

I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА
ДАННИТЕ

**Становище на Европейския надзорен орган по защита на данните относно текущите преговори,
водени от Европейския съюз за Търговско споразумение за борба с фалшифицирането (АСТА)**

(2010/С 147/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

като взе предвид Договора за създаване на Европейския съюз, и по-специално член 16 от него,

като взе предвид Хартата на основните права на Европейския съюз, и по-специално член 8 от нея,

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ⁽¹⁾,

като взе предвид Директива 2002/58/ЕО 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 ⁽²⁾,

като взе предвид Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни ⁽³⁾, и по-специално член 41 от него,

ПРИ НАСТОЯЩОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

1. Европейският съюз участва в преговори за изготвяне на Търговско споразумение за борба с фалшифицирането (АСТА). Тези преговори започнаха през 2007 г. между първоначална група от заинтересовани страни, след което продължиха в по-широка група участници; към днешна дата в преговорите участват Австралия, Канада, Евро-

пейският съюз, Япония, Корея, Мексико, Мароко, Нова Зеландия, Сингапур, Швейцария и Съединените щати. Европейската комисия получи мандат от Съвета да встъпи в тези преговори през 2008 г.

2. Европейският надзорен орган по защита на данните (ЕНОЗД) отчита, че трансграничната търговия с фалшиви и пиратски стоки е явление, будещо нарастваща загриженост, което често включва участието на организирани престъпни мрежи и налага въвеждането на подходящи механизми за сътрудничество на местно равнище за борба с този вид престъпност.
3. ЕНОЗД подчертава, че водените от Европейския съюз преговори за многостранно споразумение с основен предмет упражняването на правата върху интелектуална собственост повдигат значими въпроси във връзка с въздействието на предприетите мерки за борба с фалшифицирането и пиратството върху основните права на физическите лица, и по-специално върху правата им на неприкосновеност на личния живот и защита на данните.
4. Във връзка с това ЕНОЗД изразява своето съжаление, че Европейската комисия не се е консултирала с него относно съдържанието на това споразумение. Поради това ЕНОЗД прие по собствена инициатива настоящото становище на основание на член 41, параграф 2 от Регламент (ЕО) № 45/2001, за да предостави на Комисията насоки относно аспектите, свързани с неприкосновеността на личния живот и защитата на данните, които следва да бъдат взети предвид при воденото на преговорите за АСТА.

II. АКТУАЛНО СЪСТОЯНИЕ И ПРЕДВИДЕНО СЪДЪРЖАНИЕ
НА АСТА

5. Седмият кръг от преговорите се проведе в Мексико от 26 до 29 януари 2010 г. с цел сключване на споразумението през 2010 г. До момента, обаче, не е публикуван официален проектотекст на споразумението.

⁽¹⁾ ОВ L 281, 23.11.1995 г., стр. 31.

⁽²⁾ ОВ L 201, 31.7.2002 г., стр. 37.

⁽³⁾ ОВ L 8, 12.1.2001 г., стр. 1.

6. Преговорите се водят с оглед приемане на ново многостранно споразумение, което има за цел по-ефикасно обезпечаване на упражняването на правата върху интелектуална собственост и борба с фалшифицирането и пиратството. Ако това ново споразумение бъде прието, то ще въведе по-ефективни международни стандарти за действия срещу значителните нарушения на права върху интелектуална собственост. Генерална дирекция „Търговия“ на Европейската комисия е посочила по-конкретно, че „документът е насочен срещу дейностите по фалшифициране и пиратство, които засягат съществено търговски интереси, а не срещу дейности на граждани“ ⁽⁴⁾.
7. Що се отнася до съдържанието на споразумението, в документа *Резюме на основните обсъждани елементи*, публикуван от генерална дирекция „Търговия“ на Европейската комисия през ноември 2009 г., се посочва, че дейностите за постигане на целта на АСТА за борба с пиратството и фалшифицирането ще имат три основни компонента: i) международно сътрудничество; ii) практики по правоприлагане и iii) определяне на законодателна рамка за упражняване на права върху интелектуална собственост в няколко области и по-специално в цифровата среда ⁽⁵⁾. Предвидените мерки ще бъдат свързани по-конкретно с правни процедури (като разпореждания и временни мерки), ролята и отговорностите на доставчиците на интернет услуги за възпиране нарушенията на авторски права в интернет и мерките за трансгранично сътрудничество за недопускане на движението на стоки през границите. Публикуваната информация, обаче, представя само в общи линии споразумението и не разглежда в детайли конкретни мерки.
8. ЕНОЗД отбелязва, че, макар че обявената цел на АСТА е да преследва само значителни нарушения на права върху интелектуална собственост, не може да се изключи възможността в приложното поле на споразумението да попаднат дейности на отделни граждани, особено във връзка с осъществяването на мерки за упражняване на права в цифровата среда. ЕНОЗД подчертава, че това налага да бъдат предвидени подходящи гаранции за защита на основните права на физическите лица. Освен това обхватът на законодателството за защита на данните включва всички физически лица, включително тези, които потенциално участват в дейности по фалшифициране и пиратство; със сигурност борбата срещу значителните нарушения ще включва и обработка на лични данни.
9. Във връзка с това ЕНОЗД настоятелно приканва Европейската комисия да започне публичен и прозрачен диалог относно АСТА, например посредством процедура на публична консултация, което също така ще помогне да се гарантира, че мерките, които ще бъдат приети, съответстват на нормативните изисквания на ЕС относно неприкосновеността на личния живот и защитата на данните.
- споразумението, да осигурят подходящ баланс между изискванията за защита на правата върху интелектуална собственост и на правата на физическите лица на неприкосновеност на личния живот и защита на данните.
11. ЕНОЗД подчертава, че неприкосновеността на личния живот и защитата на данните са основни ценности на Европейския съюз, признати в член 8 от Европейската конвенция за защита на правата на човека и основните свободи и в член 7 и член 8 от Хартата на основните права на ЕС ⁽⁶⁾, които трябва да бъдат зачитани във всички политики и правила, приемани от ЕС съгласно член 16 от Договора за функционирането на Европейския съюз (ДФЕС).
12. Освен това ЕНОЗД подчертава, че всяко споразумение относно АСТА, постигнато от ЕС, трябва да е съобразено с правните задължения, наложени на ЕС във връзка със законодателството относно неприкосновеността на личния живот и защитата на данните, както се посочва по-специално в Директива 95/46/ЕО, Директива 2002/58/ЕО ⁽⁷⁾ и в съдебната практика на Европейския съд по правата на човека ⁽⁸⁾ и на Съда на ЕС ⁽⁹⁾.
13. Правата на неприкосновеност на личния живот и на защита на данните трябва да бъдат отчетени от самото начало на преговорите, а не когато схемите и процедурите са вече определени и договорени и е твърде късно да се търсят алтернативни решения, съответстващи на принципа за неприкосновеност на личния живот.
14. С оглед на ограничения обем на информацията, предоставена за публично ползване, ЕНОЗД отбелязва, че не е в състояние да направи анализ на конкретните разпоредби на АСТА. Поради това в своето становище ЕНОЗД ще се съсредоточи върху разглеждане на потенциалните заплахи за неприкосновеността на личния живот и защитата на данните, произтичащи от възможни конкретни мерки, които според наличната информация може да бъдат предприети в изпълнение на споразумението в следните две области: обезпечаването на упражняването на правата върху интелектуална собственост в цифровата среда (глава IV) и механизмите за международно сътрудничество (глава V).
10. ЕНОЗД призовава настоятелно ЕС, и по-специално Европейската комисия, която е получила мандат да сключи

III. ОБХВАТ НА БЕЛЕЖКИТЕ НА ЕНОЗД

10. ЕНОЗД призовава настоятелно ЕС, и по-специално Европейската комисия, която е получила мандат да сключи

⁽⁴⁾ Вж. http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, стр. 2.

⁽⁵⁾ Вж. бележка под линия 2 по-горе.

⁽⁶⁾ Харта на основните права на Европейския съюз, ОВ С 303, 14.12.2007 г., стр. 1.

⁽⁷⁾ Директива 2002/58/ЕО 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.

⁽⁸⁾ Която тълкува основните елементи и условия, предвидени в член 8 от Европейската конвенция за защита на правата на човека и основните свободи (ЕКЗПЧОС), приета в Рим на 4 ноември 1950 г., във връзка с прилагането им в различни области. Вж. по-специално съдебната практика, цитирана в текста на настоящото становище.

⁽⁹⁾ Вж. по-конкретно: дело C-275/06, *Productores de Música de España (Promusicae)*, ECR [2008], стр. I-271 и дело C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, все още непубликувано.

