MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **12** | NUMBER **1** | SUMMER **2018** | ISSN **1802-5943**

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (www.rowanlegal.com/cz/)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

licensed as peer-reviewed scientific journal by the Research and Development
Council of the Government of the Czech Republic
listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **12** | NUMBER **1** | SUMMER **2018**

LIST OF ARTICLES

LIST OF REVIEWS

DOI 10.5817/MUJLT2018-1-1

ENHANCED FUNCTIONALITY BRINGS NEW PRIVACY AND SECURITY ISSUES – AN ANALYSIS OF EID*

by

TAMÁS SZÁDECZKY**

As compared with traditional paper-based versions and the standard username--password login to e-Government services, the new electronic identity and travel documents have made on-site electronic and on-line authentication of citizen more comfortable and secure.

The biometric passport was introduced in Hungary in 2006. A decade later the electronic identity card (eID) was implemented. The reason for the improvement of such documents is twofold: enhancing security features and performing new functions. The development is certainly welcome, but it also generates new types of risks, with which governments and citizens must take into account.

In this paper, I will first analyze the most widespread technologies of data storage cards from the passive elements to the chipcards, including the biometric passport. The objective is to provide an overview of the technical development as a background to my paper. I will then proceed to an analysis of the relevant EU and national legal background, data elements, data protection and the functions (ePASS, eID, eSIGN) of the new Hungarian and German identity card, as well as the security risks and protection properties of the eID-type documents. The paper concludes with a summary of the lessons learned from and the risks involved in the current solutions in Hungary and Germany.

* The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled *„Public Service Development Establishing Good Governance"* in the Miklós Zrínyi Habilitation Program.

** szadeczky.tamas@uni-nke.hu, Associate Professor, Institute of E-Government, National University of Public Service, Hungary.

KEY WORDS

Chip Data Protection, E-Passport, Hungary eID, Protection of Government Issued Documents

1. INTRODUCTION

The primary technology used to manage physical access and identification of persons is the card, which is widely used as a means of possession-based authentication for several years now.

Such cards are designed to store data for identity or access purposes. These tools are categorized per the storage method and device type. Both the storage capacity, security, and usability depend on the technology of these devices.

The most straightforward data storage option is provided by passive solutions, such as punched cards, barcodes, and magnetic stripes, also used in bank cards. A later version includes memory chips for data storage, without the possibility of data processing, e.g. encryption. These solutions have been used for a long time for official documents, primarily to ensure efficient machine data processing.

2. DATA STORAGE ON CARDS

A well-known data card type is the magnetic card. Here the data carrier is a magnetic metal stripe, sealed on a plastic sheet. This medium requires contact between the card and the reader. The magnetic reader heads, known from the tape recorder, have to be in physical contact with the card. The technology is specified by several standards, such as the ISO 7811, ISO 7812, ISO 7813 and the ISO 4909. The amount of data stored is limited to about a hundred bytes. For example, in the case of a bank card, the same data is stored as shown on the surface, completed with a couple of control data.[1] Its use is still ongoing, due to its simplicity. It is also suitable for identification without supervision. Using a PIN code, you can increase security significantly. Its counterfeiting can be done by reading the magnetic stripe and magnetizing a blank card, so it does not require sophisticated knowledge. Consequently, visual identification is also

[1] See Visdómine, L. P. (2002) *Track format of magnetic stripe cards*. [online] Available from: http://www.gae.ucm.es/~padilla/extrawork/tracks.html [Accessed 10 September 2017].

essential here. For this reason, bank cards typically feature hologram document security elements.

One or two-dimensional barcode cards are also used for identification. The amount of data stored is smaller than on magnetic cards. In the case of one-dimensional (linear) barcode, capacity is a few bytes. The encoding is defined in international standards, widely used are EAN 8 or EAN 13, introduced in 1978. As a further development of the linear barcode, the square data matrix code appeared in the early 1990's. The black-and--white data matrix has a data storing capacity of up to 2335 alphanumeric characters.[2] Similar is the today's fashionable QR code, shown in Figure 1. It can also be read easily by mobile devices, thanks to its design.

Figure 1: QR code[3]

The drawback of these methods is that the barcode is readable for unauthorized persons, it can be copied, and it can be counterfeited. To prevent reading data out, the barcode may have a top coat which can only read by infrared light. By this method, counterfeiting can be significantly complicated.

Figure 2: An earlier version of the USA residency permit[4]

---

[2] See Eiler, E. (2008) Kódnyomtatás és nyomtatott vonalkód rendszerek (Code printing and printed barcode systems), *Magyar Grafika (Hungarian Graphic)*, 2008(5), p. 44.

[3] Kaywa AG. *Kaywa QR Code generator* [online] Available from: https://qrcode.kaywa.com [Accessed 20 August 2017].

[4] Department of Homeland Security. *U. S. Citizenship and Immigration Services: Acceptable Documents*. [online] Available from: https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents [Accessed 15 September 2017].

Because of its high cost, the laser card is a less popular method. A stripe like a compact disc is sealed on a hard-plastic data carrier, which a laser beam can read in a width of 1.6 to 3.5 cm. The amount of data that can be stored (from 1.1 MB to 2.8 MB) is far higher than the previous methods. In the top line of Figure 2 is a one-dimensional barcode, an optical (laser) data storage under it. At the bottom, there is an MRZ (Machine Readable Zone) code, which simplifies machine data reading.

The standard feature of the cards described so far is that it is not possible or it is very difficult to change their data content. They do not contain active elements, which would allow their safer use. If it is necessary to change the stored data, another method should be applied. A more reliable solution is the use of memory circuits, where data is stored in an electronically programmable non-volatile memory circuit (EEPROM). For convenience reasons, the memory chip is embedded in a larger plastic card. They are used, for example, in Hungarian phone cards. Counterfeiting in the case of commercial memory circuits is not excessively burdensome. The hacker should only attach the reader to a computer and emulate a memory card with credits available.

The use of cards was revolutionized by the introduction of active cards, on which it is not only possible to write and read the data, but the card can do data processing and other mathematical operations. The microcontroller is the core element of the active tags. The microcontroller is a quasi--complete computer, practically made on an integrated circuit card (chip). It contains a processor, a non-volatile memory (ROM, FLASH), a random--access memory (RAM), input/output units (I/O), and other auxiliary elements (such as a real-time clock and similar). The microcontroller enables the implementation of the fourth-generation encryption systems, providing proactive protection for stored data and access. Depending on the type, its storing capacity may range from 1 to 256 kilobytes. Using a microcontroller, you can also create contact and contactless (touchless or proximity) data cards. Such contact data cards are the smart cards (chip cards). These were used in Hungary in the old type of higher education student ID cards, as well as on bank cards (EMV chip). Microcontrollers are also the primary means of storing the private key of the electronic signature (this is done on the SSCD, a secure electronic signature device). There are several international standards relating to chip cards, both from functionality and

security considerations,[5] for example, the ISO/IEC 7816. To read the data, the reader must have direct electronic contact with the microcontroller outlets. Apparently, this is the fastest and safest way of data transfer.

