I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye a hálózatsemlegességről, a forgalomkezelésről, valamint a magánélet és a személyes adatok védelméről

(2012/C 34/01)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Unió működéséről szóló szerződésre, és különösen annak 16. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára, és különösen annak 7. és 8. cikkére,

tekintettel a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvre ([1]),

tekintettel a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletre ([2]), és különösen annak 41. cikke (2) bekezdésére,

tekintettel az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvre ([3]),

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. **BEVEZETÉS**

I.1. **Háttér**

1. 2011. április 19-én a Bizottság elfogadta a „Nyílt internet és hálózatsemlegesség Európában” című közleményt ([4]).

2. Ez a vélemény az európai adatvédelmi biztos e közleményre adott válaszának tekinthető, és célja az, hogy részt vegyen az Európai Unióban a hálózatsemlegességről folytatott szakpolitikai vitában, különös figyelmet fordítva az adatvédelemhez és a magánélethez kapcsolódó szempontokra.

([1]) HL L 281., 1995.11.23., 31. o., „adatvédelmi irányelv”.
([2]) HL L 8., 2001.1.12., 1. o., „adatvédelmi rendelet”.
([3]) HL L 201., 2002.7.31., 37. o.; a 2009. november 25-i 2009/136/EK európai parlamenti és tanácsi irányelv által módosított irányelv („elektronikus hírközlési adatvédelmi irányelv”).
([4]) COM(2011) 222 végleges.

3. A vélemény az európai adatvédelmi biztos által a Bizottságnak az európai nyílt internetről és hálózatsemlegességről folytatott nyilvános konzultációjára adott válaszra ([5]) épít, amely a bizottsági közlemény előzménye volt. Az európai adatvédelmi biztos emellett figyelembe vette a hálózatsemlegességről szóló tanácsi következtetések tervezetét ([6]), amelyet a közelmúltban dolgoztak ki.

I.2. **A hálózatsemlegesség fogalma**

4. A hálózatsemlegesség fogalma arra a folyamatban lévő vitára utal, hogy a internetszolgáltatóknak ([7]) meg lehet-e engedni, hogy korlátozzák, szűrjék vagy blokkolják az internet-hozzáférést vagy más módon befolyásolják az internet teljesítményét. A hálózatsemlegesség fogalmának alapját az a nézet képezi, amely szerint az interneten található információkat részrehajlás nélkül, a tartalomtól, a címzettől és a forrástól függetlenül kell továbbítani, és a felhasználók szabadon eldönthetik, milyen alkalmazásokat, szolgáltatásokat és hardvereszközöket kívánnak használni. Ez azt jelenti, hogy az internetszolgáltatók nem kezelhetnek – tetszésük szerint – kiemelten bizonyos alkalmazásokat vagy szolgáltatásokat (például a „peer-to-peer" (P2P) rendszereket), és nem is lassíthatják az azokhoz való hozzáférést ([8]).

5. A hálózatforgalom szűrése, blokkolása és ellenőrzése fontos kérdéseket vet fel – amelyeket gyakran nem, vagy csak érintőlegesen vesznek figyelembe – a kommunikáció titkosságával és az egyének magánéletének és személyes adatainak tiszteletben tartásával kapcsolatban, amikor azok az internetet használják. Bizonyos ellenőrzési technikák például magukban foglalják többek között a kommunikáció tartalmának, a megtekintett weboldalaknak, az elküldött és a fogadott e-maileknek, illetve ezek idejének nyomon követését, lehetővé téve a közlések szűrését.

6. A hírközlési adatok ellenőrzésével az internetszolgáltatók megsérthetik a kommunikáció titkosságát, amely az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (EJEE) 8. cikke és az Európai Unió Alapjogi Chartájának (a továbbiakban: a Charta) 7. és 8. cikke által garantált alapvető jog. A titkosságot ezenkívül egy uniós másodlagos jogszabály is védi: az elektronikus hírközlési adatvédelmi irányelv 5. cikke.

I.3. **A vélemény tárgya és felépítése**

7. Az európai adatvédelmi biztos úgy véli, hogy egy hálózatsemlegességről folytatott komoly szakpolitikai vitának foglalkoznia kell a kommunikáció titkosságának kérdésével, valamint a magánélettel és az adatvédelemmel kapcsolatos egyéb szempontokkal is.

8. Ez a vélemény hozzájárul ehhez a folyamatban lévő uniós vitához. Három célja van:

— Hangsúlyozza a magánélet védelme és az adatvédelem fontosságát a hálózatsemlegességről folytatott vitában. Különösen kiemeli a kommunikáció titkosságára vonatkozó meglévő szabályok tiszteletben tartásának szükségességét. Csak az ilyen szabályoknak megfelelő gyakorlatok engedhetők meg.

— A hálózatsemlegesség viszonylag új – technológiai – lehetőségekkel függ össze, és kevés tapasztalat áll rendelkezésre a jogi keret alkalmazásáról. Ez a vélemény ezért iránymutatással szolgál azzal kapcsolatban, hogy a hálózatforgalom szűrése, blokkolása és ellenőrzése során az internetszolgáltatóknak miként kell alkalmazniuk és betartaniuk az adatvédelmi jogi keretet. Mindez egyaránt hasznos lehet az internetszolgáltatók és a jogi keret végrehajtásáért felelő hatóságok számára.

— Az adatvédelem és a magánélet védelme terén a vélemény azonosítja a különleges figyelmet igénylő területeket, amelyek esetében európai szintű fellépés válhat szükségessé. Ez különösen fontos az Unió szintjén jelenleg folyamatban lévő vita, valamint azon szakpolitikai intézkedések fényében, amelyeket a Bizottság azok eredményeképpen kezdeményezhet.

([5]) Az európai adatvédelmi biztos válaszában hangsúlyozta az adatvédelemmel és a magánélet tiszteletben tartásával kapcsolatos kérdések, illetve egyéb meglévő jogok és értékek figyelembevételének fontosságát. A válasz a következő címen érhető el: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Ez a helyhez kötött és a mobil hálózatokhoz való hozzáférést egyaránt magában foglalja.

([8]) Az elv mindamellett nem vonatkozik azokra az internetszolgáltatókra, amelyek a sávszélességgel vagy a letölthető adatmennyiség meghatározásával korlátozzák, hogy egy előfizető egy adott előfizetés keretében milyen sebességgel, mennyi információt tud le- vagy feltölteni. Ezért a hálózatsemlegesség elve értelmében az internetszolgáltatók továbbra is kínálhatnak olyan internet-előfizetéseket, amelyek például a sebességgel vagy az adatmennyiséggel kapcsolatos kritériumok alapján korlátozzák az internet-hozzáférést, amennyiben ez nem jelenti konkrét tartalmak előnyben részesítését, illetve diszkriminálását.

9. Az európai adatvédelmi biztos tisztában van azzal, hogy a hálózatsemlegesség kérdése más problémákat is felvet, amelyekkel a vélemény az alábbiakban foglalkozni fog – ilyenek például az információhoz való hozzáféréssel kapcsolatos kérdések. Ezekkel a témákkal a vélemény csak annyiban foglalkozik, amennyiben azok az adatvédelemhez és a magánélet védelméhez kapcsolódnak, illetve hatással vannak azokra.

10. A vélemény a következő részekből áll: A II. szakasz először rövid áttekintést nyújt az internetszolgáltatók internetszűréssel kapcsolatos gyakorlatairól. A III. szakasz felvázolja az Unió hálózatsemlegességre vonatkozó jogi keretét. A IV. szakasz egy technikai leírással folytatódik, amit a magánéletre gyakorolt hatások értékelése követ, az alkalmazott technikától függően. Az V. szakasz a magánélet és az adatok védelmére vonatkozó hatályos uniós jogi keret alkalmazásának gyakorlati részleteit elemzi. Ezt az elemzést alapul véve a VI. szakasz javaslatokat fogalmaz meg a további szakpolitikák kidolgozására vonatkozóan, és azonosítja azokat a területeket, ahol szükségessé válhat a jogi keret egyértelműsítése és javítása. A VII. szakasz a következtetéseket tartalmazza.

II. **HÁLÓZATSEMLEGESSÉG ÉS FORGALOMKEZELÉSI POLITIKÁK**

A forgalomkezelési politikák fokozott alkalmazása

11. Az internetszolgáltatók régebben csak meghatározott körülmények esetén ellenőrizték és befolyásolták a hálózat forgalmát. Például az internetszolgáltatók a hálózat biztonságának fenntartása – például a vírusok elleni küzdelem – érdekében alkalmaztak ellenőrzési technikákat és korlátozták az információáramlást. Tehát általában véve az internet úgy növekedett, hogy közben nagymértékben megőrizte a semlegességét.

12. Az elmúlt években azonban egyes internetszolgáltatók érdeklődni kezdtek a hálózatforgalom ellenőrzése iránt, azzal a céllal, hogy lehetővé tegyék a differenciálást, és hogy különböző politikákat alkalmazhassanak például bizonyos szolgáltatások blokkolása vagy más szolgáltatásokhoz való hozzáférés előnyben részesítése érdekében. Ezt „forgalomkezelési politikának" is nevezik ([9]).

13. Az internetszolgáltatóknak számos okuk van az internetforgalom ellenőrzésére és differenciálására. A forgalomkezelési politikák például segíthetik az internetszolgáltatókat abban, hogy nagy forgalmú időszakokban kezelni tudják az internetforgalmat azáltal, hogy kiemelten kezelnek bizonyos, az idő szempontjából érzékeny forgalmakat, például a videoadatfolyam-átvitelt, és kevésbé fontosként kezelnek az idő szempontjából nem annyira érzékeny, más típusú internetforgalmakat, például a P2P-t ([10]). Ezenkívül a forgalomkezelés az internetszolgáltatók számára – többféle módon is – potenciális bevételi forrást jelenthet. Az internetszolgáltatók egyrészről díjat számolhatnak fel a tartalomszolgáltatóknak – például azoknak, amelyek szolgáltatásai magasabb sávszélességet igényelnek – cserébe azért, hogy kiemelt bánásmódot (és ennélfogva sebességet) biztosítanak számukra. Ez azt jelentené, hogy egy meghatározott szolgáltatáshoz – például az igény szerinti videoletöltést biztosító szolgáltatáshoz – való hozzáférés gyorsabb lehet egy olyan hasonló szolgáltatáshoz való hozzáférésnél, amely nem kérte a nagy sebességű adatátvitelt. Bevételre olyan előfizetők révén is szert lehet tenni, akik hajlandók magasabb (vagy alacsonyabb) díjakat fizetni bizonyos típusú, differenciált előfizetésekért. Például a P2P-rendszerekhez való hozzáférést nem biztosító előfizetés olcsóbb lehet, mint az, amely korlátlan hozzáférést biztosít.

