GIOVANNI PITRUZZELLA
FŐTANÁCSNOK INDÍTVÁNYA
Az ismertetés napja: 2023. április 27.[1]

C-340/21. sz. ügy

VB
kontra
Natsionalna agentsia za prihodite

(a Varhoven administrativen sad [legfelsőbb közigazgatási bíróság, Bulgária] által benyújtott előzetes döntéshozatal iránti kérelem)

„Előzetes döntéshozatal – A személyes adatok védelme – (EU) 2016/679 rendelet – Az adatkezelő feladatai – Az adatkezelés biztonsága – A személyes adatok kezelése biztonságának megsértése – Az adatkezelő tétlenségével okozott nem vagyoni kár – Kártérítési kereset”

A hatóság birtokában lévő személyes adatok hackertámadás következtében történő jogellenes terjesztése megalapozhatja-e az adatkezeléssel érintett nem vagyoni kárának megtérítését kizárólag azon az alapon, hogy az utóbbi személy fél az adataival való esetleges jövőbeli visszaéléstől? Melyek az adatkezelő felelősségre vonásának kritériumai? Hogyan oszlik meg a bizonyítási teher az eljárás során? Milyen terjedelmű a bírósági felülvizsgálat?

I. Jogi háttér

1. A 2016/679 rendelet[2] (a továbbiakban: rendelet) „Fogalommeghatározások” című 4. cikke a következőképpen rendelkezik:

„E rendelet alkalmazásában:

[…]

12. »adatvédelmi incidens«: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

[1] Eredeti nyelv: olasz.

[2] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) (HL 2016. L 119., 1. o.; helyesbítések: HL 2016. L 314., 72. o., HL 2018. L 127., 2. o., HL 2021. L 74., 35. o.)

[…]”.

2. „A személyes adatok kezelésére vonatkozó elvek” című 5. cikk a következőképpen szól:

„(1) A személyes adatok:

[…]

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (»integritás és bizalmas jelleg«).

(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására (»elszámoltathatóság«)”.

3. Ugyanezen rendeletnek „Az adatkezelő feladatai” című 24. cikke kimondja:

„(1) Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

(2) Ha az az adatkezelési tevékenység vonatkozásában arányos, az (1) bekezdésben említett intézkedések részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

(3) A 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti kötelezettségeit.”

4. „Az adatkezelés biztonsága” című 32. cikk a következőket írja elő:

„(1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

[…]

(2) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

(3) Az adatkezelő, illetve az adatfeldolgozó 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja

annak bizonyítása részeként, hogy az e cikk (1) bekezdésében meghatározott követelményeket teljesíti.

[…]”

5. Ugyanezen rendeletnek „A kártérítéshez való jog és a felelősség” című 82. cikke a következőképpen rendelkezik:

„(1) Minden olyan személy, aki e rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

(2) Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet az e rendeletet sértő adatkezelés okozott. […]

(3) Az adatkezelő, illetve az adatfeldolgozó mentesül az e cikk (2) bekezdése szerinti felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.”

II. A tényállás, az eljárás és az előzetes döntéshozatalra előterjesztett kérdések

6. 2019. július 15-én a bolgár médiában az a hírt terjedt, hogy a Natsionalna agentsia za prihodite (nemzeti adóhatóság, Bulgária, a továbbiakban: NAP)[3] informatikai rendszeréhez való jogosulatlan hozzáférésre került sor, valamint hogy az interneten közzétettek több millió ember – állampolgárok és külföldiek – adóügyi és társadalombiztosítási adatait magában foglaló információkat.

7. Ennélfogva nem vagyoni kár megtérítése iránt több személy, köztük V. B., az alapeljárás felperese keresetet indított a NAP ellen.

8. A jelen ügyben az alapeljárás felperese arra hivatkozással indított keresetet az Administrativen sad Sofia-grad (szófiai közigazgatási bíróság, Bulgária, a továbbiakban: ASSG) előtt, hogy a NAP megsértette a nemzeti szabályokat, valamint azt a kötelezettségét, hogy adatkezelőként a 679/2016 rendelet 24. és 32. cikke értelmében a személyes adatokat úgy kezelje, hogy a megfelelő technikai vagy szervezési intézkedések végrehajtásával „biztosítsa a személyes adatok megfelelő biztonságát”. A felperes ezután azt állította, hogy nem vagyoni kár érte őt, amely a személyes adatokkal való esetleges jövőbeli visszaélés miatti aggodalmak és félelmek formájában nyilvánult meg.

9. Az ellenérdekű fél ezzel szemben azt hangsúlyozta, hogy az alapeljárásban nem érkezett a felperestől olyan kérelem, amely megjelölte volna, hogy pontosan mely személyes adatokhoz fértek hozzá. Emellett a feltörés hírét követően találkozókat hívott össze szakértőkkel a polgárok jogainak és érdekeinek védelme érdekében. A NAP szerint a hackertámadás és az állítólagosan hivatkozott kár között nem állt fenn okozati összefüggés, mivel a hatóság a vonatkozó nemzetközi szabványoknak megfelelően bevezetett valamennyi folyamatirányító rendszert és információbiztonság-kezelési rendszert.

[3] A NAP a rendelet 4. cikkének 7. pontja értelmében vett adatkezelőnek minősül. A nemzeti jog szerint a NAP a pénzügyminiszter felügyelete alá tartozó, a közjogi és törvényben meghatározott magánjogi, pénzügyminisztériumi és állami követelések megállapításáért, biztosításáért és behajtásáért felelős szakhatóság. A ráruházott közhatalmi jogkörök gyakorlása során személyes adatokat kezel.

10. Az elsőfokú bíróság, az ASSG (szófiai közigazgatási bíróság) elutasította a keresetet, mivel úgy vélte, hogy a hatóságot nem terheli felelősség az adatok terjesztéséért, hogy a megtett intézkedések megfelelőségére vonatkozó bizonyítási teher a felperest terheli, és végül, hogy semmilyen nem vagyoni kár nem téríthető meg.

11. Az elsőfokú ítéletet ezt követően megtámadták a Varhoven administrativen sad (legfelsőbb közigazgatási bíróság, Bulgária) előtt. Az alapeljárás felperese érvelése során hangsúlyozta, hogy az elsőfokú bíróság tévesen osztotta meg a bizonyítási terhet a biztonsági intézkedések elfogadásának elmulasztását illetően. Emellett a nem vagyoni kárra nem vonatkozhat a bizonyítási teher, amennyiben tényleges és nem csupán lehetséges nem vagyoni kárról van szó.

12. A NAP a maga részéről megerősítette, hogy adatkezelőként megtette a szükséges technikai és szervezési intézkedéseket, és vitatta a tényleges nem vagyoni kár bizonyítottságát. A negatív előérzet és a félelem ugyanis nem megtérítendő érzelmi állapotok.

13. A kérdést előterjesztő bíróság eltérő eredményekre jutott azon egyedi eljárások tekintetében, amelyeket a károsultak külön-külön indítottak a NAP ellen a nem vagyoni kár megtérítése iránt.

14. E körülmények között a kérdést előterjesztő bíróság felfüggesztette az eljárást, és előzetes döntéshozatal céljából a következő kérdéseket terjesztette a Bíróság elé:

„1. Úgy kell-e értelmezni [a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet)] 24. és 32. cikkét, hogy annak megállapításához, hogy a meghozott technikai és szervezési intézkedések nem megfelelőek, elegendő, ha a személyes adatoknak az (EU) 2016/679 rendelet 4. cikkének 12. pontja értelmében vett jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés valósul meg olyan személyek közreműködésével, akik nem alkalmazottai az adatkezelő szervezetének, és akik nem állnak az adatkezelő ellenőrzése alatt?

2. Az első kérdésre adott nemleges válasz esetén, mi a bírósági felülvizsgálat tárgya és terjedelme annak vizsgálata során, hogy megfelelőek-e az adatkezelő által az (EU) 2016/679 rendelet 32. cikke alapján hozott technikai és szervezési intézkedések?

3. Az első kérdésre adott nemleges válasz esetén úgy kell-e értelmezni az elszámoltathatóság (EU) 2016/679 rendelet (74) preambulumbekezdésével összefüggésben értelmezett 5. cikkének (2) bekezdése és 24. cikke szerinti elvét, hogy az (EU) 2016/679 rendelet 82. cikkének (1) bekezdése szerinti peres eljárás során az adatkezelőt terheli a rendelet 32. cikke alapján hozott technikai és szervezési intézkedések megfelelőségével kapcsolatos bizonyítási teher? Tekinthető-e a szakértői vélemény beszerzése annak megállapításához szükséges és elégséges bizonyítéknak, hogy olyan esetben, mint a jelen ügybeli, az adatkezelő által hozott technikai és szervezési intézkedések megfelelőek voltak-e, ha a személyes adatok jogosulatlan közlését és az azokhoz való jogosulatlan hozzáférést »hackertámadás« eredményezi?