IV. ОБЕЗПЕЧАВАНЕ НА УПРАЖНЯВАНЕТО НА ПРАВАТА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ В ЦИФРОВАТА СРЕДА

IV.1. Необходимостта от анализ на последиците за неприкосновеността на личния живот/защитата на данните от „политиката на прекъсване на достъпа до интернет след три предупреждения“

15. Според Европейската комисия с АСТА ще се въведе законодателна рамка за борба с пиратството в цифровата среда ⁽¹⁰⁾. Тази рамка ще установи условията за търсене на отговорност от доставчиците на интернет услуги и други онлайн посредници ⁽¹¹⁾ за неправомерно ползване на материали, предмет на авторски права, предавани чрез техните съоръжения. Рамката може да предвижда също и налагане на мерки и правни средства за защита по отношение на потребители на интернет на основание на неправомерно качване или изтегляне на материали, предмет на авторски права. Макар че липсва подробна официална информация за такава рамка, въз основа на информацията, достъпна чрез различни канали, може са предположи, че тя вероятно ще включва налагане на задължения на доставчиците на интернет услуги да въведат „политики на прекъсване на достъпа до интернет след три предупреждения“, наричани също и схеми за „степенуван отговор“. Подобни схеми ще позволят на носителите на авторски права да извършват наблюдение върху потребителите на интернет и да разкриват предполагаеми нарушения на авторски права. След като се свържат с доставчика на интернет услуги на предполагаемия нарушител, доставчикът следва да предупреди потребителя, идентифициран като нарушител; достъпът на нарушителя до интернет ще бъде прекъснат след отправяне на три предупреждения.
16. Успоредно с преговорите за АСТА някои държави-членки, между които Франция, прилагат политики на прекъсване на достъпа до интернет след три предупреждения. Такива политики се обсъждат и на различни форуми на ЕС, като провеждания понастоящем с помощта на генерална дирекция „Вътрешен пазар и услуги“ Диалог на заинтересованите страни относно незаконното качване и изтегляне, във връзка с приемането на Съобщението на Комисията Усъвършенстване на упражняването на правата на интелектуална собственост в рамките на вътрешния пазар ⁽¹²⁾. Дискусии на тази тема се провеждат и в Европейския парламент в контекста на текущия дебат по проект за резолюция на Парламента относно усъвършенстването на упражняването на правата на интелектуална собственост в рамките на вътрешния пазар (известен като Докладът „Gallo“).

⁽¹⁰⁾ Вж. бележка под линия 2 по-горе.

⁽¹¹⁾ Различните онлайн посредници могат да бъдат определени в съответствие с техните функционални роли. На практика, обаче, посредниците обикновено изпълняват по няколко от тези функции. Онлайн посредниците включват: а) доставчици на достъп: потребителите се свързват с мрежата посредством установяване на връзка със сървър на доставчика на достъп; б) прожеви доставчици: те предоставят рутери, т.е. необходимите технически средства за предаване на данни; в) доставчици на хостинг: те предоставят под наем дисково пространство на своите сървъри, на което потребителите или доставчиците на съдържание могат да качат съдържание. Потребителите могат да качват и изтеглят материали в онлайн услуга, като бюлетин или P2P мрежи.

⁽¹²⁾ Съобщение на Комисията до Съвета, Европейския парламент и Европейския икономически и социален комитет — Усъвършенстване на упражняването на правата на интелектуална собственост в рамките на вътрешния пазар, Брюксел, 11 септември 2009 г., COM(2009) 467 окончателен.

17. Подобни практики представляват значително вмешателство в частната сфера на физическите лица. Те предполагат извършване на общо наблюдение върху дейностите на потребителите на интернет, включително върху тези, които са напълно законни. Те засягат милиони потребители на интернет, които спазват законите, включително много деца и юноши. Тези практики се осъществяват от частни лица, а не от правоприлагащи органи. Освен това, понастоящем интернет има централно значение за почти всички аспекти на съвременния живот, поради което прекъсването на достъпа до интернет може да има много големи последици, като например изолиране на физическите лица от тяхната работа, култура, приложения на електронното правителство и т.н.

18. На този фон е уместно да се оцени доколко тези политики съответстват на законодателството на ЕС за защита на данните и неприкосновеността на личния живот, и по-специално дали политиките на прекъсване на достъпа до интернет след три предупреждения са необходима мярка за гарантиране упражняването на правата върху интелектуална собственост. Във връзка с това следва по-нататък да се направи анализ дали съществуват други методи, които представляват по-малко вмешателство.

19. Все още не е ясно дали политиките на прекъсване на достъпа до интернет след три предупреждения ще бъдат включени в АСТА. Въвеждането на такива политики, обаче, се обмисля и в други области и те имат потенциално изключително голямо въздействие върху защитата на личните данни и неприкосновеността на личния живот. Поради тези причини ЕНОЗД счита за необходимо да разгледа тези политики в настоящото становище. Преди да пристъпи към посочения по-горе анализ, ЕНОЗД ще опише накратко приложимата рамка за защита на данните и неприкосновеност на личния живот.

20. Трябва да се отбележи, че в допълнение към защитата на данните и неприкосновеността на личния живот политиките на прекъсване на достъпа до интернет след три предупреждения пораждаат загриженост и във връзка с други ценности, като правото на справедлив процес и свободата на словото. Настоящото становище, обаче, ще разгледа само въпросите, свързани със защитата на личните данни и неприкосновеността на личния живот на физическите лица.

IV.2. Политиките на прекъсване на достъпа до интернет след три предупреждения и прилагането на законодателната рамка на ЕС за защита на данните/неприкосновеност на личния живот

Как може да бъдат въведени политики на прекъсване на достъпа до интернет след три предупреждения?

21. Казано накратко, прилагайки политики на прекъсване на достъпа до интернет след три предупреждения, носителите на авторски права ще идентифицират с помощта на автоматизирани технически средства, които могат да бъдат предоставени от трети страни, предполагаеми нарушения на

авторски права, като извършват наблюдение върху дейностите на потребителите на интернет, например посредством проследяване на форуми и блогове, или като се включват в реет-то-реет мрежи, представяйки се за потребители, споделящи файлове, за да идентифицират лица, споделящи файлове, за които се предполага, че споделят материали, предмет на авторски права⁽¹³⁾.

22. След като идентифицират потребители на интернет, за които се предполага, че извършват нарушения на авторски права, чрез събиране на техните Internet Protocol (IP) адреси, носителите на авторски права ще изпращат IP адресите на тези потребители на съответния доставчик или доставчици на интернет услуги, които ще изпращат на своите абонати, ползващи тези IP адреси, предупреждения относно тяхното предполагаемо участие в нарушения на авторски права. Получаването на определен брой предупреждения от доставчика на интернет услуги ще води до автоматично прекратяване или временно спиране на достъпа на потребителя до интернет от страна на доставчика⁽¹⁴⁾.

Приложимата законодателна рамка на ЕС относно защитата на данните/неприкосновеността на личния живот

23. Политиките на прекъсване на достъпа до интернет след три предупреждения трябва да отговарят на изискванията, произтичащи от правото на неприкосновеност на личния живот, предвидено в член 8 от Европейската конвенция за защита на правата на човека и основните свободи и член 7 от Хартата на основните права на Европейския съюз, както и от правото на защита на данните, предвидено в член 8 от Хартата на основните права и член 16 от ДФЕС, и допълнително уредени в Директива 95/46/ЕО и Директива 2002/58/ЕО.
24. По мнението на ЕНОЗД извършването на наблюдение върху поведението на потребителите на интернет и събирането на данни за техните IP адреси е равностойно на нарушение на техните права на зачитане на личния им живот и кореспонденцията им; с други думи, става дума за незачитане на правото им на неприкосновеност на личния живот. Това становище съответства на съдебната практика на Европейския съд по правата на човека⁽¹⁵⁾.
25. Директива 95/46/ЕО е приложима⁽¹⁶⁾, защото политиките на прекъсване на достъпа до интернет след три предупреждения предполагат обработване на IP адреси, които

във всички случаи при съответните обстоятелства следва да се считат за лични данни. IP адресите са идентификационни номера, които имат вид на поредици от цифри, разделени с точки, например: 122.41.123.45. Потребителят получава достъп до интернет след сключване на договор с доставчик на интернет услуги. Когато потребителят желае да се свърже с интернет, той ползва IP адрес, определен от устройството, което използва за достъп до мрежата (например компютър)⁽¹⁷⁾.

26. Когато потребител извършва определено действие, например качва материали в интернет, той може да бъде идентифициран от трети страни посредством IP адреса, който използва. Например, потребителят, ползващ IP адрес 122.41.123.45, е качил материали, за които се предполага, че нарушават авторски права, чрез P2P услуга в 15,00 ч. на 1 януари 2010 г. Доставчикът на интернет услуги има възможност да свърже използвания IP адрес с името на потребителя, на когото е предоставил адреса, и по този начин да установи неговата самоличност.

