A BÍRÓSÁG ÍTÉLETE (harmadik tanács)

2023. december 14.*

„Előzetes döntéshozatal – A természetes személyek védelme a személyes adatok kezelése vonatkozásában – (EU) 2016/679 rendelet – 5. cikk – Az ilyen adatkezelésre vonatkozó elvek – 24. cikk – Az adatkezelő feladatai – 32. cikk – Az adatkezelés biztonságának garantálása érdekében hozott intézkedések – Az ilyen intézkedések megfelelőségének értékelése – A bírósági felülvizsgálat terjedelme – Bizonyításfelvétel – 82. cikk – A kártérítéshez való jog és a felelősség – Az adatkezelő esetleges felelősség alóli mentesítése harmadik felek által elkövetett jogsértés esetén – A személyes adatokkal való esetleges visszaéléstől való félelemre alapított, nem vagyoni kár megtérítése iránti kérelem”

A C-340/21. sz. ügyben,

az EUMSZ 267. cikk alapján benyújtott előzetes döntéshozatal iránti kérelem tárgyában, amelyet a Varhoven administrativen sad (legfelsőbb közigazgatási bíróság, Bulgária) a Bírósághoz 2021. június 2-án érkezett, 2021. május 14-i határozatával terjesztett elő a

VB

és

a **Natsionalna agentsia za prihodite**

között folyamatban lévő eljárásban,

A BÍRÓSÁG (harmadik tanács),

tagjai: K. Jürimäe tanácselnök, N. Piçarra, M. Safjan, N. Jääskinen (előadó) és M. Gavalec bírák,

főtanácsnok: G. Pitruzzella,

hivatalvezető: A. Calot Escobar,

tekintettel az írásbeli szakaszra,

figyelembe véve a következők által előterjesztett észrevételeket:

– a Natsionalna agentsia za prihodite képviseletében R. Spetsov,

– a bolgár kormány képviseletében M. Georgieva és L. Zaharieva, meghatalmazotti minőségben,

* Az eljárás nyelve: bolgár.

– a cseh kormány képviseletében O. Serdula, M. Smolek és J. Vláčil, meghatalmazotti minőségben,

– Írország képviseletében M. Browne Chief State Solicitor, A. Joyce, J. Quaney és M. Tierney, meghatalmazotti minőségben, segítőjük: D. Fennelly BL,

– az olasz kormány képviseletében G. Palmieri, meghatalmazotti minőségben, segítője: E. De Bonis avvocato dello Stato,

– a portugál kormány képviseletében P. Barros da Costa, A. Pimenta, J. Ramos és C. Vieira Guerra, meghatalmazotti minőségben,

– az Európai Bizottság képviseletében A. Bouchagiar, H. Kranenborg és N. Nikolova, meghatalmazotti minőségben,

a főtanácsnok indítványának a 2023. április 27-i tárgyaláson történt meghallgatását követően,

meghozta a következő

Ítéletet

1 Az előzetes döntéshozatal iránti kérelem a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv 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.; a továbbiakban: általános adatvédelmi rendelet) 5. cikke (2) bekezdésének, 24. és 32. cikkének, valamint 82. cikke (1)–(3) bekezdésének értelmezésére vonatkozik.

2 E kérelmet a VB természetes személy és a Natsionalna agentsia za prihodite (nemzeti adóhatóság, Bulgária, a továbbiakban: NAP) között azon nem vagyoni kár megtérítése tárgyában folyamatban lévő jogvita keretében terjesztették elő, amely az említett személyt állítása szerint amiatt érte, hogy e hatóság állítólag nem teljesítette a személyes adatok kezelőjeként rá háruló jogi kötelezettségeket.

Jogi háttér

3 Az általános adatvédelmi rendelet (4), (10), (11), (74), (76), (83), (85) és (146) preambulumbekezdése a következőképpen szól:

„(4) […] Ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja [az Európai Unió Alapjogi Chartájában] elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen ami a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, […] a hatékony jogorvoslathoz és a tisztességes eljáráshoz […] való jogot illeti.

[…]

(10) A természetes személyek következetes és magas szintű védelmének biztosítása és a személyes adatok [Európai] Unión belüli áramlása előtti akadályok elhárítása érdekében a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait minden tagállamban azonos szintű védelemben kell részesíteni. A természetes személyeknek a személyes adataik kezeléséhez kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell. […]

(11) Ahhoz, hogy a személyes adatok az Unió egész területén hatékony védelemben részesüljenek, az érintettek jogait, valamint a személyes adatokat kezelő, illetve az adatkezelést meghatározó személyek kötelezettségeit megerősíteni és részletesen meghatározni szükséges […]

[…]

(74) 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.

[…]

(76) Az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot olyan objektív értékelés alapján kell felmérni, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e.

[…]

(83) A biztonság fenntartása és az e rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot – ideértve a bizalmas kezelést is –, figyelembe véve a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés – mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

[…]

(85) Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. Következésképpen, amint az adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül […] bejelenteni köteles az illetékes felügyeleti hatóságnál […]

[…]

(146) 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 e rendeletet sértő adatkezelés magában foglalja az e rendelettel összhangban elfogadott, felhatalmazáson alapuló jogi aktusokat és végrehajtási jogi aktusokat, valamint az e rendeletben foglalt szabályokat pontosító tagállami jogot [helyesen: az e rendelettel és az e rendeletben foglalt szabályokat pontosító tagállami joggal összhangban elfogadott, felhatalmazáson alapuló jogi aktusokat és végrehajtási jogi aktusokat] sértő adatkezelést is. Az érintetteket az őket ért kárért teljes és tényleges kártérítés illeti meg. […]”

4 E rendelet „Fogalommeghatározások” című 4. cikke a következőképpen rendelkezik:

„E rendelet alkalmazásában:

1) »személyes adat«: azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ;

2) »adatkezelés«: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége […];

[…]

7) »adatkezelő«: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; […]

[…]

10) »harmadik fél«: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

[…]

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;

[…]”

5 Az említett rendeletnek „A személyes adatok kezelésére vonatkozó elvek” című 5. cikke a következőket írja elő:

„(1) A személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni (»jogszerűség, tisztességes eljárás és átláthatóság«);

[…]

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«).”

6 Az általános adatvédelmi rendeletnek „Az adatkezelő feladatai” című 24. cikke értelmében:

„(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.”

7 Az általános adatvédelmi rendeletnek „Az adatkezelés biztonsága” című 32. cikke a következőképpen rendelkezik:

„(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:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

(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.

[…]”

8 E rendeletnek „Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog” című 79. cikkének (1) bekezdése a következőket írja elő:

„A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a felügyeleti hatóságnál történő panasztételhez való, 77. cikk szerinti jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak e rendeletnek nem megfelelő kezelése következtében megsértették az e rendelet szerinti jogait.”