A contactless realization of the proximity card (RFID card) is the micro controller's active data card. The embedded microcontroller is substantially the same as the one used in smart cards. The main difference is that its connection to the reader is made at radio frequency. Its operating principle is that the data card has a large coil antenna, which is connected to the microcontroller. Per the basic design, the card does not contain a power source, but it takes the operating power of the electromagnetic field, generated by the reader. So, while the card is getting closer to the reader, it automatically turns on, and it emits a modulated signal. For example, the card sends an identification number. The reader will check if this identification number is included in its database and, depending on the result, it permits entry. The shortcoming of this system is easily recognizable since only the electromagnetic field of the given frequency is required to obtain the data. So the card reveals its identification number to any reader, including a malicious person's reader. He/she only writes this identification number to an empty card to maliciously copy the original one. To prevent this copying, the reader can also be combined with reader identification. At the time when the card reaches the electromagnetic space, it only indicates its presence, and the reader sends its identification code. The card will only reveal its identification number if the code is listed on the list of authorized readers stored in the card's memory. Data transfer can also be protected by encryption of data transfer, for example, using cryptography or a public key infrastructure (PKI) technology.[6] Because of the radio frequency transmission, the speed of communication and therefore the amount of stored data is also several orders of magnitude smaller than the ones of the contact smart cards. Usually, a length of the 26… 37-bit code is used. The standard reading distance of several centimeters can even be increased up to ten meters (long range proximity) with a built-in battery. Proximity technology is described in the ISO/IEC 14443 standard. In order for these cards to be used in public documents for authentication functions, cards must be improved and configured securely.

[5] See Hassler, V. (1995) *IT Security and Smart Card Standards. Graz*, Austria: Institutes for Information Processing Graz.

[6] Apparently, this is the case with e-Passport and eID solutions. The basic design shows only the security of proximity (RFID) card security.

3. BIOMETRIC IDENTIFICATION IN CARD TECHNOLOGY

The next generation of active cards is their combination with biometric security elements. The most characteristic feature of the human integument is the face, which, due to the underdevelopment of other senses of Homo Sapiens (e.g. smelling), is the primary means of identification of persons in addition to its socio-communication function. Its application is instinctive, and the human race applies it from the beginning. The first trace of using other biometric features was the use of fingerprint in China in the 14th Century, to identify children, which was recorded by the explorer, Joao de Barros.[7] In Europe, first Alphonse Bertillon, a Paris police officer introduced a body-size-based identification system in 1890, for identification of criminals. His method was not successful because of a mass occurrence of false positives. The fingerprint was first used for forensic aims by Richard Edward Henry, at Scotland Yard, based on Bertillon's work. In the 20th century, Karl Pearson at the University College of London, who dealt with applied mathematics, made significant discoveries in biometrics. In the 1960s, considerable progress was made in signature – dynamics analysis, which, however, remained in the military and national security applications. With the increasing threat of terror, the state enforcement of biometric identification in the United States and Western Europe has increased dramatically.

Currently the following biometric features are widely used for identification:

- fingerprint;
- hand geometry;
- palm print;
- vein pattern;
- grip dynamics recognition;
- skull thermal image;
- 2D facial features;
- 3D facial features;
- iris (iris diaphragm) recognition;
- retina (peripheral vein network) recognition;

[7] See Osborn, A. (2005) *Biometrics history. Looking at biometric technologies from the past to the present*. [online] Available from: http://ezinearticles.com/?Biometrics-History----Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 [Accessed 2 September 2017].

- voice recognition;
- signature dynamics;
- keystroke dynamics;
- DNA;
- recognition of posture.

They are applied to identify people with different success. By mathematical description and storage of biometric features, it is possible to make a more accurate identification, based on individual data.

In the history of travel documents, by the integration of data cards as complementary element and biometrics, as a higher degree of personal bound, a new generation was created, which means significantly higher reliability in the area of document security.

Figure 3: e-Passport[8]

After the United States, the introduction of electronic Passports (e-Passports), shown in Figure 3, has also begun in the European Union. The main reasons for this are increasing the security of travel documents, as well as remaining in the US Visa Waiver Program, which means the visa--free regime of the EU states. For Hungary, the introduction of e-Passport aimed at getting into the program at that time. The e-Passport is an incorporation of a contactless chip card, described above, into the passport. First, saving only the data page, and then the fingerprint as well. E-Passport was first introduced in Sweden in October 2005 in Europe according to the Council of the European Union.[9] In Hungary, since August 2006, the full content of the data page was found in the storage

[8] Bundesamt für Sicherheit in der Informationstechnik. *The electronic passport*. [online] Available from: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EPassport/epassport_node.htm [Accessed 20 June 2017].

element, together with the photo and signature as well. The fingerprint is also stored since 2008.

By the Council's decision, until 28th June 2009, all the EU states had to move on to apply e-Passports, also containing fingerprints, which triggered resistance of recognized data protection specialists in many EU countries. The new EU-level data protection legislation (GDPR) categorizes biometric data in special category of personal data.[10]

Security measures have been implemented to protect the stored data, but the exact control depends on the member country.[11] Apart from conventional document security procedures (embedded photo and signature, unique patterns, special paints), the electronic storage unit destroys the stored content because of a physical attack.[12] On the other hand, the chip is capable of active authentication, which is done by using the integrated PKI private key, and there is also the digital certificate of the passport publisher in it. For the access to the data page, the Basic Access Control (BAC) method is used. Its operation is as follows: similar to the ID card, the MRZ code can be found in the lower part of the passport data page. The MRZ code contains essential information about the document and its owner, which simplifies machine reading of data. Obtaining the passport number, the birth date and the validity period, the reader generates an access key. The e-Passport will only send stored data to the reader at radio frequency after getting this access key. The physical access to the card is proven this way. This method has insufficient security features. Breaking the key by using the brute force method, because of the approximately 50-bit entropy, is theoretically more than 35 years. However, some data analysis (choosing birth time intervals, tracing passport numbering) reduces entropy to 35-bit so that the key can be

[9] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[10] 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). *Official Journal of the European Union* (L 119/1) 4 May. Article 9 (1). Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 7 May 2018].

[11] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[12] See Jóri, A.; Hegedűs, B.; Kerekes, Zs. (eds.) et al. (2010) *Adatvédelem és információszabadság a gyakorlatban. (Data protection and freedom of information in the practice).* Complex, Budapest.

broken within 3 hours.[13] It has been proven, that the communication, having Basic Protection (BAC), has been cracked in several cases and the data content has been accessed.[14] This encryption is unsuitable for protecting fingerprints, so a more secure procedure has been developed, which is called the Extended Access Control (EAC).[15] The EAC is based on ICAO Doc 9303, but it is not a uniform standard. Member States should also consider the change of numbering to a broader range, or random allocation within the field.

4. EID PROTECTION OPTIONS

In eID documents like in electronic passports a chip is embedded. The stored data can be accessed through a contact or radio interface. As this personal data can be potentially abused, countermeasures should be implemented. By radio interface cards remote reading is possible, by a directional antenna from up to several meters. Thus it is not enough to solve the security by physical protection alone. Under physical protection in this case we mean that we take care of the card and only give it to the one, with whom we want to share its full data content. The potential attack includes eavesdropping on the communication, the acquisition of saved data for example by skimming, as well as tracing. During tracing, the attacker prepares a profile of the target, following the geographic movement of the card. Unfortunately, the latter is allowed by the ISO 14443 standard, which requires the unique identification of the chip card, before communication.[16]

One of the most typical ways of protection is encryption, where the encryption algorithm is known by all compatible card readers, but with the symmetric encryption key, only readers, with whom we want to share the data, have the possibility of decryption. In this case, we encounter the key distribution problem, so if you have one hundred thousand readers, you either use the same password for all, and you cannot change

[13] Robroch, H. (2006) *ePassport Privacy Attack. Cards Asia Singapore.* [online] Available from: https://pdfs.semanticscholar.org/828a/70de925744617be3d2886442cd0e88058c25.pdf [Accessed 27 October 2017].

[14] See Papp, Z. (2010) Az új technológiák veszélyei: RFID és az elektronikus útlevél (Hazards of new technologies: RFID and e-Passport), *Hadmérnök (Military Engineer)*, 5(4), pp. 248–254.

[15] See Moses, T. (2010) *Protecting Biometric Data with Extended Access Control.* [online] Available from: https://www.entrust.com/wpcontent/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf [Accessed 4 September 2017].