27. Позовавайки се на определението за лични данни, съдържащо се в член 2 на Директива 95/46/ЕО: „всяка информация, свързана с идентифицирано или подлежащо на идентификация лице („съответно физическо лице“); за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер“⁽¹⁸⁾, можем да заключим единствено, че IP адресите и информацията за действията, свързани с тези адреси, са лични данни във всички случаи, които имат отношение към темата. В действителност IP адресът служи като идентификационен номер, който позволява да се открие името на потребителя, на който този IP адрес е бил предоставен. Освен това информацията, която се събира за потребителя, ползващ IP адреса („той/тя е качил/качила определени материали в интернет страницата ZS в 15,00 ч. на 1 януари 2010 г.“), е свързана със, т.е. очевидно се отнася до действия на подлежащо на установяване физическо лице (ползвателят на IP адреса), и следователно също трябва да се счита за лични данни.

⁽¹³⁾ P2P технологията представлява разпределена софтуерна архитектура, която позволява даден компютър да се свърже с други компютри и да обменя пряко данни с тях.

⁽¹⁴⁾ Възможните алтернативни санкции включват ограничаване на функционалността на връзката към интернет, например намаляване на скоростта на връзката, обема на прехвърляните данни и т.н.

⁽¹⁵⁾ Вж. по-специално ЕСПЧ, 26 юни 2006 г., *Weber и Saravia срещу Германия* (dec.), № 54934/00, параграф 77 и ЕСПЧ, 1 юли 2008 г., *Liberty и други срещу Обединеното кралство*, № 58243/00.

⁽¹⁶⁾ Съдът е възприел широкообхванат подход по отношение на приложимостта на Директива 95/46/ЕО, чиито разпоредби трябва да се тълкуват с оглед на член 8 от Европейската конвенция за защита на правата на човека и основните свободи. В своето решение от 20 май 2003 г., *Rundfunk*, обединени дела C-465/00, C-138/01 и C-139/01, ECR [2003], стр. I-4989, параграф 68, Съдът заявява, че „разпоредбите на Директива 95/46/ЕО, доколкото те уреждат дейности по обработване на лични данни, при които е възможно да бъдат нарушени основни свободи, и по-специално правото на неприкосновеност на личния живот, трябва по необходимост да се тълкуват в светлината на основните права, които, съгласно установената съдебна практика, са неразделна част от общите принципи на правото, чието спазване гарантира Съдът“.

⁽¹⁷⁾ IP адресът, предоставен от доставчика на интернет услуги на потребителя физическо лице, може да бъде еднакъв винаги, когато последният ползва интернет (т.нар. статични IP адреси). Други IP адреси са динамични, което означава, че доставчикът на достъп до интернет предоставя различен IP адрес на своите клиенти при всяко тяхно свързване с интернет. Разбира се, доставчикът на интернет услуги може да свърже IP адреса с потребителя, на когото е предоставил (динамичния или статичен) IP адрес.

⁽¹⁸⁾ Съображение 26 допълва това определение: „като имат предвид, че принципите на защита трябва да се прилагат за всяка информация, отнасяща се до идентифицирано лице или подлежащо на идентификация лице; като имат предвид, че за да се определи дали едно лице подлежи на идентификация, следва да се разглежда съвкупността от всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице с цел идентифицирането на даденото лице; като имат предвид, че принципите на защита не се отнасят до данни, които са направени анонимни по начин, който прави невъзможно идентифицирането на съответното физическо лице; ...“.

28. Тези виждания се споделят изцяло от работната група по член 29, която е заявила в свой документ, посветен на въпросите, свързани със защитата на данните по отношение на правата върху интелектуална собственост, че IP адресите, които биват събирани с цел обезпечаване упражняването на права върху интелектуална собственост, т.е. за идентифициране на потребители на интернет, за които се предполага, че са нарушили права върху интелектуална собственост, представляват лични данни, доколкото те се използват за принудително упражняване на такива права срещу дадено физическо лице ⁽¹⁹⁾.
29. Приложима е и Директива 2002/58/ЕО, тъй като политиките на прекъсване на достъпа до интернет след три предупреждения предполагат събиране на данни за трафика и комуникациите. Директива 2002/58/ЕО регламентира използването на такива данни и предвижда прилагане на принципа на поверителност на комуникациите, осъществявани посредством публични комуникационни мрежи, и на данните, съдържащи се в тези комуникации.

IV.3. Дали политиките на прекъсване на достъпа до интернет след три предупреждения представляват необходима мярка?

30. Член 8 от ЕКЗПЧОС въвежда принципа на необходимост, съгласно който всяка мярка, която нарушава правото на неприкосновеност на личния живот на физическите лица, се допуска само, ако представлява необходима мярка в едно демократично общество за постигане на законна цел ⁽²⁰⁾. Принципът на необходимост е залегнал и в член 7 и член 13 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО ⁽²¹⁾. Принципът изисква извършване

на анализ на пропорционалността на мярката, която трябва да бъде оценена въз основа на баланс на засегнатите интереси, който се разглежда в контекста на демократичното общество като цяло ⁽²²⁾. Освен това той предполага и извършване на проверка за наличие на алтернативни мерки, които представляват по-малко вмешателство.

31. Макар че ЕНОЗД признава значението на упражняването на правата върху интелектуална собственост, той застъпва позицията, че политиката на прекъсване на достъпа до интернет след три предупреждения, в практикуваната понастоящем форма (включваща определени елементи на обща приложимост), представлява непропорционална мярка, поради което не може да се счита за необходима мярка. Освен това ЕНОЗД е убеден, че съществуват алтернативни решения, които представляват по-малко вмешателство, както и че предвидените политики могат да се прилагат по начин, представляващ по-малко вмешателство, или с по-ограничен обхват. Подходът на „три предупреждения“ поражда проблеми и на по-конкретно юридическо ниво. Тези заключения ще бъдат обяснени по-долу.

Политиките на „три предупреждения“ са непропорционални

32. ЕНОЗД желае да подчертае значителните последствия от наложените мерки. В това отношение трябва да се изтъкнат следните елементи:

- i) фактът, че извършването (без привличане на вниманието) наблюдение ще засегне милиони физически лица и всички потребители, независимо дали по отношение на тях са налице подозрения;
- ii) извършването на наблюдението предполага системно записване на данни, някои от които могат да послужат за завеждане на граждански и дори наказателни дела срещу граждани; това означава, също така, че част от събраната информация представлява и чувствителни данни по смисъла на член 8 от Директива 95/46/ЕО, която изисква по-ефикасни гаранции за защита;
- iii) може да се очаква, че в резултат на наблюдението ще възникнат множество случаи на необосновани подозрения. Въпросът дали е налице нарушение на авторски права няма очевиден отговор „да“ или „не“. В много случаи съдилищата трябва да анализират значителни обеми технически и юридически детайли, описани на десетки страници, за да се произнесат дали е налице нарушение ⁽²³⁾;

⁽¹⁹⁾ Работна група по член 29, Работен документ относно въпросите на защитата на данните, свързани с права върху интелектуална собственост (WP 104), приет на 18 януари 2005 г. Тази работна група е създадена в изпълнение на член 29 от Директива 95/46/ЕО. Тя действа като независим европейски надзорен орган по въпросите на защитата на данните и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО. Вж. Също становище № 4/2007 на работната група относно понятието за лични данни (WP 136), прието на 20 юни 2007 г., и по-специално стр. 16.

⁽²⁰⁾ Член 8 от ЕКЗПЧОС съдържа изрично изискване всяка намеса или ограничение да бъдат „необходими в едно демократично общество“.

⁽²¹⁾ Член 13 от Директива 95/46/ЕО допуска налагане на ограничение, само когато подобно ограничение представлява „необходима мярка за гарантиране на: а) националната сигурност; б) отбраната; в) обществената сигурност; г) предотвратяването, разследването, разкриването и преследването на утаени престъпления или за нарушения на етичните кодекси при регламентираните професии; г) предотвратяването, разследването, разкриването и преследването на утаени престъпления или за нарушения на етичните кодекси при регламентираните професии; е) функции по наблюдение, проверка или регламентиране, свързани, дори случайно, с упражняването на официални правомощия в случаите, посочени в букви в), г) и д); ж) защита на съответното физическо лице или на правата и свободите на други лица“. Член 15 от Директива 2002/58/ЕО съдържа изискването „такова ограничаване да представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО“.

⁽²²⁾ Вж. също ЕСПЧ, 2 август 1984 г., *Malone срещу Обединеното кралство*, серия А № 82, стр. 32, параграфи 81 и следващи и ЕСПЧ, 4 декември 2008 г., *Marper срещу Обединеното кралство* [GC], № 30562/04 и № 30566/04, параграфи 101 и следващи.

