съгласно директивата, за други цели, ако данните в противен случай е нямало да бъдат запазени⁶⁷. Държавите-членки са длъжни да определят публичен орган, който да отговаря за наблюдението на прилагането на тези принципи, действайки напълно независимо, като това може да са същите органи като изискваните съгласно директивата за защита на данните⁶⁸.

⁶⁶ В предложението на Комисията за директива относно запазването на данни през 2005 г. се предвиждаше период на запазване от една година за данни за телефония и шест месеца за интернет данни.

⁶⁷ Член 13, параграф 1 от Директива 95/46/ЕО.

⁶⁸ Член 28 от Директива 95/46/ЕО.

Петнадесет държави-членки са транспонирали всички тези принципи в съответното законодателство. Четири държави-членки (Белгия, Естония, Испания и Латвия) са транспонирали два или три от тези принципи, но не предвиждат изрично унищожаването на данни в края на периода на запазване. Две държави-членки (Италия и Финландия) предвиждат унищожаването на данни. Не е ясно какви конкретни мерки за техническа и организационна сигурност, например надеждно удостоверяване и разширено управление на регистрационните файлове за достъп⁶⁹, се прилагат. Двадесет и две държави-членки разполагат с наблюдаващ орган, който следи прилагането на принципите. В повечето случаи това е органът за защита на данните. Подробностите са представени в таблица 4.

Таблица 4: Защита на данните и сигурност на данните и наблюдаващи органи		
<i>Държава-членка</i>	<i>Разпоредби за защита на данните и за сигурност на данните в националното законодателство</i>	<i>Наблюдаващ орган</i>
Белгия	Операторите трябва да гарантират, че предаването на данни не може да се прихване от трета страна, и трябва да отговарят на стандартите на Европейския институт за стандарти в далекосъобщенията (ЕИСД) за сигурност на далекосъобщенията и законно прихващане ⁷⁰ . Принципът за задължително унищожаване на данните в края на периода на запазване изглежда не е разгледан.	Институтът за пощенски услуги и далекосъобщения
България	Законът, с който се транспонира директивата, включва изискване за прилагане на четирите принципа ⁷¹ .	Комисията за защита на личните данни наблюдава обработването и съхранението на данни с цел да гарантира спазване на задълженията. Парламентарна комисия в Народното събрание наблюдава процедурите за разрешаване и достъп до данните.
Чешката република ⁷²	Директивата не е транспонирана.	
Дания	Има разпоредби за четирите принципа ⁷³ .	Националната агенция за ИТ и далекосъобщения наблюдава задължението, съгласно което доставчиците на електронни съобщителни мрежи и услуги трябва да гарантират, че техническото оборудване и системи позволяват достъп на полицията до информация за трафика на далекосъобщенията.

⁶⁹ Надеждното удостоверяване включва двойни механизми за удостоверяване, например парола плюс биометрични данни или парола плюс устройство за удостоверяване с оглед да се гарантира физическото присъствие на отговорното за обработката на данни за трафика лице. Разширеното управление на регистрационните файлове за достъп включва подробно проследяване на достъпа и операциите по обработка чрез запазване на регистрационни файлове, в които се отбелязва самоличността на потребителя, момента на достъп и файловете, предмет на достъп.

⁷⁰ Член 6 от Кралски указ от 9 януари 2003 г.

⁷¹ Член 4, алинея 1 от Закона за електронните съобщения (изменен) от 2010 г.

⁷² Член 87, алинея 3 и член 88 от Закон 127/2005, изменен със Закон 247/2008; член 2 от Закон 336/2005; член 3, алинея 4 от Закон 485/2005; член 28, алинея 1 от Закон 101/2000.

⁷³ Закон за обработката на лични данни; Изпълнителна заповед № 714 от 26 юни 2008 г. относно предоставянето на електронни съобщителни мрежи и услуги.

Таблица 4: Защита на данните и сигурност на данните и наблюдаващи органи		
Държава-членка	Разпоредби за защита на данните и за сигурност на данните в националното законодателство	Наблюдаващ орган
Германия	Директивата не е транспонирана.	
Естония	Законът, с който се транспонира директивата, съдържа разпоредби за три от четирите принципа. Няма изрична разпоредба за четвъртия принцип, макар че всички лица, чиято неприкосновеност на личния живот е била нарушена от дейности, свързани с надзор, могат да поискат чрез съдебно решение ⁷⁴ унищожаване на данните.	Органът за технически надзор е отговорният орган.
Ирландия ⁷⁵	Законът, с който се транспонира директивата, включва изискване за прилагане на четирите принципа.	Определеният съдия има право да разследва и да докладва дали компетентните национални органи спазват разпоредбите на закона, с който се транспонира директивата.
Гърция ⁷⁶	Законът, с който се транспонира директивата, включва изискване за прилагане на четирите принципа, както и допълнително изискване към операторите да изготвят и прилагат план, с който да се гарантира спазването на принципите под надзора на лице, назначено да отговаря за сигурността на данните.	Органът за защита на личните данни и органът за гарантиране на поверителността на съобщенията.
Испания ⁷⁷	Разпоредбите за сигурност на данните обхващат три от четирите принципа (качество и сигурност на запазените данни, достъп от упълномощени лица и защита срещу неупълномощена обработка).	Агенцията за защита на данните е отговорният орган.
Франция ⁷⁸	Законът, с който се транспонира директивата, включва изискване за прилагане на четирите принципа.	Националната комисия за информатика и свободи осъществява надзор на спазването на задълженията.
Италия	Няма изрични разпоредби за сигурността на запазените данни, макар че има общо изискване за унищожаване или правене на анонимни на данни за трафика и консенсусна обработка на данни за местоположението ⁷⁹ .	Органът за защита на данните наблюдава спазването на директивата от страна на операторите.

⁷⁴ Член 111, алинея 9 от Закона за електронните съобщения; член 122, алинея 2 от Наказателно-процесуалния кодекс.

⁷⁵ Членове 4, 11 и 12 от Проектозакона за съобщенията (запазване на данни) от 2009 г.

⁷⁶ Член 6 от Закон 3917/2011.

⁷⁷ Член 8 от Закон 25/2007, член 38, алинея 3 от Общия закон за далекосъобщенията. Законът (член 9) се позовава на изключението от правата на достъп и на отменяне, предвидени в Основен закон 15/1999 за защита на личните данни (членове 22 и 23).

⁷⁸ Член D.98-5 от Кодекса за пощите и електронните съобщения (CPCE); член L-34-1, параграф V от Кодекса за пощите и електронните съобщения (CPCE); член 34 от Закон № 78-17; член 34-1 от Кодекса за пощите и електронните съобщения (CPCE); член 11 от Закон № 78-17 от 6 януари 1978 г.

⁷⁹ Членове 123 и 126 от Кодекса за защита на данните.

Таблица 4: Защита на данните и сигурност на данните и наблюдаващи органи		
Държава-членка	Разпоредби за защита на данните и за сигурност на данните в националното законодателство	Наблюдаващ орган
Кипър ⁸⁰	Законът, с който се транспонира директивата, съдържа разпоредби за всеки от четирите принципа.	Комисарят за защита на личните данни наблюдава прилагането на закона, с който се транспонира директивата.
Латвия ⁸¹	Законът, с който се транспонира директивата, съдържа разпоредби за два от принципите: поверителност и упълномощен достъп до запазените данни и унищожаване на данните в края на периода на запазване.	Държавната инспекция по данните осъществява надзор на защитата на личните данни в сектора на електронните съобщения, но не и достъпа и обработката на запазените данни.
Литва ⁸²	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Държавната инспекция по защита на данните осъществява надзор на прилагането на закона, с който се транспонира директивата, и отговаря за предоставяне на статистически данни на Европейската комисия.
Люксембург ⁸³	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Органът за защита на данните.
Унгария ⁸⁴	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Парламентарният комисар за защита на данните и свобода на информацията.
Малта ⁸⁵	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Комисарят за защита на данните.
Нидерландия ⁸⁶	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Агенцията за радиосъобщения осъществява надзор на спазването на задълженията на доставчиците на интернет и далекосъобщителни услуги. Органът за защита на данните осъществява надзор на общата обработка на лични данни. Подробностите във връзка със сътрудничеството между двата органа са описани в протокол.
Австрия	Директивата не е транспонирана.	
Полша	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа ⁸⁷ .	Органът за защита на данните.
Португалия	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа ⁸⁸ .	Португалският орган за защита на данните.

⁸⁰ Членове 14 и 15 от Закон 183(I)/2007.

⁸¹ Член 4, алинея 4 и член 71, алинеи 6—8 от Закона за електронните съобщения.

⁸² Член 12, алинея 5, член 66, алинеи 8 и 9 от Закона за електронните съобщения, изменен на 14 ноември 2009 г.

⁸³ Член 1, алинея 5 от Закона от 24 юли 2010 г.

⁸⁴ Член 157 от Закон C/2003, изменен със Закон CLXXIV/2007, член 2 от Указ 226/2003 и Закон LXIII/1992 за защита на данните.

⁸⁵ Членове 24 и 25 от Законово известие 198/2008; член 40, буква b) от Закона за защита на данните (глава 440).