9 A fent említett rendeletnek „A kártérítéshez való jog és a felelősség” című 82. cikke (1) és (3) bekezdésében kimondja:

„(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.”

Az alapeljárás és az előzetes döntéshozatalra előterjesztett kérdések

10 A NAP a bolgár pénzügyminiszter felügyelete alá tartozó hatóság. Jogköreinek gyakorlása során, amelyek többek között köztartozások megállapítására, biztosítására és behajtására irányulnak, az általános adatvédelmi rendelet 4. cikkének 7. pontja értelmében vett személyesadat-kezelőként jár el.

11 2019. július 15-én a média feltárta, hogy a NAP informatikai rendszeréhez történő jogosulatlan hozzáférésre került sor, és hogy e kibertámadást követően az interneten közzétették az említett rendszerben található személyes adatokat.

12 Ezen események több mint hatmillió bolgár, illetve külföldi állampolgárt érintettek. Közülük több százan – köztük az alapeljárás felperese is – olyan nem vagyoni károk megtérítése iránti keresetet nyújtottak be a NAP ellen, amelyek a személyes adataik közléséből eredtek.

13 Az alapeljárás felperese e körülmények között indított keresetet az Administrativen sad Sofia-grad (szófiai közigazgatási bíróság, Bulgária) előtt annak érdekében, hogy a NAP fizessen meg számára 1000 bolgár leva (BGN) (hozzávetőleg 510 euró) összeget kártérítés címén az általános adatvédelmi rendelet 82. cikke és a bolgár jog rendelkezései alapján. E kérelem alátámasztása érdekében azt állította, hogy nem vagyoni kár érte őt a személyes adatoknak az általános adatvédelmi rendelet 4. cikke 12. pontjának megsértése, közelebbről az adatbiztonság abból eredő megsértése folytán, hogy a NAP nem teljesítette a többek között az e rendelet 5. cikke (1) bekezdésének f) pontjából, valamint 24. és 32. cikkéből eredő kötelezettségeit. Nem vagyoni kára abból a félelemből ered, hogy a hozzájárulása nélkül nyilvánosságra hozott személyes adatait a jövőben visszaélésszerűen felhasználják, vagy hogy ő maga zsarolás, támadás vagy akár emberrablás áldozatává válik.

14 Ellenkérelmében a NAP mindenekelőtt arra hivatkozott, hogy az alapeljárás felperese nem kért tőle információkat arra vonatkozóan, hogy pontosan mely adatokhoz fértek hozzá. Ezt követően a NAP annak bizonyítására irányuló dokumentumokat nyújtott be, hogy előzetesen minden szükséges intézkedést megtett annak érdekében, hogy megelőzze az informatikai rendszerében tárolt személyes adatok megsértését, valamint annak érdekében, hogy e jogsértést követően korlátozza e jogsértés hatásait, és megnyugtassa az állampolgárokat. Ezenkívül a NAP szerint nem állt fenn okozati összefüggés az állítólagos nem vagyoni kár és az említett jogsértés között. Végül előadta, hogy mivel ő maga is a munkavállalóinak nem minősülő személyek szándékos támadásának áldozata volt, nem tehető felelőssé az e támadás következtében bekövetkező károkért.

15 2020. november 27-i határozatával az Administrativen sad Sofia-grad (szófiai közigazgatási bíróság) elutasította az alapeljárás felperesének keresetét. E bíróság megállapította egyrészt, hogy a NAP adatbázisához való jogosulatlan hozzáférés harmadik személyek által elkövetett, informatikai kalózkodás eredménye, másrészt pedig, hogy az alapeljárás felperese nem bizonyította, hogy a NAP mulasztást követett el a biztonsági intézkedések elfogadása tekintetében. Ezenkívül úgy ítélte meg, hogy e felperest nem érte megtérítendő nem vagyoni kár.

16 Az alapeljárás felperese az említett határozattal szemben felülvizsgálati kérelmet nyújtott be a Varhoven administrativen sadhoz (legfelsőbb közigazgatási bíróság, Bulgária), amely a jelen ügyben a kérdést előterjesztő bíróság. Felülvizsgálati kérelmének alátámasztására előadja, hogy az elsőfokú bíróság tévesen alkalmazta a jogot a NAP által hozott biztonsági intézkedésekre vonatkozó bizonyítási teher telepítése során, és hogy ez utóbbi nem bizonyította, hogy e

tekintetben nem követett el mulasztást. Ezenkívül az alapeljárás felperese azt állítja, hogy a személyes adatainak esetleges jövőbeli visszaélésszerű felhasználásától való félelem tényleges, nem pedig feltételezett nem vagyoni kárnak minősül. Ellenkérelmében a NAP ezen érvek mindegyikét vitatja.

17 A kérdést előterjesztő bíróság mindenekelőtt annak lehetőségét vizsgálja, hogy a személyes adatok megsértésének megállapítása önmagában lehetővé teszi annak megállapítását, hogy az ezen adatok adatkezelője által tett intézkedések nem voltak „megfelelőek” az általános adatvédelmi rendelet 24. és 32. cikke értelmében.

18 Ugyanakkor abban az esetben, ha ennek megállapítása nem elegendő a fenti következtetés levonásához, a kérdést előterjesztő bíróság egyrészt azon felülvizsgálat terjedelmével kapcsolatban vet fel kérdést, amelyet a nemzeti bíróságoknak az érintett intézkedések megfelelőségének értékelése érdekében el kell végezniük, másrészt pedig a bizonyításfelvételre vonatkozó azon szabályokat illetően, amelyeket e körben mind a bizonyítási teher, mind pedig a bizonyítási eszközök tekintetében alkalmazni kell, különösen akkor, ha e bíróságok előtt a hivatkozott rendelet 82. cikke alapján kártérítési keresetet indítottak.

19 Ezt követően e bíróság azt kívánja megtudni, hogy az említett rendelet 82. cikkének (3) bekezdésére tekintettel az a tény, hogy a személyes adatok megsértése harmadik személyek által elkövetett cselekményből, a jelen esetben kibertámadásból ered, olyan tényezőnek minősül-e, amely szisztematikusan mentesíti ezen adatok adatkezelőjét az érintettnek okozott kárért fennálló felelősség alól.

20 Végül az említett bíróság arra keresi a választ, hogy az általános adatvédelmi rendelet 82. cikkének (1) bekezdése értelmében vett „nem vagyoni kárnak” minősülhet-e önmagában a valamely személy által érzett azon félelem, hogy személyes adatait a jövőben – a jelen esetben az azokhoz való jogosulatlan hozzáférést és a kiberbűnözők általi nyilvánosságra hozatalukat követően – visszaélésszerűen felhasználhatják. Igenlő válasz esetén e személy mentesülne annak bizonyítása alól, hogy harmadik személyek a kártérítési kérelmének előterjesztését megelőzően jogellenesen használták fel ezeket az adatokat, például visszaéltek a személyazonosságával.