4. Úgy kell-e értelmezni az (EU) 2016/679 rendelet 82. cikkének (3) bekezdését, hogy – mint a jelen ügyben – a személyes adatoknak olyan személy közreműködésével megvalósuló »hackertámadás« révén az (EU) 2016/679 rendelet 4. cikkének 12. pontja értelmében vett jogosulatlan közlése és az azokhoz való jogosulatlan hozzáférés, akik nem az adatkezelő

szervezetének alkalmazottai, és akik nem az adatkezelő ellenőrzése alatt állnak, olyan körülménynek minősül, amelyért az adatkezelőt semmilyen módon nem terheli felelősség, és amely alapján mentesül a felelősség alól?

5. Úgy kell-e értelmezni az (EU) 2016/679 rendelet (85) és (146) preambulumbekezdésével összefüggésben értelmezett 82. cikkének (1) és (2) bekezdését, hogy a személyes adatokhoz való jogosulatlan hozzáférésként és azok »hackertámadás« révén történő terjesztésével megvalósuló adatvédelmi incidens – olyan esetben, mint a jelen ügybeli – önmagában az érintett személy személyes adatokkal való esetleges jövőbeli visszaéléssel kapcsolatos aggodalma, negatív előérzete, félelme a nem vagyoni kár tágan értelmezendő fogalmába tartozik, és kártérítésre jogosít akkor is, ha az ilyen visszaélést nem állapították meg és/vagy az érintett személyt nem érte további kár?"

III. Jogi elemzés

A. Előzetes megjegyzések

15. A jelen ügy érdekes és részben újszerű kérdéseket vet fel a rendelet több rendelkezésének értelmezésével kapcsolatban. [4]

16. Az előzetes döntéshozatalra előterjesztett öt kérdés mindegyike ugyanazt a kérdést járja körül: az olyan személynek okozott nem vagyoni kár megtérítése feltételeinek kérdését, akinek a hatóság birtokában lévő személyes adatait hackertámadást követően közzétették az interneten.

17. A könnyebb kifejtés érdekében az előzetes döntéshozatalra utaló végzésben szereplő, előzetes döntéshozatalra előterjesztett valamennyi kérdésre külön-külön összefoglaló válaszokat fogok javasolni, bár tisztában vagyok azzal, hogy vannak bizonyos fogalmi átfedések, mivel az első négy kérdés mindegyike az adatkezelőnek a rendelet rendelkezéseinek megsértéséért való felelősségre vonásának feltételeire irányul, [5] az ötödik pedig konkrétabban a nem vagyoni kár fogalmára vonatkozik a kártérítés szempontjából. [6]

18. Szeretném felhívni a figyelmet arra, hogy jelenleg több ügy van folyamatban a Bíróság előtt a rendelet 82. cikkével kapcsolatban, és az egyikben a főtanácsnok már ismertette indítványát, amelyet a jelen elemzés során figyelembe veszek. [7]

[4] Az 5. cikk (2) bekezdése (amely az adatkezelők elszámoltathatóságának elvére vonatkozik), a 24. cikk (amely az adatkezelő által annak biztosítása érdekében meghozandó intézkedésekre vonatkozik, hogy az adatkezelése megfeleljen e rendeletnek), a 32. cikk (amely erre a kötelezettségre vonatkozik kifejezetten az adatkezelés biztonságát illetően) és a 82. cikk (1)–(3) bekezdése (amely az e rendelet megsértéséből eredő károk megtérítésére, valamint az adatkezelő azon lehetőségére vonatkozik, hogy intézkedéseket fogadjon el e rendelet tiszteletben tartásának biztosítása érdekében), valamint a (74), (85) és (146) preambulumbekezdés, amelyek a fent említett cikkekhez kapcsolódnak.

[5] a) az első arra a kérdésre keresi a választ, hogy a bevezetett intézkedések elégtelenségére lehet-e következtetni a rendszerek puszta megsértéséből; b) a második az említett intézkedések megfelelősége bírósági felülvizsgálatának terjedelmére vonatkozik; c) a harmadik magára a megfelelőségre vonatkozó bizonyítási teherre és a bizonyítékok gyűjtésének bizonyos technikai módszereire vonatkozik; d) a negyedik arra vonatkozik, hogy a felelősség kizárása szempontjából milyen jelentősége van annak, hogy a rendszer elleni támadás kívülről érkezett.

[6] Ami a rendelet hivatkozott rendelkezéseit illeti, az első három kérdés az adatkezelő felelősségének szempontjaira vonatkozik a meghozandó intézkedések megfelelőségével kapcsolatban (5., 24. és 32. cikk), a negyedik és ötödik kérdés pedig a felelősség kizárásának feltételeire és a megtérítendő nem vagyoni kár fogalmára (82. cikk).

[7] Lásd: Campos Sánchez-Bordona főtanácsnok Österreichische Post (Személyes adatok kezeléséhez kapcsolódó nem vagyoni kár) ügyre vonatkozó indítványa (C-300/21, EU:C:2022:756).

19. A felvetett kérdések vizsgálata előtt helyénvalónak tartom, hogy néhány előzetes megjegyzést tegyek a rendelet elveiről és céljairól, amelyek hasznosak lesznek az előzetes döntéshozatalra előterjesztett egyes kérdések megoldásához.

20. A rendelet 24. cikke általánosságban határozza meg az adatkezelő azon kötelezettségét, hogy megfelelő technikai és szervezési intézkedéseket hajtson végre annak biztosítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történjen, és hogy képes legyen annak bizonyítására, míg a 32. cikk az adatkezelés biztonsága tekintetében határozza meg konkrétabban ugyanezt a kötelezettséget. A 24. és a 32. cikk konkrétabban határozza meg azt, amiről az 5. cikk (2) bekezdése már rendelkezik, amely a „személyes adatok kezelésére vonatkozó elvek" között bevezeti az „elszámoltathatóság elvét". Ez logikusan következik az „integritásnak és bizalmas jellegnek" az 5. cikk (1) bekezdésének f) pontjában foglalt elvéből, kiegészíti azokat, és mindkettőt a rendelet alapjául szolgáló kockázatalapú megközelítés fényében kell értelmezni.

21. Az elszámoltathatóság elve a rendelet egyik alappillére és egyik legjelentősebb újítása. A rendelet az adatkezelőre ruházza annak feladatát, hogy proaktív lépéseket tegyen a rendeletnek való megfelelés biztosítása érdekében, és készen álljon annak bizonyítására. [8]

22. A jogtudomány valódi kulturális változásként beszélt a „felelősségvállalási kötelezettség teljes terjedelmének" hatásáról. [9] Nem annyira a jogi kötelezettségnek való formális megfelelés vagy a pontos intézkedés, mint inkább az elfogadott átfogó vállalati stratégia mentesíti az adatkezelőt az adatvédelmi szabályoknak való megfelelésért való felelősség alól.

23. Az elszámoltathatóság elve által megkövetelt technikai vagy szervezési intézkedéseknek a 24. cikkben meghatározott tényezőkre tekintettel kell „megfelelőnek" lenniük: az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett kockázat valószínűsége és súlyossága.

24. A 24. cikk tehát annak érdekében követeli meg az intézkedések megfelelőségét, hogy bizonyítani lehessen az adatkezelésnek a rendelet elveivel és rendelkezéseivel való összhangját.

25. A 32. cikk ezzel szemben az elszámoltathatóság elvét a „kockázat mértékének megfelelő szintű biztonság" garantálása érdekében meghozandó konkrét intézkedésekre vetíti ki. Így pedig kiegészíti a technikai és szervezési intézkedések előkészítése során már előirányzott, figyelembe veendő tényezőket a tudomány és technológia állásával, valamint a végrehajtás költségeivel.