[16] See Naumann, I.; Hogben, G. (2008) Privacy features of European eID card specifications, *Network Security*, August.

the compromised keys, or each reader uses a separate password, but then passport management is challenging. The control of the readers' passwords on the issued cards is impossible from an organizational point of view. This method can only be applied in a closed system, for example, in the case of a corporate solution.

With authentication controls, we want to limit access to data. In this case, a short identification code should be provided from the reader's side, which can be called a PIN (Personal Identification Number), CAN (Card Access Number) or code. The reader device uses this piece of information to identify itself with the card. The card gives out the stored data only to the reader, which is determined in this way. The communication can optionally be encrypted, which can happen with a session key, used in the given connection, with a predetermined symmetric key, or the public key-secret key pair, used for asymmetric encryption. The latter may be, for example, supplied with a service provider certification, operated by the issuing authority. The memory of the card can be divided into several parts, according to the confidentiality of the data. The Spanish electronic identity card's memory is divided into three sections, for example, access to the public portion is not restricted, access to the secret area requires the PIN code of the card, while only public administration have access to the protected area.[17]

The plan of the electronic European Health Insurance Cards offers an exciting authentication option, which defines authentication between two smart cards. In doing so, health data, stored on the health insurance card (HIC) of the patient, can be accessed only with the health professional card (HPC) of the doctor, thus ensuring the protection of medical data.

Access to data may also be restricted by using an identifier. In this case, eID shares only a user ID (UID) with the service provider, who logs into a central database, to retrieve the data that can be accessed by him/her by the UID. However, public administration, regardless of all these, may have direct access to the data, stored on the card. This solution can also raise several questions, including data protection issues, affecting the use of a single identifier, a central database, accessible by market participants and similar problems.

[17] Sotirov, A. et al. (2009) Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Halevi, S. (eds.) *CRYPTO, LNCS 5677*, pp. 55–69.

The protection of the privacy is more efficiently implemented by modifying the previous ID configuration method, with the use of hashes. A fingerprint is generated from an input data with a so-called hash function, which is a trapdoor function, which means, that performing it in one direction is simple, but in the other direction, it is a complicated mathematical task. This algorithm generates a constant amount of data (128–512 byte) from any amount of data. A change of a single bit in the input data set will change at least 50 percent of the output bits (this is the avalanche effect). The amount of data, applied as output, is called a fingerprint since it characterizes the input data amount nearly in a unique way. The input cannot be generated from the hash code. In practice, typically the SHA-256, SHA-512, SHA-3 or the Whirlpool, or the algorithms are encountered. The use of obsolete algorithms, like the MD5, SHA-1 or RIPEMD-160 is no longer secure for electronic signatures or similar purposes.[18] If the hash value is formed from the UID by a usage-dependent identifier, we make it harder for malicious providers to merge personal data, which are stored in various databases. Practically the decryption of the original (unified) UID from those is a mathematically impossible task.

An additional way of privacy protection is that the card does not provide personal data, stored on it, but only offers the possibility of comparison. In this case the reader optically reads the data and sends it to the chip. The chip only confirms that the sent data are the same as the data stored in the secure container. An example of this solution is the checking of the fingerprint pattern. The reading device reads the fingerprint of the person, who shows the identity document. The reader generates a digital model from the optical picture, which can be interpreted by the card. The card compares it with the fingerprint data, stored in its storage and provides a percentage-probability value to the reader, regarding the probability of the match. In this case, the reliability of the card is essential, so the card must provide the answer to the reader, not the attacker.

It is also possible to identify the user if the card is capable of electronic signature. One option is when the card creates a protected channel with the system, which requires the identification, using a key-exchange protocol (e.g. Diffie–Hellman Key Exchange). The other option is if the system

[18] Ibid.

requesting the authentication sends a generated (pseudo) random dataset and it is electronically signed and returned by the person to be identified. Although technically both solutions are right, misuse of the data is more likely in the latter case, if the data package to be signed is not random, but targeted generated data.

5. NEW IDENTITY CARD IN HUNGARY

Instead of the former paper-based identity card, the Government Decree No. 168 of 1999 (XI. 24.) issued a plastic card-based identity card from January 2000, shown in Figure 4. This step aligns with the initiative of the government to increase information security in e-governmental relations.[19] In addition, the ID1 (85.6 mm x 53.98 mm)[20] standard card size and water resistance are also favored by the cardholders. Its disadvantage or just property was that it did not contain the address, which was issued to the legitimate holder on a separate card (the same size) on the residence permit certificate. This document has undergone several minor updates.

Figure 4: Hungarian Identity Card between 2000–2015[21]

A significant change happened by introducing the electronic Personal Identification Card (eID or "eSzemélyi" in Hungarian), from 1st January 2016, shown in Figure 5, by the Government Decree No. 414 of 2015 (XII. 23.). In addition to the altered design and the new type of security features, the eID has introduced a contactless, active storage device,

[19] For detailed analysis of improving security legislation see Szádeczky, T. (2014): Information Security – Strategy, Codification and awareness. In: Nemeslaki, A. (ed.): *ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary*. Budapest, pp. 109–122.

[20] Defined in the ISO/IEC 7810 standard.

[21] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-03001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-03001/index.html [Accessed 20 September 2017].

accessible via a radio interface, that is similar to the one that has already been used for a decade for electronic passports.

Figure 5: Hungarian Identity Card from 2016[22]

The visual content of the eID is practically the same as that of the old identity card. The optical and electronic data content of the new type of identity card is included in the relevant Hungarian Act.[23] These data have been edited in Table 1.

Information Contained	Visually[24]	In machine (MRZ) code	In storage device[25]
Name of the citizen	Yes	Yes	Yes
Name of citizen, in a minority language	At the request of the citizen, belonging to the minority[26]	N/A	N/A
Place of birth	Yes	N/A	Yes
Date of birth	Yes	Yes	Yes
Nationality	Yes	Yes	Yes
Mother's name	Yes	Yes	Yes
Gender	Yes	Yes	Yes

[22] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-05001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-–05001/index.html [Accessed 20 September 2017].

[23] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29.

[24] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29. Paragraph 2.

[25] The document, "without deadlines", which is available for those, over 65 years old, is in fact a document, the validity of which is 60 years, and it does not contain any storage element, see *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29/E. Paragraph 2.

[26] *Hungarian Government Decree No. 414 of 2015 (XII. 23.) on issuing of ID cards and collection of facial photo and signature.* Hungary. Section 33. Paragraph 1.

Facial Image	Yes	Yes	Yes
Signature	In case of literate person aged over 12 years	N/A	In case of literate person aged over 12 years
Validity	Yes	Yes	Yes
Document ID	Yes	Yes	Yes
Issue Date	Yes	Yes	Yes
Issuing Authority	Yes	Yes	Yes
Travel restrictions on traveling abroad	In specific cases and ways	N/A	In specific cases and ways
Code number (CAN), needed to start legitimate access to the data, recorded in the storage element	If there is a storage element	N/A	N/A
Fingerprint	N/A	N/A	In case of a person aged over 12 years, if he/she has not refused it, and if he/she is not physically unable to enroll
Data needed to create the electronic signature	N/A	N/A	At the request of the citizen
Social security identification number	N/A	N/A	Yes
Tax identification number	N/A	N/A	Yes
The electronic, unique identifier of the identity card	N/A	N/A	Yes
No more than two emergency phone numbers to be notified	N/A	N/A	At the request of the citizen

Table 1: Data content of the Hungarian eID[27]

The validity of the permanent identity card is three years, under the age of 18, and six years above that. Identity cards may be issued "without a deadline" for people aged above 65 years (the validity of which is in fact 60 years), and they do not contain any electronic storage element. The duration of the validity of the identification card, as a rule, fits the birth date of the eligible person.[28]

[27] Edited by the author, based on *Hungarian Act LXVI of 1992 on register of citizens' personal data and address*.