21 E körülmények között a Varhoven administrativen sad (legfelsőbb közigazgatási bíróság) úgy határozott, hogy az eljárást felfüggeszti, és előzetes döntéshozatal céljából a következő kérdéseket terjeszti a Bíróság elé:

„1) Úgy kell-e értelmezni [az 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 általános adatvédelmi 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 [az általános adatvédelmi rendelet] 32. cikke alapján hozott technikai és szervezési intézkedések?

3) Az első kérdésre adott nemleges válasz esetén úgy kell-e értelmezni az elszámoltathatóság [az általános adatvédelmi rendelet] (74) preambulumbekezdésével összefüggésben értelmezett 5. cikkének (2) bekezdése és 24. cikke szerinti elvét, hogy [az e rendelet] 82. cikkének (1) bekezdése szerinti peres eljárás során az adatkezelőt terheli [az ugyanezen] 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 »hekkertámadás« eredményezi?

4) Úgy kell-e értelmezni [az általános adatvédelmi rendelet] 82. cikkének (3) bekezdését, hogy – mint a jelen ügyben – a személyes adatoknak olyan személy közreműködésével megvalósuló »hekkertámadás« révén [az általános adatvédelmi 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 általános adatvédelmi rendelet] (85) és (146) preambulumbekezdésével összefüggésben értelmezett 82. cikkének (1) és (2) bekezdését, hogy a személyes adatokhoz való jogosulatlan hozzáférésként és azok »hekkertámadás« 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?”

Az előzetes döntéshozatalra előterjesztett kérdésekről

Az első kérdésről

22 Első kérdésével a kérdést előterjesztő bíróság lényegében arra keresi a választ, hogy az általános adatvédelmi rendelet 24. és 32. cikkét úgy kell-e értelmezni, hogy a személyes adatoknak az e rendelet 4. cikkének 10. pontja értelmében vett „harmadik felek” általi jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés önmagában elegendő annak megállapításához, hogy a szóban forgó adatkezelő által megtett technikai és szervezési intézkedések nem voltak e a 24. és 32. cikk értelmében véve „megfelelőek”.

23 Elöljáróban emlékeztetni kell arra, hogy az állandó ítélkezési gyakorlat szerint a jelentésének és hatályának meghatározása érdekében a tagállami jogokra kifejezett utalást nem tartalmazó uniós jogi rendelkezést, így az általános adatvédelmi rendelet 24. és 32. cikkét is az egész Unióban általában önállóan és egységesen kell értelmezni, amelynek során többek között figyelembe veszik a szóban forgó rendelkezés szövegét, az általa követett célokat, és azon szövegkörnyezetet, amelybe illeszkedik (lásd ebben az értelemben: 1984. január 18-i Ekro ítélet, 327/82, EU:C:1984:11, 11. pont; 2019. október 1-jei Planet49 ítélet, C-673/17, EU:C:2019:801, 47. és 48. pont; 2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 29. pont).

24 Először is, ami a releváns rendelkezések szövegét illeti, meg kell állapítani, hogy az általános adatvédelmi rendelet 24. cikke a személyes adatok kezelője számára általános kötelezettséget ír elő arra vonatkozóan, hogy megfelelő technikai és szervezési intézkedéseket tegyen annak biztosítása érdekében, hogy az említett adatkezelést e rendeletnek megfelelően végezzék, és azt bizonyítani tudja.

25 E célból e 24. cikk az (1) bekezdésében felsorol néhány, az ilyen intézkedések megfelelőségének értékelése során figyelembe veendő tényezőt, ezek az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett kockázat valószínűsége és súlyossága. E rendelkezés a fentieket kiegészíti azzal, hogy az említett intézkedéseket szükség esetén felül kell vizsgálni és naprakésszé kell tenni.

26 E célból az általános adatvédelmi rendelet 32. cikke pontosítja az adatkezelőnek és az esetleges adatfeldolgozónak az ezen adatkezelés biztonságával kapcsolatos kötelezettségeit. Így e cikk (1) bekezdése úgy rendelkezik, hogy az utóbbiaknak a tudomány és technológia állása, a megvalósítás költségei, továbbá az érintett adatkezelés jellege, hatóköre, körülményei és céljai figyelembevételével megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk a jelen ítélet előző pontjában említett kockázatok mértékének megfelelő szintű adatbiztonság garantálása érdekében.

27 Ugyanígy az említett cikk (2) bekezdése kimondja, hogy a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

28 Ezenkívül a fenti rendelet 24. cikkének (3) bekezdése és 32. cikkének (3) bekezdése egyaránt tartalmazza, hogy az adatkezelő vagy az adatfeldolgozó az e cikkek (1) bekezdésében foglalt követelményeknek való megfelelést azon az alapon bizonyíthatja, hogy az említett rendelet 40. és 42. cikkében előírtaknak megfelelően jóváhagyott magatartási kódexet vagy jóváhagyott tanúsítási mechanizmust alkalmaz.

29 Az általános adatvédelmi rendelet 32. cikkének (1) és (2) bekezdésében szereplő, a „kockázat mértékének megfelelő szintű adatbiztonságra” és a „biztonság megfelelő szintjére” való hivatkozás arról tanúskodik, hogy e rendelet kockázatkezelési rendszert vezet be, és egyáltalán nem kívánja megszüntetni a személyes adatok megsértésének kockázatát.

30 Így az általános adatvédelmi rendelet 24. és 32. cikkének szövegéből kitűnik, hogy e rendelkezések annak előírására szorítkoznak, hogy az adatkezelő olyan technikai és szervezési intézkedéseket fogadjon el, amelyek célja a személyes adatok megsértésének a lehető legnagyobb mértékben történő elkerülése. Az ilyen intézkedések megfelelőségét konkrétan kell értékelni, megvizsgálva, hogy ezen intézkedéseket e adatkezelő hajtotta-e végre, figyelembe véve az említett cikkekben szereplő különböző kritériumokat, az érintett adatkezeléshez konkrétan kapcsolódó adatvédelmi szükségleteket, valamint az érintett adatkezelésből eredő kockázatokat.

31 Következésképpen az általános adatvédelmi rendelet 24. és 32. cikkét nem lehet úgy értelmezni, hogy a személyes adatok jogosulatlan közlése vagy az ilyen adatokhoz való, harmadik személy általi jogosulatlan hozzáférés anélkül is elegendő annak megállapításához, hogy az érintett adatkezelő által elfogadott intézkedések nem voltak e rendelkezések értelmében megfelelőek, hogy lehetővé tennék az utóbbi adatkezelő számára az ellenkező bizonyítását.