14. Amellett, hogy az internetszolgáltatóknak megvan az okuk a forgalomkezelési politikák alkalmazására, más felek szintén érdekeltek lehetnek abban, hogy az internetszolgáltatók forgalomkezelési politikákat alkalmazzanak. Ha az internetszolgáltatók irányítják hálózataikat és ellenőrzik azokat a tartalmakat, amelyek eszközeiken áthaladnak, valószínűleg fokozzák az állítólagosan jogtalan felhasználás – például a szerzői jogok megsértése vagy pornográf tartalom – felderítésére irányuló képességüket.

([9]) Lásd például az OFCOM 2011. május 27-én elfogadott „Site blocking to reduce online copyright infringement" (Weboldalak blokkolása az online szerzői jogi jogsértések visszaszorítása érdekében) c. jelentését http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Egyes internetszolgáltatók már csomagszűrő rendszereket alkalmaznak a hálózatukban hálózatkezelési vagy más célokra, ezért úgy véljük, hogy ez alkalmazható, bár rendkívül összetett rendszernek bizonyul, és magas költségeket hordoz azok számára, akik még nem futtatnak ilyen szolgáltatásokat. Figyelembe véve a szükséges tőkeberuházást, előfordulhat, hogy rövid és középtávon a mélyreható csomagszűrést (DPI) csak a nagyobb internetszolgáltatók alkalmazhatják."

([10]) A valós idejű alkalmazások – például a videoadatfolyam-átvitel – minősége többek között a latenciától, azaz a hálózat terheltségéből adódó válaszidőtől is függ.

Egyéb fontos érdekek, ideértve az adatvédelmet és a magánélet védelmét

15. Ez a tendencia vitát váltott ki az ilyen típusú gyakorlatok jogszerűségéről és különösképpen arról, hogy szükség van-e további jogszabályban rögzített egyedi hálózatsemlegességi kötelezettségek kidolgozására.

16. A forgalomkezelési politikák internetszolgáltatók általi fokozott alkalmazása korlátozhatja az információhoz való hozzáférést. Ha ez a magatartás hétköznapi gyakorlattá válna, és a felhasználók számára nem lenne elérhető (vagy rendkívül drága lenne) a jelenlegi ismereteink szerinti teljes körű internetes hozzáférés, az veszélyeztetné az információkhoz való hozzáférést és a felhasználók lehetőségét arra, hogy az általuk szabadon választott alkalmazások vagy szolgáltatások igénybevételével fel-, illetve letölthessék a kívánt tartalmakat. A hálózatsemlegesség jogilag kötelező érvényű elve megoldást jelenthet erre a problémára.

17. Ezzel az európai adatvédelmi biztos elérkezett az internetszolgáltatók forgalomkezelési tevékenységei kapcsán felmerülő adatvédelmi és a magánélet védelmével kapcsolatos szempontokhoz. Ezek a következők:

— Amikor az internetszolgáltatók azzal a kizárólagos céllal végeznek forgalmiadat-feldolgozást, hogy továbbítsák az információáramot a küldőtől a fogadó félhez, általában korlátozott személyesadat-feldolgozást végeznek ([11]). Hasonlóan ahhoz, ahogyan a postai szolgáltatás feldolgozza a levél borítékján foglalt információkat, az internetszolgáltató is feldolgozza a közlésnek a fogadóhoz való továbbításához szükséges információkat. Ez nem ellentétes az adatvédelemmel, a magánélet védelmével és a kommunikáció titkosságával kapcsolatos jogi követelményekkel.

— Ugyanakkor amennyiben az internetszolgáltatók abból a célból vizsgálják meg a hírközlési adatokat, hogy megkülönböztessék az egyes közlésfolyamokat és egyedi politikákat alkalmazzanak, ami kedvezőtlen lehet az egyének számára, a következmények nagyobb jelentőségűek. Az egyes esetek körülményeitől és az elvégzett elemzés típusától függően az adatfeldolgozás nagymértékben beavatkozhat az egyén magánéletébe és személyes adataiba. Ez nyilvánvalóbb akkor, amikor a forgalomkezelési politikák felfedik az egyének internetes kommunikációinak tartalmát, ideértve többek között az elküldött és a fogadott e-maileket, a megnyitott weboldalakat, valamint a le-, illetve feltöltött fájlokat.

III. A HÁLÓZATSEMLEGESSÉGRE VONATKOZÓ UNIÓS JOGI KERET ÁTTEKINTÉSE ÉS TOVÁBBI SZAKPOLITIKAI FEJLEMÉNYEK

III.1. A jogi keret rövid ismertetése

18. 2009-ig az EU jogalkotási eszközei nem tartalmaztak olyan rendelkezéseket, amelyek kifejezetten tiltották volna az internetszolgáltatók számára az internetforgalom szűrését vagy blokkolását, vagy azt, hogy külön díjakat számítsanak fel az előfizetők számára a szolgáltatásokhoz való hozzáférésért. Mindamellett olyan rendelkezéseket sem tartalmaztak, amelyek kifejezetten elismerték volna ezt a gyakorlatot. A helyzet némiképp bizonytalan volt.

19. A 2009. évi távközlési csomag az internet nyitottságát támogató rendelkezéseivel megváltoztatta a körülményeket. Az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló irányelv (a „keretirányelv") 8. cikkének (4) bekezdése például kötelezi a szabályozó hatóságokat, hogy mozdítsák elő a végfelhasználók lehetőségét arra, hogy hozzáférjenek a választásuk szerinti tartalomhoz, alkalmazásokhoz vagy szolgáltatásokhoz ([12]). Ez a rendelkezés nem az egyes szolgáltatók szintjén, hanem a hálózat egészére alkalmazandó. A közelmúltban elfogadott tanácsi következtetéstervezetek szintén felhívták a figyelmet arra, hogy fenn kell tartani az internet nyitottságát ([13]).

([11]) Ez nem foglalja magában azokat a műveleteket, amelyek célja a hálózati biztonság növelése és a káros forgalom felderítése, valamint a számlázáshoz és összekapcsoláshoz szükséges műveleteket. Ugyanígy nem tartoznak ide az adatmegőrzésről szóló irányelvből eredő kötelezettségek (az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (HL L 105., 2006.4.13., 54. o.) („adatmegőrzési irányelv").

([12]) A 2002. március 7-i 2002/21/EK irányelv az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról. A 2009/140/EK irányelvvel és az 544/2009/EK rendelettel módosított irányelv (HL L 337., 2009.12.18., 37. o.).

([13]) Lásd a 3. cikk e) pontját, amelyben a Tanács elismeri, hogy „fenn kell tartani az internet nyitottságát, miközben biztosítani kell, hogy továbbra is magas színvonalú szolgáltatásokat nyújthasson egy olyan keretben, amely előmozdítja és tiszteletben tartja az olyan alapvető jogokat, mint a véleménynyilvánítás szabadsága és a vállalkozás szabadsága", és a 8. cikk d) pontját, amely felkéri a tagállamokat, hogy „tekintsék szakpolitikai célnak az internet nyitottságának és semlegességének előmozdítását".

20. Az egyetemes szolgáltatási irányelv ([14]) ennél konkrétabb kötelezettségeket fogalmaz meg. A 20. és a 21. cikk átláthatósági követelményeket állapít meg a szolgáltatásokhoz vagy alkalmazásokhoz való hozzáférésre és/vagy azok használatára vonatkozó korlátozások tekintetében. Az irányelv előírja a szolgáltatások minimális minőségi szintjét is.

21. Az internetszolgáltatók azon gyakorlatai tekintetében, amelyek magukban foglalják az egyének kommunikációinak ellenőrzését, az egyetemes szolgáltatási irányelvet és az elektronikus hírközlési adatvédelmi irányelvet módosító irányelv ([15]) (28) preambulumbekezdése hangsúlyozza, hogy az „alkalmazott technológiától és a korlátozások típusától függően e korlátozások esetében szükséges lehet a felhasználó […] elektronikus hírközlési adatvédelmi irányelv szerinti beleegyezése". Ekképpen a (28) preambulumbekezdés emlékeztet arra, hogy a közlések ellenőrzésén alapuló mindennemű korlátozáshoz szükség van az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdése szerinti hozzájárulásra. Az alábbi IV. szakasz tovább elemzi az 5. cikk (1) bekezdésének elemzését, és az adatok és a magánélet védelme jogi keretének egészét.

22. Végül az egyetemes szolgáltatási irányelv 22. cikkének (3) bekezdése felhatalmazza a nemzeti szabályozó hatóságokat, hogy – szükség esetén – a szolgáltatásminőség romlásának és a hálózati adatforgalom akadályozásának vagy lelassulásának megelőzése érdekében a szolgáltatás minőségével kapcsolatban minimumkövetelményeket határozzanak meg az internetszolgáltatókra vonatkozóan.

23. A fentiek azt jelentik, hogy európai uniós szinten jelentős törekvés van a nyílt internet megteremtésére (lásd a keretirányelv 8. cikkének (4) bekezdését). Ez a hálózat egészére vonatkozó szakpolitikai célkitűzés azonban nem kapcsolódik közvetlenül az egyes internetszolgáltatókra vonatkozó tilalmakhoz vagy kötelezettségekhez. Másként megfogalmazva: az internetszolgáltató alkalmazhat a bizonyos alkalmazásokhoz való hozzáférést esetleg kizáró forgalomkezelési politikát, amennyiben a felhasználók teljes körű tájékoztatást kapnak, és ahhoz szabadon, kifejezetten és egyértelműen hozzájárulásukat adták.

24. A helyzet a tagállamok függvényében változhat. Egyes tagállamokban az internetszolgáltatók – meghatározott feltételek mellett – forgalomkezelési politikát alkalmazhatnak bizonyos alkalmazások, például a VoIP blokkolása érdekében (az olcsóbb internet-előfizetések esetében), ha ehhez előfizetőik előzetes tájékoztatásukat követően önkéntes, kifejezett és egyértelmű beleegyezésüket adták. Más tagállamok a hálózatsemlegesség elvének megerősítése mellett döntöttek. 2011 júliusában például a holland parlament olyan törvény fogadott el, amely általános jelleggel megtiltja a szolgáltatóknak az internetes alkalmazások vagy szolgáltatások (például a VoIP) forgalmának akadályozását vagy lassítását, kivéve, ha ez a forgalomtorlódás hatásainak minimalizálása érdekében, integritási vagy biztonsági okokból, a levélszemét elleni küzdelem céljából vagy bírósági határozat értelmében szükséges. ([16])

III.2. **A hálózatsemlegességről szóló közlemény**

25. A hálózatsemlegességről szóló közleményében ([17]) az Európai Bizottság megállapította, hogy a hálózatsemlegességet illetően a helyzet ellenőrzésre és további elemzésre szorul. A Bizottság mindamellett kivárási politika alkalmazása mellett döntött az újabb szabályozási intézkedések megtétele előtt.