26. A megfelelőség fogalma megköveteli, hogy az informatikai rendszerek védelme érdekében elfogadott megoldások elérjenek egy elfogadható szintet mind technikai (az intézkedések megfelelősége), mind minőségi (a védelem hatékonysága) szempontból. A szükségesség, a relevancia és az arányosság elvének való megfelelés biztosítása érdekében az adatkezelési műveleteknek nemcsak megfelelőnek, hanem kielégítőnek is kell lenniük az általuk elérni kívánt célok tekintetében. E logikát követve döntő szerepet játszik az adattakarékosság elve, amely szerint az adatkezelés minden szakaszában folyamatosan törekedni kell a biztonsági kockázatok csökkentésére. [10]

[8] C. Docksey, *Article 24. Responsibility of the controller*, in C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, 561. o. Az adatvédelmi szabályozásokban foglalt elveknek és kötelezettségeknek minden szinten át kell hatniuk a szervezetek kulturális szövetét, ahelyett, hogy a jogi osztály által kipipálandó jogi követelmények halmazának tekintenék azokat.

[9] E. Belisario, G. Riccio, G. Scorza, *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, 301. o.

[10] E. Belisario, G. Riccio, G. Scorza, *GDPR*, hiv., 380. o.

27. A rendelet egésze a kockázatmegelőzésre és az adatkezelő elszámoltathatóságára irányul, tehát egy olyan teleologikus megközelítésre, amely a hatékonyság szempontjából a lehető legjobb eredményre törekszik, azaz távol áll a felelősségtől való megszabadulás érdekében a konkrét eljárások betartásának puszta kötelezettségével kapcsolatos formális logikától. [11]

28. A 24. cikk nem tartalmaz kimerítő listát a „megfelelő” intézkedésekről: eseti alapon kell értékelni azokat. Ez összhangban van a rendelet filozófiájával, amelyből kiderül, hogy az elfogadandó eljárásokat a konkrét helyzet gondos értékelése alapján kell inkább kiválasztani, hogy azok a lehető leghatékonyabbak legyenek. [12]

B. Az előzetes döntéshozatalra előterjesztett első kérdés

29. Első kérdésével az előterjesztő bíróság lényegében azt kérdezi, hogy úgy kell-e értelmezni a rendelet 24. és 32. cikkét, hogy a 4. cikk 12. pontjában meghatározott „adatvédelmi incidens” bekövetkezése önmagában elegendő annak megállapításához, hogy az adatkezelő által meghozott technikai és szervezési intézkedések nem voltak „megfelelőek” az adatvédelem biztosítására.

30. A rendelet 24. és 32. cikkének megfogalmazásából következik, hogy az adatkezelőnek a rendeletnek való megfelelés biztosítása érdekében végrehajtandó technikai és szervezési intézkedések megválasztásakor figyelembe kell vennie az említett cikkekben felsorolt és a fentiekben hivatkozott számos értékelési tényezőt.

31. Az adatkezelőnek van némi mozgástere a konkrét helyzetre tekintettel legmegfelelőbb intézkedések meghatározása tekintetében, de ez a választás ugyanakkor esetlegesen bírósági felülvizsgálat tárgyát képezheti a tekintetben, hogy a meghozott intézkedések megfelelnek-e a rendeletben foglalt valamennyi kötelezettségnek és célnak.

32. Különösen a biztonsági intézkedések tekintetében a 32. cikk (1) bekezdése előírja az adatkezelő számára, hogy vegye figyelembe a „tudomány és technológia állását”. Ez azt jelenti, hogy a végrehajtandó intézkedések technológiai szintje az intézkedések meghozatalakor észszerűen lehetségesre korlátozódik: vagyis az intézkedésnek a veszély megelőzésére való alkalmasságát a tudomány, a technika, a technológia és a kutatás mindenkori állása által kínált megoldásokkal kell összevetni, figyelembe véve – amint azt látni fogjuk – a végrehajtás költségeit is.

33. Előfordulhat, hogy az intézkedések egy adott időpontban „megfelelőek”, és ennek ellenére a kiberbűnözők, akik olyan kifinomult eszközöket használnak, amelyek alkalmasak még a legkorszerűbb biztonsági intézkedéseket is megsérteni, megkerülik azokat.

[11] Ennélfogva, amint azt látni fogjuk, az előzetes döntéshozatalra előterjesztett első és negyedik kérdésre nemleges választ kell adni. Nem lehet automatizmusra következtetni a rendelet rendelkezéseiből: a személyes adatok nyilvánosságra hozatalának puszta ténye nem elegendő annak megállapításához, hogy a megtett technikai és szervezési intézkedések nem megfelelőek, és az, hogy maga a nyilvánosságra hozatal az adatkezelő szervezetén kívüli személyek beavatkozásának eredményeként és az adatkezelő ellenőrzési körén kívül történt, sem elegendő a felelősség kizárásához.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, 201. o. Az európai jogalkotó tehát túllép az adatkezelés biztonságának az előre meghatározott biztonsági intézkedések meglétén alapuló felfogásán, és a kockázatalapú információs rendszerek kezelésére vonatkozó nemzetközi szabványoknak megfelelő saját módszertant fogad el: előírja a kockázatcsökkentő intézkedések azonosítását, amelyek figyelmen kívül hagyják az előre konfigurált és általánosan alkalmazható ellenőrző listákat. Így a nemzetközi iránymutatásokhoz és szabványokhoz szükséges folyamodni. A kockázatértékelés eredménye tehát kötelező érvényűvé válik, amikor a szervezet döntéseket hoz az azonosított kockázatok mérséklése érdekében, és ezzel elszámoltathatóvá teszi magát.

34. Másrészt nem tűnik logikusnak az a feltételezés, hogy az uniós jogalkotó szándéka az volt, hogy az adatkezelő részére előírja a személyes adatok bármely megsértésének megelőzését, függetlenül a biztonsági intézkedések bevezetésekor tanúsított gondosságtól. [13]

35. A fent említettek szerint a rendelet nézőpontja eltávolodik az automatizmustól, és nagy fokú elszámoltathatóságot követel meg az adatkezelővel szemben, ami azonban nem vezethet ahhoz, hogy az adatkezelő ne legyen képes bizonyítani, hogy helyesen teljesítette a rá rótt kötelezettségeket.

36. A 32. cikk (1) bekezdése előírja továbbá, hogy – amint azt már említettem – figyelembe kell venni a szóban forgó technikai és szervezési intézkedések „megvalósítás[ának] költségeit". Ebből következik, hogy ezen intézkedések megfelelőségének értékelését az érintett érdekei – amelyek általában a magasabb szintű védelem felé hajlanak –, valamint az adatkezelő gazdasági érdekei és technológiai kapacitása – amelyek néha alacsonyabb szintű védelem felé hajlanak – közötti egyensúlyra kell alapozni. Ennek a mérlegelésnek tiszteletben kell tartania az arányosság általános elvének követelményeit.

37. Ezen túlmenően a rendszertani értelmezés szerint a jogalkotó számol a rendszerek megsértésének lehetőségével; a 32. cikk (1) bekezdésének c) pontja a javasolt intézkedések közé sorolja a fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani. Az ilyen képességnek a kockázatnak megfelelő biztonsági szintet biztosító biztonsági intézkedések között történő előírása értelmetlen lenne, ha megállapítást nyerne, hogy a rendszerek puszta megsértése önmagában bizonyítja maguknak az intézkedéseknek az elégtelenségét.

C. Az előzetes döntéshozatalra előterjesztett második kérdés

38. Második kérdésével az előterjesztő bíróság lényegében azt kérdezi, hogy mi a bírósági felülvizsgálat tárgya és terjedelme annak vizsgálata során, hogy megfelelőek-e az adatkezelő által a rendelet 32. cikke alapján hozott technikai és szervezési intézkedések.

39. Tekintettel a gyakorlatban előforduló helyzetek változatosságára, a rendelet, amint azt már említettem, nem állapít meg kötelező rendelkezéseket az adatkezelő által a rendelet követelményeinek teljesítése érdekében meghozandó technikai és szervezési intézkedések meghatározására. A meghozott intézkedések megfelelőségét ezért esetenként kell értékelni, megvizsgálva, hogy a konkrét intézkedések alkalmasak voltak-e a kockázat észszerű megelőzésére és a jogsértés negatív hatásainak minimalizálására.

