Andor Gál*

The Protection of the Right to Information Self-Determination in the Hungarian Criminal Law

1. Aims of the Paper

The regulation of data protection law in Europe is undergoing a radical change and is up for renewal. Thus, the domestic regulation of the right to information self-determination is (also) directly affected by the data protection reform of the European Union, in the framework of which the European Parliament and the Council, as co-legislators, decided to adopt two EU legislative acts in 2016: the General Data Protection Regulation (hereinafter: GDPR)[1] became applicable from 25 May 2018, while the Directive (EU) 2016/680 (hereinafter: Directive)[2] has been effective from 6 May 2018. Due to the regulative character of the GDPR, it has a direct effect in the national law of the Member States, so it is valid in the Hungarian legal system without transposition.[3] By contrast, the Directive does not have direct effect in the law of the Member States, however its provisions were required to be transposed into national law until 6 May 2018.

Regarding the criminal law protection of personal data, it is worth noting that the GDPR has no unifying effect in this regulatory area, as stated in Preamble-Paragraph (149): "Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice." According to this, after the entry into force of the GDPR the development of criminal data protection rules remains a

* Senior Lecturer, PhD (Institute of Criminal Law and Criminal Science, Faculty of Law, University of Szeged, Hungary); e-mail: andor.gal@juris.u-szeged.hu.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[3] According to the primary reason of the passing of this regulation, that uniform rules can prevent certain large multinationals from carrying out their data management activities in countries which provide them the most favourable rules. See the General Ministerial Reasoning of the Act XXXVIII of 2018.

full competence of the Member States.[4]

On the basis of all this, in order to ensure the proper entry into force of the regulation and the fulfilment of the narrow legislative obligation arising from the GDPR, as well as the transposition of the rules of the Directive, it became necessary to amend new legislation in the Hungarian national law. In this context, the relevant rules of Act C of 2012 on the Criminal Code (hereinafter: CC) have been renewed since 25 May 2018, while the provisions of the code on the protection of personal data[5] were amended only later, with effect from 26 July 2018.

These changes obviously influence the rules of criminal law protection of personal data, as well as the framework of criminal liability. Therefore, the main purpose of this paper is to present the key and current features which determine the regulation on the protection of personal data in the Hungarian criminal law.

First, I am going to define the content of the protected individual interest. In connection with this, I am going to present the certain stages of the development of legal protection, and the current prevailing interpretation of the *ratio legis* of the criminal offence.

In the second step of my examination, I will focus specifically on the circumstances how have been incorporated the new rules of GDPR into the national criminal law.

After that, I will analyse the elements (object, conduct and unlawfulness of the perpetration) of the statutory definition of the crime *"Misuse of personal data"* which is regulated in the Hungarian Criminal Code.

Before drawing my final conclusions, I would like to present a case, which illustrates some of the issues related to the new legal background.

2. Protected Interest

The interest at the centre of the criminal law intervention has an individual nature, because in this case the special purpose of criminal law regulation is to protect the right to information self-determination. The independent existence and regulation of this right is the result of the legal development generated by the quick technological and social transformation of our

[4] With regard to criminal sanctions to address data protection wrongs, nothing has changed: member states can choose to create them or not. DE HEART, Paul: "The EU data protection reform and the (forgotten) use of criminal sanctions." *International Data Privacy Law*, 2014/4. p. 262. For an explanation of the relationship between the GDPR and the application of criminal sanctions, see SZABÓ, Endre Győző: „Az adatvédelmi bírságról – GDPR szabályainak elemzése" ["About the Administrative Fines –Analysis of the Rules of GDPR"] *Alkotmánybírósági Szemle [Journal of the Constitutional Court]*, 2018/2. p. 35.

[5] Act CXII of 2011 on the Right to Information Self-Determination and on Freedom of Information (hereinafter: Info. Act).

society.[6]

In the Hungarian law system, we can distinguish between three different development stages of data protection law.