⁸⁶ Член 13, алинея 5 от Закона за далекосъобщенията. Пълното заглавие на протокола за сътрудничество е „*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 Членове 180a и 180e от Закона за далекосъобщенията.

Таблица 4: Защита на данните и сигурност на данните и наблюдаващи органи		
<i>Държава-членка</i>	<i>Разпоредби за защита на данните и за сигурност на данните в националното законодателство</i>	<i>Наблюдаващ орган</i>
Румъния	Директивата не е транспонирана.	
Словения ⁸⁹	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Комисарят по информационните въпроси.
Словакия ⁹⁰	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа.	Националният регулаторен орган и орган за определяне на цените в областта на електронните съобщения осъществява надзор на защитата на личните данни.
Финландия	Законът, с който се транспонира директивата, съдържа изрична разпоредба единствено за изискването данните да се унищожават в края на периода на запазване ⁹¹ .	Финландският орган за регулиране на съобщенията осъществява надзор на спазването на разпоредбите за запазването на данни от страна на операторите. Омбудсманът за защита на данните осъществява надзор на общата законност на обработката на лични данни.
Швеция	Директивата не е транспонирана.	
Обединеното кралство	Законът, с който се транспонира директивата, съдържа разпоредби за четирите принципа ⁹² .	Комисарят по информационните въпроси осъществява надзор на запазването и/или обработката на съобщителни данни (и всякакви други лични данни) и извършва подходящи проверки във връзка със защитата на данните. Комисарят по прихващането на данни (действащ или пенсиониран старши съдия) осъществява надзор на придобиването на съобщителни данни съгласно RIPA от страна на публичните органи. Трибуналет с правомощия за разследване разследва жалби за злоупотреба с данни, ако те са придобити в съответствие със законодателството за транспониране на директивата (RIPA).

Транспонирането на член 7 е непоследователно. Запазените данни потенциално са от много лично и чувствително естество и трябва да се прилагат високи стандарти за защита на данните и сигурност на данните по време на целия процес на съхранение, извличане и използване по последователен и прозрачен начин с оглед да се сведе до минимум рискът от нарушения на неприкосновеността на личния живот и да се запази доверието на гражданите. Комисията ще проучи вариантите за повишаване на стандартите за сигурност на данните и защита на данните, включително чрез въвеждането на решения, при които се спазва принципът за „защита на личния живот още при разработването“, с оглед да се гарантира спазването на тези стандарти както при съхранението, така и при предаването. Тя ще вземе предвид също и препоръките за минимални механизми за защита и за мерки за техническа и организационна сигурност,

⁸⁸ Член 7, алинеи 1 и 5 и член 11 от Закон 32/2008; членове 53 и 54 от Закона за защита на личните данни.

⁸⁹ Член 107а, алинея 6 и член 107с от Закона за електронните съобщения.

⁹⁰ Член 59а от Закона за електронните съобщения; член S33 от Закон № 428/2002 за защита на личните данни.

⁹¹ Член 16, алинея 3 от Закона за електронните съобщения.

⁹² Член 6 от Наредбата за запазване на данните.

направени от Работната група за защита на данните по член 29 в доклада ѝ относно второто действие по принудително изпълнение⁹³.

4.7. Статистика (член 10)

Държавите-членки са длъжни да предоставят на Комисията ежегодна статистика за запазването на данни, включително:

- случаи, при които информацията е била предоставена на компетентните органи в съответствие с приложимото национално право;
- времето, изтекло от датата на запазване на данните, до датата, на която компетентни органи са поискали предаването на данните (т.е. актуалност на данните); както и
- случаите, при които не е могло да се отговори на искането за данни.

При отправянето на искане за статистически данни съгласно тази разпоредба Комисията поиска от държавите-членки да предоставят подробности относно случаи на отделни „искания“ за данни. Предоставените статистически данни обаче се различаваха по обхват и степен на подробности: в своите отговори някои държави-членки правят разграничение между различните видове съобщения, някои посочват актуалността на данните към момента на искането, докато други предоставят само годишна статистика без подробна разбивка. Деветнадесет държави-членки⁹⁴ предоставиха статистика относно броя на исканията за данни за 2009 г. и/или 2008 г. В това число се включват Ирландия, Гърция и Австрия, в които са се отправяли искания за данни въпреки липсата на законодателство за транспониране по това време, както и Чешката република и Германия, чието законодателство за запазването на данни беше отменено. Седем държави-членки, които са транспонирали директивата, не са предоставили статистически данни, въпреки че Белгия предостави прогнозен брой на ежегодните искания за данни във връзка с телефония (300 000).

Надеждните количествени и качествени данни са от решаващо значение с оглед да се демонстрира необходимостта и ползата от мерките за сигурност като запазването на данни. Това беше признато в плана за действие от 2006 г. относно определяне нивото на престъпността и ефективността на наказателното правосъдие⁹⁵, в който беше включена цел да се разработят методи за редовно събиране на данни в съответствие с директивата и статистическите данни да се включат в базата данни Евростат (при условие че отговарят на стандартите за качество). Изпълнението на тази цел не беше възможно предвид фактът, че повечето държави-членки транспонираха напълно директивата едва през последните две години и използваха различни тълкувания за източника на статистическите данни. В бъдещото си предложение за преразглеждане на

⁹³ Становище 3/2006 (WP119) на Работната група за защита на данните по член 29; Доклад 01/2010.

⁹⁴ Чешката република, Дания, Германия, Естония, Ирландия, Гърция, Испания, Франция, Кипър, Латвия, Литва, Малта, Нидерландия, Австрия, Полша, Словения, Словакия, Финландия и Обединеното кралство.

⁹⁵ Съобщение (2006) 437 на Комисията относно „Разработване на съгласувана и цялостна стратегия на ЕС за определяне нивото на престъпността и ефективността на наказателното правосъдие: План за действие на ЕС за периода 2006—2010 г.“.

правната рамка на запазването на данни, заедно с прегледа на плана за действие относно статистическите данни, Комисията ще цели разработването на осъществими процедури за измерване и докладване, които дават възможност за прозрачно и смислено наблюдение на запазването на данни и които не водят до непропорционална тежест върху системите на наказателно правосъдие и правоприлагащите органи.

4.8. Транспониране в държавите от ЕИП

Законодателство за запазване на данни е налице в Исландия, Лихтенщайн и Норвегия⁹⁶.

4.9. Решения на конституционните съдилища относно законите за транспониране на директивата

През октомври 2009 г. Конституционният съд на Румъния, през март 2010 г. Федералният конституционен съд на Германия и през март 2011 г. Конституционният съд на Чешката република отмениха законите за транспониране на директивата в своите съответни юрисдикции на основание неконституционност. Съдът на Румъния⁹⁷ прие, че може да се разреши засягане на основните права, при условие че се спазват определени правила и че са предвидени адекватни и достатъчни механизми за защита срещу евентуален акт на държавен произвол. Но въз основа на съдебната практика на Европейския съд за правата на човека⁹⁸ съдът счете закона за транспониране за двусмислен по обхват и цел и с недостатъчни механизми за защита, както и че „непрекъснато правно задължение“ за запазване на всички данни за трафика в продължение на шест месеца е несъвместимо с правата на неприкосновеност на личния живот и свободата на изразяване от член 8 на Европейската конвенция за правата на човека.

Конституционният съд на Германия⁹⁹ също обяви, че запазването води до определено схващане за надзора, което би могло да накърни свободното упражняване на основните права. Той изрично обяви, че запазването на данни за строго ограничени употреби, придружено от достатъчно високо ниво на сигурност на данните, не би нарушило непременно германската конституция. Съдът подчерта обаче, че запазването на такива данни съставлява сериозно ограничение на правото на неприкосновеност на личния живот и следователно трябва да се допуска в особено ограничен брой случаи, както и че период на запазване от шест месеца представлява горна граница („*an der Obergrenze*“) на това, което може да се счита за пропорционално (параграф 215). Данни следва да се искат само когато вече са налице подозрения за сериозно престъпление или доказателства за заплаха за обществената сигурност и извличането на данни следва да е забранено за определени защитени съобщения (т.е. съобщения, свързани с емоционални или социални нужди), при които се разчита на поверителност. Данните следва също така да се кодират с прозрачен надзор на използването им.

⁹⁶ В Исландия законът, с който се транспонира директивата, е Закон за далекосъобщенията 81/2003 (изменен през април 2005 г.). В Лихтенщайн това е Законът за далекосъобщенията от 2006 г. В Норвегия законът, с който се транспонира директивата, беше одобрен на 5 април 2011 г. и понастоящем предстои да получи кралско одобрение.

⁹⁷ Решение № 1258 от 8 октомври 2009 г. на Конституционния съд на Румъния.

⁹⁸ ЕСПЧ, *Rotaru*/Румъния (2000 г.), *Sunday Times*/Обединеното кралство (1979 г.) и принц *Hans-Adam* на Лихтенщайн/Румъния (2001 г.).

⁹⁹ *Bundesverfassungsgericht*, 1 BvR 256/08, параграфи 1—345.