⁽²³⁾ В някои случаи съдилищата трябва да определят дали материалите са в действителност предмет на авторски права, кои права са нарушени, дали употребата може да се счита за случай на допустима употреба, приложимия закон, дължимите обезщетения за вреди и т.н.

- iv) потенциалните последици от наблюдението, които могат да включват прекъсване на достъпа до интернет. Това би било намеса в упражняването на правата на физическите лица на свобода на изразяване, свобода на информацията и достъп до културата, приложения на електронното правителство, пазари и електронна поща, а в някои случаи и в трудовите им дейности. В този контекст е особено важно да се има предвид, че последиците ще бъдат почувствани не само от предполагаемия нарушител, но от всички членове на семейството му, които използват същата връзка с интернет, включително ученици, които използват интернет във връзка със своето обучение;
- v) фактът, че обикновено оценката ще се извършва и решението ще се взема от частни лица (носителите на авторски права или доставчиците на интернет услуги). В свое предишно становище ЕНОЗД вече е изразил своята загриженост във връзка с извършването от частния сектор наблюдение върху физически лица (например доставчиците на интернет услуги или носителите на авторски права) в области, които попадат по принцип в сферата на компетентност на правоприлагащите органи ⁽²⁴⁾;
33. ЕНОЗД не е убеден, че ползите от мерките са по-съществени от отрицателните последици от тях по отношение на основните права на физическите лица. Защитата на авторските права е от интерес за носителите на правата и за обществото. Ограниченията на основните права, обаче, не изглеждат обосновани, ако съпоставим строгостта на мерките, т.е. мащаба на вмешателството в неприкосновеността на личния живот, илюстриран с изброените по-горе елементи, с очакваните ползи, изразяващи се във възпиране на нарушенията на правата върху интелектуална собственост, по-голямата част от които са малки по мащаб. Както се посочва в становището на генералния адвокат Kokott по делото *Promusicae*: „Не е сигурно ... дали споделянето на файлове („file sharing“) между физически лица, особено когато не се извършва с цел набавяне на имотна облага, застрашава защитата на авторските права в толкова голяма степен, че да обоснове прилагането на това изключение. Наистина все още е спорен въпросът доколко споделянето на файлове („file sharing“) между физически лица причинява действителни вреди“ ⁽²⁵⁾.
34. Във връзка с това следва да припомним и реакцията на Европейския парламент по отношение на „схемите, включващи три предупреждения“ в контекста на прегледа на пакета за телекомуникациите, и по-конкретно във връзка с изменение 138 на Рамковата директива ⁽²⁶⁾. С това изменение беше предвидено, че всички мерки, които водят до ограничаване на основните права и свободи, може да бъдат налагани единствено ако са целесъобразни, пропорционални и необходими в едно демократично общество, и тяхното прилагане подлежи на подходяща процедурна защита в съответствие с Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността. Всички тези мерки, свързани с достъпа на крайните ползватели или с ползването от тях на услуги и приложения посредством електронни съобщителни мрежи, които водят до ограничаване на основните права и свободи, може да бъдат налагани единствено ако са целесъобразни, пропорционални и необходими в едно демократично общество, и тяхното прилагане подлежи на подходяща процедурна защита в съответствие с Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността. Всички тези мерки, свързани с достъпа на крайните ползватели или с ползването от тях на услуги и приложения посредством електронни съобщителни мрежи, които водят до ограничаване на основните права и свободи, може да бъдат налагани единствено ако са целесъобразни, пропорционални и необходими в едно демократично общество, и тяхното прилагане подлежи на подходяща процедурна защита в съответствие с Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността.
35. В това отношение ЕНОЗД подчертава, също така, че всяка мярка, ограничаваща основните права, ще бъде предмет на внимателна оценка както на равнище ЕС, така и на национално равнище. Във връзка с това може да се направи паралел между Директива 2006/24/ЕО за запазване на данни ⁽²⁸⁾, която предвижда отклонение от общия принцип за защита на данните, изискващ заличаване на данните, когато те вече не са необходими за целите, за които са били събрани. Тази директива съдържа изискването данните за трафика да се запазват за целите на борбата с тежките престъпления. Трябва да се подчертае, че запазване на данни се допуска само във връзка с „тежки престъпления“, че запазването се ограничава до „данните за трафика“, което по принцип изключва информацията за съдържанието на комуникациите, и че са предвидени строги гаранции. Въпреки това са изразени съмнения относно съвместимостта на тази директива със стандартите за основните права; румънският конституционен съд е постановил, че запазването на всички данни е несъвместимо с основните права ⁽²⁹⁾; понастоящем подобен случай се разглежда и от германския конституционен съд ⁽³⁰⁾.
- Наличие на други средства, представляващи по-малко вмешателство
36. Изложените по-горе констатации се подкрепят от факта, че съществуват други средства за постигане на същата цел, които представляват по-малко вмешателство. ЕНОЗД призовава настоятелно да бъдат проучени и изпробвани подобни модели, представляващи по-малко вмешателство.
- ⁽²⁴⁾ Окончателната формулировка на така нареченото 138-о изменение гласи следното: „Член 1, параграф 3, буква а). Мерките, вземани от държавите-членки по отношение на достъпа на крайните ползватели до или ползването от тях на услуги и приложения чрез електронни съобщителни мрежи, зачитат основните права и свободи на физическите лица, гарантирани в Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността. Всички тези мерки, свързани с достъпа на крайните ползватели или с ползването от тях на услуги и приложения посредством електронни съобщителни мрежи, които водят до ограничаване на основните права и свободи, може да бъдат налагани единствено ако са целесъобразни, пропорционални и необходими в едно демократично общество, и тяхното прилагане подлежи на подходяща процедурна защита в съответствие с Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността. Всички тези мерки, свързани с достъпа на крайните ползватели или с ползването от тях на услуги и приложения посредством електронни съобщителни мрежи, които водят до ограничаване на основните права и свободи, може да бъдат налагани единствено ако са целесъобразни, пропорционални и необходими в едно демократично общество, и тяхното прилагане подлежи на подходяща процедурна защита в съответствие с Европейската конвенция за защита на правата на човека и основните свободи, както и в общите принципи на правото на Общността.“
- ⁽²⁵⁾ Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г., ОВ L 105, 13.4.2006 г., стр. 54.
- ⁽²⁶⁾ <http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html>
- ⁽²⁷⁾ <http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html>
- ⁽²⁸⁾ Становище на Европейския надзорен орган по защита на данните от 23 юни 2008 г. относно предложение за решение на Европейския парламент и на Съвета за създаване на многогодишна програма на Общността за защита на децата при използване на интернет и други комуникационни технологии, ОВ C 2, 7.1.2009 г., стр. 2.
- ⁽²⁹⁾ Вж. делото, цитирано в бележка по линия 8, точка 106.
- ⁽³⁰⁾ Вж. Директива 2009/140/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г., ОВ L 337, 18.12.2009 г., стр. 37.