2.1. Initial Stage: protection of personal data as a personal secret

Prior to the 1970s, the need for a personal secret within the framework of general personality law arose. Thus, the development of legal protection of private secrets can be regarded as a precursor to the protection of personal data, because before the spread of automated processing of data the subject matter of the regulation was limited to secrets.[7]

2.2. First Generation of Data Protection Law: protection the natural person from the information databases

However, with the advancement of information technology, it has been possible to automate the processing of data in standardized records, which has also necessitated the independent protection of individual, otherwise not confidential facts. The so defined law primarily had a protective function: the so-called first-generation data protection laws primarily protected citizens from computerized records.[8] The weakness of this solution was that the right was necessarily granted by the state, although it was the state that posed the greatest threat to the exercise of these rights.[9]

2.3. Second Generation of Data Protection Law: acknowledgement of the right to information self-determination

Second-generation data protection regulations in the 1990s have reformed the content of the law by not only treating it as a right of protection, but by adding active rights to it.[10] The

[6] For a detailed presentation, see SZŐKE, Gergely László: „Az adatvédelem szabályozásának történeti áttekintése" ["Historical Overview of Data Protection Regulation"] *Infokommunikáció és jog [Journal of Infocommunication and Law]*, 2013/3. pp. 107-112.

[7] JÓRI, András: „59. § [A magánszférajogok]" {„§ 59 [Privacy Rights]} In: Jakab, András (ed.): *Az Alkotmány kommentárja II [Commentary of the Constitution II]*. Századvég, Budapest, 2009. p. 2176.

[8] MAJTÉNYI, László: „Az információs jogok" ["Informational Rights"]. In: Halmai, Gábor – Tóth, Gábor Attila (ed.): Emberi jogok [Human Rights]. Osiris, Budapest, 2006. p. 582.

[9] MAJTÉNYI, László: *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága [Freedoms of Information. Data Protection and Access to Information of Public Interest]*. Complex, Budapest, 2006. p. 118.

[10] The starting point for this was the so-called "census resolution" of the German Constitutional Court from 1983, which explicitly acknowledged the existence of the right to information self-determination. See JÓRI, András:

technological change of this era would have made the regulation of technology hopeless: the legislator, therefore, instead of regulating technology, has armed the individual with the active right to information self-determination.[11]

In the 1990s, the Constitutional Court played a key role in the recognition of the right to information self-determination in Hungary.[12] The Court emphasized: "The right to the protection of personal data is not interpreted as a traditional right of protection, but also – taking into account its active side – as a right of information self-determination."[13] As regards the content of the right, the Court stated that "[…] the essence of the right to information self-determination is that the data subject can know and follow the way and circumstances of the use of his or her personal data, first of all the state must ensure the preconditions of exercising this right."[14]

2.4. Conclusion

Based on all this, the fundamental right to the protection of personal data is to be understood as the right to self-determination of information, where the data is not the property of the right holder, but has the right to have disposal of such data.[15] From a criminal law perspective, it should be noted, that this right is primarily exercised in a negative sense, meaning that everyone has to refrain from processing data in the absence of a proper legal basis.

3. Criminal Offence of Misuse of Personal Data

In Hungary, the first act of data protection was come into force in 1993.[16] At that time, the legislator is so considered, that it is necessary to create "high and comprehensive" legislation,

Adatvédelmi kézikönyv [Handbook of Personal Data Protection Law]. Osiris, Budapest, 2005. pp. 24-25.

[11] JÓRI (Fn. 10.) p. 27.

[12] See SÓLYOM, László: *Az alkotmánybíráskodás kezdetei Magyarországon [The Beginning of the Jurisdiction of the Constitutional Court in Hungary]*. Osiris, Budapest, 2001. pp. 463-464.

[13] This decision of the Constitutional Court can be considered as a direct antecedent of the first Hungarian data protection law. As the decision rules: "It is the duty of the legislator to enact a law on the protection of personal data and access to information of public interest in accordance with Articles 59 and 61 of the Constitution, and to ensure that these principles are guaranteed in area-specific laws, too." Decision 15/1991. (IV. 13.) of the Constitutional Court.

[14] Decision 15/1991. (IV. 13.) of the Constitutional Court.

[15] In his monograph published in 1983, László SÓLYOM pointed out that in the process of development of the right of personality, its separation from the legal definition of property, and its shift towards autonomy are the decisive moments. As a result, it is possible for special personality rights to flourish. In doing so, the author acknowledged the possibility of establishing the right to information self-determination. SÓLYOM, László: *A személyiségi jogok elmélete [The Theory of Personality Rights]*. Közgazdasági és Jogi Könyvkiadó, Budapest, 1983. p. 306.

[16] Act LXIII of 1993 on the Protection of Personal Data and the Disclosure of Information of Public Interest

which covers all relevant elements of data management. According to MAJTÉNYI, the basis of this legal policy approach was the prominent role of information rights in the "bloodless Hungarian rule of law revolution".[17] Accordingly, the *per se* protection of personal data has been established simultaneously in the Hungarian criminal law.