32 Ez az értelmezés annál is inkább érvényes, mivel az általános adatvédelmi rendelet 24. cikke kifejezetten előírja, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy az általa végrehajtott intézkedések megfelelnek e rendeletnek, amely lehetőséget a megdönthetetlen vélelem alkalmazása esetén elveszítené.

33 Másodszor, rendszertani és teleologikus tényezők megerősítik az általános adatvédelmi rendelet 24. és 32. cikkének ezen értelmezését.

34 Ami egyrészt azt a szövegkörnyezetet illeti, amelybe e két cikk illeszkedik, meg kell állapítani, hogy az általános adatvédelmi rendelet 5. cikkének (2) bekezdéséből kitűnik, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy tiszteletben tartotta a személyes adatok kezelésére vonatkozó, az említett cikk (1) bekezdésében rögzített elveket. E kötelezettséget megismétli és pontosítja e rendelet 24. cikkének (1) és (3) bekezdése, valamint 32. cikkének (3) bekezdése az adatkezelő által végzett adatkezelés során az ilyen adatok védelmét szolgáló technikai és szervezési intézkedések végrehajtására vonatkozó kötelezettséget illetően. Márpedig az ezen intézkedések megfelelőségének bizonyítására vonatkozó ilyen kötelezettségnek nem lenne értelme, ha az adatkezelő köteles lenne az említett adatok valamennyi megsértését megakadályozni.

35 Ezenkívül az általános adatvédelmi rendelet (74) preambulumbekezdése hangsúlyozza, hogy 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, az alkalmazott intézkedések hatékonyságát is beleértve, és e tevékenységeknek figyelembe kell venniük a szóban forgó adatkezelés jellemzőivel és az általa jelentett kockázattal kapcsolatos kritériumokat, amelyeket szintén a rendelet fenti 24. és 32. cikke határoz meg.

36 Hasonlóképpen, e rendelet (76) preambulumbekezdése szerint a kockázat valószínűsége és súlyossága az adatkezelés sajátosságaitól függ, és a kockázatot objektív értékelés alapján kell felmérni.

37 Egyébiránt az általános adatvédelmi rendelet 82. cikkének (2) és (3) bekezdéséből az következik, hogy bár az adatkezelő felelős az e rendeletet sértő adatkezelés által okozott kárért, mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

38 Másrészt, a jelen ítélet 31. pontjában kifejtett értelmezést az általános adatvédelmi rendelet (83) preambulumbekezdése is alátámasztja, amelynek első mondata kimondja, hogy „[a] biztonság fenntartása és az e rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket […] alkalmaz”. Ezzel az uniós jogalkotó kinyilvánította azon szándékát, hogy „csökkentse” a személyes adatok megsértésének kockázatait, anélkül hogy azt állította volna, hogy azok kiküszöbölhetők.

39 A fenti indokokra tekintettel az első kérdésre azt a választ kell adni, hogy az általános adatvédelmi rendelet 24. és 32. cikkét úgy kell értelmezni, hogy a személyes adatok jogosulatlan közlése vagy az ilyen adatokhoz az e rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” általi jogosulatlan hozzáférés önmagában nem elegendő annak megállapításához, hogy a szóban forgó adatkezelő által végrehajtott technikai és szervezési intézkedések nem voltak e 24. és 32. cikk értelmében véve „megfelelőek”.

A második kérdésről

40 Második kérdésével a kérdést előterjesztő bíróság lényegében arra vár választ, hogy az általános adatvédelmi rendelet 32. cikkét úgy kell-e értelmezni, hogy az adatkezelő által e cikk alapján végrehajtott technikai és szervezési intézkedések megfelelőségét a nemzeti bíróságoknak konkrétan kell vizsgálniuk, többek között figyelembe véve az érintett adatkezeléshez kapcsolódó kockázatokat.

41 E tekintetben emlékeztetni kell arra, hogy amint az első kérdés megválaszolása során kiemelésre került, az általános adatvédelmi rendelet 32. cikke megköveteli, hogy az adott esettől függően az adatkezelő és az adatfeldolgozó – az e cikk (1) bekezdésében szereplő értékelési szempontok figyelembevételével – megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Ezenkívül e cikk (2) bekezdése példálózó jelleggel felsorol néhány olyan tényezőt, amely releváns az érintett adatkezelés által jelentett kockázatra tekintettel biztosítandó adatbiztonság megfelelő szintjének értékelése során.

42 Az említett 32. cikk (1) és (2) bekezdéséből következik, hogy az ilyen műszaki és szervezési intézkedések megfelelőségét két lépésben kell értékelni. Egyrészt azonosítani kell a személyes adatok megsértésének az érintett adatkezelésből eredő kockázatait, valamint azoknak a természetes személyek jogaira és szabadságaira gyakorolt esetleges következményeit. Ezt az értékelést konkrét módon, az azonosított kockázatok valószínűségi és súlyossági fokának figyelembevételével kell elvégezni. Másrészt meg kell vizsgálni, hogy az adatkezelő által végrehajtott intézkedések igazodnak-e ezen kockázatokhoz, figyelembe véve a tudomány és technológia állását, a megvalósítás költségeit, valamint a fenti adatkezelés jellegét, hatókörét, körülményeit és céljait.

43 Kétségtelen, hogy az adatkezelő bizonyos mérlegelési mozgástérrel rendelkezik a kockázatnak megfelelő adatbiztonsági szint biztosítása érdekében végrehajtandó megfelelő technikai és szervezési intézkedések meghatározását illetően, amint azt az általános adatvédelmi rendelet 32. cikkének (1) bekezdése megköveteli. Ugyanakkor a nemzeti bíróságnak lehetőséggel kell rendelkeznie arra, hogy értékelje az adatkezelő által elvégzett összetett elemzést, és ennek során megbizonyosodjon arról, hogy az utóbbi által elfogadott intézkedések alkalmasak-e az ilyen szintű adatbiztonság biztosítására.

44 Ez az értelmezés egyébiránt biztosítja egyrészt a személyes adatok védelmének hatékonyságát, amelyet e rendelet (11) és (74) preambulumbekezdése hangsúlyoz, másrészt pedig az adatkezelővel szembeni hatékony bírósági jogorvoslathoz való jogot, amelyet az említett rendelet (4) preambulumbekezdésével összefüggésben értelmezett 79. cikkének (1) bekezdése részesít védelemben.