37. Във връзка с това ЕНОЗД припомня, че изменената Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги (наричана „Директива за правата на гражданите“), която е част от неотдавна реформирания телекомуникационен пакет, съдържа определени правила и процедури за ограничаване на малките по размер нарушения на авторските права сред потребителите⁽³¹⁾. Тези процедури включват задължение за държавите-членки да изготвят стандартизирана информация от обществен интерес на различни теми, като изрично се посочват нарушенията на авторските права и сродните им права и правните последици от тях⁽³²⁾. Държавите-членки могат да изискат от доставчиците на интернет услуги да предоставят тази информация на всички свои клиенти, както и да я включат в текста на сключваните от тях договори.
38. Целта на системата е да информира физическите лица и да ги мотивира да се въздържат от разпространение на информация, предмет на авторски права, и от дейности, представляващи нарушения на права върху интелектуална собственост, като се избягва извършването на наблюдение върху използването на интернет и, произтичащите от такова наблюдение проблеми, свързани с неприкосновеността на личния живот и защитата на данните. Директивата за правата на гражданите трябва да бъде въведена в действие през 2011 г.; това означава, че описаните процедури все още не са в сила. В резултат все още ползите от тези процедури не са изпробвани на практика. Поради това е твърде рано да се пренебрегват потенциалните положителни резултати от тези нови процедури и да се възприемат „политиките на прекъсване на достъпа до интернет след три предупреждения“, които ограничават в далеч по-голяма степен основните права.
39. В допълнение към горното трябва да напомним, че Директива 2004/48/ЕО от 28 април 2004 г. относно упражняването на права върху интелектуална собственост предвижда различни инструменти за обезпечаване упражняването на правата върху интелектуална собственост пред съдилищата (разгледани по-долу в параграфи 43 и следващи)⁽³³⁾.
40. Директивата относно упражняването на права върху интелектуална собственост е транспонирана в законодателствата на държавите-членки неотдавна. Все още е твърде рано да се оцени дали нейните разпоредби обезпечават в достатъчна степен упражняването на правата върху интелектуална собственост. Следователно необходимостта от замяна на действащата система, основана на съдебни производства, която все още не е изпитана на практика, е най-малко съмнителна. Това повдига неизбежния въпрос защо не е възможно извършването на нарушения да се преследват ефикасно по съдебен път чрез налагане на предвидените в законодателството граждански и наказателни санкции за нарушенията на авторските права. Следователно, преди да предложи такива политически мерки, Комисията следва да предостави надеждна информация, от която е видно, че действащата законодателна рамка е неефективна и не дава очакваните резултати.
41. Освен това не е ясно дали са сериозно обмисляни алтернативни икономически бизнес модели, които не включват систематично наблюдение върху физическите лица. Например, ако носителите на авторски права докажат своите загуби, произтичащи от използването на P2P мрежи, те и доставчиците на интернет услуги биха могли например да въведат пробно диференцирани цени за достъп до интернет, като част от таксите, заплащани от потребителите с неограничен достъп, се предоставят на носителите на авторски права.
- Възможността за извършване на индивидуализирано наблюдение по начин, представляващ по-малко вмешателство*
42. Наред с прилагането на напълно различни модели, което следва да бъде проучено и изпробвано, както е посочено по-горе, във всички случаи е възможно да се извършва и индивидуализирано наблюдение по начин, представляващ по-малко вмешателство.
43. Целта на упражняване на правата върху интелектуална собственост може да бъде постигната и посредством наблюдение само върху ограничен брой физически лица, за които се предполага, че участват в значителни нарушения на авторските права. Директивата относно упражняването на права върху интелектуална собственост съдържа някои насоки в това отношение. Тя урежда условията, при които компетентните органи могат да разпоредят предоставяне на лични данни, съхранявани от доставчици на достъп до интернет, за целите на упражняването на права върху интелектуална собственост. В член 8 е предвидено, че компетентните съдебни органи могат да нареждат на доставчиците на интернет услуги да предоставят съхранявани от тях лични данни за лица, заподозрени в нарушения на авторски права (например данни за произхода и мрежите за разпространение на стоките или услугите, които нарушават права върху интелектуална собственост) в отговор на обосновано и пропорционално искане в случаи на нарушения, извършени в *търговски мащаб*⁽³⁴⁾.
44. Следователно критерият за „търговски мащаб“ има определящо значение. Съгласно този критерий наблюдението може да е пропорционално в ограничен брой
- ⁽³¹⁾ Вж. Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г., ОВ L 337, 18.12.2009 г., стр. 11.
- ⁽³²⁾ По-конкретно, член 21, параграф 4 от Директива 2009/136/ЕО предвижда, че „Държавите-членки може да изискват предприятията, посочени в параграф 3, да разпространяват безплатно информация от обществен интерес на съществуващи и нови абонати, когато е уместно, чрез същите средства като тези, обичайно използвани от тях за комуникация с абонатите. В този случай тази информация се предоставя от съответните публични органи в стандартизиран формат и обхваща, *inter alia*, следните въпроси: а) най-разпространените начини на използване на електронни съобщителни услуги за извършване на незаконни дейности или разпространяване на вредно съдържание, по-специално когато то може да засегне правата и свободите на други лица, включително нарушаването на авторското право и сродните му права, и правните последици от тях (...)“ Освен това, съгласно член 20, параграф 2 „Държавите-членки може да изискват също така договорът да включва информация, която може да бъде предоставена от съответните публични органи за тази цел, свързана с използването на електронни съобщителни мрежи и услуги за извършване на незаконни дейности или разпространение на вредно съдържание, както и със средствата за защита срещу рискове за личната сигурност, неприкосновеността на личния живот и личните данни, както е посочено в член 21, параграф 4, и която се отнася до предоставяната услуга“.
- ⁽³³⁾ ОВ L 157, 30.4.2004 г., стр. 45 (по-нататък в текста: „Директивата относно упражняването на права върху интелектуална собственост“).
- ⁽³⁴⁾ Това е потвърдено и в съображение 14 от Директивата относно упражняването на права върху интелектуална собственост.

конкретни *ad hoc* ситуации, когато са налице добре обосновани подозрения за нарушения на авторски права в търговски мащаб. Този критерий обхваща ситуации на доказани нарушения на авторски права, извършени от физически лица с цел набавяне по търговски начин на преки или непреки икономически облаги.

45. За да се приложи на практика контролът, основан на този критерий, носителите на авторски права могат да осъществяват индивидуализирано наблюдение на определени IP адреси, за да установят мащаба на нарушенията на авторските права. Това означава, че с оглед на същите цели носителите на авторски права следва да имат право да съхраняват данни за предполагаеми случаи на нарушения. Подобна информация следва да се използва само след установяване мащаба на нарушението. Става дума например за доказуеми случаи на значителни нарушения, както и на незначителни нарушения, извършвани за продължителен период от време с цел набавяне на търговски предимства или финансови облаги. Изискването за продължително извършване на нарушението за определен период от време е подчертано и разяснено по-долу във връзка с разглеждането на принципа на запазване.
46. Това означава, че в такива случаи събирането на информация за целите на доказване на предполагаеми нарушения, извършени чрез интернет, може да се счита за пропорционално и необходимо във връзка с подготовката на правни процедури, включително съдебни производства.
47. ЕНОЗД счита, че като допълнителна гаранция операциите по обработване на данни, извършвани с цел събиране на такива доказателства, следва да подлежат на предварителна проверка и одобрение от националните органи по защита на данните. Тази позиция се основава на факта, че операциите по обработване на данни биха представлявали специфичен риск по отношение на правата и свободите на физическите лица с оглед на техните цели, т.е. предприемане на действия за упражняване на права, които могат да се окажат неправомерни, и в светлината на чувствителния характер на събраните данни. Фактът, че обработването включва извършване на наблюдение върху електронните комуникации, е допълнителен фактор, предполагащ упражняване на засилен надзор.
48. ЕНОЗД счита, че критерият за „търговски мащаб“, предвиден в Директивата относно упражняването на права върху интелектуална собственост, е много подходящ елемент за определяне на обхвата на наблюдението с оглед спазване на принципа на пропорционалност. Освен това, липсват надеждни доказателства, че съгласно критериите, залегнали в Директивата относно упражняването на права върху интелектуална собственост, ефективните съдебни процедури срещу нарушения на авторски права са невъзможни или неефективни. Например данни от страни като Германия, където от 2008 г. насам след транспонирането на Директивата относно упражняването на права върху интелектуална собственост са постановени около 3 000 съдебни заповеди, задължаващи доставчици на интернет услуги да предоставят на съдилищата данни за 300 000 абонати на интернет услуги, изглежда показват обратното.
49. За да обобщим, тъй като Директивата относно упражняването на права върху интелектуална собственост е в действие от само две години, е трудно да обосновем една

замяна от страна на законодателите на критериите, залегнали в тази директива, с методи, представляващи по-голямо вмешателство, при положение, че ЕС едва започва да изпробва на практика вече въведените методи. По същата причина е трудно да разберем необходимостта от замяна на действащата система, основана на съдилищата, с друг тип мерки (в допълнение към въпросите, свързани с принципа за справедлив процес, които не са разглеждани тук).

IV.4. Съответствие на политиките на прекъсване на достъпа до интернет след три предупреждения с конкретни разпоредби за защита на данните

50. Съществуват и други, по-конкретни правни основания да твърдим, че подходът на три предупреждения е проблематичен от гледна точка на защитата на данните. ЕНОЗД би желал да подчертае спорното правно основание за обработването, изисквано съгласно Директива 95/46/ЕО, както и предвиденото в Директива 2002/58/ЕО задължение за заличаване на файловете с данни за дейността на потребителите.

Правно основание за обработване

51. Схемите, основаващи се на подхода на три предупреждения, включват обработване на лични данни, някои от които ще бъдат използвани в рамките на съдебните или административни процедури, насочени към прекъсване на достъпа до интернет на многократни нарушители. От тази гледна точка подобни данни отговарят на критериите за чувствителни данни съгласно член 8 от Директива 95/46/ЕО. В член 8, параграф 5 е предвидено, че „Обработването на данни, отнасящи се до закононарушения, наказателни присъди или мерки за сигурност, може да се извършва само под контрола на официален орган, или ако националното законодателство предвижда подходящи гаранции ...“.
52. Във връзка с това е уместно да припомним споменатия по-горе документ, изготвен от работната група по член 29, в който е разгледан въпросът за обработването на съдебни данни⁽³⁵⁾. Работната група заявява, че „Макар, разбира се, всяко лице да има правото да обработва съдебни данни в процеса на водения от него съдебен спор, принципът тук не отива по-далеч от това да се даде възможност за допълнително разследване, събиране и централизиране на лични данни от трети страни, в т.ч. най-вече систематично разследване от общ характер като например търсене в интернет (...). Това разследване е от компетентността на съдебните органи“⁽³⁶⁾. Въпреки че събирането на индивидуализирани конкретни данни, особено в случаи на тежки нарушения, може да е необходимо за доказване и упражняване на правно защитими искове, ЕНОЗД споделя изцяло становищата на работната група по член 29 относно липсата на правно основание за провеждане на широкомащабни проучвания, включващи обработване на големи обеми от данни за потребители на интернет.
53. Описаната по-горе дискусия относно принципа на пропорционалност и критерият за „търговски мащаб“ имат значение за определяне на условията, при които ще бъде узаконено събирането на IP адреси и свързана с тях информация.