The current criminal law protection of personal data is based on the statutory definition of the so-called criminal offence of "Misuse of personal data". The text of the statutory definition as follows:

"Misuse of personal data

Section 219 (1) A person who, by violating a provision laid down in an Act or a binding legal act of the European Union on the protection or processing of personal data and for financial gain or causing significant harm to interests,

a) processes personal data in an unauthorised manner or in deviation from the purpose of processing, or

b) fails to take measures to safeguard such data

is guilty of a misdemeanour and shall be punished by imprisonment for up to one year.

(2) A person who, by violating a provision laid down in an Act or a binding legal act of the European Union on the protection or processing of personal data, fails to perform his obligation to provide information that is necessary for the data subject to exercise his right of access and, as a result, causes significant harm to the interests of one or more other persons, shall be punished under paragraph (1).

(3) The punishment shall be imprisonment for up to two years, if the misuse of personal data is committed concerning sensitive data or criminal personal data.

(4) The perpetrator is guilty of a felony and shall be punished by imprisonment for up to three years, if the misuse of personal data is committed by a public officer or by abusing a public mandate."

This statutory definition is a so-called framework disposition,[18] the content of which are fulfilled with the binding legal instrument of the European Union, if the material scope of the GDPR in the case of the specific data processing is given. In other cases, the application of

[17] MAJTÉNYI (Fn. 8.) p. 578.

[18] By adopting HOLLÁN's definition, it can be stated that, framework dispositions include those criminal provisions which define the scope of conduct to be punished by reference to a legal norm specified in other legislation. HOLLÁN, Miklós: „A nemzeti büntetőjog keretényállásai és az uniós jog" ["The Framework Dispositions of the National Criminal Law and the European Law"] *Miskolci Jogi Szemle [University of Miskolc Law Journal],* 2018/2. pp. 19–20.

national law arises.

Thus, in the greatest number of cases the elements of the statutory definition can be only interpreted through the enforcement of the GDPR. However, in the case of data processing excluded from the material scope of the GDPR, the relevant legal rules are defined by Info. Act as a subsidiary legal statute. For example, the GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. In comparison, the applicability of the rules of the GDPR to manual data processing is created just by the Hungarian national law [Info. Act Section 2, Para (4)].

In addition, from the view of the lawfulness of data processing sectoral data protection regulations may become relevant.[19]

A GDPR területi hatályát a származási ország, illetve a célzott hatás elvei alapozhatják meg. Előbbi szerint a rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel[20] rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem [5. cikk (1) bek.].[21] A célzott hatás elve alapján a rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:

- áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért,
- az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó [GDPR 3. cikk (2) bek.].

Hangsúlyozni szükséges, hogy a GDPR területi hatályának megléte nem jelenti automatikusan azt, hogy az adott adatkezelés esetében a Btk. területi-személyi hatálya is fennáll. Utóbbi

[19] As an example see Act XLVII of 1997 on the Processing and Protection of Data Concerning Health and of Related Data.

[20] Ezen ismérvet az ún. Weltimmo-ügyben (C-230/14.) az Európai Unió Bírósága is értelmezte. A testület álláspontja szerint e feltétel adott, ha az adatkezelő a tagállam területén tartós jelleggel akár csekély mértékű valós és tényleges tevékenységet fejt ki. Az ügy ismertetésére lásd JÓRI András: „A Fővárosi Közigazgatási és Munkaügyi Bíróság ítélete a Nemzeti Adatvédelmi és Információszabadság Hatóság döntésének hatályon kívül helyezéséről. Az adatvédelem bírói kontrollja” *Jogesetek Magyarázata*, 2013/3. 48-54.

[21] Ehhez lásd BARTÓKI-GÖNCZY Balázs: A felhőalapú szolgáltatások és a személyes adatok védelme az új európai adatvédelmi rendelet tükrében” In: Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* ELTE-ÁJK, Budapest, 2017. 379.

kritériummal összefüggésben a Btk. 3. §-ban meghatározott elvek vizsgálata szükséges. Ennek alapján, ha bármely objektív tényállási elemet megalapozó körülmény (pl. adatkezelés vagy a sértett jelentős érdeksérelme) Magyarországon realizálódik, a Btk. alkalmazható,[22] továbbá az aktív és passzív személyi elv alapján abban az esetben is, ha az elkövető vagy a sértett magyar állampolgár.[23] Ezen felül a büntetőkódex hatályát megalapozhatja az ún. képviseleti elv is [Btk. 3. § (2) bek. a) pont aa) alpont.].