([14]) Az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról szóló, 2009. november 25-i 2009/136/EK európai parlamenti és tanácsi irányelv (HL L 337., 2009.12.18., 11. o.) által módosított 2002/22/EK irányelv. Összehasonlításképpen lásd még az 1. cikk (3) bekezdését, amely kimondja, hogy ez az irányelv nem ad felhatalmazást, de nem is tiltja az internetszolgáltatók számára, hogy korlátozzák az egyes szolgáltatások vagy alkalmazások végfelhasználók általi hozzáférését és/vagy használatát, amennyiben ezt a nemzeti jogszabályok megengedik és összhangban van a közösségi joggal, de kötelezettséget ír elő az ilyen feltételekről való tájékoztatásra vonatkozóan.

([15]) Az Európai Parlament és a Tanács 2009. november 25-i 2009/136/EK irányelve az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról.

([16]) Az eredeti holland módosítás a következő címen található: https://zoek.officielebekendmakingen.nl/kst-32549-A.html A sajtóbeszámolók szerint az ilyen szakpolitikai lehetőség alkalmazásának indoka nem az adatvédelmi vagy a magánélet védelmével kapcsolatos megfontolásokhoz kapcsolódott, hanem annak biztosításához, hogy a felhasználókat ne fosszák meg az információkhoz való hozzáféréstől, illetve ne korlátozzák abban. Ezért úgy tűnik, hogy ezt a módosítást az információhoz való hozzáféréssel kapcsolatos megfontolások motiválták.

([17]) L. 4. lábjegyzet.

26. A bizottsági közlemény felismerte, hogy minden intézkedés és további szabályozási lépés esetében az adatvédelmi és személyiségi jogi szempontok részletekbe menő értékelésére kerülne sor. A tanácsi következtetéstervezetek szintén kitértek az érintett adatvédelmi és személyiségi jogi kérdésekre ([18]).

27. Az adatok és a magánélet védelme szempontjából megvizsgálandó kérdés az, hogy elégséges-e a kiváráson alapuló politika. Noha az adatvédelemmel és a magánélet védelmével kapcsolatos jogi keret – jelenleg – bizonyos óvintézkedéseket ír elő, különösen a közlések titkosságának elvén keresztül, szükségesnek tűnik a megfelelőség szintjének szorosabb ellenőrzése, és néhány nem igazán egyértelmű szemponttal kapcsolatban iránymutatások közzététele. Emellett javaslatokat szükséges előterjeszteni arra vonatkozóan, hogy – a műszaki fejlődés fényében – miként tehető egyértelművé és hatékonyabbá a keret. Ha az ellenőrzés azt tárja fel, hogy a piac a közlések és a jogi kereteknek való megfeleléssel kapcsolatos kérdések jelentős mértékű, valós idejű ellenőrzése felé halad, akkor jogszabályi intézkedések válnak szükségessé. Ezzel kapcsolatban a VI. szakasz tartalmaz konkrét javaslatokat.

IV. **A MŰSZAKI HÁTTÉR ÉS A KAPCSOLÓDÓ, A MAGÁNÉLET ÉS AZ ADATOK VÉDELMÉVEL ÖSSZEFÜGGŐ EGYÉB SZEMPONTOK**

28. Mielőtt mélyebben a témába merülnénk, fontos, hogy jobban áttekintsük azokat az ellenőrzési technikákat, amelyeket az internetszolgáltatók a forgalomkezelési politika alkalmazása érdekében használhatnak, és hogy mindez hogyan hathat a hálózatsemlegesség elvére. Az ilyen műszaki megoldásokból eredő, a magánélet védelmére és az adatvédelemre gyakorolt hatás számottevő mértékben változik annak függvényében, hogy mely műszaki megoldást (vagy megoldásokat) alkalmazzák. Ez a technikai háttér elengedhetetlen az V. szakaszban ismertetett adatvédelmi jogi keret megértéséhez és megfelelő alkalmazásához. Meg kell jegyezni azonban, hogy folyamatosan változó és komplex területről van szó. Az alábbi ismertető ezért nem tekinthető kimerítő jellegűnek és teljes mértékben naprakésznek, hanem csupán a jogi érvelés megértéséhez elengedhetetlenül szükséges technikai információk közlésére szolgál.

IV.1. **Az információ továbbítása az interneten keresztül: alapok**

29. Amikor a felhasználó közlést továbbít az interneten keresztül, a továbbított információt a rendszer csomagokra osztja. A rendszer ezeket a csomagokat továbbítja az interneten a feladótól a címzetthez. Mindegyik csomag magában foglalja – többek között – a forrásra és a címre vonatkozó információkat. Az internetszolgáltatók emellett e csomagokat a különféle forgalomáramoknak az internetszolgáltató hálózatán belüli kezelésére szolgáló további rétegekbe és protokollokba ([19]) zárhatják.

30. Visszautalva a postai levél analógiájára: a hálózati átviteli protokoll használata annak felel meg, amikor a postai levet a postai szolgáltató által leolvasandó címzéssel ellátott borítékba tesszük, majd megbízzuk a postát a küldemény kézbesítésével. A postai szolgáltatás további protokollokat használhat belső továbbítási műveletei során az összes továbbítandó boríték kezelésére, és ennek az a célja, hogy mindegyik boríték megérkezzen az eredetileg a feladó által ráírt címre. E technológiai megoldás alkalmazása esetén mindegyik csomagnak két része van. Az egyik az *IP-hasznosadat*, amely a közlés tartalmát foglalja magában, és a levélnek felel meg. Ez a rész tartalmazza a kizárólag a címzettnek szóló információt. A csomag másik része az *IP-fejléc*, amely – többek között – a címzett és a feladó címét tartalmazza, és a borítéknak felel meg. Az IP-fejléc teszi lehetővé az internetszolgáltatók és a többi közvetítő számára a hasznosadatnak a forráscímtől a célcímhez való irányítását.

31. Az internetszolgáltatók és a más közvetítők biztosítják azt, hogy a hálózaton való továbbításukkor az IP-csomagok áthaladjanak az IP-fejlécadatokat elolvasó, az útválasztási táblázatokkal összevető és őket a cél felé vezető út következő csomópontja felé továbbító csomópontokon. Ez a folyamat a teljes

([18]) Lásd a 4. cikk e) pontját, amelyben a Tanács felhívja a figyelmet „egyes, főként a fogyasztók és az adatvédelmi hatóságok részéről a személyes adatok védelme tekintetében felmerülő aggályokra”.

([19]) Ahogyan azt a IV.2. szakasz részletesebben ismerteti, a protokollok a végfelhasználók között továbbított információt egyezményes módon kódolják – például http, ftp stb. kódban –, hogy a kommunikációban részt vevők megérthessék egymást.

hálózaton a lehető legkevesebb memóriafelhasználáson alapuló megközelítés szerint zajlik, mivel a rendszer az egyes csomópontokhoz érkező valamennyi csomagot semlegesen kezeli. Amint megtörtént az egyes csomagoknak a következő csomópontba történő továbbítása, már nem szükséges további adatokat tárolni az útválasztóban ([20]).

IV.2. **Ellenőrzési technikák**

32. Ahogyan azt fentebb szemléltettük, az internetszolgáltatók azért olvassák el az IP-fejléceket, hogy továbbítani tudják őket végcéljuk felé. Ahogy azonban korábban említettük, sor kerülhet a forgalom (így például az IP-fejléc és az IP-hasznosadat) más célokból és különféle jellegű technológiai megoldások igénybevételével történő elemzésére. Az új tendenciák között megjelenhet például a felhasználók által használt egyes alkalmazások (például a P2P) forgalmának lelassítása, vagy – másik lehetőségként – bizonyos szolgáltatások, például a megrendelt videoszolgáltatások forgalmi sebességének növelése a prémium előfizetők esetében. Noha *műszaki értelemben* valamennyi ellenőrzési technika csomagszűrést folytat, mindezt más és más mélységben végzik. Az ellenőrzési technikáknak két fő kategóriája van. Az egyik kizárólag az IP-fejlécen alapul, a másik az IP-hasznosadatra is támaszkodik.

Az IP-fejlécadat alapján. Az IP-csomag fejlécének vizsgálata néhány olyan mezőt mutat meg, amelyek lehetővé teszik az internetszolgáltató számára több, a forgalomkezelésre szolgáló politika alkalmazását. Ezek a technikák kizárólag az IP-fejlécek folyamatadatainak ellenőrzésén alapulnak, ami – elméletben – teljesen más, útválasztási információs célra (azaz a forgalom differenciálására) volna használatos. A forrás IP-címet megvizsgálva az internetszolgáltató a címet konkrét előfizetőhöz rendelheti hozzá, és meghatározott politikákat alkalmazhat, például a csomagot egy lassúbb vagy egy gyorsabb ág felé irányíthatja. A cél szerinti IP-címet megvizsgálva az internetszolgáltató szintén alkalmazhat sajátos politikákat, például a meghatározott webhelyekhez való hozzáférés blokkolását vagy szűrését.

Mélyebbre hatoló vizsgálat alapján. A csomagok mélyebbre hatoló vizsgálata lehetővé teszi az internetszolgáltató számára a kizárólag a közlés címzettjének szóló információkhoz való hozzáférést. Visszatérve a postai szolgáltatással kapcsolatos példához, ez a megközelítés annak felel meg, mintha kibontanák a borítékot és elolvasnák a levelet, hogy egy meghatározott hálózati politika alkalmazása érdekében elemezzék a közlés tartalmát (amely az IP-csomagok belsejébe van zárva). A vizsgálat elvégzésének különféle módjai vannak, ezek mindegyike más és más fenyegetést jelent az érintettre nézve.

— *A protokollok elemzésén és a statisztikai adatokon alapuló, mélyebbre hatoló csomagvizsgálat.* Az IP-protokoll mellett, amely célja az adatok interneten keresztüli továbbításának lehetővé tétele, léteznek olyan további protokollok is, amelyek az egyezményes módon továbbított információt kódolják (átvitel, munkamenet, bemutató és alkalmazás stb.). E protokollok célja annak biztosítása, hogy a kommunikációban részt vevő felek megérthessék egymást. Vannak például olyan protokollok, amelyek az internet böngészéséhez ([21]), és vannak, amelyek a fájlátvitelhez ([22]) kapcsolódnak. Ezért a protokollok vizsgálatán alapuló és statisztikai elemzéssel kombinált vizsgálati technikák célja az azt meghatározó sajátos minták vagy „ujjlenyomatok" keresése, hogy mely protokollok vannak használatban ([23]). Ezek a vizsgálati technikák lehetővé teszik az internetszolgáltatók számára a kommunikáció típusának megértését és – bizonyos esetekben – az adott alkalmazott szolgáltatás vagy alkalmazás azonosítását, így például az olyan VoIP kommunikációs szolgáltatások esetében, amelyeknél a felhasznált protokoll az adott forgalmazóra vagy szolgáltatóra kifejezetten jellemző. A kommunikáció típusának ismerete önmagában is lehetővé teheti az internetszolgáltató számára egyes konkrét forgalomkezelési politikák alkalmazását, például az internetes forgalom blokkolása érdekében. Előfordulhat az is, hogy ez az első lépés, amely lehetővé teszi az internetszolgáltató számára a további elemzés végrehajtását, ami a metaadatokhoz és a kommunikáció tartalmához való teljes mértékű hozzáférést is szükségessé teheti.