45 Következésképpen az általános adatvédelmi rendelet 32. cikke alapján végrehajtott technikai és szervezési intézkedések megfelelőségének felülvizsgálata érdekében a nemzeti bíróságnak nem annak megállapítására kell szorítkoznia, hogy az érintett adatkezelő milyen módon kívánt eleget tenni az e cikkből eredő kötelezettségeinek, hanem ezen intézkedéseket érdemben meg kell vizsgálnia az említett cikkben említett valamennyi szempontra, valamint az adott ügy sajátos körülményeire és a fenti bíróságnak ezzel kapcsolatban rendelkezésére álló bizonyítékokra tekintettel.

46 Az ilyen vizsgálathoz az adatkezelő által végrehajtott intézkedések jellegének és tartalmának, az ezen intézkedések alkalmazása módjának és az ezen intézkedések által biztosítandó adatbiztonsági szintre gyakorolt gyakorlati hatásainak konkrét elemzése szükséges, figyelembe véve az ezen adatkezeléssel járó kockázatokat.

47 Következésképpen a második kérdésre azt a választ kell adni, hogy az általános adatvédelmi rendelet 32. cikkét úgy kell értelmezni, hogy az adatkezelő által e cikk alapján végrehajtott technikai és szervezési intézkedések megfelelőségét a nemzeti bíróságoknak konkrétan kell vizsgálniuk, ennek során figyelembe kell venniük az érintett adatkezeléshez kapcsolódó kockázatokat, és értékelniük kell, hogy ezen intézkedések jellege, tartalma és végrehajtása igazodik-e a fenti kockázatokhoz.

A harmadik kérdésről

A harmadik kérdés első részéről

48 Harmadik kérdésének első részével a kérdést előterjesztő bíróság lényegében arra vár választ, hogy az adatkezelő felelősségének az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében kimondott és az általános adatvédelmi rendelet 24. cikkében pontosított elvét úgy kell-e értelmezni, hogy az e rendelet 82. cikkén alapuló kártérítési kereset keretében az érintett adatkezelőt terheli annak bizonyítása, hogy az általa az említett rendelet 32. cikke alapján végrehajtott adatbiztonsági intézkedések megfelelőek voltak.

49 E tekintetben először is emlékeztetni kell arra, hogy az általános adatvédelmi rendelet 5. cikkének (2) bekezdése rögzíti a felelősség elvét, amelynek értelmében az adatkezelő felel a személyes adatok kezelésére vonatkozó, e cikk (1) bekezdésében meghatározott elvek betartásáért, és előírja, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy ezen elveket tiszteletben tartotta.

50 Közelebbről, az adatkezelőnek – az e rendelet 5. cikke (1) bekezdésének f) pontjában foglalt, a személyes adatok integritása és bizalmas jellege elvének megfelelően – az ilyen adatok kezelését úgy kell végeznie, hogy megfelelő technikai vagy szervezési intézkedések révén biztosítva legyen azok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve, és képesnek kell lennie annak bizonyítására, hogy ezen elvet tiszteletben tartották.

51 Arra is rá kell mutatni, hogy mind az általános adatvédelmi rendelet (74) preambulumbekezdésének fényében értelmezett 24. cikkének (1) bekezdése, mind pedig e rendelet 32. cikkének (1) bekezdése arra kötelezi az adatkezelőt, hogy a személyes adatok általa vagy a nevében végzett kezelése tekintetében megfelelő műszaki és szervezési intézkedéseket hajtson végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik.

52 Az általános adatvédelmi rendelet 5. cikke (2) bekezdésének, 24. cikke (1) bekezdésének és 32. cikke (1) bekezdésének szövegéből egyértelműen kitűnik, hogy az érintett adatkezelőre hárul annak bizonyítása, hogy a személyes adatok kezelését úgy végzi, hogy annak során az e rendelet 5. cikke (1) bekezdésének f) pontja és 32. cikke értelmében véve biztosítva van ezen adatok megfelelő biztonsága (lásd analógia útján: 2023. május 4-i Bundesrepublik Deutschland

[Elektronikus igazságügyi fiók] ítélet, C-60/22, EU:C:2023:373, 52. és 53. pont; 2023. július 4-i Meta Platforms és társai [Közösségi hálózat általános felhasználási feltételei] ítélet, C-252/21, EU:C:2023:537, 95. pont).

53 E három cikk tehát általánosan alkalmazandó szabályt tartalmaz, amelyet az általános adatvédelmi rendelet ellentétes rendelkezése hiányában az e rendelet 82. cikkén alapuló kártérítési kereset keretében is alkalmazni kell.

54 Másodszor meg kell állapítani, hogy a fenti szó szerinti értelmezés az általános adatvédelmi rendelet által követett célok figyelembevétele folytán is megerősítést nyer.

55 Egyrészt, mivel az általános adatvédelmi rendeletben említett adatvédelmi szint a személyes adatok kezelői által elfogadott biztonsági intézkedésektől függ, az adatkezelőket, tekintettel arra, hogy rájuk hárul ezen intézkedések megfelelőségének bizonyítása, arra kell ösztönözni, hogy mindent megtegyenek annak megakadályozása érdekében, hogy az e rendeletnek nem megfelelő adatkezelési műveletekre kerüljön sor.

56 Másrészt, ha úgy kellene tekinteni, hogy az említett intézkedések megfelelőségére vonatkozó bizonyítási teher az általános adatvédelmi rendelet 4. cikkének 1. pontjában meghatározott érintettekre hárul, ebből az következne, hogy az e rendelet 82. cikkének (1) bekezdésében előírt kártérítéshez való jog jelentős részben elveszítené hatékony érvényesülését, jóllehet az uniós jogalkotó – amint azt e rendelet (11) preambulumbekezdése említi – mind e személyek jogait, mind pedig az adatkezelők kötelezettségeit meg kívánta erősíteni e rendelet korábbi rendelkezéseihez képest.

57 A harmadik kérdés első részére tehát azt a választ kell adni, hogy az adatkezelő felelősségének az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében kimondott és az általános adatvédelmi rendelet 24. cikkében pontosított elvét úgy kell értelmezni, hogy az e rendelet 82. cikkén alapuló kártérítési kereset keretében az érintett adatkezelőt terheli annak bizonyítása, hogy az általa az említett rendelet 32. cikke alapján végrehajtott adatbiztonsági intézkedések megfelelőek voltak.

A harmadik kérdés második részéről

58 Harmadik kérdésének második részével a kérdést előterjesztő bíróság lényegében arra keresi a választ, hogy az általános adatvédelmi rendelet 32. cikkét és az uniós jog tényleges érvényesülésének elvét úgy kell-e értelmezni, hogy az adatkezelő által e cikk alapján végrehajtott biztonsági intézkedések megfelelőségének értékelése céljából az igazságügyi szakértői vélemény szükséges és elégséges bizonyítéknak minősül.