5.2. A tényállás szerkezeti felépítése

A törvényi tényállásnak három alapesete különböztethető meg.[24] A Btk. 219. § (1) bekezdés a) pontja a jogosulatlan adatkezelést *(első alapeset)*, b) pontja az adatbiztonsági mulasztást *(második alapeset)* szabályozza. E változatok esetében a tényállásszerűséghez haszonszerzési célzat fennállta, vagy – alternatív tényállási elemként – az elkövetési magatartásokkal okozati összefüggésben jelentős érdeksérelem kiváltása szükséges. Ezen alakzatok elsősorban a jogszerűség, célhoz kötöttség és adattakarékosság adatvédelmi elvek[25] érvényesülését hivatottak biztosítani, ily módon jellemzően az információs önrendelkezési jog negatív oldalát védik.

A Btk. 219. § (2) bekezdésében meghatározott *harmadik alapeset* a hozzáféréshez való joghoz kapcsolódó tájékoztatási kötelezettség elmulasztását rendeli büntetni. Az alaptényállás dogmatikai természetét tekintve vegyes mulasztás, ahol a tényállás a jelentős érdeksérelmet eredményként szabályozza.

Terjedelmi korlátok okán e dolgozat kizárólag az első alapeset tényállási elemeinek részletesebb vizsgálatát végzi el.

6. Objektív tényállási elemek

6.1. Elkövetési tárgy

A bűncselekmény *elkövetési tárgya* a személyes adat, míg az adat által azonosított vagy

[22] A belföldön való elkövetés tényét a cselekményegység elve alapján szükséges vizsgálni. Lásd NAGY Ferenc: *A magyar büntetőjog általános része.* HVG-Orac, Budapest, 2010. 79.
[23] Vö. Btk. 3. § (1) bek. c) pont és (2) bek. b) pont.
[24] Ugyanígy SZOMORA Zsolt: „Btk. XXI. Fejezet" In: Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvhöz.* Complex, Budapest, 2013. 459.
[25] Lásd GDPR 5. cikk (1) bek. a)-c) pontok.

azonosítható természetes személy a bűncselekmény sértettjének tekinthető.[26] Kiemelendő, hogy csak a természetes személyre vonatkozó adat lehet az elkövetés tárgya, így bűncselekmény nem követhető el szervezet (jogi személy, személyösszesség) vagy elhunyt személy adatával összefüggésben.[27] Lényeges kritérium, hogy a személyes adatnak megszemélyesítettnek kell lennie, vagyis az adatalany és az információ között összefüggésnek kell lennie.

A személyes adat GDPR szerinti fogalom-meghatározásának[28] lényegi eleme, hogy ezen ismérv alapja lehet az érintettel kapcsolatba hozható *bármely információ*. E megfogalmazás nem hagy kétséget afelől, hogy a jogvédelem a személyre vonatkozó állítások valamennyi fajtájára, minden olyan információra kiterjed, amely kötődik az egyénhez, és a helyzetét valamilyen módon befolyásolja vagy befolyásolhatja.[29] Ennek megfelelően az információ lehet szubjektív vagy objektív megítélés eredménye, továbbá a valósággal ellentétes, hamis tartalmú is.[30]

6.2. Elkövetési magatartás

Az első alapeset elkövetési magatartása konjunktív: a jogosulatlan vagy céltól eltérő adatkezelés az adatvédelmi háttérszabályok megsértésével történik. Megjegyezhető, hogy a jogosulatlan adatkezelés önmagában az adatvédelmi szabályok megszegését jelenti, így a tényállásszerűség akkor is fennállhat, ha további adatvédelmi jogsértés a jogosulatlan adatkezeléshez nem kapcsolódik.

Az adatkezelés fogalmát a GDPR a – a személyes adat ismérvéhez hasonlóan – rendkívül széles körűen határozza meg. A normatív értelmezés szerint: „a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett *bármely művelet vagy műveletek összessége*, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy

[26] Így PÉTERFALVI Attila – ESZTERI Dániel: „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata” In: Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* ELTE-ÁJK, Budapest, 2017. 407. Ezzel ellentétes SZOMORA álláspontja, aki szerint a személyes adat eszmei jellegére tekintettel elkövetési tárgynak nem tekinthető. SZOMORA (2013) i.m. 459.

[27] Bővebben lásd JÓRI (2018) i.m. 54-62.