40. Bár kétségtelenül igaz, hogy az ilyen intézkedések megválasztása és végrehajtása az adatkezelő szubjektív megítélésének körébe tartozik, mivel a rendeletben említett intézkedések csak példák, a bíróság vizsgálata nem korlátozódhat annak ellenőrzésére, hogy az adatkezelő eleget tesz-e a 24. és 32. cikk szerinti kötelezettségeinek, azaz hogy (formálisan) gondoskodott-e bizonyos technikai és szervezési intézkedésekről. A bíróságnak a rendelkezésére álló bizonyítékok és a konkrét ügy körülményei alapján konkrétan elemeznie kell ezen intézkedések tartalmát, alkalmazásuk módját és gyakorlati hatásait. Amint azt a portugál kormány helyesen megjegyezte, „úgy tűnik, hogy a kötelezettségek teljesítésének módja elválaszthatatlan az elfogadott intézkedések tartalmától,

[13] A megfelelőség fogalma egyértelműen azt a szándékot mutatja, hogy nem minden elvontan lehetséges technikai és szervezési intézkedésnek kell jelentőséget tulajdonítani. Ebben az értelemben: M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, *Giappichelli*, 2019, 1059. o.

annak bizonyítása érdekében, hogy az adatkezelő – figyelembe véve a konkrét adatkezelést (annak jellegét, hatókörét, körülményeit és céljait), a rendelkezésre álló technológiák jelenlegi állását és költségeit, valamint a polgárok jogaira és szabadságaira jelentett kockázatokat – minden szükséges és megfelelő intézkedést megtett annak érdekében, hogy az alapul szolgáló kockázat mértékének megfelelő biztonsági szintet biztosítson”. [14]

41. A bírósági felülvizsgálat során tehát figyelembe kell venni a 24. és 32. cikkben foglalt valamennyi tényezőt, amelyek – amint azt már említettem – számos kritériumot sorolnak fel a megfelelőség értékelésére, és példákat adnak a megfelelőnek tekinthető intézkedésekre. Ezen túlmenően, amint arra a Bizottság és a második kérdéssel kapcsolatban észrevételeket benyújtó valamennyi tagállam rámutatott, a 32. cikk (1)–(3) bekezdése hangsúlyozza, hogy „a kockázat mértékének megfelelő szintű adatbiztonságot [kell] garantál[ni]”, és e célból más lényeges tényezőket is megjelöl, mint például a rendelet 40., illetve 42. cikke szerinti, az adatkezelő által jóváhagyott magatartási kódex vagy tanúsítási rendszer.

42. A magatartási kódexek vagy tanúsítási rendszerek elfogadása hasznos értékelési elemnek bizonyulhat a bizonyítási kötelezettség teljesítése és a kapcsolódó bírósági felülvizsgálat szempontjából. Azzal a pontosítással azonban, hogy nem elegendő, ha az adatkezelő csatlakozott a magatartási kódexhez, hanem az elszámoltathatóság elvének megfelelően az ő feladata annak bizonyítása, hogy az abban előírt intézkedéseket ténylegesen elfogadta. A tanúsítás viszont „önmagában bizonyítékot jelent az elvégzett adatkezelési műveleteknek a rendeletnek való megfelelésére, még akkor is, ha a gyakorlatban megcáfolható”. [15]

43. Végül meg kell jegyezni, hogy ezeket az intézkedéseket a 24. cikk (1) bekezdése értelmében felül kell vizsgálni és szükség esetén aktualizálni kell. Ezt is a nemzeti bíróságnak kell majd értékelnie. A rendelet [16] 32. cikkének (1) bekezdése ugyanis az adatkezelőnek előírja az adatkezelési tevékenységeket megelőző és követő folyamatos ellenőrzés és nyomon követés kötelezettségét, valamint az elfogadott intézkedések fenntartását és esetleges aktualizálását, mind a jogsértések megelőzése, mind pedig azok hatásainak esetleges korlátozása céljából.

44. Inkább kizárnám azonban annak lehetőségét, hogy a soron következő ítélet tartalmazza a lényeges elemek listáját, mint a portugál kormány által javasolt listát. [17] Ez teret adna az ellentétes értelmezéseknek, mivel a lista nyilvánvalóan nem lehet teljes.

[14] Írásbeli észrevételek, 31. pont.

[15] M. Gambini, *Responsabilità*, hiv., 1067. o. A tanúsítvány birtoklása tehát a bizonyítási teher megfordulását eredményezi a tanúsítvány jogosultja javára, akinek megkönnyíti annak bizonyítását, hogy a rendelet szerinti kötelezettségeknek megfelelően járt el.

[16] A d) pontban kifejezetten előírva, hogy a megfelelőség megállapítása kiterjed az elfogadott intézkedések hatékonyságára, amelyeket rendszeresen kell tesztelni, felmérni és értékelni, mind a kezdeti szakaszban, mind pedig rendszeres időközönként, valamennyi adatkezelés biztonsága hatékonyságának garantálása érdekében, függetlenül azok kockázati szintjétől; és a c) pontban szintén kifejezetten előírva, hogy a végrehajtott technikai és szervezési intézkedéseknek fizikai vagy műszaki incidens esetén képesnek kell lenniük arra, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani. Lásd: M. Gambini, *Responsabilità*, hiv., 1064. és 1065. o.

[17] Az írásbeli észrevételek 30. pontja: „az adatkezelőnek kell bizonyítania, hogy hogyan értékelte a szóban forgó adatkezelési művelethez kapcsolódó valamennyi tényezőt és körülményt, és különösen az elvégzett kockázatelemzés eredményét, az azonosított kockázatokat, az e kockázatok csökkentésére talált konkrét intézkedéseket, a piacon rendelkezésre álló technológiai megoldások fényében választott lehetőségek indokoltságát, az intézkedések hatékonyságát, a technikai és szervezési intézkedések közötti összefüggést, az adatkezeléssel foglalkozó alkalmazottak képzését, az adatkezelési műveletek kiszervezését, beleértve az információs technológia fejlesztését és karbantartását, valamint az adatkezelő általi ellenőrzés és az adatfeldolgozóknak a GDPR 28. cikke értelmében a személyes adatok általuk történő feldolgozására vonatkozóan adott pontos utasítások meglétét; hogyan értékelték a kommunikációs és információs rendszereket támogató infrastruktúrát, és hogyan minősítették az érintettek jogaira és szabadságaira jelentett kockázat szintjét”.

D. Az előzetes döntéshozatalra előterjesztett harmadik kérdés

45. Harmadik kérdésének első részével az előterjesztő bíróság lényegében annak megállapítását kéri a Bíróságtól, hogy az elszámoltathatóságnak a rendelet (74) preambulumbekezdésével[18] összefüggésben értelmezett 5. cikkének (2) bekezdésében és 24. cikkében foglalt elvére tekintettel, a 82. cikk szerinti kártérítési kereset keretében az adatkezelőt terheli-e a rendelet 32. cikke alapján hozott technikai és szervezési intézkedések megfelelőségével kapcsolatos bizonyítási teher.

46. A fenti megfontolások lehetővé teszik számomra, hogy röviden igenlő választ adjak erre a kérdésre.

47. A rendelet szövege, környezete és céljai ugyanis egyértelműen arra utalnak, hogy a bizonyítási teher az adatkezelőt terheli.

48. A rendelet több rendelkezésének szövegéből következik, hogy az adatkezelőnek „tudnia” kell igazolni azt, vagy „képesnek” kell lennie annak „bizonyítására”, hogy a rendelet szerinti kötelezettségeit teljesíti, és különösen hogy e célból megfelelő intézkedéseket hajtott végre, amint azt a (74) preambulumbekezdés, az 5. cikk (2) bekezdése és a 24. cikk (1) bekezdése meghatározza. Amint a portugál kormány rámutat, a fent említett (74) preambulumbekezdés előírja, hogy az adatkezelőt terhelő bizonyítási teher magában foglalja a szóban forgó intézkedések „hatékonyságának” igazolását.

49. Úgy tűnik számomra, hogy ezt a szó szerinti értelmezést a következő gyakorlati és teleologikus megfontolások is alátámasztják.

50. Ami a bizonyítási teher megosztását illeti, a 82. cikken alapuló kártérítési kereset keretében az adatkezelővel szemben keresetet indító érintettnek kell bizonyítania először a rendelet megsértését, másodszor azt, hogy kárt szenvedett, és harmadszor azt, hogy a két előző elem között okozati összefüggés áll fenn, amint azt az előzetes döntéshozatalra előterjesztett ötödik kérdésre vonatkozó valamennyi írásbeli észrevételben megjegyezték. E három feltétel együttesen érvényesül, amint az a Bíróság és a Törvényszék állandó ítélkezési gyakorlatából is kitűnik az Unió szerződésen kívüli felelősségével összefüggésben.[19]

51. Úgy vélem azonban, hogy a rendelet megsértésének bizonyítására vonatkozó felperesi kötelezettség nem terjedhet olyan messzire, hogy megkövetelje a felperestől annak bizonyítását, hogy az adatkezelő által elfogadott technikai és szervezési intézkedések a 24. és 32. cikk értelmében nem megfelelőek.