[28] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 29/E.

The identification card falls within the scope of national development competence, for which the European Union lays down security and functional requirements. As a document that can be used for proof of identity, the eID belongs to the highest document protection category.[29] According to the requirements, it must be protected against full or partial forgery. For protection methods, the chemical, physical, technical, technological and administrative procedures, and digital security methods shall be used together.[30] Specific protection solutions have been defined in the document protection plan, and they are not publicly available. However, the picture of the document and specific security elements of it are publicly available in the European Public Register of Authentic Travel and Identity Documents Online (PRADO) system.

According to the Regulation on the Protection of Security Documents, the electronic security document contains a data storage device, which is capable of storing the data. It is integrated into the material. In addition to the document protection categories, the law also names the document information security categories.[31]

In case of the eID, the following requirements apply:

- the stored data are encrypted, the encryption algorithm is at least RSA 2048;
- limitation of recording, writing and overwriting of the data;
- application of extended access protocol;
- protected communication channel between the data storage and the reader;
- manufacturer's certification of the data storage.

The storage element is an electronic data carrier unit,[32] which has a certificate (CC EAL5+) according to the Common Criteria for Information Technology Security Evaluation, and it is qualified as a secure signature creation device (SSCD).[33]

---

[29] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary. Section 5/A (5)

[30] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary.

[31] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary. Appendix 2., II.

[32] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address.* Hungary. Section 19.

[33] See Szádeczky, T. (2010) Pillars of IT Security, *Studia Iuridica Auctoritate Universitatis Pécs Publicata*, 2010(147), pp. 247–268.

6. EID IN GERMANY AND IN EUROPE

A number of EU member states have already implemented an eID solution, but this does not mean that all are implementing eID functions to the National ID like Germany and Hungary. Here eID refers to the Electronic Identification (eID) function for using public and private services. Table 2 shows the form of the eID solution per country. As of today, 14 member states have implemented a national ID-based eID solution.

Member State	Form of the eID
Austria	other forms
Belgium	National ID
Bulgaria	National ID
Croatia	other forms
Cyprus	online
Czech Republic	National ID
Denmark	online
Estonia	National ID
Finland	other forms
France	online
Germany	National ID
Greece	online
Hungary	National ID
Ireland	online
Italy	National ID
Latvia	National ID
Lithuania	National ID
Luxembourg	National ID
Malta	National ID
Netherlands	National ID
Poland	N/A
Portugal	National ID
Romania	N/A

Slovakia	National ID
Slovenia	other forms
Spain	National ID
Sweeden	other forms
United Kingdom	other forms

Table 2: eID solutions in the EU[34]

The Hungarian eID solution is apparently[35] based on the German National Identity Card ("neue Personalauseis" in German) and the Electronic Residence Permit, shown in Figures 6 and 7.[36]

Figure 6: German identity card from 2011[37]

The German federal government introduced the new electronic identity card in 2011 to change the old paper-based ones.[38] The validity of the permanent document over 24 years is ten years. In contrast to the free Hungarian eID, the standard German eID (permanent, over 24 years) costs 28,80 Euro.[39]

---

[34] Edited by the author, based on PRADO and the data collected by the European Commission. Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID [Accessed 6 February 2018].

[35] No official communication was found about a German–Hungarian cooperation on this topic but hardware, software and reader type shows that the German solution was the sample for the Hungarian government.

[36] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC [Accessed 15 November 2017].

[37] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) DEU-BO-02001.* [online] Available from: http://www.consilium.europa.eu/prado/en/DEU-BO-02001/image-166166.html [Accessed 13 November 2017].

[38] *German Act on Identity Card 2009 (Personalausweisgesetz - PAuswG)*, BGBl. I S. 1346. Germany.

7. FUNCTIONALITY AND SECURITY

Both the German and the Hungarian electronic identity cards have three main functions:

1. Electronic Travel Document (ePASS) function;
2. Electronic Identification (eID) function;
3. Electronic Signature (eSIGN) function.

The purpose of the Electronic Travel Document (ePASS) is to ensure cross-border access as regulated in the Schengen Agreement. Therefore, in this aspect, it can only replace the passport just in specific cases.

The electronic identification function makes the usage of the e-government functions more efficient. It is also planned that cross--border service will be available later, the area also appears as the European Union Common List of Basic Public Services List (EU CLBPS, a Common List of Basic Public Services) or otherwise as a 12+8-list element.[40] The eID functions are defined in the electronic IDentification, Authentication and trust Services (eIDAS)[41] and in the Connecting Europe Facility (CEF).[42] Nonetheless, implementation in the Member States is slow and far from what is expected in both the degree of application and the content.[43] The cooperation between the EU member states is at a high level[44], and as of 29 September 2018, the recognition of notified eID solutions will

---

[39] *German Decree on Identity Card Price* (*Personalausweisgebührenverordnung, PauswGebV*) *2010,* BGBl. I S. 1477. Germany. § 1 (1) 2.

[40] See Szabó, A. B. (2016) Okmányvédelem és az elektronikus személyazonosító igazolvány (Document security and the electronic ID card), *Hadmérnök (Military Engineer)*, 11(1), pp. 13–17.

[41] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (L 53/14) 25 Febr. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

[42] Regulation (EU) No. 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No. 913/2010 and repealing Regulations (EC) No. 680/2007 and (EC) No. 67/2010. *Official Journal of the European Union* (L 348/129) 20 December. Available from: http://data.europa.eu /eli/reg/2013/1316/oj [Accessed 7 May 2018].

[43] See Siddhartha, A. (2008) National e-ID card schemes: A European overview, *Information Security Technical Report*, 2008(13), pp. 46–53.

[44] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (L 53/14) 25 Febr. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

become mandatory. The Hungarian eID itself, according to the available information, is ready to be notified. However, as of today, the only notified solution is the German National Identity Card and the Electronic Residence Permit.[45] In fact, the problem lies not with the issuer, but at the acceptance,[46] because member states are not yet ready to accept another member states' eID card.[47] The reason for that is hardware, firmware and software incompatibilty.

The electronic signature (eSIGN) function is, in contrast to the previous two features, entirely in the interest of the user. It is possible to create an electronic signature on any document with the embedded PKI key pair with S/MIME certificates. The process of creating an electronic signature is as follows: a specific hash function (e.g. SHA-256) generates a hash code (fingerprint) from the data. A PKI cryptographic private key (of the signer) encrypts this hash code, so we get the electronic signature, which will be a data packet, independent of the input document (but might be attached to it). The signed document and the electronic signature can be sent to a recipient via a public channel, such as an e-mail. The recipient deciphers the electronic signature with our public key, so he/she gets the hash code which we have created. In the meantime, he/she also produces the fingerprint from the document sent and compares these two. If they are the same, it shows that there is no change in the signed document, and, that the signature of the document was carried out by a specific key. However, this does not link the private key to a natural person, it does not prove that it has not been revoked, and it is not possible to determine the time of signature either. To solve these issues, additional functions should be used.

There are two ways to solve the problem of connecting a key to a person, i.e. to address the authenticity problem: on the one hand, by the web of trust

---

[45] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC [Accessed 15 November 2017].

[46] Hornung, G. (2005) *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren (The digital identity. Legal problems of chipcard-IDs: digital national ID, electronic social security card, JobCard-process).* Nomos, Baden Baden, p. 379.