Конституционният съд на Чешката република¹⁰⁰ отмени законодателството за транспониране на директивата на основание на това, че то не е достатъчно точно и ясно формулирано, а представлява мярка, която засяга основните права. Съдът изрази критики относно ограничението на целите, което счита за недостатъчно тясно предвид мащаба и обхвата на изискването за запазване на данни. Той счете, че в законодателството за транспониране на директивата определението на компетентните органи, които имат достъп и могат да използват запазените данни, както и на процедурите за получаването на такъв достъп и право на използване, не е достатъчно ясно, за да гарантира целостта и поверителността на данните. Затова отделните граждани не разполагат с достатъчно гаранции и защитни механизми срещу възможна злоупотреба с власт от страна на публичните органи. Съдът не отправя критики срещу самата директива и обявява, че в нея са заложили достатъчни механизми, за да може Чешката република да я транспонира, спазвайки конституцията. Обаче в забележка *obiter dictum* съдът все пак изразява съмнение относно необходимостта, ефикасността и адекватността на запазването на данни за трафика предвид появата на нови методи за извършване на престъпна дейност, като например използването на анонимни SIM карти.

Тези три държави-членки понастоящем обмислят как да транспонират директивата отново. Дела относно запазването на данни бяха образувани и пред конституционния съд на България, което доведе до преработване на закона за транспониране на директивата, пред конституционния съд на Кипър, който постанови, че съдебните разпоредения, издадени съгласно закона за транспониране на директивата, са неконституционни и пред конституционния съд на Унгария, където дело относно липсата на законовите цели на обработката на данни в закона за транспониране все още се разглежда¹⁰¹.

В бъдещото си предложение за преразглеждане на правната рамка на запазването на данни Комисията ще вземе предвид въпросите, повдигнати от националната съдебна практика.

4.10. Текущо прилагане на директивата

Комисията очаква държавите-членки, които все още не са транспонирали напълно директивата или все още не са приели законодателство, което да заменя законодателството за транспониране, отменено от националните съдилища, да го сторят възможно най-скоро. Ако това не се случи, Комисията си запазва правото да упражни правомощията си, дадени ѝ по силата на Договорите на ЕС. Съдът на ЕС постанови, че понастоящем две държави-членки, които не са транспонирали директивата (Австрия и Швеция), са нарушили задълженията си, произтичащи от правото на ЕС¹⁰². През април 2011 г. Комисията реши да заведе второ дело срещу Швеция пред Съда на ЕС поради неизпълнение на решението по дело C-185/09, като поиска налагането на финансови санкции по член 260 от Договора за функционирането на Европейския съюз след

¹⁰⁰ Решение на Конституционния съд на Чешката република от 22 март по Закон № 127/2005 и Указ № 485/2005. Вж. по-специално параграфи 45—48, 50—51 и 56.

¹⁰¹ Върховен административен съд на България, решение № 13627 от 11 декември 2008 г.; Върховен съд на Кипър, апелативно дело № 65/2009, 78/2009, 82/2009 и 15/2010-22/2010 от 1 февруари 2011 г.; жалбата пред Конституционния съд на Унгария беше подадена на 2 юни 2008 г. от унгарския Съюз за граждански свободи.

¹⁰² Съответно дело C-189/09 и дело C-185/09.

решение на шведския парламент да отложи приемането на законодателството за транспониране на директива с 12 месеца. Комисията продължава да следи отблизо положението в Австрия, която предостави график за предстоящото приемане на законодателството за транспониране.

5. РОЛЯ НА ЗАПАЗЕНИТЕ ДАННИ В НАКАЗАТЕЛНОТО ПРАВОСЪДИЕ И ПРАВОПРИЛАГАНЕТО

В този раздел се обобщават функциите на запазените данни, както са описани от държавите-членки в подадената от тях информация за целите на оценката.

5.1. Обем на запазените данни, до които компетентните национални органи са имали достъп

Обемът както на трафика на далекосъобщенията, така и на исканията за достъп до данни за трафика се увеличава. Статистическите данни, предоставени от 19 държави-членки за 2008 г. и/или 2009 г., показват, че като цяло в ЕС всяка година се отправят над 2 милиона искания за данни, със значителни разлики между държавите-членки — от по-малко от 100 годишно (Кипър) до над 1 милион (Полша). Според информацията за вида поискани данни, която беше предоставена от дванадесет държави-членки за 2008 г. или за 2009 г., най-често исканият вид данни е свързан с мобилната телефония (вж. таблици 5, 8 и 12). В статистическите данни не се посочва точната цел, за която всяко искане е било подадено. Чешката република, Латвия и Полша посочват, че в случая на данни за мобилна телефония компетентните органи е трябвало да подадат същото искане до всеки от главните мобилни оператори и следователно действителният брой искания за всеки случай са били значително по-малко от това, което показва статистиката.

Няма очевидно обяснение за тези вариации, макар че броят на населението, преобладаващите тенденции в престъпността, ограниченията на целите, условията за достъп и разходите за придобиване на данни са все уместни фактори.

5.2. Актуалност на запазените данни, до които е бил даден достъп

Въз основа на статистическа разбивка, предоставена от девет държави-членки¹⁰³ за 2008 г. (вж. обобщението в таблица 5 и допълнителни подробности в приложението), когато е било направено (първоначалното) искане за достъп, около 90 % от данните, до които компетентните органи са получили достъп през тази година, са датирани отпреди шест месеца или по-малко и около 70 % — отпреди три месеца или по-малко.

Таблица 5: Преглед на актуалността на запазените данни, до които е бил получен достъп в девет държави-членки, предоставили разбивка по видове данни през 2008 г.				
<i>Актуалност</i>	<i>Фиксирана телефония</i>	<i>Мобилна телефония</i>	<i>Интернет данни</i>	<i>Общо</i>
По-малко от 3	61 %	70 %	56 %	67 %

¹⁰³ Чешката република, Дания, Естония, Ирландия, Испания, Кипър, Латвия, Малта и Обединеното кралство.

Таблица 5: Преглед на актуалността на запазените данни, до които е бил получен достъп в девет държави-членки, предоставили разбивка по видове данни през 2008 г.

<i>Актуалност</i>	<i>Фиксирана телефония</i>	<i>Мобилна телефония</i>	<i>Интернет данни</i>	<i>Общо</i>
месеца				
От 3 до 6 месеца	28 %	18 %	19 %	19 %
От 6 до 12 месеца	8 %	11 %	18 %	12 %
Над 1 години	3 %	1 %	7 %	2 %

Според повечето държави-членки използването на запазени данни на повече от три и дори на повече от шест месеца не е толкова често, но може да бъде изключително важно. Използването на тези данни като цяло попада в три категории. Първо, свързаните с интернет данни като цяло се искат по-късно от другите видове доказателства в хода на наказателните разследвания. Анализът на данни за фиксирана мрежова и мобилна телефония често води до потенциални улики, които на свой ред водят до последващи искания за по-стари данни. Ако например по време на разследване бъде намерено дадено име въз основа на данни от фиксирана мрежова или мобилна телефония, разследващите лица могат да искат да установят Internet Protocol (IP) адреса, който се използва от това лице, и да искат да установят с кого е контактувало лицето в определен период от време посредством този IP адрес. При такъв сценарий разследващите лица вероятно ще поискат данни, които да позволят проследяването и на съобщения с други IP адреси и самоличността на лицата, които са използвали тези IP адреси.

Второ, при разследвания на особено сериозни престъпления, поредица от престъпления, организирана престъпност и терористични актове като цяло се разчита на по-стари запазени данни, които отразяват времето, необходимо за планиране на тези престъпления, за да бъдат разкрити моделите на престъпно поведение и отношенията между съучастниците в престъпление, както и да се установи престъпното намерение. Дейностите, свързани със сложни финансови престъпления, често се разкриват едва след няколко месеца. Трето, по изключение държавите-членки също така са отправяли искания за данни за трафика, съхранявани в друга държава-членка, която обикновено може да разкрие тези данни само със съдебно разрешение в отговор на съдебна поръчка, издадена от съдия в отправящата искането държава-членка. Този вид взаимна правна помощ може да е отнеме доста време, което обяснява защо някои от поисканите данни в тези случаи са на повече от шест месеца.

5.3. Трансгранични искания за запазени данни

Наказателните разследвания и преследвания могат да включват доказателства или свидетели от или събития, случили се на територията на повече от една държава-членка. Според статистическите данни, предоставени от държавите-членки, по-малко от 1 % от всички искания за запазени данни са касаели данни, съхранявани в друга държава-членка. Правоприлагащите органи посочиха, че предпочитат да отправят искания за данни до националните оператори, които може да съхраняват съответните данни, а не да започват процедура за взаимна правна помощ, която може да отнеме много време без никаква гаранция, че ще бъде предоставен достъп до данните. Рамково решение 2006/960/ПВР за опростяване обмена на информация и сведения между

правоприлагащите органи на държавите-членки на Европейския съюз¹⁰⁴, в което се определят срокове за предоставяне на информация след отправяне на искане от друга държава-членка, не се прилага, защото запазените данни се считат за информация, получена чрез принуда, което излиза извън обхвата на този инструмент. Независимо от това нито една държава-членка или правоприлагащ орган не са призовавали за допълнително улесняване на трансграничния обмен на данни.