[18] A (74) preambulumbekezdés szerint: „A személyes adatoknak az adatkezelő által vagy az adatkezelő nevében végzett bármilyen jellegű kezelése tekintetében az adatkezelő hatáskörét és felelősségét szabályozni kell. Az adatkezelőt kötelezni kell különösen arra, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek e rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is az e rendelet által előírt szintű. Ezeket az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni”.

[19] Lásd különösen: a Bíróság 2019. szeptember 5-i Európai Unió kontra Guardian Europe és Guardian Europe kontra Európai Unió ítélete (C-447/17 P és C-479/17 P, EU:C:2019:672, 147. pont); 2021. október 28-i Vialto Consulting kontra Bizottság ítélete (C-650/19 P, EU:C:2021:879, 138. pont); valamint a Törvényszék 2021. január 13-i Helbert kontra EUIPO ítélete (T-548/18, EU:T:2021:4, 116. pont); 2021. szeptember 29-i Kočner kontra Europol ítélete (T-528/20, nem tették közzé, 61. pont), amelyekben emlékeztetnek arra, hogy három feltételnek kell teljesülnie, nevezetesen „az uniós intézménnyel szemben kifogásolt magatartás jogellenessége, a kár tényleges jellege, valamint az ezen intézmény magatartása és a hivatkozott kár közötti okozati összefüggés fennállása”.

52. Amint arra a Bizottság rámutat, e bizonyítékok bemutatása a gyakorlatban gyakran szinte lehetetlen, mivel az érintettek általában nem rendelkeznek az ilyen intézkedések elemzéséhez szükséges ismeretekkel, és nem férnek hozzá a vitatott adatkezelésért felelős adatkezelő birtokában lévő valamennyi információhoz sem, különösen az adatkezelés biztonságának garantálása érdekében alkalmazott módszerek tekintetében. Ezenfelül az adatkezelő esetenként azzal is érvelhet, hogy e tények közlésének az érintettekkel szembeni megtagadása azon a jogszerű okon alapul, hogy többek között éppen biztonsági okokból nem hozza nyilvánosságra belső ügyeit, vagy akár a titoktartás körébe tartozó elemeket.

53. Ennélfogva, ha a bizonyítási teher az érintett személyt terhelné, a gyakorlatban az eredmény az lenne, hogy a 82. cikk (1) bekezdése szerinti jogorvoslati jog terjedelme nagymértékben leszűkülne. Véleményem szerint ez nem felel meg az uniós jogalkotó szándékainak, aki a rendelet elfogadásával az érintettek jogait és az adatkezelők kötelezettségeit kívánta megerősíteni a rendelettel felváltott 95/46 irányelvhez képest. Ezért logikusabb és jogilag védhetőbb, hogy az adatkezelő köteles a kártérítési keresettel szembeni védekezés keretében bizonyítani, hogy az említett rendelet 24. és 32. cikke szerinti kötelezettségeinek a ténylegesen megfelelő intézkedések meghozatalával eleget tett.

54. Az előterjesztő bíróság a harmadik kérdésének második részében lényegében azt kérdezi a Bíróságtól, hogy az igazságügyi szakértői vélemény szükséges és elégséges bizonyítéknak tekinthető-e a személyes adatok kezelője által végrehajtott technikai és szervezési intézkedések megfelelőségének értékeléséhez olyan helyzetben, amikor a személyes adatokhoz való jogosulatlan hozzáférés és azok nyilvánosságra hozatala hackertámadás eredménye.

55. Úgy vélem – amint azt (lényegében) a bolgár és az olasz kormány, Írország és a Bizottság is hangsúlyozta –, hogy az e kérdésekre adott válasznak az állandó ítélkezési gyakorlatunkon kell alapulnia, amely szerint az adott területre vonatkozó uniós szabályozás hiányában az egyének jogainak védelmére irányuló bírósági eljárásokra vonatkozó részletes eljárási szabályok meghozatala az eljárási autonómia elve alapján az egyes tagállamok belső jogrendjébe tartozik, feltéve azonban, hogy ezek a szabályok az uniós jog által szabályozott helyzetekben nem lehetnek kedvezőtlenebbek a hasonló jellegű belső jogi helyzetekre vonatkozókhoz képest (az egyenértékűség elve), és nem tehetik gyakorlatilag lehetetlenné vagy rendkívül nehézzé az uniós jog által biztosított jogok gyakorlását (a tényleges érvényesülés elve).

56. A jelen ügyben megjegyzem, hogy a rendelet nem tartalmaz olyan rendelkezést, amelynek célja az elfogadható bizonyítási módszerek és azok bizonyító erejének meghatározása, különös tekintettel azokra a vizsgálati cselekményekre (mint például a szakértői vélemény), amelyeket a nemzeti bíróságok elrendelhetnek vagy azoknak el kell rendelniük annak eldöntése érdekében, hogy az adatkezelő megtette-e a rendelet értelmében vett megfelelő intézkedéseket. Ezért úgy vélem, hogy az adott területre vonatkozó harmonizált szabályok hiányában az egyes tagállamok belső jogrendjébe tartozik ezen eljárási szabályok meghozatala az egyenértékűség és a tényleges érvényesülés elvének betartása mellett.

57. A „tényleges érvényesülés” fent említett „elve”, amelynek értelmében a független bíróságnak pártatlan értékelést kell elvégeznie, sérülhetne, ha az „elégséges” jelzőt a kérdést előterjesztő bíróság által véleményem szerint annak tulajdonított értelemben kellene érteni, vagyis, hogy a szakértői véleményből automatikusan arra lehet következtetni, hogy az adatkezelő által elfogadott intézkedések megfelelőek. [20]

[20] Írásbeli észrevételek, 39. pont.

E. Az előzetes döntéshozatalra előterjesztett negyedik kérdés

58. Negyedik kérdésével az előterjesztő bíróság lényegében azt kérdezi, hogy a rendelet 82. cikkének (3) bekezdését úgy kell-e értelmezni, hogy e rendelet megsértése (amely – mint a jelen ügyben – a személyes adatoknak a 4. cikk 12. pontja értelmében vett „jogosulatlan közlését" és az azokhoz való „jogosulatlan hozzáférést" foglalja magában), amelyet olyan személyek követtek el, akik nem az adatkezelő alkalmazottai, és nem állnak az adatkezelő ellenőrzése alatt, olyan körülménynek minősül, amelyért az adatkezelőt semmilyen módon nem terheli felelősség, és amely alapján mentesül a felelősség alól a 82. cikk (3) bekezdése értelmében.

59. A kérdésre adott válasz egyenesen következik a rendelet általános filozófiájáról fentebb elmondottakból: nincs automatizmus, ezért pusztán az a tény, hogy a személyes adatok jogosulatlan közlésére vagy a személyes adatokhoz való jogosulatlan hozzáférésre az adatkezelő ellenőrzési körén kívül eső személyek révén került sor, nem mentesíti az adatkezelőt a felelősség alól.

60. Először is szó szerint értelmezve meg kell jegyezni, hogy sem a 82. cikk (3) bekezdése, sem a (146) preambulumbekezdés nem határoz meg olyan különleges feltételeket, amelyeknek teljesülniük kell ahhoz, hogy az adatkezelő mentesüljön a felelősség alól, kivéve annak bizonyítását, hogy „a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség". Ebből a megfogalmazásból egyrészt az következik, hogy az adatkezelő csak akkor mentesülhet a felelősség alól, ha bizonyítja, hogy a szóban forgó kárt előidéző eseményért nem terheli felelősség, másrészt pedig hogy az e rendelkezés által megkövetelt bizonyítási szint magas, tekintettel a „semmilyen módon" kifejezés használatára, amint arra a Bizottság rámutatott. [21]

61. A 82. cikkben és általában véve a rendelet egészében előírt felelősségi rendszer széleskörű vita tárgyát képezte a különböző tagállamok jogirodalmában. Az ugyanis a szerződésen kívüli felelősség hagyományos elemeit tartalmazza, de olyan elemeket is magában foglal, amelyek a rendelkezések szerkezetében közelebb viszik azt a szerződéses felelősséghez vagy akár az objektív felelősség formájához, az adatkezelési tevékenység eredendő veszélyessége miatt. Nem ez a részletes vita ismertetésének a helye, de véleményem szerint a 82. cikk nem tűnik úgy, mintha objektív felelősségi rendszert határozna meg. [22]

62. A személyes adatok megsértéséből eredő kár bekövetkezhet annak vétkes következményeként, hogy a személyek adatkezelési tevékenységhez kapcsolódó jogait és szabadságait érintő kockázatokra tekintettel nem hoztak észszerű és egyébként megfelelő technikai és szervezési intézkedéseket a kár megelőzése érdekében. Ezek a kockázatok szigorítják a kár megelőzésére és elkerülésére vonatkozó kötelezettséget, kiterjesztve az adatkezelőt terhelő gondossági kötelezettséget. Az adatkezelőket terhelő magatartási kötelezettségek és a károkozó esetében előírt mentesítő bizonyítékra vonatkozó rendelkezés összehangolt olvasatából tehát a

[21] A Bíróság állandó ítélkezési gyakorlatának megfelelően, amely szerint az általános szabály alóli kivételek szigorúan értelmezendők, a felelősségnek a 82. cikk (3) bekezdése szerinti esetleges kizárását is szigorúan kell értelmezni. Lásd analógia útján: 2020. október 15-i Association française des usagers de banques ítélet (C-778/18, EU:C:2020:831, 53. pont); 2022. április 5-i Commissioner of An Garda Síochána és társai ítélet (C-140/20, EU:C:2022:258, 40. pont).