59 E tekintetben emlékeztetni kell arra, hogy az állandó ítélkezési gyakorlat szerint az adott területre vonatkozó uniós szabályozás hiányában a jogalanyok számára biztosított jogok védelmének garantálására irányuló bírósági felülvizsgálatra vonatkozó eljárási szabályok meghozatala az eljárási autonómia elve alapján az egyes tagállamok belső jogrendjére tartozik, azzal a feltétellel azonban, hogy e szabályok 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) (2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 53. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

60 A jelen ügyben meg kell állapítani, hogy az általános adatvédelmi rendelet nem ír elő az igazságügyi szakértői véleményhez hasonló bizonyíték elfogadására és bizonyító erejére vonatkozó olyan szabályokat, amelyeket az e rendelet 82. cikkén alapuló kártérítési keresetet elbíráló és az e rendelet 32. cikkére tekintettel az érintett adatkezelő által végrehajtott biztonsági intézkedések megfelelőségének értékeléséért felelős nemzeti bíróságoknak alkalmazniuk kell. Következésképpen a jelen ítélet előző pontjában felidézetteknek megfelelően és erre vonatkozó uniós jogszabályok hiányában az egyes tagállamok belső jogrendjének kell a jogalanyok e 82. cikkből eredő jogainak védelmére irányuló keresetek részletes szabályait meghatározni, és különösen a bizonyítási eszközökre vonatkozó azon szabályokat, amelyek az ilyen intézkedések megfelelőségének ezen összefüggésben való értékelését, az egyenértékűség és a tényleges érvényesülés fent említett elvének tiszteletben tartása mellett lehetővé teszik (lásd analógia útján: 2022. június 21-i Ligue des droits humains ítélet, C-817/19, EU:C:2022:491, 297. pont; 2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 54. pont).

61 A jelen eljárásban a Bíróság nem rendelkezik olyan információval, amely kétséget ébresztene az egyenértékűség elvének tiszteletben tartását illetően. Más a helyzet a tényleges érvényesülés elvével való összeegyeztethetőséget illetően, mivel a harmadik kérdés második részének szövege az igazságügyi szakértői vélemény beszerzését „szükséges és elégséges bizonyítási eszközként” említi.

62 Különösen sértheti a tényleges érvényesülés elvét az olyan nemzeti eljárási szabály, amelynek értelmében szisztematikusan „szükséges”, hogy a nemzeti bíróságok igazságügyi szakértői vélemény beszerzését rendeljék el. Az ilyen szakértői vélemény szisztematikus igénybevétele ugyanis feleslegesnek bizonyulhat az eljáró bíróság rendelkezésére álló egyéb bizonyítékokra, különösen – amint azt a bolgár kormány az írásbeli észrevételeiben jelezte – a személyes adatok védelmére vonatkozó intézkedések tiszteletben tartásának egy független és törvény által létrehozott hatóság általi ellenőrzésének eredményeire tekintettel, amennyiben e felülvizsgálat újabb keletű, mivel az említett intézkedéseket az általános adatvédelmi rendelet 24. cikkének (1) bekezdése értelmében szükség esetén felül kell vizsgálni és naprakésszé kell tenni.

63 Ezenkívül, amint arra az Európai Bizottság az írásbeli észrevételeiben rámutatott, a tényleges érvényesülés elve sérülhet, ha az „elégséges” kifejezést úgy kell érteni, mint amely annyit tesz, hogy a nemzeti bíróságnak kizárólag vagy automatikusan igaszságügyi szakértői véleményből kell arra vonatkozó következtetést levonnia, hogy az érintett adatkezelő által végrehajtott adatbiztonsági intézkedések az általános adatvédelmi rendelet 32. cikke értelmében „megfelelőek”. Márpedig az e rendelet által biztosított jogok védelme, amely elérésének eszköze az említett tényleges érvényesülés elve, és különösen az e rendelet 79. cikkének (1) bekezdésében biztosított, az adatkezelővel szembeni hatékony bírósági jogorvoslathoz való jog, megköveteli, hogy pártatlan bíróság az érintett intézkedések megfelelőségét objektív módon értékelje, ahelyett hogy ilyen következtetésre szorítkozna (lásd ebben az értelemben: 2023. január 12-i Nemzeti Adatvédelmi és Információszabadság Hatóság ítélet, C-132/21, EU:C:2023:2, 50. pont).

64 A fenti indokokra tekintettel a harmadik kérdés második részére azt a választ kell adni, hogy az általános adatvédelmi rendelet 32. cikkét és az uniós jog tényleges érvényesülésének elvét úgy kell értelmezni, hogy az adatkezelő által e cikk alapján végrehajtott adatbiztonsági intézkedések megfelelőségének értékelése céljából az igazságügyi szakértői vélemény nem tekinthető szisztematikusan szükséges és elégséges bizonyítéknak.

A negyedik kérdésről

65 Negyedik kérdésével a kérdést előterjesztő bíróság lényegében arra vár választ, hogy az általános adatvédelmi rendelet 82. cikkének (3) bekezdését úgy kell-e értelmezni, hogy az adatkezelő mentesülhet a valamely személy által elszenvedett kár megtérítésének e rendelet 82. cikkének (1) és (2) bekezdésében előírt kötelezettsége alól kizárólag azon az alapon, hogy e kár a személyes adatok jogosulatlan közléséből vagy az ilyen adatokhoz az említett rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” általi jogosulatlan hozzáférésből ered.

66 Elöljáróban pontosítani kell, hogy az általános adatvédelmi rendelet 4. cikkének 10. pontjából az következik, hogy „harmadik személynek” minősülnek többek között azok a személyek, akik nem azonosak azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak. Ez a meghatározás olyan személyekre terjed ki, akik nem az adatkezelő alkalmazottai, és nem állnak az adatkezelő ellenőrzése alatt, azaz olyanokra, mint akiket az előterjesztett kérdés említ.

67 Ezt követően először is emlékeztetni kell arra, hogy az általános adatvédelmi rendelet 82. cikkének (2) bekezdése úgy rendelkezik, hogy „[az] adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet az e rendeletet sértő adatkezelés okozott”, és hogy e cikk (3) bekezdése úgy rendelkezik, hogy az adott esettől függően az adatkezelő vagy az adatfeldolgozó mentesül e felelősség alól, „ha bizonyítja, hogy a kár bekövetkeztéért őt semmilyen felelősség nem terheli”.