5.4. Полза от запазените данни в наказателни разследвания и преследвания

Въпреки че общият брой на докладваните искания за данни не отразява непременно ползата от данните в отделните наказателни разследвания, държавите-членки посочват, че запазването на данни е най-малкото полезно, а в някои случаи абсолютно необходимо¹⁰⁵, за предотвратяване и борба с престъпленията, включително за защита на жертвите на престъпления и за оправдаване на невинни лица в наказателните производства. Успешното издаване на осъдителни присъди зависи от признания за вина, свидетелски показания или доказателства, получени в рамките на криминалистични анализи. Беше докладвано, че запазените данни за трафика са се оказали необходими за свързване със свидетелите на злополука, които в противен случай е нямало да бъдат идентифицирани, и за осигуряване на доказателства или улики, водещи до установяване на съучастие в престъпление. Някои държави-членки¹⁰⁶ в допълнение заявиха, че използването на запазени данни е спомогнало да се изясни невинността на лица, заподозрени в престъпления, без да се прибегва към други методи за наблюдение, като прихващането на съобщения и претърсването на жилища, които биха могли да се считат за по-голямо вмешателство.

Няма общо определение на понятието „сериозно престъпление“ в ЕС и съответно няма статистика на ЕС за броя сериозни престъпления или разследвания или преследвания на сериозни престъпления, макар че редовно се публикуват данни за престъпления и правосъдие. Общият брой исканията за запазени данни, докладван от 19-те държави-членки, които са предоставили някакви данни за 2009 г. и/или 2008 г., беше около 2,6 милиона. Ако се направи сравнение с последните статистически данни за престъпления и наказателно правосъдие, налични за тези 19 държави-членки, които се отнасят за всички докладвани престъпления, а не само за сериозните престъпления, може да се заключи, че е имало малко над две искания на един полицейски служител годишно или около 11 искания за всеки 100 регистрирани престъпления¹⁰⁷.

¹⁰⁴ Рамково Решение 2006/960/ПВР на Съвета от 18 декември 2006 г. за опростяване обмена на информация и сведения между правоприлагащите органи на държавите-членки на Европейския съюз (ОВ L 386, 29.12.2006 г., стр. 89—100 и ОВ L 200, 1.8.2007 г., стр. 637—648).

¹⁰⁵ Чешката република счита запазването на данни за „абсолютно необходимо в голям брой случаи“. Унгария посочва, че то е „необходимо за обичайните дейности [на правоприлагащите органи]“. Словения заявява, че липсата на запазени данни би „парализирало функционирането на правоприлагащите органи“. Полицейска служба на Обединеното кралство описва наличието на данни за трафика като „жизненоважно ... за разследването на терористичните заплахи и сериозните престъпления“.

¹⁰⁶ Германия, Полша, Словения и Обединеното кралство.

¹⁰⁷ През 2007 г. в ЕС-27 е имало 1,7 млн. полицейски служители, като 1,2 млн. от тях са били заети в 19-те държави-членки, предоставили статистически данни относно исканията за запазени данни. През 2007 г. полицията в ЕС е регистрирала 29,2 млн. престъпления, като 24 млн. от тях са били регистрирани в 19-те държави-членки, предоставили статистически данни (източник: Евростат 2009 г.).

Въз основа на предоставените статистически данни и обяснителни примери, които свързват използването на запазените данни за съобщения за предишни периоди с броя осъдителни присъди, оправдателни присъди, прекратени дела и предотвратени престъпления, може да се направят няколко заключения по отношение на ролята и ползата от запазените данни за наказателните разследвания.

Събиране на доказателствени улики

На първо място, запазените данни позволяват събиране на доказателствени улики, които водят до престъпление. Те се използват, за да се установят или да потвърдят други видове доказателства относно дейностите и взаимоотношенията между заподозрените лица. Данни за местоположението се използват по-специално от правоприлагащите органи и от ответниците за изключване на заподозрени лица от местопрестъплението и за потвърждаване на алибита. Следователно тези доказателства могат да доведат до отстраняването на лица от наказателните разследвания, като така се премахва необходимостта от събиране на доказателства с по-голяма степен на вмешателство, или да доведат до издаване на оправдателни присъди по делата. Белгия се посочва осъждането през 2008 г. на извършителите на отвлечане на служител от наказателното отделение на съда на Антверпен, при което данни за местоположението, свързващи дейностите на извършителите в три отделни града, са били от решаващо значение за убеждаване на съдебните заседатели в съучастието им. По друго дело — за убийство през 2007 г., свързано с банда мотоциклетисти, данни за местоположението от мобилните телефони на извършителите доказаха, че те са се намирали във въпросния район към момента на извършване на убийството и доведоха до частично признание¹⁰⁸. Според Белгия, Ирландия и Обединеното кралство някои престъпления, при които има комуникация чрез интернет, могат да се разследват *единствено* чрез запазването на данни: например заплахите за насилие в дискуссионните форуми често не оставят друга следа освен данни за трафика в кибернетичното пространство. Подобно е положението в случай на престъпления, извършени по телефона. Унгария и Полша описват случай на измама на възрастни лица в края на 2009 г. — началото на 2010 г., извършена чрез телефонни обаждания, по време на които извършителите се представяли за членове на семейството, нуждаещи се от заеми, като тези лица е можело да бъдат идентифицирани само чрез запазените данни за телефония.

Започване на наказателни разследвания

На второ място, има случаи, в които поради липсата на доказателства, получени чрез криминалистичен анализ или от очевидец, единственият начин да се започне наказателно разследване е да се направи справка в запазените данни. Германия посочва примера на убийството на полицейски служител, при което нападателят е избягал с превозното средство на жертвата, а след това го е изоставил. Било е възможно установяването на това, че след това нападателят е направил телефонно обаждане за друг вид транспорт. Не е имало доказателства, получени чрез криминалистичен анализ или от очевидец, във връзка със самоличността на убиеца и властите са разчитали на наличието на такива данни за трафика, които да им позволят да продължат

¹⁰⁸ Национална агенция за подобряване на полицейските дейности (Обединеното кралство), „Журнал за разследване на убийства и сериозни инциденти“ (*The Journal of Homicide and Major Incident Investigation*), том 5, брой 1, пролет 2009 г., стр. 39—51.

разследването. В случаите на свързани с интернет сексуални посегателства срещу деца запазването на данни е било абсолютно необходимо за провеждане на успешно разследване. Наред с други техники на разследване, запазването на данни позволява идентифицирането на потребителите на съдържание с детска порнография¹⁰⁹, както и идентифицирането и спасяването на децата жертви. Чешката република докладва, че без достъп до свързаните с интернет запазени данни е щяло да бъде невъзможно започването на разследвания като част от „Операция Вилма“ срещу мрежа от ползватели и разпространители на детска порнография. На равнище ЕС ефективността на операция „Спасение“ (провеждана със съдействието на Европол) за защита на децата срещу посегателства е била възпрепятствана поради липсата на законодателство за транспониране на директивата за запазване на данни, което е попречило на някои държави-членки да разследват участници в широка международна педофилска мрежа, използващи IP адреси, чиято актуалност може да датира отпреди една година.

При разследването на престъпления в кибернетичното пространство IP адресът често е първата улика. Чрез извличане на данни за трафика правоприлагащите органи могат да установят абоната зад IP адреса, преди да вземат решение дали да започнат наказателно разследване. Това може също така да позволи на полицията да предупреди потенциални жертви на атаки в кибернетичното пространство: когато полицията успее да конфискува сървър за командване и контрол (command-and-control), използван от оператори на Botnet, тя може да види само IP адресите, свързани към този сървър, но чрез достъп до запазените данни полицията може да идентифицира и да предупреди потенциални жертви, които притежават тези IP адреси.

Запазените данни като неразделна част от наказателното разследване

На трето място, въпреки че повечето правоприлагащи органи и съдилища в повечето държави-членки не водят статистика за вида доказателства, които са се оказали от решаващо значение за издаването на осъдителни или оправдателни присъди, то запазените данни са неделимо свързани с наказателното разследване и преследване в ЕС. Някои държави-членки посочват, че те невинаги са могли да определят отчетливо въздействието на запазените данни върху успешното провеждане на наказателните разследвания и преследвания, защото съдилищата вземат предвид всички доказателства, които им се представят, и рядко считат, че отделно доказателство е било определящо¹¹⁰. Нидерландия докладва, че от януари до юли 2010 г. данни за трафика за предишни периоди са били решаващ фактор в 24 съдебни решения. Финландия докладва, че в 56 % от 3 405 искания запазените данни са били сметени или за „важни“, или за „съществени“ за разкриването и/или преследването на престъпните деяния. Обединеното кралство предостави данни, чиято цел беше да се изрази количествено въздействието от запазването на данни върху наказателните преследвания. Държавата-членка докладва, че за три от нейните правоприлагащи органи запазените данни са

¹⁰⁹ По проекта „*Measurement and analysis of p2p activity against paedophile content*“ („Измерване и анализ на дейностите с равноправен достъп срещу педофилското съдържание“), финансиран от Програмата за по-безопасен интернет, беше предоставена точна информация относно педофилските дейности в системата с равноправен достъп *eDonkey*, като по този начин стана възможно идентифицирането на 178 000 ползватели (от общо 89 милиона проверени ползватели), които са поискали педофилско съдържание.

¹¹⁰ Белгия, Чешката република и Литва.