⁽³⁵⁾ Вж. параграф 28 от настоящото становище.

⁽³⁶⁾ Подчертаването е наше.

54. Доставчиците на интернет услуги могат да направят опити за узаконяване на обработване, извършвано от носители на авторски права, като впишат в договорите си със своите клиенти клаузи, допускащи извършване на наблюдение върху техните данни и прекъсване на техните абонаменти. Със сключването на подобни договори ще се счита, че клиентите са дали своето съгласие за извършването на наблюдение. Подобна практика повдига, обаче, съществения въпрос дали физическите лица могат да дават съгласието си на доставчиците на интернет услуги за обработване на данни, което ще се извършва не от самите доставчици, а от трети страни, които не са под техен контрол.

55. Второ, съществува и въпросът за валидността на съгласието. Член 2, буква з) от Директива 95/46/ЕО определя съгласието като „всяко свободно изразено, конкретно и информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него“. Важно изискване е, че за да бъде валидно съгласието, независимо от обстоятелствата, при които е дадено, то трябва да е свободно дадено, конкретно и информирано волеизявление на субекта на данните съгласно определението в член 2, буква з) от директивата. ЕНОЗД има сериозни съмнения дали физическите лица, от които се иска да дадат съгласието си за извършване на наблюдение върху техните действия в интернет, ще имат действителна възможност за избор, особено поради факта, че алтернативата на съгласието е да се лишат от достъп до интернет, с което биха били засегнати много други области от техния живот.

56. Трето, твърде спорно е дали подобно наблюдение би могло да се счита за *необходимо* за изпълнението на договор, по който субектът на данните е страна, съгласно изискването на член 7, буква б) от Директива 95/46/ЕО, тъй като наблюдението очевидно не е предмет на договора, сключен от субекта на данните, а само средство за доставчика на интернет услуги да обслужва други интереси.

Заличаване на файлове с данни за дейността на потребителите

57. Съгласно Директива 2002/58/ЕО, и по-специално член 6 от нея, събиране и съхраняване на данни за трафик, като IP адреси, се допуска само на основания, пряко свързани с комуникационната услуга, включително за целите на фактуриране на услугата, управление на трафика и предотвратяване на измами. С отпадането на тези основания данните трябва да бъдат заличени. Това задължение не засяга задълженията по Директивата за запазване на данни, която, както е посочено по-горе, съдържа изискванията за съхраняване на данни за трафик и тяхното предоставяне на полицейските и прокурорските служби за подпомагане на разследвания **само на тежки престъпления** ⁽³⁷⁾.

58. В съответствие с горното доставчиците на интернет услуги следва да заличават всички файлове с данни за дейността на потребителите на интернет, които вече не са необходими за посочените цели. Имайки предвид, че файловете с данни за дейността на потребителите не са необходими за изготвяне на фактури, следва да се приеме, че три или четири седмици е достатъчен срок за ползване на тези файлове от доставчиците на интернет услуги за целите на управлението на трафика ⁽³⁸⁾.

59. Това означава, че когато носители на авторски права се обърнат към доставчици на интернет услуги след изтичането на посочения по-горе ограничен период, последните не следва да разполагат с файловете с данни за дейността на потребителите, свързващи IP адресите със съответните потребители. Запазване на файловете с данни след изтичането на този период следва се допуска само при наличие на основания, свързани с целите, предвидени в закона.

60. На практика това означава, че няма да е възможно да бъдат удовлетворени исканията на носители на авторски права, отправени към доставчиците на интернет услуги, освен ако тези искания са отправени много бързо, просто защото доставчиците вече няма да разполагат с исканата информация. С това се определя обхватът на приемливите практики на наблюдение, описани в предходния раздел.

Рискове от разширяване на разглежданата практика

61. Освен това ЕНОЗД се опасява не само за въздействието на политиките на прекъсване на достъпа до интернет след три предупреждения по отношение на неприкосновеността на личния живот и защитата на данните, но също и от разпространение на приложението на подобни политики в нови области. Ако политиките на прекъсване на достъпа до интернет след три предупреждения бъдат допуснати, те могат да се превърнат в наклонена плоскост към узаконяване на още по-широко наблюдение върху действията на потребителите на интернет — в различни области и за различни цели.

62. ЕНОЗД призовава Комисията да гарантира, че с АСТА няма да бъдат въведени повече мерки, противоречащи на действащия режим на ЕС за обезпечаване упражняването на права върху интелектуална собственост, който защита основните права и свободи, както и гражданските свободи, като правото на защита на личните данни.

V. СВЪРЗАНИ СЪС ЗАЩИТАТА НА ДАННИТЕ СЪОБРАЖЕНИЯ, ЗАСЯГАЩИ МЕХАНИЗМИТЕ ЗА МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО

63. Един от предложените от участниците в преговорите по АСТА начини за решаване на проблема с упражняването на правата върху интелектуална собственост е засилване на международното сътрудничество с поредица от мерки, които

⁽³⁷⁾ Вж. параграф 35 от настоящото становище.

⁽³⁸⁾ Управлението на трафика включва анализ на трафика в компютърната мрежа с цел оптимизиране или гарантиране на нейното функциониране, намаляване на времето на изчакване и/или увеличаване на използваемата честотна лента.

биха направили възможно ефективното упражняване на правата върху интелектуална собственост в областите на териториална компетентност на страните по АСТА.

64. Въз основа на наличната информация може да се предположи, че редица от планираните мерки за обезпечаване упражняването на правата върху интелектуална собственост ще включват осъществяване на международен обмен на информация за предполагаеми нарушения на права върху интелектуална собственост между публичните органи (митнически, полицейски и съдебни органи), но също така и между публични и частни лица (като доставчици на интернет услуги и организации на носители на авторски права). Подобно предаване на данни повдига множество въпроси от гледна точка на защитата на данните.

V.1. Законен, необходим и пропорционален ли е обменът на данни, предвиден в контекста на АСТА?

65. На сегашния етап на процеса на преговори, на който редица конкретни елементи, свързани с обработването на данни, са все още неопределени или неизвестни, е невъзможно да се установи дали предложените мерки съответстват на основните принципи на защита на данните и законодателството на ЕС в областта на защитата на данните.
66. На първо място може да се постави въпросът дали предаването на данни на трети страни в контекста на АСТА е законно. Необходимостта от приемане на мерки на международно равнище в тази област може да се постави под въпрос, доколкото между държавите-членки на ЕС не е налице съгласие относно хармонизирането на мерките за обезпечаване на упражняването в цифровата среда и видовете наказателни санкции, които следва да се налагат⁽³⁹⁾.
67. С оглед на горното изглежда, че принципите на необходимост и пропорционалност на предаването на данни по силата на АСТА ще бъдат спазени по-лесно, ако предметът на споразумението бъде ограничен изрично до борбата с най-сериозните нарушения на права върху интелектуална собственост, вместо да се допуска предаване на големи обеми данни във връзка с всеки случай на подозрение за нарушения на права върху интелектуална собственост. Подобен подход предполага да се определи прецизно съдържанието на понятието „най-сериозни нарушения на права върху интелектуална собственост“, във връзка с които се допуска предаване на данни.
68. Освен това следва да се отдели особено внимание на лицата, участващи в обмена на данни, както и на това дали данните ще бъдат обменяни само между публични органи или ще се осъществява и обмен между частни лица и публични органи. Както посочихме по-горе, участието на частни лица в област, която по принцип попада в сферата на компетентност на правоприлагащите органи, поражда редица опасения⁽⁴⁰⁾. Условието, при които частните

действащи лица ще участват в събиране и обмен с публични органи на лични данни, свързани с нарушения на права върху интелектуална собственост, следва да бъдат строго ограничени до конкретни обстоятелства, и да бъдат съпроводени с подходящи гаранции.