68 Ezenkívül az általános adatvédelmi rendelet (146) preambulumbekezdése, amely kifejezetten annak 82. cikkéhez kapcsolódik, első és második mondatában kimondja, hogy „[az] adatkezelő vagy az adatfeldolgozó az e rendeletet sértő adatkezelés miatt okozott kárt köteles megtéríteni”, és „[őt] a kártérítési kötelezettség alól abban az esetben mentesíteni kell, ha bizonyítja, hogy a kár bekövetkeztéért őt semmilyen felelősség nem terheli”.

69 E rendelkezésekből egyrészt az következik, hogy az érintett adatkezelőnek főszabály szerint meg kell térítenie az e rendelet ezen adatkezeléssel összefüggésben történő megsértésével okozott kárt, másrészt pedig az, hogy csak akkor mentesülhet a felelősség alól, ha bizonyítja, hogy az e kárt okozó esemény bekövetkeztéért őt semmilyen felelősség nem terheli.

70 Így, amint azt a „semmilyen” melléknévnek a jogalkotási eljárás során történő, szándékolt hozzáadása jelzi, azokat a körülményeket, amelyek között az adatkezelő az általános adatvédelmi rendelet 82. cikke alapján fennálló polgári jogi felelősség alóli mentesülésre hivatkozhat, szigorúan azokra a körülményekre kell korlátozni, amelyekben az adatkezelő bizonyítani tudja, hogy a kár nem tudható be neki.

71 Amennyiben, mint a jelen ügyben is, a személyes adatoknak az általános adatvédelmi rendelet 4. cikkének 12. pontja értelmében vett megsértését kiberbűnözők, tehát az e rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” követték el, e jogsértés nem tudható be az adatkezelőnek, kivéve ha ez utóbbi az említett jogsértést az általános adatvédelmi rendeletben előírt valamely kötelezettség, különösen az őt az ugyanezen rendelet 5. cikke (1) bekezdésének f) pontja, valamint 24. és 32. cikke alapján terhelő adatvédelmi kötelezettség megsértésével tette lehetővé.

72 Így a személyes adatok harmadik fél általi megsértése esetén az adatkezelő az általános adatvédelmi rendelet 82. cikkének (3) bekezdése alapján mentesülhet a felelőssége alól annak bizonyításával, hogy nincs okozati összefüggés az adatvédelmi kötelezettség esetleges megsértése és a természetes személy által elszenvedett kár között.

73 Másodszor, az e 82. cikk (3) bekezdésének fenti értelmezése megfelel az általános adatvédelmi rendelet azon célkitűzésének is, amely a személyes adataik kezelése tekintetében természetes személyek magas szintű védelmének biztosítására irányul, és amelyet e rendelet (10) és (11) preambulumbekezdése mond ki.

74 E megfontolások összességére tekintettel a negyedik kérdésre azt a választ kell adni, hogy az általános adatvédelmi rendelet 82. cikkének (3) bekezdését úgy kell értelmezni, hogy az adatkezelő nem mentesülhet a valamely személy által elszenvedett kár megtérítésének e rendelet 82. cikkének (1) és (2) bekezdésében előírt kötelezettsége alól kizárólag azon az alapon, hogy e kár a személyes adatok jogosulatlan közléséből vagy az ilyen adatokhoz az említett rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” általi jogosulatlan hozzáférésből ered, hanem ezen adatkezelőnek ilyen esetben bizonyítania kell, hogy a vonatkozó kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

Az ötödik kérdésről

75 Ötödik kérdésével a kérdést előterjesztő bíróság lényegében arra vár választ, hogy az általános adatvédelmi rendelet 82. cikkének (1) bekezdését úgy kell-e értelmezni, hogy a személyes adatainak harmadik személyek általi esetleges visszaélésszerű felhasználásától való félelem, amelyet az érintett e rendelet megsértése folytán érez, önmagában az e rendelkezés értelmében vett „nem vagyoni kárnak” minősülhet.

76 Ami először is az általános adatvédelmi rendelet 82. cikke (1) bekezdésének szövegét illeti, meg kell jegyezni, hogy az előírja, hogy „[m]inden olyan személy, aki e rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult”.

77 E tekintetben a Bíróság rámutatott, hogy az általános adatvédelmi rendelet 82. cikke (1) bekezdésének szövegéből világosan kiderül, hogy a „kár” vagy az „elszenvedett kár” megléte az említett rendelkezésben említett kártérítéshez való jog egyik feltételét képezi, akárcsak az általános adatvédelmi rendelet megsértésének fennállása, valamint az e kár és az e jogsértés közötti okozati kapcsolat megléte, mivel e három feltétel együttes feltétel (2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 32. pont).

78 Egyébiránt a Bíróság mind nyelvtani, mind rendszertani, mind pedig teleologikus jellegű megfontolásokra támaszkodva úgy értelmezte az általános adatvédelmi rendelet 82. cikkének (1) bekezdését, hogy azzal ellentétes az olyan nemzeti szabály vagy gyakorlat, amely az e rendelkezés értelmében vett „nem vagyoni kár” megtérítését annak a feltételnek rendeli alá, hogy az érintett által elszenvedett kárnak el kell érnie egy bizonyos súlyossági küszöböt (2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 51. pont).

79 Ennek felidézését követően a jelen ügyben hangsúlyozni kell, hogy az általános adatvédelmi rendelet 82. cikkének (1) bekezdése nem tesz különbséget azon esetek között, amikor e rendelet rendelkezéseinek bizonyított megsértését követően az érintett által állított „nem vagyoni kár” egyrészt a személyes adatainak harmadik személyek általi olyan visszaélésszerű felhasználásához kapcsolódik, amely a kártérítés iránti kérelmének időpontjában már bekövetkezett, vagy másrészt ahhoz az e személy által érzett félelemhez, hogy a jövőben ilyen felhasználásra sor kerülhet.

80 Ennélfogva az általános adatvédelmi rendelet 82. cikke (1) bekezdésének szövege nem zárja ki, hogy az e rendelkezésben szereplő „nem vagyoni kár” fogalma magában foglalja a kérdést előterjesztő bíróság által említetthez hasonló helyzetet, amikor az érintett az e rendelkezés alapján történő kártérítés érdekében az attól való félelmére hivatkozik, hogy a személyes adatait harmadik személyek a jövőben e rendelet megsértése folytán visszaélésszerűen felhasználják.

81 E szó szerinti értelmezést másodszor megerősíti az általános adatvédelmi rendelet (146) preambulumbekezdése, amely kifejezetten az e rendelet 82. cikkének (1) bekezdésében előírt kártérítéshez való jogra vonatkozik, és harmadik mondatában megemlíti, hogy „[a] kár fogalmát a Bíróság ítélkezési gyakorlatának fényében tágan kell értelmezni, mégpedig oly módon, hogy az teljes mértékben tükrözze e rendelet célkitűzéseit”. Márpedig a „nem vagyoni kár” e 82. cikk (1) bekezdése értelmében vett fogalmának olyan értelmezése, amely nem foglalja magában azokat a helyzeteket, amikor az említett rendelet megsértésével érintett személy az azzal kapcsolatos félelmére hivatkozik, hogy a saját személyes adatait a jövőben visszaélésszerűen felhasználják, nem felel meg e fogalom uniós jogalkotó által követett tág értelmezésének (lásd analógia útján: 2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 37. és 46. pont).