([20]) Az internethálózati berendezések ugyanakkor az IP-csomagoknak a lehető leghatékonyabb útvonalra való irányítása érdekében a tevékenységet naplózó, a forgalmi statisztikákat feldolgozó és a más hálózati berendezésekkel információcserét folytató útválasztási protokollokat alkalmaznak. Ha például egy hálózati ág túlterhelt vagy megszakad, és az útválasztó erről értesül, akkor útválasztási táblázatát az ezt az ágat nem használó más alternatív ággal frissíti. Nem szabad megfeledkezni arról az adatgyűjtésről és -feldolgozásról sem, amelyre bizonyos esetekben számlázási célból vagy akár az adatmegőrzési irányelv követelményeivel összhangban kerülhet sor.

([21]) Http (hiperszöveg-továbbítási protokoll) vagy HTML (hiperszöveges jelölőnyelv).

([22]) Ftp (állománytovábbítási protokoll).

([23]) Az alkalmazott protokollok azonosításának többféle módja van. Lehetséges többek között a belső protokollok meghatározott mezőinek keresése, például a kapcsolat létrehozásához használt portok meghatározása érdekében. A közlésáram statisztikai jellemzése kikövetkeztethető például meghatározott mezők elemzéséből, a két IP-cím között egyidejűleg használt protokollok korrelációja alapján.

— *A közlés tartalmának elemzésén alapuló, mélyebbre hatoló csomagvizsgálat.* Végezetül lehetséges a metaadatok ([24]), valamint magának a közlés tartalmának a vizsgálata. E technika keretében az eredeti közlésfolyamat részét képező valamennyi IP-csomagot feltörik annak érdekében, hogy a közlés eredeti tartalma teljes mértékben rekonstruálható és elemezhető legyen. A káros vagy jogsértő tartalmak – így a vírusok vagy a gyermekpornográfia – észleléséhez például magát a tartalmat szükséges rekonstruálni ahhoz, hogy az elemezhető legyen. Meg kell jegyezni, hogy néha a közlés a végpontok között teljes mértékben titkosítható a részt vevő felek által, ez pedig meggátolja az internetszolgáltatókat abban, hogy elemezzék a közlés tartalmát.

IV.3. **A magánélet védelmét és az adatvédelmet érintő kihatások**

33. Az IP-fejléceken és különösen a csomagvizsgálaton alapuló vizsgálati technikák magukban foglalják az említett adatok vizsgálatát és szűrését, így súlyos következményekkel járnak a magánélet védelme és az adatvédelem tekintetében. Ellentétesek lehetnek a közlések titkosságához való joggal is.

34. Az egyének közléseibe való betekintésnek már önmagában is komoly, a magánélet védelmével és az adatvédelemmel kapcsolatos következményei vannak. A probléma azonban ennél is szélesebb körű, mivel – az ellenőrzéssel és a feltöréssel elérni kívánt hatásoktól függően – a magánélet védelmével kapcsolatos hatások tovább súlyosbodhatnak. Nem mindegy, hogy a közléseket például a rendszer megfelelő működésének biztosítása, avagy az egyénekre potenciálisan hatást gyakorló politikák alkalmazása érdekében vizsgálják. Amikor a forgalmi és kiválasztási politikák célja kizárólag a hálózati torlódások kialakulásának megelőzése, akkor azok rendszerint nem gyakorolnak komolyabb hatást az egyének magánéletére. A forgalomkezelési politikák célja azonban lehet meghatározott tartalmi információk blokkolása vagy a közlés befolyásolása, például a viselkedésalapú reklámtevékenységen keresztül. Ilyen esetekben a hatások sokkal beavatkozóbb jellegűek. A probléma még kritikusabbá válik, ha megértjük, hogy az ilyen jellegű információk gyűjtése nem csak az egyének kis csoportját érintően történik meg, hanem általános alapon, az internetszolgáltató valamennyi ügyfelére kiterjedően ([25]). Amennyiben minden internetszolgáltató alkalmazza a szűrési technikákat, az az internethasználat általános ellenőrzéséhez vezethet. Továbbá amennyiben a feldolgozott információ típusára koncentrálunk, akkor a magánélet védelmére leselkedő kockázatok nyilvánvalóan nagyon nagyok, mivel az összegyűjtött információ nagy része valószínűleg nagyon szenzitív, és – az összegyűjtését követően – hozzáférhetővé válik az internetszolgáltatók és azok számára, akik az internetszolgáltatóktól információkat szerezhetnek. Az információ emellett kereskedelmi szempontból is nagyon értékes lehet. Ez magában hordozza annak a veszélyét, hogy az eredeti funkciókat jóval szélesebb körre terjesztik ki, így a kezdeti cél nagyon könnyen átalakulhat az összegyűjtött információk kereskedelmi vagy más célú kiaknázásává.

35. Az ellenőrzési, vizsgálati és szűrési technikák megfelelő alkalmazását a vonatkozó, az adatok és a magánélet védelmét biztosító olyan eszközökkel összhangban kell megvalósítani, amelyek határt szabnak annak tekintetében, hogy mit és milyen feltételek mellett lehet megtenni. A továbbiakban a magánélet és az adatok védelmére vonatkozó hatályos európai uniós jogi keret szerint alkalmazandó védintézkedéseket tekintjük át.

V. **A MAGÁNÉLET ÉS AZ ADATOK VÉDELMÉRE VONATKOZÓ UNIÓS JOGI KERET ALKALMAZÁSA**

36. Az EU adatvédelmi keretrendszere technológiai szempontból semleges; mint ilyen, nem konkrét – például a fentiekben ismertetett – vizsgálati technikákat szabályoz. Az elektronikus hírközlési adatvédelmi irányelv a nyilvános hálózatokon keresztül nyújtott elektronikus hírközlési szolgáltatások esetében szabályozza a magánélet védelmét (jellemzően az internet-hozzáférés és a telefonszolgáltatás

([24]) Mindegyik protokoll fejlécében olyan meghatározott mezők találhatók, amelyek további tájékoztató jellegű adatokat közölnek a továbbított közlésről. Ezért e mezők tartalma a közléssel kapcsolatos metaadatnak tekinthető. Példa e mezőkre a használt port száma: amennyiben például ez a szám a 80, akkor elég valószínű, hogy a közlés típusa webböngészés.

([25]) A nyomon követési funkciók alkalmazása természetesen nem kizárólag az internetszolgáltatókra jellemző. A hirdetésihálózat-szolgáltatók szintén képesek arra, hogy harmadik féltől származó cookie-k segítségével nyomon kövessék a felhasználókat a különféle webhelyeken keresztül. Ezt a jelenséget mutatja be például az a közelmúltban közzétett tudományos cikk, amely szerint a Google az első 100 webhelyből 97 webhelyen van jelen, ami azt jelenti, hogy a Google nyomon tudja követni azokat a felhasználókat, akik nem utasítják vissza a harmadik féltől származó cookiekat akkor, amikor ezeket a népszerű oldalakat böngészik. Lásd: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay: *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning* (2011. július 29.). A cikk az SSRN webhelyén érhető el, a következő címen: http://ssrn.com/abstract=1898390 A felhasználók harmadik féltől származó cookie-k alkalmazásával való nyomon követésével a 29. cikk alapján létrehozott munkacsoport is foglalkozott. Lásd a 2/2010. számú véleményt a viselkedésalapú online reklámról, elfogadás időpontja: 2010. június 22. (WP 171).

területén) ([26]), az adatvédelmi irányelv pedig általában szabályozza az adatfeldolgozást. Ez az átfogó jogi keretrendszer különféle kötelezettségeket állapít meg a forgalmi és közlési adatokat feldolgozó és ellenőrző internetszolgáltatókra vonatkozóan.

V.1. **A forgalmi és tartalmi adatok feldolgozásának jogszabályi alapjai**

37. Az adatvédelmi jogszabályok szerint a személyes adatok feldolgozásához – például a forgalmi és közlési adatok feldolgozásához – megfelelő jogszabályi alapra van szükség. Ezen általános követelmény mellett bizonyos esetekben különleges követelmények is fennállhatnak.

38. Ebben az esetben az internetszolgáltatók által feldolgozott személyesadat-típus a közlések forgalmi adataihoz és tartalmához kötődik. A közlések tartalmát és a forgalmi adatokat egyaránt a levéltitokhoz való jog védi, amelyet az EJEE 8. cikke és a Charta 7. és 8. cikke garantál. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1), „A közlések titkossága" című bekezdése konkrétan előírja a tagállamok számára, hogy biztosítaniuk kell a nyilvános hírközlő hálózatok és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások segítségével történő közlések és az azokra vonatkozó forgalmi adatok titkosságát. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdése ugyanakkor előírja azt is, hogy bizonyos esetekben – a felhasználók jóváhagyásával – megengedhető a forgalmi és tartalmi adatoknak az internetszolgáltató által elvégzett feldolgozása. Mindamellett ebben az esetben is „megtiltják a közlések és az azokra vonatkozó forgalmi adatok felhasználókon kívüli személyek által történő, az érintett felhasználó hozzájárulása nélküli meghallgatását, lehallgatását, tárolását vagy más módon történő elfogását vagy megfigyelését, kivéve, ha az ilyen személy a 15. cikk (1) bekezdésével összhangban jogszerűen jár el." Ennek részletezése az alábbiakban olvasható.

39. Az érintett felhasználók jóváhagyása mellett az elektronikus hírközlési adatvédelmi irányelv más olyan jogalapokat is előír, amelyek indokolhatják az internetszolgáltatók forgalmiadat- és kommunikációsadat-feldolgozási tevékenységének jogszerűségét. Ebben az esetben a feldolgozás megfelelő jogalapját i. a szolgáltatás nyújtása; ii. a szolgáltatás biztonságának szavatolása és iii. a torlódás minimalizálása jelenti. A forgalommal vagy a közléssel kapcsolatos adatokon alapuló forgalomkezelési politikák legitimizálásának további lehetséges alapjait az alábbi iv. pontban ismertetjük.

i. A szolgáltatásnyújtás jogalapja

40. Ahogyan azt a IV. szakasz is szemlélteti, az internetszolgáltatók az IP-fejlécekre vonatkozó információkat az egyes IP-csomagok céljukhoz való irányítása érdekében dolgozzák fel. Az elektronikus hírközlési adatvédelmi irányelv 6. cikkének (1) és (2) bekezdése lehetővé teszi a forgalmi adatoknak a közlés továbbítása érdekében történő feldolgozását: azaz az internetszolgáltatók feldolgozhatják a szolgáltatásnyújtáshoz szükséges információt.

ii. A szolgáltatás biztonsága szavatolásának jogalapja

41. Az elektronikus hírközlési adatvédelmi irányelv 4. cikke értelmében az internetszolgáltatónak általános érvényű kötelessége, hogy megfelelő intézkedéseket tegyen szolgáltatásai biztonságának biztosítása érdekében. A vírusszűrés gyakorlata magában foglalhatja az IP-fejlécek és az IP-hasznosadatok feldolgozását. Figyelembe véve azt, hogy az elektronikus hírközlési adatvédelmi irányelv 4. cikke megköveteli az internetszolgáltatótól a hálózat biztonságának biztosítását, ez a rendelkezés a szigorúan e cél elérésére irányuló, az IP-fejléceken és a tartalmon alapuló ellenőrzési technikákat legitimizálja. A gyakorlatban ez azt jelenti, hogy az internetszolgáltatók – az arányosság elve által megszabott korlátokon belül (lásd az V. szakasz 3. pontját) – a vírusok elleni küzdelem és általában a hálózat biztonságának biztosítása érdekében foglalkozhatnak a közlési adatok ellenőrzésével és szűrésével ([27]).