[47] See the current implementation report at CEF Digital. *Country overview: eIDAS-Node Implementation*. [online] Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID [Accessed 15 November 2017].

method, used by PGP.[48] This way, each person's keys are signed by the persons, trusting each other. So if the recipient knows any person signing the sender's key or he/she can trace back the signatures to a trusted person, then this will also guarantee the reliability of the person. The disadvantage of this method is that it requires extensive trust networks, i.e. that two people who do not know each other have a common acquaintance. The other way is to use the S/MIME system. Here the reliability of the parties is certified by a third party, trusted by each side, through a certificate, which is an electronic data set including the public key as well. The third party is a Certificate Service Provider, CSP, considered as a trustworthy person by the government, who checks the association of the key and the key holder before issuing the certificate, for example by requiring to provide an identity card. These certification providers form a certification chain, with the highest certification authority (CA) at the top. These CAs are accepted by the public at large, and hence, the rest of the certification chain also becomes reliable.

Authentication of the signing time is done by the Time Stamping Authority (TSA), who provides the exact time with their electronic signature, which the sender will incorporate into the electronic signature of the document. The application for the time stamp is carried out online via the Internet. The reliability of the TSA is ensured by its certificate, which can be traced back to a CA along the certification chain. The use of electronic signatures or certificates is usually limited. Typically, a key pair can only be used for electronic signature or encryption or setting up a secure link (SSL). If one wants to use several functions from these, more key pairs or certificates may be needed.

The e-signature and time stamping service, related to the new identity card, is provided by the NISZ National Infocommunications Service Company Ltd., as a government authentication service provider. The certification applied in the Hungarian eID corresponds to the requirements of the eIDAS Regulation[49], just like the German eID.[50]

---

[48] See Alfarez, A.-R. (1997) The PGP Trust Model. *EDI-Forum*, April.

[49] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257/73) 28 August. Available from: http://data.europa.eu/eli/reg/2014/910/oj [Accessed 7 May 2018].

[50] Hornung, G.; Engemann, C. (2016) *Der digitale Bürger und seine Identität (The digital citizen and his identity).* Nomos, Baden Baden, p. 207.

The Hungarian eSzig Card Management Utility[51] can be used to activate and change the electronic PIN codes and to see e-signature certificates. It runs on the 7, 8, 8.1, 10 32 and 64-bit versions of the Microsoft Windows. It also supports the versions of the Apple Mac OS X Yosemite, El Capitan, Sierra, and some Linux distributions and versions (CentOS 7, Debian 8, SuSe 13.2, Ubuntu 14.04.5 LTS).[52] Its developer is ID&Trust Ltd., a small Hungarian business operating on the international chip card market.

The German desktop-based application is called "AusweisApp2". It has a different design, but similar functionality: the user may see the data stored on the card and may change the PIN code. There is also a function where the links to the available services are collected. The developer is Governikus GmbH & Co. KG. In both cases, the Ministry of Interior is responsible for the development and the operation. Both applications are lack of integrated functions. Thus the citizen does not need to use them regularly. But active usage is required for the acceptance of e-government services.[53]

8. CONCLUSION

With the development of card-based data storage technology and the increasing data storage and processing capacity of the cards, they can be used more and more efficiently for access and personal identification. With increasing complexity, the volume and quality of the stored data are also growing. Earlier, there was far less personal data printed on the card. The development in functionality, in addition, poses a new data protection risk.

From the functional side by the introduction of the electronic identity card (eID), the Hungarian government, similarly to some other EU governments, like Belgium, Estonia, and Germany, has made a considerable leap in e-government and it has opened up a number of widely available functions.

The electronic identification and electronic signature functions may revolutionize the e-government and electronic literacy, since the governments provide all the required elements. In Hungary, this means

[51] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/ [Accessed 24 September 2017].

[52] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/kartyaolvaso_alkalmazas [Accesed 24 September 2017].

[53] Bieler, F. Schwarting, G. (2007) *e-Government. Perspektive – Probleme – Lösungsansätze (Perspective, Problems, Solutions).* Erich Schmidt Verlag, Berlin, p. 271.

free access to both of above functions, which makes the critical element of the electronic literacy widely accessible. Using of "may" is due to the skepticism of the author: by the appearance of electronic signature in the 2000s and then the rapid legislation, made the professionals hope for a wide range of application, which eventually did not happen. In any case, the governments do indeed create at least the possibility of development by providing the new type of identity cards.

All new technologies and increasing complexity also generate new types of risks, which the governments and citizens must take into consideration. Cryptographic measures are effective against a lot of attacks, e.g. using well-known algorithms with large keys protects us from eavesdroppers. However, cryptography does not defend us in every case. The Estonian eID was using a well-known, certified chip, but the implementation was vulnerable to the Coppersmith attack for some years. Because of this, 750,000 valid Estonian eIDs became compromised, which is the worst nightmare of any issuers.[54] Nevertheless, in some cases, tracking is by design possible. In such cases, the citizen will need to apply additional technical and organizational measures.

LIST OF REFERENCES

[1] Alfarez, A.–R. (1997) The PGP Trust Model. *EDI-Forum*, April.

[2] Bieler, F. Schwarting, G. (2007) *e-Government. Perspektive – Probleme – Lösungsansätze (Perspective, Problems, Solutions)*. Erich Schmidt Verlag, Berlin.

[3] Bundesamt für Sicherheit in der Informationstechnik. *The electronic passport*. [online] Available from: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EPassport/epassport_node.htm [Accessed 20 June 2017].

[4] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic Identification pursuant to Article 12(7) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (L 53/14) 25 February. Available from: http://data.europa.eu/eli/dec_impl/2015/296/oj [Accessed 7 May 2018].

[54] See Goodin, D. (2017) *Millions of high-security crypto keys crippled by newly discovered flaw, ars technica.* [online] Available from: https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/ [Accessed 16 November 2017].

[5] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union* (L 385/1) 29 December. Available from: http://data.europa.eu/eli/reg/2004/2252/oj [Accessed 7 May 2018].

[6] Department of Homeland Security. *U. S. Citizenship and Immigration Services: Acceptable Documents*. [online] Available from: https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents [Accessed 15 September 2017].

[7] Eiler, E. (2008) Kódnyomtatás és nyomtatott vonalkód rendszerek (Code printing and printed barcode systems), *Magyar Grafika (Hungarian Graphic)*, 2008(5), pp. 42–47.

[8] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* (2017/C 319/3) 26 September. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017.319.01.0003.01.ENG&toc=OJ:C:2017:319:TOC

[9] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-03001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-03001/index.html [Accessed 20 September 2017].

[10] European Council and Council of the European Union. (2017) *Public Register of Authentic Travel and Identity Documents Online (PRADO) HUN-BO-05001.* [online] Available from: http://www.consilium.europa.eu/prado/en/HUN-BO-05001/index.html [Accessed 20 September 2017].

[11] *German Act on Identity Card 2009* (*Personalausweisgesetz – PauswG),* BGBl. I S. 1346. Germany.

[12] *German Decree on Identity Card Price (Personalausweisgebührenverordnung, PauswGebV) 2010,* BGBl. I S. 1477. Germany.

[13] Goodin, D. (2017) *Millions of high-security crypto keys crippled by newly discovered flaw, ars technica*. [online] Available from: https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys750kestonian-ids/ [Accessed 16 November 2017].

[14] Hassler, V. (1995) *IT Security and Smart Card Standards*. Graz, Austria: Institutes for Information Processing Graz.

[15] Hornung, G. (2005) *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren (The digital identity. Legal problems of chipcard-IDs: digital national ID, electronic social security card, jobCard-process)*. Nomos, Baden Baden.

[16] Hornung, G.; Engemann, C. (2016) *Der digitale Bürger und seine Identität (The digital citizen and his identity)*. Nomos, Baden Baden.

[17] *Hungarian Act LXVI of 1992 on register of citizens' personal data and address*. Hungary.

[18] *Hungarian Government Decree No. 414 of 2015 (XII. 23.) on issuing of ID cards and collection of facial photo and signature*. Hungary.

[19] *Hungarian Government Decree No. 86 of 1996. (VI. 14.) on the protection of security documents.* Hungary.