V.2. Законодателство за защита на данните, приложимо към предаването на данни в контекста на АСТА

Общ режим по отношение на предаването на данни

69. Общата законодателна рамка за защита на данните, приложима в ЕС, е уредена с Директива 95/46/ЕО. В член 25 и член 26 от Директива 95/46/ЕО е регламентиран режимът, който се прилага по отношение на предаването на данни на трети страни. Член 25 съдържа изискването данни да се предават само на страни, които гарантират достатъчна степен на защита, като в противен случай такова предаване е по принцип забранено.
70. Достатъчността на защитата, осигурена от третите страни, се оценява във всеки отделен случай от Европейската комисия, която е приела няколко решения, с които признава достатъчния характер на защитата, осигурена от редица страни, въз основа на обстоен анализ, извършен от работната група по член 29⁽⁴¹⁾.
71. ЕНОЗД отбелязва, че повечето от участниците в АСТА не са включени в изготвения от Комисията списък на страните, гарантиращи достатъчна степен на защита на данните, с изключение на Швейцария и по отношение на определени обстоятелства Канада и САЩ. За всички останали участници в АСТА не се счита, че гарантират достатъчна степен на защита. Това означава, че, за да бъде допуснато предаване на данни от ЕС на тези страни, трябва да бъде изпълнено едно от условията, предвидени в член 26, параграф 1 от Директива 95/46/ЕО, или страните по предаването на данни трябва да докажат наличие на достатъчни гаранции в съответствие с член 26, параграф 2 от директивата.

Специален режим за предаване на данни в областта на наказателното правораздаване

72. Директива 95/46/ЕО е основният правен инструмент на ЕС в областта на защитата на данните, нейното приложно поле понастоящем е ограничено, тъй като от нейния обхват са изрично изключени случаи, засягащи *inter alia* дейностите на държавата в областта на наказателното право (член 3). Обменът на данни за целите на наказателното правораздаване попада следователно извън приложното поле на

⁽³⁹⁾ Предложение за криминализиране понастоящем се обсъжда от Съвета, COM(2006) 168 от 26 април 2006 г.

⁽⁴⁰⁾ Вж. параграфи 32 и 52 от настоящото становище. Вж. също Становището на ЕНОЗД от 11 ноември 2008 г. относно Окончателния доклад на контактната група на високо равнище ЕС—САЩ относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни, ОВ С 128, 6.6.2009 г., стр. 1.

⁽⁴¹⁾ Вж. решенията относно достатъчната защита, приети от Европейската комисия по отношение на Аржентина, Канада, Швейцария, публикуваните от правителството на САЩ принципи за „сфера на неприкосновеност на личния живот“ и правителството на Съединените щати в контекста на споразумението за резервационните данни на пътниците, Гърнзи, остров Ман и Джързи; решенията са достъпни в интернет на адрес: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

Директива 95/46/ЕО и е предмет на общите принципи на защита на данните, залегнали в Конвенция № 108 на Съвета на Европа и допълнителния протокол към нея, страни по която са всички държави-членки на ЕС⁽⁴²⁾. Освен това се прилагат и приетите от ЕС правила във връзка с полицейското и съдебното сътрудничество по наказателноправни въпроси, предвидени в Рамково решение 2008/877/ПВР на Съвета⁽⁴³⁾.

73. В тези инструменти е залегнал и принципът, че в третата страна, на която се предават данни, трябва да е налице достатъчно ниво на защита на данните. Предвидени са редица дерогации, по-специално в случаите, когато третата страна предостави достатъчни гаранции за защита. Следователно, аналогично на случаите на обмен на данни по реда на Директива 95/46/ЕО, за извършване на обмен на данни в областта на наказателното правораздаване е необходимо страните по обмена на данни да предоставят достатъчни гаранции за защита.

Към нов режим на предаване на данни

74. В близко бъдеще може да се очаква ЕС да приеме на основание на член 16 от ДФЕС нови общи правила за защита на данните, приложими към всички области на дейност на Съюза. Това означава, че до няколко години може да е налице всеобхватна рамка на ЕС в областта на защитата на данните, съдържаща съгласувани правила за защита на данните, приложими към всички области на дейност на ЕС, които ще въведат еднакво ниво на гаранции по отношение на всички дейности по обработване на данни. Както посочи Viviane Reding⁽⁴⁴⁾, комисар по правосъдие, основни права и гражданство, тази нова рамка следва да функционира като единен „модерен и всеобхватен правен инструмент“ за защита на данните в ЕС. Такава рамка ще бъде особено полезна, тъй като ще внесе повече яснота и съгласуваност на правилата, приложими в ЕС по отношение на защитата на данните.
75. В международен план ЕНОЗД изтъква и приетата неотдавна от органи по защита на данните Резолюция относно международните стандарти за защита на личните данни и неприкосновеността на личния живот, която е първа стъпка към въвеждане на световни стандарти за защита на данните⁽⁴⁵⁾. Международните стандарти включват редица гаранции за защита на данните, сходни с предвидените в Директива 95/46/ЕО и Конвенция № 108. Въпреки че международните стандарти все още нямат обвързваща сила, те съдържат полезни насоки по отношение на принципите на защита

на данните, които могат да се прилагат на доброволна основа от трети страни, с цел постигане на съвместимост на тяхната правна рамка със стандартите на ЕС. ЕНОЗД е убеден, че страните по АСТА следва да вземат предвид и принципите, залегнали в Международните стандарти, когато обработват лични данни с произход от ЕС.

V.3. Необходимост от прилагане на подходящи гаранции за защита на предаването на данни от ЕС на трети страни

Какъв характер трябва да имат гаранциите, за да обезпечат ефективна защита на предаването на данни на трети страни?

76. ЕНОЗД подчертава, че в случаите, когато необходимостта от предаване на лични данни на трети страни е доказана, Европейският съюз следва да договори с получателите на данните в третите страни в допълнение към споразумението АСТА специфични инструменти, съдържащи подходящи гаранции за защита на данните, с които да бъде уреден обменът на лични данни.
77. Като правило подходящи гаранции за защита на данните следва да се съдържат в обвързващо споразумение между ЕС и третата страна получател, по силата на което страната получател се задължава да зачита законодателството на ЕС за защита на данните и да предостави на физическите лица същите права и правни средства за защита, които са предвидени в законодателството на ЕС. Необходимостта от обвързващо споразумение произтича от член 26, параграф 2 от Директива 95/46/ЕО и член 13, параграф 3, буква б) от Рамковото решение, а също така е залегнала в съществуващата практика на ЕС за сключване на специфични споразумения, с които се уреждат конкретни случаи на предаване на данни на трети страни⁽⁴⁶⁾.

78. Аналогично, съгласно Международните стандарти получателят може да бъде задължен да гарантира, че ще предостави изискваното ниво на защита за осъществяване на предаването на данни. Тези гаранции също могат да бъдат предоставени под формата на договорно задължение.

Съдържание на гаранциите, които страните по АСТА трябва да предоставят във връзка с предаване на лични данни

79. ЕНОЗД подчертава по-специално, че международният обмен на информация за целите на правоприлагането е особено чувствителна област от гледна точка на защитата на данните, защото подобна рамка може да доведе до узаконяване на предаване на големи обеми данни в област, където

⁽⁴²⁾ Конвенция за защита на физическите лица по отношение на автоматизираната обработка на лични данни, приета в Страсбург на 28 януари 1981 г., и Съвет на Европа, Допълнителен протокол към Конвенцията за защита на физическите лица по отношение на автоматизираната обработка на лични данни относно надзорните органи и трансграничните потоци от данни, Страсбург, 8 ноември 2001 г.

⁽⁴³⁾ Рамково решение на Съвета 2008/877/ПВР от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, ОВ L 350, 30.12.2008 г., стр. 60.

⁽⁴⁴⁾ Вж. Отговорите на въпросника на Европейския парламент за кандидата за комисар Viviane Reding, стр. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

⁽⁴⁵⁾ Резолюция, приета в Мадрид през ноември 2009 г.

⁽⁴⁶⁾ Например споразуменията на Европол и Евроюст със САЩ, споразумението за резервационните данни на пътниците, споразумението Swift, споразумението между Европейския съюз и Австралия относно обработката и предаването на произхождащи от Европейския съюз резервационни данни за пътниците (PNR данни) от въздушни превозвачи на Австралийската митническа служба.

въздействието върху физическите лица е особено сериозно и поради това е още по-голяма необходимостта от строги и надеждни гаранции за защита на данните.