([26]) Az elektronikus hírközlési adatvédelmi irányelv 10. preambulumbekezdése így rendelkezik: „Az elektronikus hírközlési ágazatban a 95/46/EK irányelv alkalmazandó az alapvető jogok és szabadságok védelmével kapcsolatos területekre, amelyet jelen irányelv rendelkezései nem kifejezetten szabályoznak, beleértve az adatkezelők kötelezettségeit és az egyének jogait". Az érintett hozzájárulása vonatkozásában a (17) preambulumbekezdés is meghatározó: „Ennek az irányelvnek az alkalmazásában a felhasználó vagy előfizető hozzájárulását, függetlenül attól, hogy ez utóbbi természetes vagy jogi személy-e, az érintett hozzájárulásával – amelyet a 95/46/EK irányelv határoz meg és pontosít – azonosként kell értelmezni."

([27]) A 29. cikk alapján létrehozott munkacsoport 2006. február 21-én elfogadott, 2/2006. számú véleménye az e-mailek átvilágítására vonatkozó szolgáltatásokkal kapcsolatos adatvédelmi kérdésekről (WP 118). Ebben a véleményben a munkacsoport úgy véli, hogy a szűrők 4. cikk alkalmazásában történő használata összeegyeztethető lehet az elektronikus hírközlési adatvédelmi irányelv 5. cikkével.

iii. A torlódás hatásai minimalizálásának jogalapja

42. E jogalap *indokolása* az elektronikus hírközlési adatvédelmi irányelv (22) preambulumbekezdésében található, amely a közlések tárolásának az 5. cikk (1) bekezdése szerinti tilalmát ismerteti. Ez a tilalom nem vonatkozik az adatok automatikus, közbenső és átmeneti tárolására, amennyiben az ilyen tárolásra kizárólag a továbbítás céljával kerül sor, és amennyiben a tárolásra csak a továbbításhoz és a forgalomkezeléshez szükséges ideig kerül sor, illetve amennyiben a bizalmas kezelés mindvégig garantált.

43. Amennyiben torlódás alakul ki, felmerül a kérdés, hogy az internetszolgáltató fontolóra veheti-e a forgalom korlátozását vagy késleltetését, vagy az idő szempontjából kevésbé érzékeny közlések, például a P2P- vagy az e-mail forgalom lassítását annak érdekében, hogy lehetővé tegye például a hangforgalom elfogadható minőségben való fenntartását.

44. Figyelemmel a használható hírközlő hálózat biztosításához fűződő általános társadalmi érdekekre, az internetszolgáltatók azzal érvelhetnek, hogy a forgalomnak a torlódás megszüntetése érdekében történő előrébb- vagy hátrébbsorolása olyan jogszerű intézkedés, amely a szolgáltatás megfelelő szinten való nyújtásához szükséges. Ez azt jelenti, hogy ezekben az esetekben meglenne a személyes adatok feldolgozásának általános jogalapja, és nem lenne szükség a felhasználók kifejezett hozzájárulására.

45. Ugyanakkor az ilyen módon való beavatkozás lehetősége nem korlátlan. Ha az internetszolgáltatóknak meg kell vizsgálniuk a közléseket, akkor – a titkosság szempontjából és szigorúan alkalmazva az arányosság elvét – a cél elérése érdekében a rendelkezésükre állók közül azt a módszert kell alkalmazniuk, amely a legkevésbé beavatkozó jellegű (elkerülve ezzel a mélyebbre hatoló csomagvizsgálatot), és azt csak abban az esetben szabad alkalmazniuk, ha ez a torlódás megszüntetéséhez szükséges.

iv. Az adatok más célokból történő feldolgozásának jogalapja

46. Előfordulhat, hogy az internetszolgáltatók más célból kívánják megvizsgálni a forgalommal és a tartalommal kapcsolatos adatokat – például hogy célzott előfizetéseket ajánlhassanak (például a P2P-szolgáltatásokhoz való hozzáférést korlátozó, vagy bizonyos alkalmazások esetében a sebességet növelő előfizetést). A forgalommal és a közléssel kapcsolatos adatoknak a szolgáltatásnyújtástól vagy a szolgáltatás biztonságának biztosításától vagy a torlódás kialakulásának megelőzésétől eltérő más célok érdekében való vizsgálata vagy további felhasználása kizárólag szigorú feltételek mellett, a jogszabályi keretekkel összhangban megengedett.

47. A jogszabályi keretet főként az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdése jelenti, amely az érintett felhasználók beleegyezéséhez köti a közlések és az azokra vonatkozó forgalmi adatok meghallgatását, lehallgatását, tárolását vagy más módon történő elfogását vagy megfigyelését. A gyakorlatban ez azt jelenti, hogy a közlésben érintett felhasználók beleegyezése szükséges mind a forgalommal, mind pedig a közlésekkel kapcsolatos adatoknak az 5. cikk (1) bekezdése szerinti feldolgozásának legitimizálásához.

48. Ahogyan azt a korábbiakban ismertettük, az ellenőrzési és szűrési technikák alkalmazása vagy a forgalmi adatokat alkotó IP-fejléceken, vagy pedig az IP-hasznosadatokat tartalmazó és a közlési adatokat alkotó csomagok mélyebbre hatoló vizsgálatán alapul. Ennélfogva – elvben – az említett technikáknak a szolgáltatásnyújtástól vagy a szolgáltatás biztonságának biztosításától eltérő célokra történő alkalmazása a feldolgozást lehetővé tevő jogalap, például a beleegyezés (az 5. cikk (1) bekezdése) nélkül tiltott volna. Az 5. cikk (1) bekezdésének alkalmazására példa az, amikor az internetszolgáltató a viselkedésalapú reklámok fogadásáért, a csomagok – és ilyen módon a közléssel kapcsolatos adatok – mélyebbre ható vizsgálatának engedélyezéséért cserébe kedvezményes árú internet-hozzáférést kínál fel ügyfeleinek. Ennélfogva ebben az esetben az 5. cikk (1) bekezdése értelmében valódi, konkrét és a megfelelő információk birtokában megtett hozzájárulás szükséges.

49. Emellett az elektronikus hírközlési adatvédelmi irányelv „Forgalmi adatok” című 6. cikke bizonyos, kifejezetten a forgalmi adatokra vonatkozó szabályokat állapít meg. A cikk rendelkezik annak lehetőségéről, hogy az internetszolgáltatók a felhasználóknak az értéknövelt szolgáltatások fogadásához való

hozzájárulása alapján feldolgozhassák azok forgalmi adatait ([28]). A rendelkezés a forgalmi adatok vonatkozásában konkrétan meghatározza az 5. cikk (1) bekezdésében előírt, hozzájárulással kapcsolatos követelményt.

50. A gyakorlatban nem minden esetben könnyű meggyőződni például arról, hogy mely esetekben szükséges a hozzájárulás, és hogy mely esetekben indokolhatja a feldolgozást a hálózat biztonsága, különösen ha az ellenőrzési technikák célja kettős (például a torlódás kialakulásának elkerülése és értéknövelt szolgáltatások nyújtása). Hangsúlyozni kell, hogy a hozzájárulás nem tekinthető az adatvédelmi elveknek való megfelelést eredményező egyszerű és rendszerszintű megoldásnak.

51. Kevés tapasztalat áll rendelkezésre a jogi keret alkalmazásával, és különösen a fentiekben vázolt különféle szempontokkal kapcsolatban. Olyan területről van szó, amelyet illetően – ahogyan azt a VI. szakaszban részletesebben is kifejtjük – további iránymutatás szükséges. Emellett vannak olyan további, a hozzájárulás megszerzéséhez kapcsolódó szempontok, amelyek szintén különös figyelmet igényelnek. E szempontokat az alábbiakban ismertetjük.

V.2. **A megfelelő információk birtokában történő hozzájárulással mint jogalappal kapcsolatos kérdések**

52. Az elektronikus hírközlési adatvédelmi irányelv 5. és 6. cikkével előírt hozzájárulás ugyanazzal a jelentéssel bír, mint az érintettnek a 95/46/EK irányelvben meghatározott és részletezett hozzájárulása ([29]). Az adatvédelmi irányelv 2. cikkének h) pontja szerint „az érintett hozzájárulása" „az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához". A 29. cikk alapján létrehozott munkacsoport a hozzájárulásról szóló 15/2011. sz. véleményében a közelmúltban foglalkozott a hozzájárulás szerepével, valamint a hozzájárulás érvényességével kapcsolatos követelményekkel ([30]).

53. A forgalommal és a tartalommal kapcsolatos adatok vizsgálatához és szűréséhez jóváhagyás megszerzését igénylő internetszolgáltatóknak ennélfogva biztosítaniuk kell, hogy a hozzájárulás az érintett szándékainak önkéntes és konkrét, továbbá a megfelelő információ birtokában történő kifejezése legyen, amellyel az érintett a vele kapcsolatos személyes adatok feldolgozásába való beleegyezését jelzi. Ezt az elektronikus hírközlési adatvédelmi irányelv (17) preambulumbekezdése is megerősíti: „Hozzájárulás bármely olyan megfelelő módon adható, amely lehetővé teszi a felhasználó szándékainak önkéntes, konkrét és a megfelelő információk birtokában történő kifejezését, ideértve valamely internetes honlap látogatása során egy rovat bejelölését." Az alábbiakban néhány gyakorlati példával szemléltetjük, hogy ezzel összefüggésben mit jelent a hozzájárulás önkéntes, konkrét és a megfelelő információk birtokában történő kifejezése.

Hozzájárulás: a szándék önkéntes, konkrét és a megfelelő információ birtokában történő kifejezése

54. *Önkéntes hozzájárulás.* A felhasználókat nem szabad olyan korlátozásoknak kitenni, amelyek az általuk igénybe venni kívánt internet-előfizetést ilyen hozzájáruláshoz kötik.