били необходими в повечето, ако не и във всички разследвания, довели до наказателно преследване или осъдителна присъда.

5.5. Технологични новости и използване на предплатени SIM карти

Правоприлагащите органи трябва да не изостават от технологичните новости, които се използват за извършване или подбуждане към престъпления. Запазването на данни е сред инструментите за наказателно преследване, които са необходими на правоприлагащите органи като средства за борба със съвременните предизвикателства на престъпността в цялото им многообразие, обем и скорост по управляем и ефективен от гледна точка на разходите начин. Редица все по-широко разпространени форми на комуникация попадат извън обхвата на директивата. Виртуалните частни мрежи (VPN), например в университетите или големите корпорации, позволяват на няколко потребители да използват интернет чрез един шлюз, като се използва един и същи IP адрес. Понастоящем обаче се въвежда нова технология, която позволява предоставяне на адреси на отделните потребители в рамките на VPN.

Делът на потребителите на мобилна телефония, които използват предплатени услуги, е различен в отделните държави в ЕС. Някои държави-членки заявиха, че анонимните предплатени SIM карти, особено закупените в друга държава-членка, биха могли да се използват и от лица, участващи в престъпна дейност, като начин да се избегне идентифициране на лицето при наказателно разследване¹¹¹. Шест държави-членки (Дания, Испания, Италия, Гърция, Словакия и България) са приели мерки, съгласно които се изисква предплатените SIM карти да се регистрират. Тези и други държави-членки (Полша, Кипър и Литва) подкрепят общеевропейска мярка за задължително регистриране на самоличността на потребителите на предплатени услуги. Не бяха предоставени доказателства за ефективността на тези национални мерки. Бяха подчертани потенциалните предели на ефикасност, например в случай на кражба на самоличност или когато SIM карта се закупува от трето лице или потребител използва роуминг с карта, закупена в трета държава. Като цяло Комисията не е убедена в необходимостта от действия на равнище ЕС в тази област на този етап.

6. ВЪЗДЕЙСТВИЕ НА ЗАПАЗВАНЕТО НА ДАННИ ВЪРХУ ОПЕРАТОРИТЕ И ПОТРЕБИТЕЛИТЕ

6.1. Оператори и потребители

В съвместна декларация до Комисията пет големи промишлени асоциации заявиха, че икономическото въздействие на директивата е „значително“ или „огромно“ за „помалките оператори“, тъй като директивата оставя „много свобода на действие“¹¹². Осем оператори представиха широко вариращи изчисления на разходите, що се отнася до капитала и оперативните разходи, които налага спазването на директивата. Тези твърдения могат да бъдат подкрепени от посочените нива на възстановяване на разходите на операторите, докладвани от четири държави-членки (вж. таблица 6).

¹¹¹ Заключение на Съвета относно борбата срещу използването на електронни съобщения за престъпни цели и относно техния анонимен характер.

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

В проучване, направено преди транспонирането на директивата в повечето държави-членки, беше установено, че разходите за въвеждане на система за запазване на данни за един доставчик на интернет услуги, който обслужва половин милион потребители, са около 375 240 EUR през първата година и след това 9 870 EUR месечно за оперативни разходи¹¹³, а разходите за въвеждане на система за извличане на данни са изчислени на 131 190 EUR, като оперативните разходи са 28 960 EUR месечно. В решението си от 2 март 2010 г. Конституционният съд на Германия обаче постанови, че налагането на задължение за съхранение „не е особено или изключително тежко за съответния доставчик на услуги, [нито] непропорционално с оглед на финансовите тежести, които понасят предприятията в резултат на задължението за съхранение“¹¹⁴. Разходите за запазване на единица данни са обратнопропорционални на големината на оператора и на нивото на стандартизация, прието от съответната държава-членка за взаимоотношенията с операторите¹¹⁵.

В своите отговори на въпросника на Комисията повечето оператори заявиха, че не са успели да изразят количествено въздействието директивата върху конкуренцията, цените на дребно за потребителите или инвестициите в нова инфраструктура и услуги.

Няма доказателства за количествено изразимо или съществено въздействие на директивата върху потребителите на електронни съобщителни услуги, а в общественото допитване от 2009 г. нямаше принос от представителите на потребителите. В проучване, проведено в Германия от името на организация на гражданското общество, се посочва, че потребителите са възнамерявали да променят своите комуникационни навици, като при определени обстоятелства избягват да използват електронни съобщителни услуги, но няма доказателства, които да потвърждават настъпването на промяна в поведението в която и да е засегната държава-членка или в ЕС като цяло¹¹⁶.

Комисията възнамерява да оцени въздействието на бъдещите изменения на директивата върху индустрията и потребителите, включително по възможност чрез специфично проучване на Евробарометър, за да измери обществените схващания.

6.2. Възстановяване на разходи

Директивата не урежда възстановяването на разходите, понесени от операторите в резултат на изискването за запазване на данни. Тези разходи могат да представляват:

- a) *оперативни разходи*, тоест оперативни или повтарящи се разходи, свързани с обслужването на бизнеса, уред, компонент, оборудване или съоръжение; и

¹¹³ Wilfried Gansterer & Michael Iger, *Data retention — The EU Directive 2006/24/EC from a Technological Perspective* („Запазването на данни — Директива 2006/24/ЕО на ЕС от технологична гледна точка“), Wien: Verlag Medien und Recht, 2008 г.

¹¹⁴ Bundesverfassungsgericht, 1 BvR 256/08, 2 март 2010 г., параграф 299.

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

¹¹⁶ Проучването е било проведено от Forsa и поръчано от АК Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

- б) *капиталови разходи*, тоест разходи за създаване на бъдещи ползи или разходи за разработване или осигуряване на части, различни от консумативи, за продукта или системата, които могат да включват разходи за работници и разноски за съоръжението като наем и комунални услуги.

Всички държави-членки осигуряват някаква форма на възстановяване, ако данните са поискани в контекста на наказателно производство в съда. Две държави-членки докладваха, че възстановяват както оперативни, така и капиталови разходи. Шест възстановяват само оперативни разходи. Комисията не е била уведомявана за други схеми за възстановяване на разходи. Подробностите са представени в таблица 6.

Таблица 6: Държави-членки, които възстановяват разходи			
Държава-членка	Оперативни разходи	Капиталови разходи	Годишни възстановени разходи (млн. EUR)
Белгия	Да	Не	22 (2008 г.)
България	Не	Не	-
Чешката република	Директивата не е транспонирана ¹¹⁷ .		
Дания	Да	Не	-
Германия	Директивата не е транспонирана.		
Естония	Да	Не	-
Ирландия	Не	Не	-
Гърция	Не	Не	-
Испания	Не	Не	-
Франция	Да	Не	-
Италия	-	-	-
Кипър	Не	Не	-
Латвия	Не	Не	-
Литва	Да, ако поискано и обосновано.	Не	-
Люксембург	Не	Не	-
Унгария	Не	Не	-
Малта	Не	Не	-
Нидерландия	Да	Не	-
Австрия	Директивата не е транспонирана.		
Полша	Не	Не	-
Португалия	Не	Не	-
Румъния	Директивата не е транспонирана.		
Словения	Не	Не	-
Словакия	Не	Не	-
Финландия	Да	Да	1
Швеция	Директивата не е транспонирана.		
Обединеното кралство	Да	Да	55 (възстановени общо за разходите, понесени в рамките на 3 години)

¹¹⁷ Преди отменянето на чешкия закона за транспониране на директивата, Чешката република възстановяваше както оперативни, така и капиталови разходи и докладва за 6,8 млн. EUR възстановени разходи за 2009 г.

От горепосоченото може да се заключи, че директивата не е постигнала напълно своята цел за създаване на равни условия за операторите в ЕС. Комисията ще обмисли вариантите за свеждане до минимум на пречките за функционирането на вътрешния пазар чрез осигуряване на последователно възстановяване на разходите, които операторите понасят за спазването на изискванията за запазване на данни, като се обръща особено внимание на малките и средните оператори.

7. ПОСЛЕДСТВИЯ ОТ ЗАПАЗВАНЕТО НА ДАННИ ЗА ОСНОВНИТЕ ПРАВА

7.1. Основните права на неприкосновеност на личния живот и на защита на личните данни

Запазването на данни представлява ограничение на правото неприкосновеност на личния живот и на защитата на личните данни, които са основни права в Европейския съюз¹¹⁸. В съответствие с член 52, параграф 1 от Хартата на основните права такова ограничение трябва да бъде предвидено в закон и да зачита основното съдържание на същите права, при спазване на принципа на пропорционалност, и да бъде обосновано като необходимо и отговарящо на целите от общ интерес, признати от Европейския съюз, или на необходимостта да се защитят правата и свободите на други хора. На практика това означава, че всяко ограничение трябва¹¹⁹:

- а) да бъде формулирано по ясен и предвидим начин;
- б) да бъде необходимо за постигането на цел от общ интерес или за защитата на правата и свободите на други хора;
- в) да бъде пропорционално на преследваната цел; и
- г) да зачита основното съдържание на засегнатите основни права.