80. ЕНОЗД подчертава, че конкретните условия и гаранции трябва да се определят индивидуално за всеки отделен случай при отчитане на всички параметри на обмена на данни. За да даде общи насоки, обаче, по-долу ЕНОЗД ще изложи някои от принципите и гаранциите, чието изпълнение и наличие третите страни трябва да докажат, за да се допусне осъществяването на предаването на данни:

— трябва да се удостовери правната обосновка за извършване на операциите по обработване на данни (т. е. дали операциите се извършват на основание на правно задължение, на съгласие, дадено от субектите на данните, или на друго валидно правно основание?), както и дали предаването на данни отговаря на първоначалната цел, с която са събрани данните. Не следва да се допуска предаване на данни извън обхвата на предвидената цел,

— обемът и видовете лични данни, предмет на обмена, следва да са ясно определени и ограничени до строго необходимото за постигане на целта на предаването. Събираните и предавани лични данни могат да включват по-специално IP адресите на потребители на интернет, датата и часа на предполагаемо извършено закононарушение и вида на закононарушението. ЕНОЗД препоръчва данните да не се свързват с конкретни физически лица на етапа на разследването и припомня, че идентифицирането на заподозрени лица следва да се извършва в съответствие със закона и под контрола на съдия. Във връзка с това ЕНОЗД изтъква, че данните, свързани с нарушения на права върху интелектуална собственост и подозрения за такива нарушения са специална категория данни, чието обработване обикновено може да се извършва само от правоприлагащи органи и изисква прилагане на допълнителни гаранции. Лицата, оправомощени да обработват данни, свързани с нарушения на права върху интелектуална собственост, и подозрения за такива нарушения, както и условията за обработване на тези данни трябва следователно да бъдат конкретно определени в съответствие с действащото законодателство за защита на данните,

— лицата, между които може да се осъществява обмен на данни, трябва да бъдат ясно определени и последващи предавания на данните на други получатели трябва да бъдат забранени по принцип, освен ако такива последващи предавания са необходими за конкретно разследване. Това ограничение има особено важно значение, защото определените получатели не следва да предоставят без основание информация на неоправомощени получатели,

— ЕНОЗД предполага, че с АСТА ще бъде уредено не само сътрудничеството между публичните органи, но ще бъдат възложени функции по обезпечаване упражня-

ването на права и на частни организации (като доставчици на интернет услуги, организации на носители на авторски права и др.). В последния случай условията и равнището на участие на частни организации в дейностите по обезпечаване упражняването на права върху интелектуална собственост трябва да бъдат предмет на внимателна оценка, т.е. мерките, предвидени в АСТА, не бива да предоставят на доставчиците на интернет услуги и организациите на носителите на авторски права *de facto* право да извършват онлайн наблюдение върху поведението на потребителите на интернет. Освен това обработването на лични данни от частни организации в рамките на дейности по право-прилагане следва да се извършва само при наличие на подходящо правно основание. Важно е също така да се уточни дали частните организации ще бъдат задължени да сътрудничат с полицейските органи и да се определи обхватът на подобно сътрудничество. То следва във всички случаи да се ограничи само до случаите на „тежки престъпления“, като определението на това понятие също трябва да бъде прецизно формулирано, тъй като не всички нарушения на права върху интелектуална собственост следва да се считат за тежки престъпления,

— използваният метод за обмен на лични данни трябва да бъде ясно определен, като по-специално трябва да се определи дали обменът ще се осъществява посредством „push“ система (по силата на която например доставчиците на интернет услуги и организациите на носители на права върху интелектуална собственост предават по своя преценка определени данни на трети страни в чужбина, като полицейски или правоприлагащи органи) или „pull“ система (при която полицейските и правоприлагащите органи биха имали пряк достъп до бази данни на частни лица или бази данни за централизирано съхранение на информация). Както подчертахме във връзка с резервационните данни за пътниците, „push“ системата е единственият вариант, съответстващ на принципите на защита на данните от гледна точка на правото на ЕС, тъй като позволява на подателя на данните в ЕС, който най-често би бил администраторът на данните, да упражнява контрол върху тяхното предаване ⁽⁴⁷⁾,

— трябва да се определи времето на запазване на личните данни от получателите, както и целта на запазването. Срокът на запазване на данните следва да е пропорционален на преследваната цел, което означава, че данните следва да бъдат премахнати или заличени, когато вече не са необходими за постигането на тази цел,

— задълженията, вменени на администраторите на данни в трети страни, следва да бъдат ясно определени. Трябва да бъдат гарантирани механизми за надзор и/или подлежащи на принудително изпълнение механизми за

⁽⁴⁷⁾ Вж. Становище № 4/2003 на работната група по член 29 относно гарантираното в САЩ ниво на защита на предаването на данни за пътниците, WP78, 13 юни 2003 г.

отчетност, за да бъдат осигурени ефективни възможности за търсене на отговорност и налагане на санкции на администраторите на данни в случаи на неразрешено обработване или други нарушения. Наред с това следва да бъдат предвидени механизми за правна защита, позволяващи на физическите лица да подават жалби пред независим орган по защита на данните и да търсят ефективна правна защита пред независим и безпристрастен трибунал ⁽⁴⁸⁾,

- сключеното от страните споразумение следва изрично да определя правата на субектите на данни по отношение на техните лични данни, когато такива данни са предмет на обработване от трета страна получател, за да се гарантира, че те разполагат с ефективни механизми за упражняване на техните права по отношение на извършвано в чужбина обработване,
- наред с горното прозрачността има решаващо значение и страните по инструмента за защита на данните трябва да се договорят как ще информират субектите на данните за извършваните дейности по обработване на данни, както и за техните права и за механизмите, чрез които те могат да ги упражняват.

VI. ЗАКЛЮЧЕНИЯ

81. ЕНОЗД приканва настоятелно Европейската комисия да започне публичен и прозрачен диалог относно АСТА, например чрез процедура на публична консултация, което ще помогне също така да се гарантира съответствието на мерките, които ще бъдат предприети, с изискванията на законодателството на ЕС за неприкосновеността на личния живот и защитата на данните.
82. ЕНОЗД призовава Европейската комисия в процеса на водените преговори по АСТА да се стреми към постигане на подходящ баланс между исканията за защита на правата върху интелектуална собственост и правото на неприкосновеност на личния живот и защита на данните. ЕНОЗД подчертава, че е особено важно за неприкосновеността на личния живот и защитата на данните да се държи сметка от самото начало на преговорите, преди да се постигнат договорености за конкретни мерки, за да се избегне необходимостта по-късно да се търсят алтернативни решения, отговарящи на изискванията за неприкосновеност на личния живот.
83. Интелектуалната собственост има важно значение за обществото и трябва да бъде защитавана, но тя не бива да се поставя над основните права на физическите лица на неприкосновеност на личния живот, защита на данните и други, като презумпцията за невиновност, ефективната съдебна защита и свободата на изразяване.
84. Доколкото актуалният вариант на текста на АСТА включва или поне непряко прокарва идеята за политики на прекъсване на достъпа до интернет след три предупреждения, споразумението ще ограничи в голяма степен основните права и свободи на европейските граждани, и най-вече правата на защита на личните данни и неприкосновеност на личния живот.
85. ЕНОЗД изразява позицията, че политиките на прекъсване на достъпа до интернет след три предупреждения не са необходими за обезпечаване упражняването на правата върху интелектуална собственост. ЕНОЗД е убеден, че съществуват алтернативни решения, представляващи по-малко вмешателство, или поне, че предвидените политики могат да се прилагат по начин, представляващ по-малко вмешателство, или с по-ограничено приложно поле, по-специално под формата на индивидуализирано *ad hoc* наблюдение.
86. Политиките на прекъсване на достъпа до интернет след три предупреждения поражда проблеми и на по-конкретно юридическо ниво, особено поради факта, че обработването на съдебни данни, по-специално от частни организации, трябва да се извършва на подходящо правно основание. Функционирането на схемите с „три предупреждения“ може наред с това да включва дългосрочно съхраняване на файлове с данни за дейността на потребителите, което би било в противоречие с действащото законодателство.
87. Освен това, доколкото АСТА предвижда осъществяване на обмен на лични данни между публични органи и/или частни организации в държавите-страни по споразумението, ЕНОЗД призовава Европейския съюз да въведе подходящи гаранции. Тези гаранции следва да се прилагат към всички случаи на предаване на данни в контекста на АСТА, независимо дали са свързани с прилагане на гражданското или наказателното законодателство или с цифрово правоприменяване, а също така следва да отговарят на принципите на защита на данните, залегнали в Конвенция № 108 и Директива 95/46/ЕО. ЕНОЗД препоръчва тези гаранции да бъдат оформени като обвързващи споразумения между ЕС и третите страни получатели на данните.
88. Наред с това ЕНОЗД би желал да бъде консултиран относно мерките за предаване на данни във връзка с прилагането на АСТА, за да удостовери тяхната пропорционалност и че те обезпечават подходящо ниво на защита на данните.

Съставено в Брюксел на 22 февруари 2010 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните

⁽⁴⁸⁾ Вж. Становището на Европейския надзорен орган по защита на данните относно Заключителния доклад на контактната група на високо равнище ЕС—САЩ относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни, 11 ноември 2008 г.