55. A magánszemély hozzájárulása nem tekinthető önkéntesnek, ha a hírközlési szolgáltatáshoz való hozzáférés érdekében hozzá kell járulniuk a hírközlési adatok ellenőrzéséhez. Ez még inkább igaz abban az esetben, ha az adott piac *valamennyi* szolgáltatója a hálózat biztonságán túlmenő célokból folytatna forgalomkezelési tevékenységet. Az egyedüli fennmaradó lehetőség ebben az esetben az lenne, hogy az érintettek egyáltalán nem fizetnek elő internetszolgáltatásra. Figyelemmel arra, hogy az internet mind a munkavégzés, mind pedig a szabadidő eltöltése céljából alapvető fontosságú eszközzé vált, az,

([28]) Az irányelv (18) preambulumbekezdése az értéknövelt szolgáltatásokat szemléltető felsorolást tartalmaz. Nem egyértelmű, hogy azok a szolgáltatások, amelyekre a forgalomkezelési politikák vonatkoznak, értelmezhetők-e a felsorolás részeként. A meghatározott tartalmak rangsorolására irányuló forgalomkezelési politikák tekinthetők a szolgáltatás minőségének biztosításaként. Például a kizárólag az IP-fejlécek feldolgozásából álló forgalomkezelés, amelynek célja a prémiumárazású játékszolgáltatások biztosítása, amelyek esetében a felhasználók személyes játékforgalma elsőbbséget élvez a hálózaton, értéknövelt szolgáltatásnak tekinthető. Másfelől pedig távolról sem egyértelmű, hogy bizonyos típusú forgalmak sávszélesség-szabályozással történő ellenőrzése, például a P2P-forgalom hátrébbsorolása ilyennek tekinthető-e.

([29]) Lásd az elektronikus hírközlési adatvédelmi irányelv (17) preambulumbekezdését és 2. cikkének f) pontját.

([30]) Elfogadás időpontja: 2011. július 13. (WP 187).

hogy valaki nem fizet elő az internetszolgáltatásra, nem lehet valós alternatíva. Ennek az lenne az eredménye, hogy az egyéneknek nem lenne tényleges választási lehetősége, azaz nem volna lehetőségük arra, hogy önként adják hozzájárulásukat ([31]).

56. Az európai adatvédelmi biztos szerint egyértelműen szükség van arra, hogy a Bizottság és a nemzeti hatóságok figyelemmel kísérjék a piac alakulását, különösen azért, hogy meggyőződhessenek arról, hogy ez a forgatókönyv – azaz hogy a szolgáltatók a hírközlési szolgáltatást összekapcsolják a közlések ellenőrzésével – esetleg általánosan elterjedtté válik-e. A szolgáltatóknak anélkül kellene alternatív szolgáltatásokat – például forgalomkezelés nélküli internet-előfizetést – kínálniuk, hogy közben nagyobb költségeket terhelnének a magánszemélyekre.

57. *Kifejezett hozzájárulás.* A hozzájárulás konkrét jellegének szükségessége – ebben az esetben – megköveteli, hogy az internetszolgáltatók egyértelmű és jól érzékelhető módon kérjék a forgalom és a hírközlési adatok ellenőrzéséhez való hozzájárulást. A 29. cikk alapján létrehozott munkacsoport szerint „annak érdekében, hogy a hozzájárulás kifejezett legyen, érthetőnek kell lennie: egyértelműen és pontosan utalnia kell az adatfeldolgozás hatókörére és következményeire. Nem vonatkozhat határozatlan adatfeldolgozásitevékenység-sorozatra. Más szóval ez azt jelenti, hogy a hozzájárulás alkalmazási köre korlátozott." A megszerzett hozzájárulás nem lehet kifejezett, ha a forgalommal és a közlésekkel kapcsolatos adatok vizsgálatához való hozzájárulás „egybe van csomagolva" a szolgáltatásra való előfizetés megkötéséhez való hozzájárulással. A kifejezett jelleg a hozzájárulás megszerzéséhez célzott eszközök, például külön hozzájáruló nyilatkozati űrlap vagy erre szolgáló, az ellenőrzés céljával foglalkozó, különálló keretes rész alkalmazását teszi szükségessé (szemben az információnak a szerződés általános szerződési feltételei közé való beszúrásával és a szerződés ebben a formában való aláírásának megkövetelésével).

58. *A megfelelő információk birtokában történő hozzájárulás.* Ahhoz, hogy a hozzájárulás érvényes legyen, szükséges, hogy a megfelelő információk birtokában nyilvánítsák ki. A megfelelő előzetes tájékoztatás nyújtásának szükségessége nemcsak az elektronikus hírközlési adatvédelmi irányelvből és az adatvédelmi irányelvből ered, hanem a 2009/136/EK irányelvvel ([32]) módosított egyetemes szolgáltatási irányelv 20. és 21. cikkéből is. A tájékoztatás és a hozzájárulás szükségességét a 2009/136/EK irányelv (28) preambulumbekezdése kifejezetten megerősíti: „a felhasználókat minden esetben teljes mértékben tájékoztatni kell az elektronikus hírközlési szolgáltatások terén a szolgáltató és/vagy a hálózatszolgáltató által bevezetett felhasználásbeli korlátozásokról. E tájékoztatásnak – a szolgáltató belátása szerint – vagy a tartalom, az alkalmazás vagy az érintett szolgáltatás típusát, vagy az egyes alkalmazásokat és szolgáltatásokat, vagy mindkettőt meg kell határoznia." Ezt követően a következőképpen rendelkezik: „Az alkalmazott technológiától és a korlátozások típusától függően e korlátozások esetében szükséges lehet a felhasználó 2002/58/EK irányelv szerinti beleegyezése."

59. Figyelemmel az említett ellenőrzési technikák összetett jellegére, a kellően részletes előzetes tájékoztatás az érvényes hozzájárulás megszerzésének egyik fő kihívását jelenti. A fogyasztókat olyan módon kell tájékoztatni, hogy meg tudják érteni a feldolgozandó információt, az információ felhasználásának módját, valamint a felhasználói élményre gyakorolt hatást, továbbá a magánéletbe ilyen technikákkal történő behatolás szintjét.

60. Ez nem csak azt jelenti, hogy a tájékoztatásnak magának kell egyértelműnek és érthetőnek lennie az átlagfelhasználó számára, hanem azt is, hogy a tájékoztatást az érintett személy közvetlenül és nyilvánvaló módon kapja, hogy ne tudjon átsiklani felette.

61. *A szándék kifejezése.* A vonatkozó jogszabályi keretek szerint a beleegyezés kinyilvánításához szükség van arra, hogy a felhasználó azt megerősítő intézkedést tegyen. A hallgatólagos hozzájárulás nem felel meg ennek az elvárásnak. Emiatt az internetszolgáltatónak olyan speciális eszközöket kell alkalmaznia, amelyek kifejezetten az ahhoz való hozzájárulás megszerzésére szolgálnak, hogy a forgalomkezelési politikák alkalmazásával összefüggésben megvizsgálhassa a forgalommal és a közléssel kapcsolatos adatokat. A hozzájárulásról szóló legutóbbi véleményében a 29. cikk alapján létrehozott munkacsoport hangsúlyozta, hogy a hozzájárulás megszerzéséhez mélyrehatóan részletezni kell az adatfeldolgozás különböző alkotóelemeit.

([31]) Hasonló a PNR-adatok esete is, ahol az képezte a vita tárgyát, hogy érvényesnek tekinthető-e az utasok ahhoz való hozzájárulása, hogy foglalási adataikat az Egyesült Államok hatóságai számára továbbítsák. A munkacsoport úgy véli, hogy az utasok hozzájárulása nem lehet önkéntes, mivel a légitársaságok a járat indulása előtt kötelesek megküldeni az adatokat, és az utasoknak nincs valódi választási lehetőségük, amennyiben utazni akarnak (a 29. cikk alapján létrehozott munkacsoport 6/2002. számú véleménye az utasokra vonatkozó és egyéb adatoknak a légitársaságok által az Egyesült Államok részére való átadásáról).

([32]) Az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv módosításáról szóló, 2009. november 25-i 2009/136/EK irányelv (lásd a 15. lábjegyzet).

62. Úgy is lehetne érvelni, hogy ha a közlésben részes felek nem kívánják, hogy a közlést az internetszolgáltató a forgalomkezelési politikák alkalmazása érdekében elfogja, még mindig titkosíthatják a közlést. Gyakorlati szempontból ez a megközelítés hasznosnak tekinthető, azonban bizonyos erőfeszítést és műszaki ismereteket igényel, és nem tekinthető hasonlónak az önkéntes, kifejezett és a megfelelő információ birtokában adott hozzájáruláshoz. A titkosítási technikák alkalmazása ugyanakkor nem biztosítja a közlés maradéktalan bizalmasságát, mivel az internetszolgáltató legalább a közlés irányításához szükséges IP-fejlécadathoz hozzáférhet, továbbá lehetősége marad a statisztikai elemzésre is.

63. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdése értelmében az érintett felhasználók hozzájárulását kell megszerezni. Számos esetben a felhasználó ugyanaz a személy, mint az előfizető, ami lehetővé teszi a hozzájárulásnak a hírközlési szolgáltatásra való előfizetés pillanatában történő megszerzését. Más esetekben – például amikor egynél több személy lehet érintett – az érintett felhasználók hozzájárulását külön-külön kell megszerezni. Ez az alábbiakban részletezett gyakorlati problémákat vetheti fel.

Az összes érintett felhasználó hozzájárulása

64. Az 5. cikk (1) bekezdése felhasználói hozzájárulást ír elő a feldolgozás jogszerűségének megteremtéséhez. A hozzájárulást a közlésben érintett *valamennyi felhasználótól* meg kell szerezni. Az e mögött meghúzódó meggondolás az, hogy a közlés rendszerint legalább két személyre tartozik (a feladóra és a címzettre). Ha például az internetszolgáltató átvilágítja az e-mailre utaló IP-hasznosadatokat, akkor olyan információt vizsgál, amely az e-mail üzenet feladójával és címzettjével egyaránt kapcsolatos.

65. A forgalom és a közlések (például valamilyen internetes forgalom) ellenőrzésekor és feltörésekor elégséges lehet az internetszolgáltató számára a felhasználó, azaz az előfizető hozzájárulásának megszerzése. Ez azért van, mert a közlés másik részes fele – ebben az esetben a felkeresett webhely – nem tekinthető „érintett felhasználónak" ([33]). Összetettebb lehet azonban a helyzet akkor, ha az ilyen ellenőrzés e-mail üzenetek tartalmának – és ilyen módon az e-mail feladója és az esetleg a nem ugyanezzel az internetszolgáltatóval szerződéses kapcsolatban álló címzettje személyes adatainak – vizsgálatára is kiterjed. Ilyen esetekben az internetszolgáltató az ügyfelektől eltérő személyek személyes adatait (a nevet, az e-mail címet és az eseteleges szenzitív tartalmi adatokat) is feldolgozza. Gyakorlati szempontból az ilyen személyek hozzájárulásának megszerzése nehezebb lehet, mivel eseti alapon, nem pedig a hírközlési szolgáltatási szerződés megkötésekor kell sort keríteni rá. Nem volna valószerű az sem, ha feltételeznénk, hogy a felhasználó hozzájárulásának megadása a többi felhasználó nevében is történik, ahogyan az gyakran megtörténik a háztartások esetében.