[28] A 4. cikk 1. pontja szerint: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

[29] JÓRI (2018) i.m. 74. OSZTOPÁNI Krisztián: „Alapfogalmak” In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018. 64.

[30] OSZTOPÁNI i.m. 64.

megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés."[31]

Kiemelendő, hogy a meghatározásban rögzített felsorolás exemplifikatív jellegű, így elvben bármely személyes adatra vonatkozó művelet megfelelhet a GDPR fogalmának. Annyi azonban szükségképpen feltétel, hogy az adattal összefüggésben az elkövető valamely tevékenységet fejtsen ki, vagyis az adatnak birtokban tartása még önmagában nem tényállásszerű. Ez a következtetés a bűncselekményi tényállás további tényállási elemeiből adódik: a haszonszerzési cél érvényre juttatására vagy a jelentős érdeksérelem okozására csak a személyes adat megszerzésével vagy birtoklásával még nem nyílhat lehetőség. Ennek hangsúlyozása azért indokolt, mert ismert olyan adatvédelmi gyakorlat, amely az adat közvetlen érzékelését vagy megismerését is már adatkezelésnek tekinti.[32]

Az adatkezelés jogosulatlan jellege a megfelelő jogalap hiányát feltételezi. A jogalapok körét a GDPR 6. cikk (1) bekezdése határozza meg. E rendelkezések végérvényesen szakítanak a magyar adatvédelmi jogban korábban uralkodó duális jogalaprendszerrel, hiszen a rendelet hat különböző jogalaptípust is nevesít. Ehhez képest korábban az adatkezelés jogszerűsége az érintett hozzájárulásán vagy törvényi – kivételesen önkormányzati rendeletben lefektetett – felhatalmazáson alapulhatott.[33]

A jogalapok közül kiemelésre érdemes az ún. érdekmérlegelésen alapuló esetkör. E szerint a személyes adat kezelhető, ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek [GDPR 6. cikk (1) bek. f) pont]. E rendelkezés folytán az adatkezelők feladatává vált annak eldöntése, hogy van-e olyan jogos érdek, amely az adatkezelő vagy harmadik fél jogos érvényesítéséhez oly mértékben szükséges, hogy az az érintett önrendelkezési jogát megelőzi. Ez a jogalap azonban csak a magánszféra adatkezelései esetében releváns, figyelemmel arra, hogy annak alkalmazását a GDPR a közhatalmi szervek működésével összefüggésben kizárja.

6.3. Eredmény

[31] 4. cikk 2. pont

[32] JÓRI (2018) i.m. 89.

[33] Történeti bemutatására lásd JÓRI András: „Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig" *Alkotmánybírósági Szemle*, 2018/1. 16-21.; LIBER Ádám: „A jogos érdeken alapuló adatkezelésről" *Infokommunkáció és jog*, 2012/2. 79-88.

Az első alapeset vagylagos tényállási elemként szabályozott eredménye a jelentős érdeksérelem. Ez az érdeksérelem az információs önrendelkezési jog sérelmétől független, attól elkülönülő, további hátrányt jelent. A kényszerítés (Btk. 195. §) bűncselekményével összefüggő bírósági gyakorlat alapján megállapítható, hogy az érdeksérelem akár magán-, akár közérdek sérelme lehet.[34]

Conclusions

a) The necessity of the criminal intervention is ***justified by the overriding need to protect the individual right to information self-determination***.
b) To broaden the protection of personal data, the GDPR has created ***indefinite legal concepts*** (personal data, data processing etc.) that are ***incompatible with the fundamental requirements (nullum crimen sine lege certa)*** of criminal law.
c) The direct application of data protection law in criminal law enforcement carries with it the risk that ***courts will interpret these specific concepts differently***.
d) The range of legal grounds for data processing has been broadened, so from the view of the lawfulness of the data procession ***the scope of criminal liability has been reduced***.
e) GDPR imposes ***severe financial penalties*** on those who violate data protection rules. My question is:

Does the ultima ratio nature of criminal law prevail at all?

Összegzés

A dolgozatban által bemutatott tényállás-elemzés világossá teszi, hogy az információs önrendelkezési jog büntetőjogi védelme az adatvédelmi szabályok közelmúltban végbement

[34] Ehhez lásd pl. BH1992. 744., BH1995. 257.

változása eredményeként szintén átalakulóban van. A büntetőjogi felelősségre vonás szempontjából kiemelt jelentőséggel bíró egyes adatvédelmi alapfogalmakat illetően megállapítható, hogy azok tartalmát széles körűen határozta meg az uniós jogalkotó, amely a kriminalizáció hatókörére is kihatással van.