[20] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/ [Accessed 24 September 2017].

[21] Hungarian Ministry of Interior. (2017) *eID thematic website.* [online] Available from: http://www.kekkh.gov.hu/Eszemelyi/kartya_funkcioi/kartyaolvaso_alkalmazas [Accesed 24 September 2017].

[22] Jóri, A.; Hegedűs, B.; Kerekes, Zs. (eds.) et al. (2010) *Adatvédelem és információszabadság a gyakorlatban. (Data protection and freedom of information in the practice)*. Complex, Budapest.

[23] Kaywa AG. *Kaywa QR Code generator* [online] Available from: https://qrcode.kaywa.com [Accessed 20 August 2017].

[24] Moses, T. (2010) *Protecting Biometric Data with Extended Access Control.* [online] Available from: https://www.entrust.com/wp-content/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf [Accessed 4 September 2017].

[25] Naumann, I.; Hogben, G. (2008) Privacy features of European eID card specifications, *Network Security*, August.

[26] Osborn, A. (2005) *Biometrics history. Looking at biometric technologies from the past to the present*. [online] Available from: http://ezinearticles.com/?Biometrics-History----Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 [Accessed 2 September 2017].

[27] Papp, Z. (2010) Az új technológiák veszélyei: RFID és az elektronikus útlevél (Hazards of new technologies: RFID and e-Passport), Hadmérnök (*Military Engineer),* 5(4), pp. 248–254.

[28] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257/73) 28 August. Available from: http://data.europa.eu/eli/reg/2014/910oj [Accessed 7 May 2018].

[29] Regulation (EU) No. 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No. 913/2010 and repealing Regulations (EC) No. 680/2007 and (EC) No. 67/2010. O*fficial Journal of the European Union* (L 348/129) 20 December. Available from: http://data.europa.eu/eli/reg/2013/1316/oj [Accessed 7 May 2018].

[30] 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). *Official Journal of the European Union* (L 119/1) 4 May. Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 7 May 2018].

[31] Robroch, H. (2006) *ePassport Privacy Attack. Cards Asia Singapore.* [online] Available from: https://pdfs.semanticscholar.org/828a/70de925744617be3d2886442cd0e88058c25.pdf [Accessed 27 October 2017].

[32] Siddhartha, A. (2008) National e-ID card schemes: A European overview, *Information Security Technical Report*, 2008 (13), pp. 46–53.

[33] Sotirov, A. et al. (2009) Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Halevi, S. (eds.) *CRYPTO, LNCS 5677*, pp. 55–69.

[34] Szabó, A. B. (2016) Okmányvédelem és az elektronikus személyazonosító igazolvány (Document security and the electronic ID card), *Hadmérnök (Military Engineer),* 11 (1), pp. 13–17.

[35] Szádeczky, T. (2014): Information Security – Strategy, Codification and awareness. In: Nemeslaki, A. (Ed.): *ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary*. Budapest, pp. 109–122.

[36] Szádeczky, T. (2010) *Pillars of IT Security, Studia Iuridica Auctoritate Universitatis Pécs Publicata*, 2010 (147), pp. 247–268.

[37] Visdómine, L. P. (2002) *Track format of magnetic stripe cards*. [online] Available from: http://www.gae.ucm.es/~padilla/extrawork/tracks.html [Accessed 10 September 2017].

DOI 10.5817/MUJLT2018-1-2

"LAGOM JURISDICTION" – WHAT VIKING DRINKING ETIQUETTE CAN TEACH US ABOUT INTERNET JURISDICTION AND GOOGLE FRANCE[*]

by

DAN JERKER B. SVANTESSON[**]

The law of Internet jurisdiction is facing a crisis. While there is widespread and growing recognition that we cannot anchor Internet jurisdiction in the outdated, typically overstated, and often misunderstood, territoriality principle, few realistic alternatives have been advanced so far.

This article seeks to provide an insight into the conceptual mess that is the international law on jurisdiction; focusing specifically on the concepts of sovereignty and jurisdiction, with limited attention also given to the impact of comity, and international human rights law. These issues are studied through the lens of the so-called Google France case that comes before the CJEU in 2018. The article argues that we may usefully turn to the Swedish "lagom" concept – which allegedly stems from Viking era drinking etiquette – as a guiding principle for how we approach Internet jurisdiction.

KEY WORDS

Lagom, Comity, Google France, Internet Jurisdiction, Sovereignty, Vikings

---

[*] This article draws, and expands, on research findings discussed in: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press; Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing; and Svantesson, D. (2017) *Time for international law to take the Internet seriously.* [online] OUPblog. Available from: https://blog.oup.com/2017/10/international-law-internet/ [Accessed 7 October 2017].
I thank the two anonymous reviewers for their valuable feedback.

[**] dasvante@bond.edu.au, Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia).

1. INTRODUCTION

At the time of writing, the Court of Justice of the European Union (CJEU) is about to determine a matter regarding jurisdiction and sovereignty that goes to the very core of the Internet; the consequences of which may indeed seriously impact the future of the Internet.

The matter in question arose out of the famous (or notorious) Google Spain – right to be forgotten – case decided by the CJEU in May 2014. As is well-known, in that decision the Court recognised, or rather articulated some would say, a right variously referred to as the "right to be forgotten", the "right to delisting", and the "right to de-referencing". However, the CJEU was never asked to deal with the scope of jurisdiction question; that is, in this case the geographical scope of reach of any order requiring "delisting". As I have discussed elsewhere, Google saw the order aslimited to the EU, while the Article 29 Working Party and some of the European Data Protection Authorities (DPAs) saw the order as requiring a broader implementation of any delisting order.[1] Consequently, there now is considerable controversy about how widely – geographically speaking – search engines need to delist search results based on the so-called "right to be forgotten".

In a media release of 12 June 2015, the French data protection authority – the Commission Nationale de Informatique et Libertés (CNIL) – stated, amongst other things, that:

> *"CNIL considers that in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing. In this context, the President of the CNIL has put Google on notice to proceed, within a period of fifteen (15) days, to the requested delisting on the whole data processing and thus on all extensions of the search engine."*[2]

This dispute – commonly referred to as the Google France case – has now reached the CJEU with the following questions having been referred

---

[1] See e.g. Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press; Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[2] CNIL. (2015) *CNIL orders Google to apply delisting on all domain names of the search engine* 12 June. [online] Available from: http://www.cnil.fr/english/news-and-events/news/article/cni-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine [Accessed 2 April 2017].

to it by the Conseil d'État of France:

> *"1. Must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment of 13 May 2014 on the basis of the provisions of Articles 12 (b) and 14 (a) of Directive [95/46/EC] of 24 October 1995, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de--referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46/EC] of 24 October 1995?*
>
> *2. In the event that Question 1 is answered in the negative, must the "right to de-referencing", as established by the Court of Justice of the European Union in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States of the European Union?*
>
> *3. Moreover, in addition to the obligation mentioned in Question 2, must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46/EC] of 24 October 1995, regardless of the domain name used by the internet user conducting the search?"*[3]

[3] Google Inc. v. Commission nationale de l'informatique et des libertés (2017), C-507/17.

Thus, a bit simplified the CJEU has been asked to rule on the following: Must a search engine operator deploy the de-referencing to all of the domain names used by its search engine?

If not, must a search engine operator only remove the links on the domain name corresponding to the State in which the request is deemed to have been made or on the national extensions used by that search engine for all of the Member States of the European Union?

Must a search engine operator use "geo-blocking"? If so, only from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States?

The binary nature of the questions advanced by the Conseil d'État is both crude and inadequate, and I would rather be inclined to a different moulding of the relevant issues. In my view, we can get out of the quagmire and regain firm ground only if we realise that this is not an area that lends itself to such simplistic binary questions.[4] Rather, what we are dealing with – the appropriate protection of personality rights – will always be a matter of degree.