66. Ezzel összefüggésben az európai adatvédelmi biztos úgy véli, hogy az internetszolgáltatóknak eleget kell tenniük a hatályos jogszabályi követelményeknek, és olyan politikákat kell végrehajtaniuk, amelyek nem foglalják magukban az információk ellenőrzését és vizsgálatát. Ez még alapvetőbb az olyan harmadik felekre is kiterjedő hírközlési szolgáltatások esetében, akik nem tudnak hozzájárulni az ellenőrzéshez, különösen az elküldött és fogadott e-mailek tekintetében (ez nem érvényes akkor, ha a cél biztonsági megfontolásokon alapul).

67. Meg kell jegyezni ugyanakkor, hogy az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdését végrehajtó nemzeti jog e tekintetben nem minden esetben feltétlenül kielégítő, és hogy általában úgy tűnik, az elektronikus hírközlési adatvédelmi irányelv követelményeire vonatkozóan ezzel összefüggésben meglehetős szükség lenne hatékonyabb iránymutatásra. Az európai adatvédelmi biztos ennélfogva felkéri a Bizottságot, hogy legyen tevékenyebb e tekintetben, és indítson el egy kezdeményezést, amely nagymértékben építhet a 29. cikk alapján létrehozott munkacsoportban közreműködő felügyeleti hatóságok és más érdekelt felek eddigi munkájára. Szükség esetén egyes ügyekben a Bírósághoz lehet fordulni, hogy teljes egyértelműséget lehessen teremteni az 5. cikk (1) bekezdésének értelmezését ás következményeit illetően.

([33]) Az olyan esetek ellenére, amelyeknél az internetes forgalom személyes adatok továbbítását foglalja magában – például azonosítható természetes személyek valamely webhelyen közzétett képeit. Az ilyen információk feldolgozása jogalapot tesz szükségessé, de nem vonatkozik rá az 5. cikk (1) bekezdése, mivel az ilyen személyek nem tekinthetők „érintett felhasználónak".

V.3. **Arányosság – az adatminimalizálás elve**

68. Az adatvédelmi irányelv 6. cikkének c) pontja megállapítja az arányosság elvét ([34]), amely az internetszolgáltatókra is vonatkozik, mivel amikor ellenőrzéssel és szűréssel foglalkoznak, akkor – az irányelv értelmezésében – adatkezelőnek minősülnek.

69. Ezen elv alapján a személyes adatok csak abban az esetben dolgozhatók fel, amennyiben „gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek". Ennek az elvnek az alkalmazása magában foglalja az azzal kapcsolatos értékelés elvégzésének szükségességét, hogy az adatfeldolgozáshoz alkalmazott eszközök és felhasznált személyesadat-típusok ésszerűen alkalmasak és megfelelőek-e a célkitűzéseik eléréséhez. Ha a következtetés az, hogy a szükségesnél több adatot gyűjtöttek össze, akkor az elv nem teljesült.

70. A vizsgálati technikák bizonyos típusai vonatkozásában az arányosság elvének való megfelelést eseti alapon kell értékelni, mert elvont módszerekkel nem lehetséges következtetéseket levonni. Lehetséges azonban különféle konkrét szempontok kijelölése, amelyeket az arányosság elvének való megfelelés vizsgálatakor értékelni kell.

71. *A feldolgozott információ mennyisége.* Az internetszolgáltatók ügyfelei közléseinek a lehető legmélyrehatóbban történő ellenőrzése az esetek többségében eltúlzott és jogsértő. Az, hogy ezt az egyének számára nem nyilvánvaló eszközökkel lehet elvégezni, továbbá hogy az érintettek számára nehéz lehet a történések megértése, növeli a magánéletükre gyakorolt hatást. Az internetszolgáltatóknak fel kell mérniük, hogy mely kevésbé beavatkozó jellegű eszközök volnának alkalmazhatók a szükséges eredmény eléréséhez. Például az IP-fejlécek ellenőrzése elérheti-e a szükséges eredményt, ha a mélyrehatóbb csomagvizsgálat helyett alkalmazzák? A bizonyos protokollokra korlátozott elemzés még a mélyebbre hatoló csomagvizsgálat alkalmazásakor is biztosíthatja a szükséges információt. Az adatvédelmi garanciák, például az álnevesítés és a névtelenítés alkalmazása szintén releváns lehet. Az értékelés eredményének azt kell alátámasztania, hogy az adatfeldolgozás arányos.

72. *A feldolgozás hatásai (közvetlenül a céllal összefüggésben).* Az arányosság hiányozhat például az olyan esetekben is, amikor az internetszolgáltatók bizonyos szolgáltatásokhoz való hozzáférést kizáró forgalomkezelési politikákat használnak anélkül, hogy cserébe elérhetővé tennék a felhasználók számára az eredő előny méltányos részét.

73. Fontos emlékeztetni arra, hogy az arányosság elve továbbra is érvényesül akkor is, ha közben más kötelező jogszabályi követelmények teljesülnek, ideértve például azt is, amikor az adott internetszolgáltató hozzájárulást kapott az érintett személyektől a tartalom-ellenőrzésre. Ez azt jelenti, hogy a tartalom-ellenőrzésen keresztül folytatott adatfeldolgozás továbbra is jogsértő lehet, amennyiben megsérti az arányosság mögöttes alapelvét.

V.4. **Biztonsági és szervezési intézkedések**

74. Az elektronikus hírközlési adatvédelmi irányelv 4. cikke kifejezetten előírja az internetszolgáltató számára a következőket biztosító technikai és szervezési intézkedések végrehajtását: i. a személyes adatokhoz csak az arra jogosult személyek és jogszerű célból férhessenek hozzá; ii. a személyes adatok védve legyenek a véletlen vagy jogellenes feldolgozással szemben; és iii. biztonsági politikát hajtsanak végre a személyes adatok feldolgozása tekintetében. A cikk lehetővé teszi az illetékes nemzeti hatóságok számára az ezekkel az intézkedésekkel kapcsolatos ellenőrzések végrehajtását is.

75. Emellett – az elektronikus hírközlési adatvédelmi irányelv 4. cikkének (3) és (2) bekezdése értelmében – az internetszolgáltatónak kötelessége a személyes adatok megsértése esetén az illetékes nemzeti hatóságok, továbbá – amennyiben az adatok nyilvánosságra kerülése hátrányos következményekkel járhat rájuk nézve – az érintett személyek értesítése.

76. A közlésekben szereplő személyes adatoknak a forgalomkezelési politikák alkalmazásának céljából történő feldolgozása a forgalommal kapcsolatos adatoknál sokkal érzékenyebb természetű adatokat is hozzáférhetővé tehet az internetszolgáltatók számára.

([34]) Ahogyan azt korábban már említettük, az alapvető jogok és szabadságok védelmével kapcsolatos minden olyan területre, amelyet az elektronikus hírközlési adatvédelmi irányelv nem szabályoz kifejezetten, az adatvédelmi irányelv alkalmazandó.

77. Ezért az internetszolgáltatók által kidolgozott biztonsági politikának meghatározott garanciákat kell magában foglalnia annak biztosítására, hogy a meghozott intézkedések e kockázatokhoz igazodjanak. Ugyanakkor az ilyen intézkedéseket ellenőrző nemzeti hatóságoknak különös szigorral kell eljárniuk. Végezetül biztosítani kell azt, hogy hatékony értesítési eljárásokat dolgozzanak ki az olyan érintettek tájékoztatására, akiknek az adatai veszélybe kerültek, és akik ilyen módon hátrányt szenvedhetnek.

VI. **A POLITIKAI ÉS JOGSZABÁLYI INTÉZKEDÉSEKKEL KAPCSOLATOS JAVASLATOK**

78. A forgalommal kapcsolatos adatokon és az IP-hasznosadatoknak, azaz a közlések tartalmának vizsgálatán alapuló vizsgálati technikák felfedhetik a felhasználók internetes tevékenységét: a felkeresett webhelyeket és az azokon folytatott tevékenységeket, a P2P-alkalmazások használatát, a letöltött fájlokat, az elküldött és fogadott e-mail üzeneteket, azt, hogy kitől, milyen tárgyban és mikor kapták őket, és még sok mást. Az internetszolgáltatók esetleg arra használhatják fel ezt az információt, hogy bizonyos közléseket, például a megrendelt videoszolgáltatásokat előrébb sorolják a többihez képest. Felhasználhatják az információt a vírusok azonosítására vagy viselkedésalapú reklámtevékenységhez felhasználható profilok kialakításához is. Ezek az intézkedések összefüggenek a közlések titkosságához való joggal.

79. A magánéletre gyakorolt hatások az alkalmazott technikáktól és az egyes esetek sajátosságaitól függően lépnek fel. Minél mélyrehatóbb az összegyűjtött információ elfogása és elemzése, annál nagyobb az ellentét a közlések titkosságának elvével. Az ellenőrzés végrehajtásának célja és az alkalmazott adatvédelmi garanciák szintén kulcsfontosságú elemei az egyén magánéletébe való behatolás és a személyes adatokkal való visszaélés mértéke meghatározásának. A rosszindulatú szoftverek elleni küzdelem céljából – a vizsgált adatok megőrzésére és felhasználására vonatkozó szigorú korlátozásokkal végrehajtott – blokkolás és ellenőrzés nem hasonlítható össze az olyan helyzetekkel, amikor az információ naplózása a viselkedésalapú hirdetéseket kiszolgáló egyéni profilok létrehozása érdekében történik.

80. Elvben az európai adatvédelmi biztos úgy véli, hogy a magánélet védelmével és az adatvédelemmel foglalkozó hatályos európai uniós jogszabályi keretrendszer – megfelelő értelmezése, alkalmazása és végrehajtása esetén – alkalmas eszköz volna annak garantálására, hogy a titkossághoz való jog érvényesülhessen, továbbá hogy összességében ne érhesse fenyegetés a magánélet védelmét és a magánszemélyek adatainak védelmét ([35]). Az internetszolgáltatóknak csak abban az esetben volna megengedett az ilyen mechanizmusok alkalmazása, ha megfelelően alkalmazzák a jogi keretet. Az internetszolgáltatóknak többek között a jogi keret alábbi vonatkozó elemeit kell figyelembe venniük és tiszteletben tartaniuk:

— Az internetszolgáltatók az elektronikus hírközlési adatvédelmi irányelv 4. és 6. cikke értelmében a szolgáltatás biztonságának biztosítása és a szolgáltatás nyújtása – ideértve a torlódás kialakulásának korlátozását – céljával forgalomkezelési politikákat alkalmazhatnak.