В член 8, параграф 2 от Европейската конвенция за правата на човека също се признава, че намесата на държавните власти в правото на неприкосновеност на личния живот на дадено лице може да бъде оправдана като необходима в интерес на националната сигурност, обществената сигурност или предотвратяването на престъпления¹²⁰. Тези принципи, които лежат в основата на подхода на ЕС към запазването на данни, се повтарят в член 15, параграф 1 от директивата за правото на неприкосновеност на личния живот и електронни комуникации и в съображенията на директивата за запазване на данни.

¹¹⁸ Член 7 и член 8 от Хартата на основните права на Европейския съюз (ОВ С 83, 30.3.2010 г., стр. 389) гарантират, че всеки има право на „защита на неговите лични данни“. В член 16 от Договора за функционирането на Европейския съюз (ОВ С 83, 30.3.2010 г., стр. 1) също се гарантира, че всеки има право на „защита на личните му данни“.

¹¹⁹ Вж. контролния списък „Основни права“ на Комисията за всички законодателни предложения в Съобщението на Комисията „Стратегия за ефективно прилагане на Хартата на основните права от Европейския съюз“ (COM (2010) 573/4).

¹²⁰ Член 8 от Европейска конвенция за защита на правата на човека и основните свободи (ETS № 5), Съвет на Европа, 4.11.1950 г.

В последващата съдебна практика на Съда на Европейския съюз и на Европейския съд за правата на човека бяха определени условията, на които трябва да отговаря всяко ограничение на правото на неприкосновеност на личния живот. Тези решения са уместни от гледна точка на въпроса дали директивата трябва да се измени, по-специално по отношение на условията за достъп и използване на запазените данни.

Всички ограничения на правото на неприкосновеност на личния живот трябва да са формулирани точно и да позволяват предвидимост

По делото *Österreichischer Rundfunk* Съдът на Европейския съюз постанови, че всяка намеса в личния живот, предвидена в закона, трябва да бъде „формулирана достатъчно точно, така че гражданите да могат да съобразят поведението си по съответен начин ... [като така бъде спазено] изискването за предвидимост“.

Всички ограничения на правото на неприкосновеност на личния живот трябва да са необходими и да са налице минимални механизми за защита

По делото *Copland/Обединеното кралство*, свързано с наблюдение от страна на държавата на телефонните обаждания, кореспонденцията по електронна поща и използването на интернет от конкретно лице, Европейският съд за правата на човека постанови, че такова ограничение на правото на неприкосновеност на личния живот би могло да се счита за необходимо само ако се основава на съответно национално законодателство¹²¹. В *S. и Marper/Обединеното кралство*, свързано със запазването на ДНК профили или пръстови отпечатыци на лице, оправдано във връзка с дадено престъпление, или производството срещу което е прекратено преди да се стигне до осъдителна присъда, Съдът постанови, че такова ограничение на правото на неприкосновеност на личния живот би могло да се оправдае единствено ако отговаря на императивна обществена потребност, ако е пропорционално на преследваната цел и ако основанията, посочени от публичния орган, за да го обоснове, са уместни и достатъчни¹²². Съгласно основните принципи на защита на данните се изисква запазването на данни да е „пропорционално на целта, с която се събират, и периодът на съхранение да е ограничен“¹²³. За телефонното подслушване, тайното наблюдение и скритото събиране на данни „е от изключително значение ... да има ясни и подробни правила, които уреждат обхвата и прилагането на мерките, както и минимални защитни механизми относно *inter alia* продължителността, съхранението, използването, достъпа на трети лица, процедурите за опазване на целостта и поверителността на данните и процедурите за тяхното унищожаване, като по този начин се осигуряват достатъчни гаранции срещу риска от злоупотреба и произвол“.

Всички ограничения на правото на неприкосновеност на личния живот трябва да са пропорционални на общия интерес

¹²¹ Copland/Обединеното кралство, решение на Европейския съд за правата на човека, Страсбург, 3.4.2007 г., стр. 9.

¹²² Marper/Обединеното кралство, решение на Европейския съд за правата на човека, Страсбург, 4.12.2008 г., стр. 31.

¹²³ Marper, стр. 30.

По подобен начин в своето решение по делото *Schecke & Eifert* относно публикуването на всички получатели на земеделски субсидии в интернет¹²⁴ Съдът на Европейския съюз счете, че законодателните органи на ЕС изглежда не са предприели подходящите стъпки за постигане на баланс между зачитането на основното съдържание на правото на неприкосновеност на личния живот и общия интерес (прозрачност), признат от ЕС. По-специално Съдът счете, че законодателите не са взели предвид други условия, които да бъдат съобразени с целта и едновременно с това да засягат в по-малка степен правото на получателите на субсидии на зачитане на техния личен живот и правото на защита на техните лични данни. Съобразно с това Съдът постанови, че законодателите са надхвърлили границите на пропорционалността, тъй като „ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото“.

7.2. Критики във връзка с принципа на запазване на данни

Редица организации на гражданското общество писаха до Комисията, заявявайки, че по принцип запазването на данни е необосновано и ненужно ограничение на правото на лицата на неприкосновеност на личния живот. Те считат, че „поголовното и безразборно“ запазване на далекосъобщителни данни за трафика, местоположението и абонатите на лицата без тяхно съгласие представлява незаконно ограничаване на основните права. Вследствие на дело, заведено пред съдилищата в една държава-членка (Ирландия) от група за граждански права, въпросът за законосъобразността на директивата се очаква да бъде отнесен до Съда на Европейския съюз¹²⁵. Също така Европейският надзорен орган по защита на данните изрази съмнение относно необходимостта от мярката.

7.3. Призоваване за по-строги правила за сигурност на данните и защита на данните

В доклада на Работната група по член 29 относно второто действие по принудително изпълнение се посочва, че рисковете от нарушаване на поверителността на съобщенията и свободата на изразяване са присъщи на съхранението на данните за трафика изобщо. В него бяха отправени критики към определени аспекти от прилагането на директивата в национален план, по-специално регистрирането на данни, периодите на запазване, вида запазени данни и мерките за сигурност на данните. Работната група докладва за случаи, в които са били запазвани подробности от *съдържанието* на съобщения в интернет, извън обхвата на директивата, включително IP адреси на получатели и URL адреси на уебсайтове, горния колонтитул на електронни писма и списъка на получатели в полето „cc“. Поради това Работната група призова за поясняване, че категориите са изчерпателни и че на операторите не могат да се налагат задължения за запазване на допълнителни данни.

Европейският надзорен орган по защита на данните потвърди, че директивата „не е успяла да хармонизира националните законодателства“ и че използването на запазени

¹²⁴ Решение от 9.11.2010 г. по съединени дела Volker und Markus Schecke GbR/Land Hessen (C-92/09) и Eifert/Land Hessen (C-93/09) и Bundesanstalt für Landwirtschaft und Ernährung.

¹²⁵ На 5 май 2010 г. Върховният съд на Ирландия удовлетвори иска на *Digital Rights Ireland Limited* да се обърне към Съда на Европейския съюз по член 267 от Договора за функционирането на Европейския съюз.

данни не е строго ограничено до борбата със сериозните престъпления¹²⁶. Той заяви, че инструмент на ЕС, съдържащ правила относно задължителното запазване на данни, в случай на доказана необходимост, трябва да съдържа също и правила относно достъпа на правоприлагащите органи до данните и тяхното по-нататъшно използване. Той призова ЕС да приеме цялостна законодателна рамка, която не само да налага задължения на операторите да запазват данни, но също така да урежда начина, по който държавите-членки използват данните за целите на правоприлагането, така че да се създаде „правна сигурност за гражданите“.

Органите за защита на данните като цяло заявиха, че запазването на данни само по себе си представлява риск от потенциални нарушения на неприкосновеността на личния живот, който директивата не е отстранила на равнище ЕС, а вместо това държавите-членки са длъжни да гарантират спазването на националните правила за защита на данните. Макар да няма конкретни примери за сериозни нарушения на неприкосновеността на личния живот, рискът от нарушения на сигурността на данните остава налице и може да нараства с развитието на технологиите и тенденциите в различните форми на съобщения, независимо дали данните се съхраняват за търговски цели или за целите на сигурността, в рамките на или извън ЕС, освен ако се въведат допълнителни механизми за защита.

8. ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ

В настоящия доклад бяха подчертани редица ползи и области, в които е необходимо подобрение на настоящия режим на запазване на данни в ЕС. ЕС прие директивата в момент на повишена опасност от предстоящи терористични атаки. Оценката на въздействието, която Комисията възнамерява да направи, предоставя възможност да се оцени запазването на данни в ЕС, като се използват тестовете за необходимост и пропорционалност, като се има предвид и в интерес на вътрешната сигурност, гладкото функциониране на вътрешния пазар и укрепване на зачитането на неприкосновеността на личния живот и на основното право на защита на личните данни. Предложението на Комисията за преразглеждане на правната рамка на запазването на данни следва да се основава на следните заключения и препоръки.