Literature

ARANY-TÓTH Mariann: *Személyes adatok kezelése a munkaviszonyban.* Wolters Kluwer, Budapest, 2016.

BARTÓKI-GÖNCZY Balázs: „A felhőalapú szolgáltatások és a személyes adatok védelme az új európai adatvédelmi rendelet tükrében" In: Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* ELTE-ÁJK, Budapest, 2017. 371-387.

BENDIK Tamás: „A tagállami jog és a GDPR viszonya – az Infotv. szerepe a megváltozott szabályozási környezetben" In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018. 37-48.

BLUTMAN László: „Bírói jogalkalmazás és szöveghű értelmezés" *Jogesetek Magyarázata*, 2010/4. 94-104.

ESZTERI Dániel: „A GDPR tárgya és hatálya" In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018. 49-62.

HOLLÁN Miklós: „A nemzeti büntetőjog kerettényállásai és az uniós jog" *Miskolci Jogi Szemle*, 2018/2. 19-39.

JAKAB András: „A bírói jogértelmezés az Alaptörvény tükrében" *Jogesetek Magyarázata*, 2011/4. 86-94.

JÓRI András: Fejezet. „A személyes adat" In: Jóri András (szerk.): *A GDPR magyarázata.* HVG-Orac, Budapest, 2018. 54-87.

JÓRI András: „Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig" *Alkotmánybírósági Szemle*, 2018/1. 16-21.

JÓRI András: „A Fővárosi Közigazgatási és Munkaügyi Bíróság ítélete a Nemzeti Adatvédelmi és Információszabadság Hatóság döntésének hatályon kívül helyezéséről. Az adatvédelem bírói kontrollja" *Jogesetek Magyarázata*, 2013/3. 48-54.

JÓRI András: „59. § [A magánszférajogok]" In: Jakab András (szerk.): *Az Alkotmány kommentárja II.* Századvég, Budapest, 2009. 2167-2193.

JÓRI András: *Adatvédelmi kézikönyv.* Osiris, Budapest, 2005.

KARSAI Krisztina: „Az ultima ratio alapelvről – másképpen." In: JUHÁSZ Zsuzsanna et al. (szerk.): *Sapienti sat. Ünnepi kötet dr. Cséka Ervin egyetemi tanár 90. születésnapjára.* Acta Jur. et Pol., Szeged, 2012. 253-260.

LIBER Ádám: „A jogos érdeken alapuló adatkezelésről" *Infokommunkáció és jog*, 2012/2. 79-88.

MAJTÉNYI László: „Az információs jogok.” In: HALMAI Gábor – TÓTH Gábor Attila (szerk.): *Emberi jogok*. Osiris, Budapest, 2006. 577-635.

MAJTÉNYI László: *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága.* Complex, Budapest, 2006.

MIKOLCZI Barna – SZATHMÁRY Zoltán: *Büntetőjogi kérdések az információk korában.* HVG-Orac, Budapest, 2018.

NAGY Ferenc: *A magyar büntetőjog általános része.* HVG-Orac, Budapest, 2010.

NAGY Ferenc: „Gondolatok a jogi tárgyról” *Büntetőjogi Kodifikáció*, 2008/1. 1-8.

OSZTOPÁNI Krisztián: „Alapfogalmak” In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018. 63-94.

OSZTOPÁNI Krisztián: „Jogalapok” In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018. 111-148.

PÉTERFALVI Attila – ESZTERI Dániel: „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata” In: Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* ELTE-ÁJK, Budapest, 2017. 406-420.

SÓLYOM László: *Az alkotmánybíráskodás kezdetei Magyarországon.* Osiris, Budapest, 2001.

SÓLYOM László: *A személyiségi jogok elmélete.* Közgazdasági és Jogi Könyvkiadó, Budapest, 1983.

SZABÓ Endre Győző: „Az adatvédelmi bírságról – a GDPR szabályainak elemzése” *Alkotmánybírósági Szemle*, 2018/2. 27-35.

SZOMORA Zsolt: „Btk. XXI. Fejezet” In: Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvhöz.* Complex, Budapest, 2013. 451-481.

SZOMORA Zsolt: „A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés” *Jogelméleti Szemle*, 2008/4.

SZŐKE Gergely László: „Az adatvédelem szabályozásának történeti áttekintése.” *Infokommunikáció és jog*, 2013/3. 107-112.