[22] A polgári jogi felelősség általában objektív felelősségnek minősül, amikor a megbízott köteles minden elméletben lehetséges intézkedést megtenni a kár elkerülése érdekében, függetlenül attól, hogy ténylegesen tudott-e ezekről, vagy hogy gazdaságilag mennyire voltak életképesek. Ezzel szemben, ha a megbízottnak a biztonság fenntartása és az elvégzett tevékenységből eredő esetleges károk megelőzése érdekében meg kell tennie az érintett gazdasági ágazat szereplője által általában betartandó intézkedéseket, a kárért való felelősség a konkrét vétkesség felelősségi rendszere felé tolódik el. M. Gambini, *Responsabilità*, hiv., 1055. o.

vélelmezett vétkesség miatti súlyosbított felelősség elismerése mellett lehet érvelni a személyes adatok jogellenes kezeléséért való felelősségnek a rendelet 82. cikke által kidolgozott esetében. [23]

63. Ebből következik, hogy az adatkezelőnek lehetősége van mentesítő bizonyítékokat szolgáltatni (ami az objektív felelősség esetében nem megengedett). Ami a bizonyítási teher megosztását illeti, a rendelet 82. cikkének (3) bekezdése a károsult számára kedvező rendszert ír elő, a károkozó vétkességére vonatkozó bizonyítási kötelezettség megfordításáról rendelkezve, a fent említett, [24] a meghozott intézkedések megfelelőségére vonatkozó bizonyítási teher megfordításával teljes párhuzamban. A jogalkotó tehát azt jelzi, hogy tisztában van a bizonyítási teher ettől eltérő megosztásának elfogadásával járó veszélyekkel; ha a károkozó vétkességére vonatkozó bizonyítási terhet a károsultra hárítanák, akkor túlzottan terhessé tennék a helyzetét, és ezzel valójában veszélyeztetnék a kártérítés iránti jogorvoslatok működőképességét az új technológiák alkalmazásához kapcsolódó szabályok területén. Az érintett személy számára ugyanis különösen terhessé válhat a kár bekövetkezésének módját rekonstruálni és ahhoz hozzáférni, és ebből következően bizonyítani az adatkezelő vétkességét. Ezzel szemben az adatkezelő van a legjobb helyzetben ahhoz, hogy mentesítő bizonyítékot nyújtson be annak bizonyítására, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség. [25]

64. Az adatkezelőnek a fent ismertetett elszámoltathatóság elvével összhangban azt is bizonyítania kell, hogy mindent megtett annak érdekében, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani.

65. Visszatérve az előterjesztő bíróság kérdésére, az adatkezelő felelősségének jellegéről eddig elmondottak alapján, ha – amint azt fentebb említettem – az adatkezelő mentesülhet a felelősség alól annak bizonyításával, hogy a jogsértésért őt semmilyen módon nem terheli felelősség, akkor az a puszta tény nem tekinthető ilyennek, hogy az eseményt egy, az ellenőrzési körén kívül álló személy okozta.

66. Ha az adatkezelő kiberbűnözők támadásának áldozatává válik, a kárt okozó eseményt úgy lehet tekinteni, hogy azért nem az adatkezelőt terheli felelősség, de nem kizárt, hogy az adatkezelő hanyagsága állhatott a szóban forgó támadás hátterében, elősegítve azt a személyes adatok biztonságára irányuló, az adatkezelő által végrehajtandó intézkedések hiánya vagy elégtelensége miatt. Ezek az egyes esetekre jellemző tényértékelések, amelyeket az eljáró nemzeti bíróságnak kell megtennie az előtte benyújtott bizonyítékok fényében.

67. Az is általános tapasztalat, hogy a nagy mennyiségű személyes adatot tároló közjogi vagy magánszervezetek rendszerei ellen irányuló külső támadások sokkal gyakoribbak, mint a belső támadások. Az adatkezelőnek tehát megfelelő intézkedéseket kell hoznia különösen a külső támadások kezelésére.

68. Végül teleologikus szempontból meg kell jegyezni, hogy a rendelet a magas szintű védelem célját követi. E tekintetben a Bíróság már kiemelte, hogy a rendelet (10), (11) és (13) preambulumbekezdésével összefüggésben értelmezett 1. cikkének (2) bekezdéséből következik, hogy e rendelet az uniós intézményekre, szervekre és hivatalokra, valamint a

[23] M. Gambini, *Responsabilità*, hiv., 1059. o. Hasonlóképpen, azon nézet alapján, amely szerint a megfelelő intézkedések meghozatalának bizonyítása nem az elvárt legnagyobb gondosság puszta állításában áll, hanem a kárt előidéző külső tényező bizonyításában, amely a váratlan eseményre és a *vis maior*ra jellemző előre nem láthatóság és elkerülhetetlenség jellegzetességével rendelkezik, S. Sica, *Sub art. 82*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „[H]a *bizonyítja*, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség" (82. cikk (3) bekezdése).

[25] M. Gambini, *Responsabilità*, hiv., 1060. o.

tagállamok hatáskörrel rendelkező hatóságaira azt a feladatot rója, hogy biztosítsák az EUMSZ 16. cikkben és a Charta 8. cikkében garantált, a személyes adatok védelméhez való jogok magas szintű védelmét. [26]

69. Ha a Bíróság azt az értelmezést választaná, hogy amennyiben a rendelet megsértését harmadik személy követte el, az adatkezelőt a 82. cikk (3) bekezdése alapján automatikusan mentesíteni kell a felelősség alól, ez az értelmezés összeegyeztethetetlen lenne az említett eszköz által kitűzött védelmi céllal, mivel gyengítené az érintettek jogait, mert e felelősséget azokra az esetekre korlátozná, amikor a jogsértés az említett adatkezelő irányítása és/vagy ellenőrzése alatt álló személyeknek tudható be.

F. Az előzetes döntéshozatalra előterjesztett ötödik kérdés

70. Ötödik kérdésével a nemzeti bíróság lényegében a „nem vagyoni kár” fogalmának a rendelet 82. cikke szerinti értelmezését kéri a Bíróságtól. A nemzeti bíróság különösen azt kérdezi, hogy a rendelet (85) és (146) preambulumbekezdésével [27] összefüggésben értelmezett 82. cikkének (1) és (2) bekezdését úgy kell-e értelmezni, hogy egy olyan helyzetben, amikor az említett rendelet megsértése abban áll, hogy kiberbűnözők a személyes adatokhoz jogosulatlanul hozzáfértek és ezen adatokat jogosulatlanul nyilvánosságra hozták, az a tény, hogy az érintett fél attól, hogy személyes adataival a jövőben visszaélhetnek, önmagában kártérítésre jogosító (nem vagyoni) kárt jelenthet.

71. Sem a 82. cikk, sem a kártérítéssel kapcsolatos preambulumbekezdések nem adnak egyértelmű választ a kérdésre, de néhány hasznos elem levonható azokból az elemzéshez: a nem vagyoni kár is kártérítés tárgyát képezheti a vagyoni (vagy pénzbeli) kár mellett; a rendelet megsértése nem eredményezi automatikusan az e jogsértés által „okozott” kárt, pontosabban az adatvédelmi incidens „okozhat” fizikai, vagyoni vagy nem vagyoni kárt a természetes személyeknek; a kár fogalmát a Bíróság ítélkezési gyakorlatának fényében „tágan” kell értelmezni, hogy az teljes mértékben tükrözze a rendelet célkitűzéseit; az [érintetteket] „ért” kárért „teljes és tényleges” kártérítést kell nyújtani.