8.1. ЕС следва да подкрепя и да урежда запазването на данни като мярка за сигурност

Повечето държави-членки считат, че правилата на ЕС относно запазването на данни продължават да бъдат необходим инструмент за правоприлагането, защитата на жертвите и системите на наказателно правосъдие. Въпреки ограниченията в някои аспекти, доказателствата, под формата на статистически данни и примери, предоставените от държавите-членки, свидетелстват за изключително важната роля на запазените данни за наказателното разследване. Тези данни осигуряват ценни улики и доказателства за предотвратяване и преследване на престъпленията и гарантиране на наказателно правосъдие. Тяхното използване е довеждало до осъдителни присъди по престъпления, които може би никога не биха били решени без запазването на данни. То е довеждало и до оправдаване на невинни лица. Хармонизираните правила в тази

¹²⁶ Реч на Peter Hustinx на конференцията „Прилагане на директивата за защита на данните“ („Taking on the Data Retention Directive“), 3 декември 2010 г.

област следва да гарантират, че запазването на данни е ефективен инструментът в борбата с престъпността, че индустрията разполага с правна сигурност в рамките на гладко функциониращ вътрешен пазар и че високото ниво на зачитане на неприкосновеността на личния живот и на защитата на личните данни се прилагат последователно в целия ЕС.

8.2. Транспонирането не е еднакво навсякъде

Законодателството за транспониране на директивата е в сила в 22 държави-членки. Значителната свобода, оставена на държавите-членки, да приемат мерки за запазването на данни по силата на член 15, параграф 1 от директивата за правото на неприкосновеност на личния живот и електронни комуникации затруднява изключително много оценката на директивата за запазване на данни. Налице са значителни различия между законодателствата за транспониране на директивата в сферата на ограничението на целите, достъпа до данните, периодите на запазване, защитата на данните, сигурността на данните и статистиката. Три държави-членки са в нарушение на директивата, тъй като тяхното законодателство за транспониране беше отменено от съответните им конституционни съдилища. Две други държави-членки все още предстои да транспонират директивата. Комисията ще продължи да работи с всички държави-членки, за да подпомогне да се осигури ефективно прилагане на директивата. Тя ще продължи също така да изпълнява ролята си за принудителното изпълнение на правото на ЕС, като в крайна сметка ще използва процедурата за нарушение, ако се налага.

8.3. Директивата не е хармонизирала напълно подхода спрямо запазването на данни и не е създала равни условия за операторите

Директивата осигури, че понастоящем запазването на данни се осъществява в повечето държави-членки. Директивата сама по себе си не гарантира, че запазените данни се съхраняват, извличат и използват при пълно спазване на правото на неприкосновеност на личния живот и на защитата на личните данни. Държавите-членки носят отговорност да гарантират, че тези права се спазват. Целта на директивата беше единствено частично хармонизиране на подходите спрямо запазването на данни. Поради това не е изненада, че няма единен подход, независимо дали от гледна точка на специфични разпоредби на директивата като ограничението на целите или периодите на запазване, или от гледна точка на аспекти извън нейния обхват като възстановяването на разходи. Отвъд обаче степента на вариране, изрично предвидена в директивата, различията в прилагането на запазването на данни на национално ниво създадоха значителни затруднения на операторите.

8.4. Разходите, които операторите понасят, следва да им се възстановяват по последователен начин

Продължава да няма правна сигурност за индустрията. Задължението да се запазват и извличат данни води до значителни разходи за операторите, особено за по-малките оператори, и операторите са засегнати и им се възстановяват разходи в различна степен в някои държави-членки в сравнение с други, макар че няма доказателства секторът на далекосъобщенията като цяло да е засегнат по неблагоприятен начин в резултат на прилагането на директивата. Комисията ще проучи по какъв начин може да се осигурява последователно възстановяване на разходите на операторите.

8.5. Осигуряване на пропорционалност на интегрирания процес на съхранение, извличане и използване

Комисията ще гарантира, че всяко бъдещо предложение, свързано със запазването на данни, спазва принципа на пропорционалност и е подходящо за постигане на целта за борба със сериозните престъпления и тероризма, както и не надхвърля необходимото за постигането на тази цел. Тя ще потвърди, че всички освобождавания или ограничения, свързани със защитата на личните данни, следва да се прилагат само доколкото са необходими. Комисията ще оцени обстойно последиците от по-строгото регулиране на съхранението, достъпа и използването на запазени данни за ефективността и ефикасността на системата на наказателно правосъдие и на правоприлагането, за неприкосновеността на личния живот и за разходите на публичната администрация и на операторите. По-специално следните области трябва да се проучат в оценката на въздействието:

- последователност на ограничението на целта, с която се запазват данни, и на видовете престъпления, за които до запазените данни може да се получи достъп и те да се използват;
- по-голямо хармонизиране, и по възможност съкращаване, на периодите на задължително запазване на данни;
- гарантиране на независим надзор на исканията за достъп и като цяло на режима на запазване и достъп до данните, прилаган във всички държави-членки;
- ограничаване на органите с право на достъп до данните;
- намаляване на категориите данни, които следва да се запазват;
- насоки относно техническите и организационните мерки за сигурност по отношение на достъпа до данните, включително процедурите за предаване;
- насоки за използване на данните, включително предотвратяване на събирането на данни; и
- разработване на приложими процедури за измерване и докладване с цел да се улесни сравнението на прилагането и оценяването на един бъдещ инструмент.

Комисията също така ще обмисли дали и как подходът на ЕС по отношение на съхраняването на данни може да допълни запазването на данни.

Като се позовава на контролния списък „Основни права“ и на подхода към управлението на информацията в областта на свободата, сигурността и правосъдието¹²⁷, Комисията ще разгледа всяка една от тези области съобразно с принципа на

¹²⁷ Вж. позоваването по-горе на съобщението относно прилагането на Хартата на основните права; „Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието“ (COM(2010) 385, 20.7.2010 г.).

пропорционалност и изискването за предвидимост. Тя ще осигури също така съгласуваност с настоящия преглед на правната рамка на ЕС за защита на данните¹²⁸.

8.6. Предстоящи стъпки

В светлината на тази оценка Комисията ще предложи преразглеждане на настоящата правна рамка на запазването на данни. Тя ще разработи редица варианти чрез консултации с правоприлагащите органи, съдебната власт, индустрията и сдруженията на потребителите, органите за защита на данните и организациите на гражданското общество. Тя ще изследва задълбочено обществените схващания за запазването на данни и неговото отражение върху поведението на лицата. Тези констатации ще бъдат взети предвид при оценката на въздействието на установените варианти на политика, която оценка ще бъде основа на предложението на Комисията.

¹²⁸ COM(2010) 609, 4.11.2010 г.

Приложение: Допълнителна статистика относно запазването на данни за трафика

Забележки за приложението:

1. Актуалност на данните означава времето, изтекло от датата на запазване на данните до датата, на която компетентният орган е поискал предаването на данните.
2. Свързани с интернет данни означава данни, касаещи интернет достъп, електронна поща по интернет и интернет телефония.
3. Статистическите данни за Чешката република, Латвия и Полша трябва да се разглеждат с определени уговорки (вж. раздел 5.1)

Статистически данни, подадени от държавите-членки за 2008 г.

Таблица 7: Искания за запазени данни за трафика по актуалност през 2008 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	102691	18440	10110	319	0	0	0	0	131560
Дания	2669	672	185	37	23	2	7	4	3599
Германия	9363	2336	985	0	0	0	0	0	12684
Естония	2773	733	157	827	0	0	0	0	4490
Ирландия	8981	2016	936	1855	90	85	78	54	14095
Гърция	Не е предоставена разбивка по актуалност.								
Испания	22629	15868	10298	4783	0	0	0	0	53578
Франция	Не е предоставена разбивка по актуалност.								
Италия	Не е предоставена информация.								
Кипър	30	4	0	0	0	0	0	0	34
Латвия	10539	2739	1368	1211	597	438	0	0	16892
Литва	55735	23817	5251	512	0	0	0	0	85315
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	810	59	0	0	0	0	0	0	869
Нидерландия	Не е предоставена разбивка по актуалност.								
Австрия	Не е предоставена разбивка по актуалност.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена разбивка по актуалност.								
Словакия	Не е предоставена информация.								
Финландия	9134	1144	448	214	268				4008
Швеция	Не е предоставена информация.								
Обединеното кралство	315350	88339	34665	19398	6385	2973	1536	1576	470222
Общо	533504	156167	64403	29156	7095*	3230*	1353*	1366*	1392281

* С изключение на Финландия

Таблица 8: Искания за запазени данни за трафика по видове данни през 2008 г. (в скобите е посочен броят случаи, в които исканията за данни не е могло да бъдат удовлетворени — ако е предоставена информация)				
Вид данни/ държава-членка	Фиксирана мрежова телефония	Мобилна телефония	Свързани с интернет данни	Общо
Белгия	Не е предоставена информация.			
България	Не е предоставена информация.			
Чешката република	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Дания	192 (0)	3273 (5)	134 (0)	3599 (5)
Германия	Не е предоставена разбивка по видове данни.			12684 (931)
Естония	4114 (1519)	376 (7)	Не е предоставена информация.	4490 (1526)
Ирландия	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Гърция	Не е предоставена разбивка по видове данни.			584
Испания	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Франция	Не е предоставена разбивка по видове данни.			503437
Италия	Не е предоставена информация.			
Кипър	3 (0)	31 (5)	0 (0)	34 (5)
Латвия	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Литва	765 (72)	84550 (5657)	Не е предоставена информация.	85315 (5729)
Люксембург	Не е предоставена информация.			
Унгария	Не е предоставена информация.			
Малта	29 (0)	748 (120)	92 (13)	869 (133)
Нидерландия	Не е предоставена разбивка по видове данни.			85000
Австрия	Не е предоставена разбивка по видове данни.			3093
Полша	Не е предоставена информация.			
Португалия	Не е предоставена информация.			
Румъния	Не е предоставена информация.			
Словения	Не е предоставена разбивка по видове данни.			2821
Словакия	Не е предоставена информация.			
Финландия	Не е предоставена разбивка по видове данни.			4008
Швеция	Не е предоставена информация.			
Обединеното кралство	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Общо				1392281