82 Egyébiránt az általános adatvédelmi rendelet (85) preambulumbekezdésének első mondata kimondja, hogy „[a]z adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, […] illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt”. Az érintettek által esetlegesen elszenvedett „károk” példálózó felsorolásából kitűnik, hogy az uniós jogalkotó e fogalmakba bele kívánta foglalni különösen a saját adataik feletti ellenőrzés e rendelet megsértése folytán történő egyszerű „elvesztését”, még akkor is, ha a szóban forgó adatok visszaélésszerű felhasználása konkrétan nem az említett személyek kárára valósult meg.

83 Harmadszor és utolsósorban, a jelen ítélet 80. pontjában szereplő értelmezést megerősítik az általános adatvédelmi rendelet célkitűzései, amelyeket teljes mértékben figyelembe kell venni a „kár” fogalmának meghatározásakor, amint arra e rendelet (146) preambulumbekezdésének harmadik mondata rámutat. Márpedig az általános adatvédelmi rendelet 82. cikke (1) bekezdésének olyan értelmezése, amely szerint a „nem vagyoni kárnak” az e rendelkezés értelmében vett fogalma nem foglalja magában azokat a helyzeteket, amelyekben az érintett kizárólag azon félelmére hivatkozik, hogy adatait harmadik személyek a jövőben visszaélésszerűen felhasználják, nem egyeztethető össze a személyes adatok Unión belüli kezelése tekintetében a természetes személyek magas szintű védelmének biztosításával, amelyre e jogi aktus irányul.

84 Ugyanakkor hangsúlyozni kell, hogy az általános adatvédelmi rendelet olyan megsértésével érintett személy, akire nézve az hátrányos következményekkel jár, köteles bizonyítani, hogy e következmények az e rendelet 82. cikke értelmében vett nem vagyoni kárt okoznak (lásd ebben az értelemben: 2023. május 4-i Österreichische Post [A személyes adatok kezeléséhez kapcsolódó nem vagyoni kár] ítélet, C-300/21, EU:C:2023:370, 50. pont).

85 Különösen, ha az ezen az alapon kártérítést kérő személy az attól való félelmére hivatkozik, hogy a jövőben az ilyen jogsértés miatt személyes adatainak visszaélésszerű felhasználása következik be, az eljáró nemzeti bíróságnak meg kell vizsgálnia, hogy e félelem az ügy sajátos körülmények között és az érintett személyre tekintettel megalapozottnak tekinthető-e.

86 A fenti indokokra tekintettel az ötödik kérdésre azt a választ kell adni, hogy az általános adatvédelmi rendelet 82. cikkének (1) bekezdését úgy kell értelmezni, hogy a személyes adatainak harmadik személyek általi esetleges visszaélésszerű felhasználásától való félelem, amelyet az érintett e rendelet megsértése folytán érez, önmagában az e rendelkezés értelmében vett „nem vagyoni kárnak” minősülhet.

A költségekről

87 Mivel ez az eljárás az alapeljárásban részt vevő felek számára a kérdést előterjesztő bíróság előtt folyamatban lévő eljárás egy szakaszát képezi, ez a bíróság dönt a költségekről. Az észrevételeknek a Bíróság elé terjesztésével kapcsolatban felmerült költségek, az említett felek költségeinek kivételével, nem téríthetők meg.

A fenti indokok alapján a Bíróság (harmadik tanács) a következőképpen határozott:

1) A természetes személyeknek a személyes adatok kezelése vonatkozásában történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) 24. és 32. cikkét

a következőképpen kell értelmezni:

a személyes adatok jogosulatlan közlése vagy az ilyen adatokhoz az e rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” általi jogosulatlan hozzáférés önmagában nem elegendő annak megállapításához, hogy a szóban forgó adatkezelő által végrehajtott technikai és szervezési intézkedések nem voltak e 24. és 32. cikk értelmében véve „megfelelőek”.

2) A 2016/679 rendelet 32. cikkét

a következőképpen kell értelmezni:

az adatkezelő által e cikk alapján végrehajtott technikai és szervezési intézkedések megfelelőségét a nemzeti bíróságoknak konkrétan kell vizsgálniuk, ennek során figyelembe kell venniük az érintett adatkezeléshez kapcsolódó kockázatokat, és értékelniük kell, hogy ezen intézkedések jellege, tartalma és végrehajtása igazodik-e a fenti kockázatokhoz.

3) Az adatkezelő felelősségének a 2016/679 irányelv 5. cikkének (2) bekezdésében kimondott és e rendelet 24. cikkében pontosított elvét

a következőképpen kell értelmezni:

az e rendelet 82. cikkén alapuló kártérítési kereset keretében az érintett adatkezelőt terheli annak bizonyítása, hogy az általa az említett rendelet 32. cikke alapján végrehajtott adatbiztonsági intézkedések megfelelőek voltak.

4) A 2016/679 rendelet 32. cikkét és az uniós jog tényleges érvényesülésének elvét

a következőképpen kell értelmezni:

az adatkezelő által e cikk alapján végrehajtott adatbiztonsági intézkedések megfelelőségének értékelése céljából az igazságügyi szakértői vélemény nem tekinthető szisztematikusan szükséges és elégséges bizonyítéknak.

5) A 2016/679 irányelv 82. cikkének (3) bekezdését

a következőképpen kell értelmezni:

az adatkezelő nem mentesülhet a valamely személy által elszenvedett kár megtérítésének e rendelet 82. cikkének (1) és (2) bekezdésében előírt kötelezettsége alól kizárólag azon az alapon, hogy e kár a személyes adatok jogosulatlan közléséből vagy az ilyen adatokhoz az említett rendelet 4. cikkének 10. pontja értelmében vett „harmadik személyek” általi jogosulatlan hozzáférésből ered, hanem ezen adatkezelőnek ilyen esetben bizonyítania kell, hogy a vonatkozó kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

6) A 2016/679 irányelv 82. cikkének (1) bekezdését

a következőképpen kell értelmezni:

a személyes adatainak harmadik személyek általi esetleges visszaélésszerű felhasználásától való félelem, amelyet az érintett e rendelet megsértése folytán érez, önmagában az e rendelkezés értelmében vett „nem vagyoni kárnak” minősülhet.

Aláírások