72. A rendelet rendelkezéseinek megfogalmazása már megtisztítja a terepet a magától értetődő kárra való esetleges utalástól: a rendelet által előírt polgári jogi felelősség fő célja, hogy az érintett számára elégtételt nyújtson, éppen az elszenvedett kár „teljes és tényleges” megtérítése révén, és hogy így a jogsértés által hátrányosan megváltoztatott jogi helyzet egyensúlyát helyreállítsa. [28]

[26] Lásd ebben az értelemben: 2021. június 15-i Facebook Ireland és társai ítélet (C-645/19, EU:C:2021:483, 44. és 45. pont).

[27] A (85) preambulumbekezdés szerint: „Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek. […]”. A (146) preambulumbekezdés szerint: „Az adatkezelő vagy az adatfeldolgozó az e rendeletet sértő adatkezelés miatt okozott kárt köteles megtéríteni. Az adatkezelőt vagy az adatfeldolgozót a kártérítési kötelezettség alól abban az esetben mentesíteni kell, ha bizonyítja, hogy a kár bekövetkeztéért őt semmilyen felelősség nem terheli. A kár fogalmát a Bíróság ítélkezési gyakorlatának fényében tágan kell értelmezni, mégpedig oly módon, hogy az teljes mértékben tükrözze e rendelet célkitűzéseit. Ez nem érinti a más uniós vagy tagállami jog megsértéséből eredő károkkal kapcsolatos esetleges kártérítési igényeket. […] Az érintetteket az őket ért kárért teljes és tényleges kártérítés illeti meg. […]”.

[28] Lásd: Campos Sánchez-Bordona főtanácsnok hivatkozott indítványa, 29. pont és 11. lábjegyzet. Ugyanebben az indítványban a főtanácsnok helyesen zárja le a szó szerinti, történeti, szövegösszefüggésen alapuló és teleologikus szempontú elemzését azzal, hogy kizárja az érintetteknek a 82. cikk alapján megtérítendő kártérítés „büntető” jellegét (27–55. pont), egyrészt megjegyezve, hogy „a tagállamoknak nem kell választaniuk (és valójában nem is választhatnak) a VIII. fejezetben szereplő, az adatvédelmet biztosító mechanizmusok között. Olyan jogsértés esetén, amely nem keletkeztet kárt, az érintett továbbra is jogosult (legalább) arra, hogy […] panaszt tegyen a felügyeleti hatóságnál”, másrészt pedig, hogy „a kompenzáció károktól függetlenül történő kilátásba helyezése valószínűleg ösztönözné – a talán nem mindig megalapozott kérelmeket tárgyaló – polgári jogvitákat, és ezáltal eltántoríthatna az adatkezelési tevékenység végzésétől” (54–55. pont).

73. Másrészt, rendszertani szempontból is, mint a trösztellenes jogban, a rendelet a védelem két pillérét írja elő: egy közjogi jellegű, a rendelet rendelkezéseinek megsértése esetén szankciókat előíró pillért és egy magánjogi jellegű, szerződésen kívüli polgári jogi felelősséget előíró pillért, amely felelősség a fent említett jellemzőkkel rendelkező, a vélelmezett vétkesség miatt súlyosbított felelősségnek minősíthető, a mentesítő bizonyítékokra is figyelemmel.[29]

74. Ennélfogva a (nem vagyoni) kár fogalmának széles körű értelmezése[30] nem vezethet annak megállapításához, hogy a jogalkotó eltekintett a tényleges „kár” fennállásának szükségességétől.

75. A valódi érdemi kérdés az, hogy a jogsértés fennállásának és az okozati összefüggésnek a megállapítását követően keletkezhet-e kártérítési jog az érintett személy személyes adatokkal való esetleges jövőbeli visszaéléssel kapcsolatos aggodalma, negatív előérzete, félelme miatt, ha az ilyen visszaélést nem állapították meg és/vagy az érintett személyt nem érte további kár.

76. A Bíróság állandó ítélkezési gyakorlata szerint a jelentésének és hatályának meghatározása érdekében a tagállami jogokra kifejezett utalást nem tartalmazó uniós jogi rendelkezést az egész Unióban általában önállóan és egységesen kell értelmezni, amelynek során figyelembe veszik a szóban forgó rendelkezés szó szerinti szövegét, szövegkörnyezetét, annak a szabályozásnak a céljait, amelynek az a részét képezi, valamint e rendelkezés keletkezését.[31]

77. A Bíróság, amint arra Campos Sánchez-Bordona főtanácsnok emlékeztetett,[32] még nem dolgozta ki a „kár” olyan általános meghatározását, amely bármely területen különbségtétel nélkül alkalmazandó lenne.[33] Ami a nem vagyoni károkat illeti, az ítélkezési gyakorlatból a következő vezethető le: amennyiben az értelmezendő rendelkezés egyik célja az egyén vagy az egyének egy bizonyos kategóriájának védelme,[34] a kár fogalmának tágnak kell lennie; e megközelítéssel összhangban a kártérítés kiterjed a nem vagyoni károkra, még akkor is, ha azt az értelmezett rendelkezés nem említi.[35]

[29] Az adatkezelési szabályok megsértésével kapcsolatos enyhe és átmeneti érzések vagy érzelmek miatti kártérítésre való jogosultság megtagadása nem teszi az érintettet teljesen kiszolgáltatottá (ebben az értelemben lásd: Campos Sánchez-Bordona főtanácsnok fent hivatkozott indítványa, 115. pont).

[30] Vagy „tágabb” a (146) preambulumbekezdés szavai szerint.

[31] Lásd: 2021. április 15-i The North of England P & I Association ítélet (C-786/19, EU:C:2021:276, 48. pont); 2021. június 10-i KRONE – Verlag ítélet (C-65/20, EU:C:2021:471, 25. pont).

[32] Lásd: Campos Sánchez-Bordona főtanácsnok hivatkozott indítványa, 104. pont.

[33] Nem határozta meg azt sem, hogy az értelmezés melyik módszere – az autonóm értelmezés vagy a nemzeti jogszabályokra való utalás – lenne előnyösebb: ez a vizsgálat tárgyát képező területtől függ. Lásd: a hibás termékekkel kapcsolatos 2001. május 10-i Veedfald ítélet (C-203/99, EU:C:2001:258, 27. pont); a légi fuvarozók felelősségéről szóló 2010. május 6-i Walz ítélet (C-63/09, EU:C:2010:251, 21. pont); a gépjárműbalesetekből eredő károkra alkalmazandó polgári jogi felelősséggel kapcsolatos 2021. június 10-i Van Ameyde España ítélet (C-923/19, EU:C:2021:475, 37. és azt követő pontok).

[34] Például a termékek fogyasztói vagy a közúti balesetek károsultjai.

[35] Az utazási csomagok területén lásd: 2002. március 12-i Leitner ítélet (C-168/00, EU:C:2002:163); a gépjárművek használatával kapcsolatos polgári jogi felelősség terén: 2013. október 24-i Haasová ítélet (C-22/12, EU:C:2013:692, 47–50. pont); 2013. október 24-i Drozdovs ítélet (C-277/12, EU:C:2013:685, 40. pont); 2014. január 23-i Petillo ítélet (C-371/12, EU:C:2014:26, 35. pont).

78. Noha a Bíróság ítélkezési gyakorlata lehetővé teszi annak megállapítását, hogy – a fentiekben kifejtettek szerint – az uniós jogban létezik a nem vagyoni kár megtérítésének elve, egyetértek Campos főtanácsnokkal abban, hogy ebből azonban olyan szabályra nem lehet következtetni, amelynek értelmében *minden* nem vagyoni kár – jelentőségének mértékétől függetlenül – megtérítendő. [36]

79. Ebben az összefüggésben releváns lehet a megtérítendő nem vagyoni károk és *a jogszerűség be nem tartásából eredő* egyéb *hátrányok* közötti megkülönböztetés, amelyek csekély jelentőségüknél fogva nem szükségszerűen keletkeztetnek kártérítésre való jogosultságot. [37]

80. A Bíróság elismeri ezt a különbséget, amikor a károkozással kapcsolatban önálló kategóriaként említi a kellemetlenségeket és a bosszúságot azon a területeken, ahol úgy véli, hogy indokolt a kártérítés. [38]

81. Empirikusan megállapítható, hogy a személyes adatok védelmére vonatkozó bármely szabály megsértése az érintett részéről valamilyen negatív reakciót vált ki. A puszta rossz érzésért járó kártérítés, amelyet a törvények más által való be nem tartása okoz, könnyen összetéveszthető a kár nélküli kártérítéssel, ami, amint azt már említettem, úgy tűnik, hogy a rendelet 82. cikke szerinti helyzetben nem alkalmazható.