Таблица 9: Искания за запазени данни за трафика за фиксирана мрежова телефония, които са били предадени, по актуалност, през 2008 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	3669	916	143	124	0	0	0	0	4852
Дания	133	28	31	0	0	0	0	0	192
Германия	Не е предоставена информация.								
Естония	1876	161	74	484	0	0	0	0	2595
Ирландия	4118	712	197	182	32	21	23	16	5301
Гърция	Не е предоставена информация.								
Испания	1948	1431	741	328	0	0	0	0	4448
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	3	0	0	0	0	0	0	0	3
Латвия	698	213	167	193	104	137	0	0	1512
Литва	251	442	0	0	0	0	0	0	693
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	28	1	0	0	0	0	0	0	29
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	54805	27052	5340	753	1135	437	1050	175	90747
Общо	67529	30956	6693	2064	1271	595	1073	191	110372

Таблица 10: Искания за запазени данни за графика за мобилна телефония, които са били предадени, по актуалност, през 2008 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	98232	17013	7518	1	0	0	0	0	122764
Дания	2433	628	143	33	20	1	7	3	3268
Германия	Не е предоставена информация.								
Естония	248	58	35	28	0	0	0	0	369
Ирландия	4326	820	230	240	57	63	52	37	5825
Гърция	Не е предоставена информация.								
Испания	17403	12114	7444	3052	0	0	0	0	40013
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	23	3	0	0	0	0	0	0	26
Латвия	8928	2298	1085	746	394	257	0	0	13708
Литва	55484	23375	14	20	0	0	0	0	78893
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	575	53	0	0	0	0	0	0	628
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	229375	52241	26228	16040	3333	521	339	1344	329421
Общо	417027	108603	42697	20160	3804	842	398	1384	594915

Таблица 11: Искания за запазени данни за трафика за свързани с интернет данни, които са били предадени, по актуалност, през 2008 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	737	412	137	168	0	0	0	0	1454
Дания	102	14	11	2	3	1	0	1	134
Германия	Не е предоставена информация.								
Естония	Не е предоставена информация.								
Ирландия	492	460	498	1422	0	0	0	0	2872
Гърция	Не е предоставена информация.								
Испания	3278	2323	2113	1403	0	0	0	0	9117
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	0	0	0	0	0	0	0	0	0
Латвия	424	150	75	219	74	34	0	0	976
Литва	Не е предоставена информация.								
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	76	3	0	0	0	0	0	0	79
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	31170	9046	3097	2605	1917	2015	147	57	50054
Общо	36279	12408	5931	5819	1994	2050	147	58	64686

Статистически данни, подадени от държавите-членки за 2009 г.

Таблица 12: Искания за запазени данни по актуалност през 2009 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	210975	56623	11620	1053	0	0	0	0	280271
Дания	2980	685	179	104	54	38	12	14	4066
Германия	Не е предоставена информация.								
Естония	4299	1836	1210	1065	0	0	0	0	8410
Ирландия	8117	1652	805	297	168	134	69	41	11283
Гърция	Не е предоставена информация.								
Испания	29775	19346	13999	6970	0	0	0	0	70090
Франция	Не е предоставена разбивка по актуалност.								514813
Италия	Не е предоставена информация.								
Кипър	31	8	1	0	0	0	0	0	40
Латвия	20758	2414	1088	796	565	475	0	0	26096
Литва	30247	35456	5886	884	0	0	0	0	72473
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	3336	362	151	174	0	0	0	0	4023
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Полша	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Словения	Не е предоставена разбивка по актуалност.								1918
Словакия	Не е предоставена разбивка по актуалност.								5214
Финландия	2000	1310	532	152	76	0	0	0	4070
Швеция	Не е предоставена информация.								
Обединеното кралство	Не е предоставена информация.								
Общо	954845	297998	110996	64021	27961	24571	14065	34683	2051085

Таблица 13: Искания за запазени данни по видове данни през 2009 г. (в скобите е посочен броят случаи, в които исканията за данни не е могло да бъдат удовлетворени — ако е предоставена информация)				
Вид данни/ държава-членка	Фиксирана мрежова телефония	Мобилна телефония	Свързани интернет данни	Общо
Белгия	Не е предоставена информация.			
България	Не е предоставена информация.			
Чешката република	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Дания	133 (0)	3771 (10)	162 (1)	4066 (11)
Германия	Не е предоставена информация.			
Естония	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Ирландия	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Гърция	Не е предоставена информация.			
Испания	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Франция	Не е предоставена разбивка по видове данни.			514813
Италия	Не е предоставена информация.			
Кипър	0 (0)	23 (3)	14 (0)	40 (3)
Латвия	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Литва	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Люксембург	Не е предоставена информация.			
Унгария	Не е предоставена информация.			
Малта	156 (10)	3693 (882)	174 (10)	4023 (902)
Нидерландия	Не е предоставена информация.			
Австрия	Не е предоставена информация.			
Полша	Не е предоставена разбивка по видове данни.			1048318
Португалия	Не е предоставена информация.			
Румъния	Не е предоставена информация.			
Словения	Не е предоставена разбивка по видове данни.			1918 (48)
Словакия	Не е предоставена разбивка по видове данни.			5214 (157)
Финландия	Не е предоставена разбивка по видове данни.			4070
Швеция	Не е предоставена информация.			
Обединеното кралство	Не е предоставена информация.			
Общо				2051082 (1069885)

Таблица 14: Искания за запазени данни за <i>фиксирана мрежова телефония</i> , които са били предадени, по актуалност, през 2009 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	9919	2907	47	36	0	0	0	0	12909
Дания	105	19	7	2	0	0	0	0	133
Германия	Не е предоставена информация.								
Естония	2254	866	599	424	0	0	0	0	4143
Ирландия	3934	337	69	70	50	39	16	11	4526
Гърция	Не е предоставена информация.								
Испания	2371	1492	844	348	0	0	0	0	5055
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	0	0	0	0	0	0	0	0	0
Латвия	744	253	157	143	68	89	0	0	1454
Литва	469	773	73	6	0	0	0	0	1321
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	83	25	18	20	0	0	0	0	146
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	Не е предоставена информация.								
Общо	19879	6672	1814	1049	118	128	16	11	29687

Таблица 15: Искания за запазени данни за <i>мобилна телефония</i> , които са били предадени, по актуалност, през 2009 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	197620	48841	472	0	0	0	0	0	246933
Дания	2777	639	162	98	47	19	12	7	3761
Германия	Не е предоставена информация.								
Естония	318	397	96	70	0	0	0	0	881
Ирландия	3669	835	220	210	115	92	50	28	5219
Гърция	Не е предоставена информация.								
Испания	24065	15648	11147	5273	0	0	0	0	56133
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	17	16	0	0	0	0	0	0	23
Латвия	18832	1912	778	515	394	263	0	0	22694
Литва	25713	19595	28	0	0	0	0	0	45336
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	2332	246	111	122	0	0	0	0	2811
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	Не е предоставена информация.								
Общо	275343	88119	13014	6288	556	374	62	35	383791

Таблица 16: Искания за запазени свързани с интернет данни, които са били предадени, по актуалност, през 2009 г.									
Актуалност на поисканите данни (месеци)/държава-членка	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Общо
Белгия	Не е предоставена информация.								
България	Не е предоставена информация.								
Чешката република	3369	4811	861	942	0	0	0	0	9983
Дания	98	27	10	4	4	7	0	1	151
Германия	Не е предоставена информация.								
Естония	315	145	56	102	0	0	0	0	618
Ирландия	489	455	502	0	0	0	0	0	1446
Гърция	Не е предоставена информация.								
Испания	3339	2206	2008	1349	0	0	0	0	8902
Франция	Не е предоставена информация.								
Италия	Не е предоставена информация.								
Кипър	12	2	0	0	0	0	0	0	14
Латвия	852	198	74	90	88	86	0	0	1388
Литва	4060	15087	1	88	0	0	0	0	19236
Люксембург	Не е предоставена информация.								
Унгария	Не е предоставена информация.								
Малта	150	14	0	0	0	0	0	0	164
Нидерландия	Не е предоставена информация.								
Австрия	Не е предоставена информация.								
Полша	Не е предоставена информация.								
Португалия	Не е предоставена информация.								
Румъния	Не е предоставена информация.								
Словения	Не е предоставена информация.								
Словакия	Не е предоставена информация.								
Финландия	Не е предоставена информация.								
Швеция	Не е предоставена информация.								
Обединеното кралство	Не е предоставена информация.								
Общо	12684	22945	3512	2575	92	93	0	1	41902