At any rate, as cannot be disputed, the dilemma facing the CJEU goes beyond pure EU law since the EU – unsurprisingly – is subject to international law. Indeed, the fact that e.g. EU law *"is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union"*[5] is not in dispute.

Thus, evaluating the Google France matter requires us to consider what international law actually tells us about jurisdiction. And evaluating that question necessitates us considering a range of core concepts in international law – most prominently – the concepts of sovereignty and jurisdiction. However, we need also briefly pay some attention to comity and some relevant aspects of international human rights law. The article then considers whether the way international law deals with Internet jurisdiction could be informed by a perhaps somewhat unorthodox source of wisdom – Viking era drinking etiquette.

However, before discussing how international law deals with

[4] I provide a detailed discussion of how to approach scope of (remedial) jurisdiction in Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, pp. 171–190.

[5] Judgement of 21 December 2011, The Air Transport Association of America and Others, C-366/10, EU:C:2011:864 , paragraph 101.

jurisdiction for a case such as this, it is relevant to first make a few observations as to how international law approaches the Internet and the legal issues to which the Internet gives rise.

2. INTERNATIONAL LAW AND THE INTERNET

Unfortunately, Internet-related legal issues are still treated as fringe issues in both public, and private, international law. Anyone doubting this claim need only take a look at the tables of content of textbooks and journals in those respective fields. However, approaching Internet-related legal issues in this manner is becoming increasingly untenable. Let us consider the following:

Tech companies feature prominently on lists ranking the world's most powerful companies. For example, on *Foreign Policy's list of "25 Companies Are More Powerful Than Many Countries"*[6] ten of the listed companies are from the tech industry, and perhaps somewhat less importantly, six of the top 10 companies on *Forbes' list of the world's most valuable brands are tech companies* (with the four top spots being Apple, Google, Microsoft and Facebook).[7]

With its more than two billion users[8], Facebook alone has more "citizens" than any country on earth; and no other communications media comes even close to the Internet's ability to facilitate cross-border interactions – interactions that often have legal implications.

While statistics arguably may be used to prove just about anything, the message stemming from the above is clear and beyond intelligent dispute – cross-border Internet-related legal issues are central matters in society and need to be treated as such also in public, and private, international law.

A particularly relevant matter is that of Internet jurisdiction. The harms caused by the current dysfunctional approach that international law takes to jurisdiction are as palpable as they are diverse. The territoriality-centric approach to jurisdiction causes severe obstacles for law enforcement's fight

---

[6] Khanna, P. (2016) *These 25 Companies Are More Powerful Than Many Countries*. [online] Foreign Policy. Available from: http://foreignpolicy.com/2016/03/15/these-25-companies-are-more-powerful-than-many-countries-multinational-corporate-wealth-power/

[7] Forbes. *The World's Most Valuable Brands.* [online] Forbes.com. Available from: https://www.forbes.com/powerful-brands/list/#

[8] Constine, J. (2017) *Facebook now has 2 billion monthly users… and responsibility.* [online] Techscrunch.com. Available from: https://techcrunch.com/2017/06/27/facebook-2-billion-users/ [Accessed 27 June 2017].

against both traditional – and cyber – crime, it undermines the protection of important human rights, it amounts to an obstacle for e-commerce and it creates uncertainties that undermine the stability online with an increased risk for cyber conflict as the result. Thus, Internet jurisdiction is one of our most important and urgent legal challenges. And we all need to get involved.

3. INTERNATIONAL LAW, SOVEREIGNTY AND JURISDICTION

Having attended a range of workshops and other meetings relating to the way we should approach Internet-related legal matters, it seems to me that the label "international law" sometimes is used as a lawyers' version of the well-known children's game "Simon says". In that game, all proposed actions are to be ignored unless prefaced with the phrase "Simon says", in which case the instructions must immediately be complied with.

At workshops and other meetings, I have too often seen the phrase "international law says" play a very similar role. Too often, proposed actions are ignored – regardless of their intrinsic value, merit or sensibility – while at the same time, any instructions prefaced with the phrase "international law says" are treated as almost holy – regardless of their lack of intrinsic value, lack of merit and lack of sensibility. The problems caused by this are augmented by the lack of scrutiny directed at whether international law also "says" other things that in fact contradict and clash with the first statement as to what "international law says".

I think there are at least two, related, reasons for this. First, international law – and even more so commentaries on international law – are replete with absolutist statements that are better suited for the political arena than they are for law; statements that then can be (ab)used in the pursuit of particular positions in legal discussions. Consider, for example, the following statement made by the Permanent Court of Arbitration in *the Island of Palmas case*:

> *"[t]erritorial sovereignty, as has already been said, involves the exclusive right to display the activities of a State."*[9]

Such a statement is clearly overly broad and open to abuse. To see that

[9] Island of Palmas (Neth. v. U. S.), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

this is so, we need only consider that it is incompatible with the nationality principle and the effects doctrine.

Second, international law is complex and inaccessible to the degree that many non-experts are forced to uncritically accept the preaching of those who claim to "know" what international law "says". This means that claims as to what international law "says" too rarely are disputed. Put simply, those who speak with conviction about what international law instructs us to do are too rarely challenged.

In this section, I want to briefly discuss *the concept of sovereignty* – a key concepts for the Google France matter, and for international law generally and a concept that I argue is much less settled than is commonly thought. I also briefly discuss *the concept of jurisdiction* and how the two concepts relate to each other.

3.1 SOVEREIGNTY – A (MISUSED) KEY CONCEPT

Perhaps the most fundamental concept in international law is the concept of sovereignty. And while various aspects of the sovereignty concept have been debated more or less constantly, reading the international law textbooks provides the sensation that sovereignty has a well-established meaning. For example, as Endicott puts it:

> *"Sovereignty, it seems, is: absolute power within a community, and absolute independence externally, and full power as a legal person in international law."*[10]

Turning to primary sources, the conventional starting point for discussions of sovereignty is found in *the Island of Palmas* case which teaches that:

> *"Sovereignty […] signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."*[11]

Put simply, conventional thinking treats the concept of sovereignty as a right to independence and exclusiveness.

Yet this conventional wisdom has come under fire recently, and the true

[10] Endicott, T. (2010) The Logic of Freedom and Power. In: Besson, S. and Tasioulas, J. (eds.) *The Philosophy of International Law*. Oxford: Oxford University Press, pp. 245–259.

[11] Island of Palmas (Neth. v. U. S.), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

nature of the concept of sovereignty is in fact far less settled than we often are led to believe. Important aspects of the current debate are showcased with great clarity in an excellent *Symposium on Sovereignty, Cyberspace, and the Tallinn Manual 2.0* published in 2017 in the American Journal of International Law Unbound.[12]

In their contribution, *Gary P. Corn* (a Staff Judge Advocate, United States Cyber Command) and *Robert Taylor* (a Former Principal Deputy General Counsel, U. S. Department of Defense) argue that:

> *„Some argue that […] sovereignty is itself a binding rule of international law that precludes virtually any action by one state in the territory of another that violates the domestic law of that other state, absent consent. However, law and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention."*[13]

While stated in the context of state cyber operations, these observations have much broader impact, and indeed, much broader appeal. In essence, *Corn and Taylor* argue that: (a) sovereignty is an underlying principle that cannot be violated *per se*, (b) but that sovereignty, as expressed in the relatively clear proscriptions against unlawful use of force and unlawful interventions, can be violated, and that (c) everything else is a grey-zone in relation to which the underlying principle of sovereignty tells us little or nothing.[14]

---

[12] Ginsburg, T. (2017). Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. *AJIL Unbound*, 111, pp. 205–206. Available from: doi: 10.1017/aju.2017.58