82. Az a tény, hogy az alapeljárásban szereplőhöz hasonló körülmények között a személyes adatokkal való visszaélés csak lehetséges, és nem tényleges, elegendő annak megállapításához, hogy az érintettet a rendelet megsértése miatt nem vagyoni kár érhette, feltéve, hogy az érintett bizonyítja, hogy az ilyen visszaéléstől való félelem ténylegesen és konkrétan valós és tényleges érzelmi jellegű kárt okozott neki. [39]

83. A puszta bosszúság (amely nem megtérítendő) és a valódi nem vagyoni kár (amely igenis megtérítendő) közötti határvonal vékony, de a nemzeti bíróságoknak, amelyeknek az a feladatuk, hogy ezt a határt eseti alapon körülhatárolják, gondosan értékelniük kell a kártérítést követelő érintett személy által szolgáltatott valamennyi bizonyítékot, amely személy felelős azért, hogy pontosan és nem általánosan olyan konkrét bizonyítékokat szolgáltasson, amelyek a személyes

[36] Lásd: Campos Sánchez-Bordona főtanácsnok hivatkozott indítványa, 105. pont. A Bíróság többek között elismerte, hogy összeegyeztethető az európai normákkal az olyan nemzeti jogszabály, amely a kártérítés kiszámítása szempontjából a balesetből következő testi sérülésekhez kapcsolódó nem vagyoni károkat a baleset eredete szerint különbözteti meg; lásd: 2014. január 23-i Petillo ítélet (C-371/12, EU:C:2014:26), rendelkező rész: az uniós joggal „nem ellentétes az olyan nemzeti szabályozás […], amely a közúti közlekedési balesetekből következő könnyű testi sérülésekből eredő nem vagyoni károk megtérítésének különös rendszerét írja elő, amely korlátozza e károk megtérítését ahhoz képest, amire nem ilyen balesetekből eredő, ugyanilyen károk megtérítése tekintetében lehetőség van”.

[37] A nemzeti jogrendszerekben az ilyen különbségtételt a társadalmi élet elkerülhetetlen velejárójának tekintik. Legújabban az adatvédelemmel kapcsolatban Olaszországban a Tribunale di Palermo (palermói bíróság), sez. I civile (I. polgári jogi tanács) 2017. október 5-i 5261. sz. ítélete, valamint Cass. Civ. (semmítőszék), a VI. tanács 17383/2020. sz. végzése. Németországban többek között az Amtsgericht Diez (diezi helyi bíróság) 2018. november 7-i 8 C 130/18. sz, ítélete; a Landgericht Karlsruhe (karlsruhei regionális bíróság) 2019. augusztus 2-i 8 O 26/19. sz. ítélete; az Amtsgericht Frankfurt am Main (frankfurt am maini helyi bíróság) 2020. július 10-i 385 C 155/19 (70). sz. ítélete. Ausztriában az Oberster Gerichtshof (legfelsőbb bíróság) 6 Ob 56/21k. sz. ítélete.

[38] Lásd: a nemzetközi légi szállítás egyes szabályainak egységesítéséről szóló, 1999. május 28-án Montrealban kötött egyezmény (kihirdette: 2005. évi VII. tv.) 19. cikke értelmében vett „károk” és a 261/2004 rendelet értelmében vett – e rendelet 7. cikke alapján a 2009. november 19-i Sturgeon és társai ítélet (C-402/07 és C-432/07, EU:C:2009:716) értelmében megtérítendő – „kényelmetlenség” közötti különbségtételre vonatkozó 2012. október 23-i Nelson és társai ítélet (C-581/10 és C-629/10, EU:C:2012:657, 51. pont). Ebben az ágazatban – akárcsak az 1177/2010 rendeletben szereplő tengeri és belvízi személyszállítási ágazatban – a jogalkotó elismerhetett egy absztrakt kategóriát annak köszönhetően, hogy a gondot jelentő tényező – és annak lényege – valamennyi érintett esetében azonos. Nem gondolom, hogy e következtetés lehetséges lenne az adatvédelem területén.

[39] Írország szerint ezek a megfontolások a gyakorlatban különösen fontosak a kiberbűnözéssel összefüggésben, mivel ha minden – akár minimálisan is – sérelmet szenvedett személy jogosult lenne a nem vagyoni kártérítésre, az erős hatással lenne különösen a közszféra adatkezelőire, amelyeket korlátozott közpénzekből finanszíroznak, és inkább a kollektív érdekeket kellene szolgálniuk, beleértve a személyes adatok biztonságának javítását (írásbeli észrevételek, 72. pont).

adatok megsértése miatt „ténylegesen elszenvedett nem vagyoni kár” fennállását eredményezhetik, még anélkül is, hogy elérné a különös súlyosság előre meghatározott küszöbét: az számít, hogy nem pusztán szubjektív, változó, személyiséggel összefüggő és személyes elemektől függő észlelésről van szó, hanem egy, bár csekély, de ellenőrizhető, a saját testi vagy pszichés szférájában vagy a társadalmi életében megmutatkozó kényelmetlenség tárgyiasításáról; az érintett személyes adatok jellege és azoknak az érintett életére vonatkozó relevanciája, és esetleg a társadalomnak az adatvédelmi incidenssel kapcsolatos e konkrét kellemetlenséggel összefüggésben az adott pillanatban érvényesülő felfogása. [40]

IV. Végkövetkeztetés

84. A fenti megfontolások összességére tekintettel azt javaslom a Bíróságnak, hogy az előzetes döntéshozatalra előterjesztett kérdésekre a következőképpen válaszoljon:

„A 2016/679 rendelet 5., 24,, 32. és 82. cikkét a következőképpen kell értelmezni:

a 4. cikk 12. pontjában meghatározott „adatvédelmi incidens” puszta fennállása önmagában nem elegendő annak megállapításához, hogy az adatkezelő által végrehajtott technikai és szervezési intézkedések nem voltak „megfelelőek” a szóban forgó adatok védelmének biztosítására;

a személyes adatokat kezelő adatkezelő által végrehajtott technikai és szervezési intézkedések megfelelőségének értékelése során az eljáró nemzeti bíróságnak az említett intézkedések tartalmának, alkalmazásuk módjának és gyakorlati hatásainak konkrét elemzésére kiterjedő vizsgálatot kell elvégeznie;

az általános adatvédelmi rendelet 82. cikke szerinti kártérítési kereset keretében a személyes adatokat kezelő adatkezelőt terheli annak bizonyítása, hogy az általa az említett rendelet 32. cikke alapján végrehajtott intézkedések megfelelőek voltak;

az eljárási autonómia elvének megfelelően az egyes tagállamok belső jogrendszere határozza meg az elfogadható bizonyítási módszereket és azok bizonyító erejét, ideértve azokat a vizsgálati cselekményeket is, amelyeket a nemzeti bíróságok elrendelhetnek vagy azoknak el kell rendelniük annak eldöntése céljából, hogy a személyes adatokat kezelő adatkezelő az említett rendelet értelmében megfelelő intézkedéseket hajtott-e végre, figyelemmel az uniós jogban meghatározott egyenértékűség és tényleges érvényesülés elvére;

az a tény, hogy az említett rendeletnek a szóban forgó kárt előidéző megsértését harmadik személy követte el, önmagában nem alapozza meg az adatkezelő felelősség alóli mentesítését, és az e rendelkezés szerinti mentességhez az adatkezelőnek kell bizonyítania, hogy a jogsértésért semmilyen módon nem terheli felelősség;

a személyes adataival való esetleges jövőbeni visszaéléstől való félelemben megnyilvánuló kár, amelynek fennállását az érintett bizonyította, kártérítéshez való jogot megalapozó nem vagyoni kárnak minősülhet, feltéve, hogy az érintett bizonyítja, hogy egyénileg őt valós és tényleges érzelmi jellegű kár érte, amely körülménynek a vizsgálata minden egyes esetben az eljáró nemzeti bíróság feladata.”

[40] Lásd: Campos Sánchez-Bordona főtanácsnok hivatkozott indítványa, 116. pont.