— Az internetszolgáltatóknak más konkrét jogalapra – és adott esetben a felhasználók hozzájárulására – van szükségük az olyan forgalomkezelési politikák alkalmazásához, amelyek magukban foglalják a forgalommal és/vagy közlésekkel kapcsolatos adatoknak a fentiektől eltérő célokra történő feldolgozását. Például a felhasználók megfelelő információk birtokában történő hozzájárulása szükséges ahhoz, hogy a magánszemélyek közléseit bizonyos alkalmazásokhoz és szolgáltatásokhoz (például a P2P- vagy a VoIP-szolgáltatáshoz) való hozzáférés korlátozása (vagy lehetővé tétele) céljából ellenőrizzék és szűrjék.

— A hozzájárulásnak önkéntesnek, kifejezettnek és a megfelelő információk birtokában kifejezettnek kell lennie. A hozzájárulást megerősítő intézkedés révén kell megadni. Ezek a követelmények hangsúlyozzák annak szükségességét, hogy erőfeszítéseket kell tenni annak biztosítására, hogy az érintettek megfelelő – közvetlen, érthető és konkrét – tájékoztatást kapjanak, hogy fel tudják mérni a gyakorlatok hatásait, és végül megalapozott döntést hozhassanak. Figyelemmel az említett technikák összetett jellegére, a felhasználók kellően részletes előzetes tájékoztatása jelenti az egyik fő kihívást az érvényes hozzájárulás megszerzése során. Emellett az ellenőrzés elutasítása nem járhat hátrányos következményekkel (például pénzügyi vonzattal) az érintett felhasználók számára.

([35]) Ez nem sértheti a jogszabály más megfontolások alapján, különösen az adatvédelemre vonatkozó uniós jogi keret általános felülvizsgálatával összefüggésben, annak érdekében történő módosításának szükségességét, hogy a jogi keret eredményességét az új műszaki megoldások és a globalizáció fényében fokozzák.

— Az arányosság elve kulcsfontosságú szerepet játszik olyankor, amikor az internetszolgáltatók forgalomkezelési politikákat alkalmaznak, akármi legyen is a feldolgozás és a cél jogalapja: szolgáltatásnyújtás, a torlódások kialakulásának megelőzése, vagy bizonyos szolgáltatásokhoz és alkalmazásokhoz való hozzáférést biztosító vagy nélkülöző célzott előfizetések kiajánlása. Ez az elv korlátozza az internetszolgáltatók lehetőségét arra, hogy oly módon ellenőrizzék az érintettek közléseinek tartalmát, amely túlzott mértékű adatfeldolgozással jár, vagy amely során az előnyöket az internetszolgáltató kizárólag magának tartja fenn. Az, hogy logisztikailag mit tehetnek meg az internetszolgáltatók, a következőktől függ: az említett technikák útján végzett beavatkozás mértéke, a kívánt eredmények (amelyek kapcsán a szolgáltatók előnyre tehetnek szert), valamint a magánélet védelmével és az adatvédelemmel kapcsolatban alkalmazott konkrét garanciák. A vizsgálati technikák alkalmazása előtt az internetszolgáltatónak értékelnie kell, hogy e technikák megfelelnek-e az arányosság elvének.

81. Noha a jogszabályi keret jelenleg tartalmazza a vonatkozó feltételeket és garanciákat, különös figyelmet kell fordítani arra, hogy az internetszolgáltatók valóban megfelelnek-e a jogszabályi követelményeknek, valóban megadják-e a fogyasztóknak a megalapozott döntéshez szükséges tájékoztatást, és betartják-e az arányosság elvét. Nemzeti szinten az e téren illetékes hatóságok közé tartoznak egyfelől a nemzeti hírközlési hatóságok, másfelől pedig a nemzeti adatvédelmi hatóságok. Európai uniós szinten illetékes testület például a BEREC. Az európai adatvédelmi biztos szintén szerephez juthat ezzel összefüggésben.

82. A megfelelőség aktuális szintjének ellenőrzése mellett – figyelemmel arra, hogy viszonylag rövid ideje nyílt meg a lehetőség a közlések tömeges, valós idejű ellenőrzésére – a jogi keret alkalmazásával kapcsolatos, e véleményben tárgyalt egyes szempontok vonatkozásában további részletekbe menő elemzésre és osztályozásra van szükség. Az iránymutatásoknak többek között a következő területekre kell kiterjedniük:

— a forgalom zökkenőmentes áramlásának biztosítása szempontjából létjogosultsággal rendelkező, adott esetben a felhasználók hozzájárulását nem igénylő ellenőrzési gyakorlatok – például a levélszemét elleni küzdelem – meghatározása. Az alkalmazott ellenőrzési technika beavatkozási foka mellett fontosak az olyan szempontok is, mint például annak mérlegelése, hogy ellenkező esetben milyen mértékű zavar keletkezhetne a forgalom zökkenőmentes áramlásában,

— annak meghatározása, hogy melyek azok a felhasználói hozzájárulást nem igénylő ellenőrzési technikák, amelyek biztonsági célokra használhatók,

— annak meghatározása, hogy az ellenőrzés mikor teszi szükségessé az egyéni hozzájárulást, különösen valamennyi érintett felhasználó hozzájárulását, valamint azon megengedhető technikai paraméterek meghatározása, amelyekkel biztosítható, hogy az adott ellenőrzési technika ne terjedjen ki a szándékolt cél vonatkozásában aránytalan adatfeldolgozásra,

— emellett a fenti három esetben iránymutatás válhat szükségessé a szükséges adatvédelmi garanciák (a cél korlátozása, biztonság stb.) alkalmazásával kapcsolatban is.

83. Figyelemmel arra, hogy e területen mind a tagállamok, mind az Unió hatáskörrel rendelkeznek, az európai adatvédelmi biztos úgy véli, hogy a harmonizált megközelítések megtalálása érdekében alapvető fontosságú a különböző nézetek és tapasztalatok megosztása. Ennek érdekében az európai adatvédelmi biztos a nemzeti szabályozó hatóságok, a 29. cikk alapján létrehozott munkacsoport, az európai adatvédelmi biztos és a BEREC képviselőit tömörítő platform vagy szakértői csoport létrehozását javasolja. E platform első célja egy – legalább a fentiekben meghatározott elemekre kiterjedő – iránymutatás kidolgozása volna a szilárd és harmonizált megközelítések, illetve az egyenlő versenyfeltételek biztosítása érdekében. Az európai adatvédelmi biztos felkéri a Bizottságot e kezdeményezés megszervezésére.

84. Végül, de nem utolsósorban: mind a nemzeti hatóságoknak, mind pedig uniós társszerveiknek, így a BEREC-nek és a Bizottságnak is nagyobb figyelmet kell fordítaniuk a piaci fejleményekre e területen. Az adatvédelem és a magánélet védelme szempontjából rendkívül problematikus volna, ha az internetszolgáltatók elkezdenének rutinszerűen forgalomkezelési politikákat alkalmazni, és a tartalomhoz és az alkalmazásokhoz való hozzáférés szűrésén alapuló előfizetéseket kínálni. Ha erre valaha is sor kerül, akkor jogszabályokat kell hatályba léptetni a helyzet kezelésére.

VII. **KÖVETKEZTETÉSEK**

85. Az, hogy az internetszolgáltatók egyre nagyobb mértékben hagyatkoznak az ellenőrzési és vizsgálati technikákra, ellentétes az internet semlegességének és a közlések titkosságának elvével. Ez komoly problémákat vet fel a felhasználók magánéletének és személyes adatainak védelmével kapcsolatban.

86. Noha az európai nyílt internetről és hálózatsemlegességről szóló bizottsági közlemény röviden kitér e kérdésekre, az európai adatvédelmi biztos úgy véli, többre van szükség ahhoz, hogy a továbbiakban kielégítő lehessen a kapcsolódó politika. Ennélfogva e véleménnyel az európai adatvédelmi biztos hozzájárul a hálózat semlegességéről, és különösen az adatvédelemmel és a magánélet védelmével kapcsolatos szempontokról folytatott szakpolitikai vitához.

87. Az európai adatvédelmi biztos úgy véli, szükség van arra, hogy a nemzeti hatóságok és a BEREC figyelemmel kísérjék a piaci helyzet alakulását. E figyelemmel kísérési tevékenységnek egyértelmű rálátást kell biztosítania arra, hogy a piac a közlések és a tömeges, valós idejű ellenőrzések felé halad-e, és rá kell világítania a jogi keretnek való megfeleléssel kapcsolatos problémákra.

88. A piac alakulásának figyelemmel kísérése során elemezni kell az új gyakorlatok által az internet vonatkozásában az adatok és a magánélet védelmére gyakorolt hatásokat is. A vélemény felvázol néhány olyan területet, amelynek előnyére válna a helyzet ilyen irányú tisztázása. Noha az uniós ügynökségek, például a BEREC, a 29. cikk alapján létrehozott munkacsoport és az európai adatvédelmi biztos megfelelő helyzetben lehet a jogi keret alkalmazási feltételeinek tisztázásához, az európai adatvédelmi biztos úgy véli, hogy a vita koordinálása és irányítása a Bizottság feladata. Ezért felkéri a Bizottságot arra, hogy e céllal indítson – valamennyi érdekeltet egyetlen platformon vagy munkacsoportban tömörítő – kezdeményezést. A további elemzést igénylő kérdések között a következő kérdésekkel kell foglalkozni:

— a forgalom zökkenőmentes áramlásának biztosítása szempontjából létjogosultsággal rendelkező és biztonsági célból végrehajtható ellenőrzési gyakorlatok meghatározása,

— annak meghatározása, hogy az ellenőrzés mikor teszi szükségessé az egyéni hozzájárulást, különösen az összes érintett felhasználó hozzájárulását, valamint azon megengedhető technikai paraméterek meghatározása, amelyekkel biztosítható, hogy az adott ellenőrzési technika ne terjedjen ki olyan adat feldolgozására, amely a szándékolt cél vonatkozásában nem arányos.

— A fenti esetekben iránymutatás válhat szükségessé a szükséges adatvédelmi garanciák (a cél korlátozása, biztonság stb.) alkalmazásával kapcsolatban is.

89. E megállapítások függvényében további jogszabályi intézkedések válhatnak szükségessé. Ilyen esetben a Bizottságnak a jogi keretek megerősítésére és a jogbiztonság biztosítására irányuló szakpolitikai intézkedéseket kell előterjesztenie. Az új intézkedéseknek egyértelművé kell tenniük a hálózatsemlegesség elvének gyakorlati következményeit (ahogyan ez egyes tagállamok esetében már meg is történt), és – különösen az internetszolgáltatóknak az ellenőrzés nélküli kapcsolat biztosítására való kényszerítésével – biztosítaniuk kell azt, hogy a felhasználók tényleges választási lehetőséget kapjanak.

Kelt Brüsszelben, 2011. október 7-én.

Peter HUSTINX

európai adatvédelmi biztos