[13] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–212. Available from: doi: 10.1017/aju.2017.57

[14] Corn and Taylor state:*"Through both custom and treaty, international law establishes clear proscriptions against unlawful uses of force and prohibits certain interventions among states. And while questions remain as to the specific scope and scale of cyber-generated effects that would violate these binding norms, the rules provide a reasonably clear framework for assessing the legality of state activities in cyberspace above these thresholds, including available response options for states. Below these thresholds, there is insufficient evidence of either state practice or opinio juris to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states "actions in cyberspace"."* Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–208. Available from: doi: 10.1017/aju.2017.57

I agree with *Corn and Taylor* that sovereignty is an underlying principle that cannot be violated *per se*. As I have argued together with *Polcak* in a discussion about dignity and sovereignty:

> *„The problem is that both of these concepts [sovereignty and privacy] too often are treated as rights on their own while they both actually consist of subsets of rights. For example, […] sovereignty is protected by tools such as jurisdictional exclusiveness over the state's territory and the duty of non--interference placed on other states."*[15]

However, in the sharpest contrast imaginable, *Schmitt and Vihul* point to international law cases where the activities in dispute where held to *"only constituted violations of sovereignty, not unlawful interventions or uses of force"*[16] and suggests that, in the light of such cases

> *"no conclusion can be drawn other than that the principle of sovereignty operates as a primary rule of international law."*[17]

This is, unsurprisingly, in line with how the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* approaches sovereignty.[18] *Schmitt and Vihul* also noted, in relation to their work on he Tallinn Manual 2.0:

> *"In Tallinn Manual 2.0, we, together with the seventeen other members of the so-called "International Group of Experts", found that violations of sovereignty could be based on two different grounds: "(1) the degree of infringement upon the target state's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions.""*[19]

While it may seem counterintuitive at a first glance, I suspect that the end result here is that *Schmitt and Vihul* give sovereignty a more limited scope of operation than do *Corn and Taylor*. After all, according to S*chmitt*

---

[15] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing, p. 63.

[16] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press.

[17] Ibid. At 215.

[18] Rule 4 states: *"A State must not conduct cyber operations that violate the sovereignty of another State"*.

[19] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55., p. 215.

and Vihul – assuming they are indeed endorsing the Tallinn Manual 2.0 definition just alluded to – violations of sovereignty must stem from one of the two different grounds they put forward, grounds that correspond with the conventional view of sovereignty. In contrast, while *Corn and Taylor* do not recognise sovereignty as a right that can be violated *per se*, they do see it as the foundation for two distinct rights – protection against the unlawful uses of force and unlawful interventions – that can be violated, as well as the foundation for a grey area.

Be that as it may, the fact that experts on this level take so fundamentally different positions on such a centrally important matter is no doubt telling in itself – also the very core concepts of international law remain in contention. And in the end, I suggest that the reality is that both *Schmitt/Vihul* and *Corn/Taylor* are wrong in part and right in part, although admittedly I am closer to side with *Corn and Taylo*r.

On my reading of the *lex lata*, sovereignty is not a right capable of being violated *per se*, rather it is as *Corn and Taylor* note the foundation for the relatively clear proscriptions against unlawful use of force and unlawful interventions. In addition, the principle of sovereignty is the foundation for a selection of other recognised international wrongs to which S*chmitt and Vihul*, as well as *Spector*, direct our attention.[20]

In other words, at this stage only two principles have sprung from the principle of sovereignty; that is proscriptions against use of force and unlawful intervention. And in addition to those rules there are pockets of clarity in what otherwise is a grey-zone. Those pockets are represented by the cases *Schmitt, Vihul* and *Spector* mention but they do not currently form comprehensive and defined rules and they certainly do not transform the principle of sovereignty into a norm of international law capable of being violated as such.

There is one more point made by *Corn and Taylor*, to which I want to draw attention:

> *„The fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace.*

[20] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55.; and Spector, P. (2017). In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223. Available from: doi: 10.1017/aju.2017.56

The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules."[21]

This is a very important observation. Not only does it provide support for the idea that sovereignty is an underlying principle rather than a right *per se*, it also highlights that whatever way in which sovereignty is dealt with in other areas, there is scope for applying it differently in the online environment. After all, if sovereignty takes the shape of *lex specialis* in other fields, it can do so in the relation to the Internet arena as well, should we conclude that that is the better option.

Before moving on to consider the concept of jurisdiction, it is interesting to pause to consider what the above means for the Google France matter. In doing so, two things stand out.

First, orders requiring global de-listing, or indeed any form of de-listing going beyond the European Union, are difficult to reconcile with the traditional understanding of sovereignty. Put simply, deciding what content is accessible, for example in New Zealand, is an exercise of a State function for New Zealand. Thus, where the EU determines what is delisted for Internet users in New Zealand, it is arguably interfering with New Zealand's sovereignty.

Second, on the more sophisticated reading of the concept of sovereignty envisaged above – that of sovereignty as a principle of international law – we need to assess how cross-border de-listing orders fit in what currently is a grey-zone. In other words, under the more sophisticated reading of the concept of sovereignty, the CJEU has considerable scope to use its creativity to contribute to a fruitful and balanced development of the international law on sovereignty.

3.2 JURISDICTION – A (MISUNDERSTOOD) KEY CONCEPT

There are many notions regarding jurisdiction in general, and Internet jurisdiction in particular, that are widely relied upon in the academic community and beyond. The two key sources for those notions are the (in)famous *Lotus case* (1927)[22], and the widely cited, but poorly understood, *Harvard Draft Convention on Jurisdiction with Respect to Crime*

[21] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–212. Available from: doi: 10.1017/aju.2017.57

[22] S.S. "Lotus" (France v. Turkey) (1927) PCIJ Series A, No. 10.

(1935)[23] – both seen to put the supremacy of the territoriality principle beyond question. With a sleep-walking like acceptance, these authorities are treated as clear, exhaustive and almighty.

However, those who have truly studied jurisdiction in detail generally take a different view. For example, *Ryngaert*[24] and *Mann*[25] have both questioned whether the *Lotus* decision remains good law. And as I have sought to show elsewhere, pretty much every aspect of how we classify jurisdictional claims – including the distinction between jurisdiction under public international law and jurisdiction under private international law, as well as the distinction between territorial and extraterritorial jurisdiction – is less settled than it often is portrayed as being and may usefully be called into question.[26]

At any rate, if we adopt the conventional classification of jurisdiction; legislative, adjudicative and enforcement, what we are dealing with in Google France must clearly fall within so-called *enforcement jurisdiction*. But what does that mean in practical terms? To gain an insight into some form of mainstream view of the applicable international law, we can usefully draw upon the conclusions reached by-the group of eminent experts who, in 2017, produced the Tallinn Manual 2.0. As noted in the Tallinn Manual 2.0:

> *"States generally do not possess enforcement authority outside their territory. Rather, such jurisdiction is an exclusive attribute of sovereignty and, as such, may only be exercised extraterritorially with the consent of the State in which the jurisdiction is to be exercised or pursuant to a specific allocation of authority under international law."*[27]

The implications of this for the Google France matter seem undisputable. In the absence of a specific ground to point to that takes the de-listing orders outside the scope of this general rule, a de-listing order going beyond the European Union, is difficult to reconcile with the traditional

[23] Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime (1935) A*merican Journal of International Law,* 29 Supp 443.

[24] Ryngaert, C. (2015) *Jurisdiction in International Law*. 2nd edition. Oxford: Oxford University Press, p. 34.

[25] Mann, F. (1996) The doctrine of Jurisdiction in International Law. In: Karl M Meesen (ed.), *Extraterritorial Jurisdiction in Theory and Practice*. Kluwer Law International, p. 66.

[26] See further: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, in particular pp. 159–170.

[27] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press, pp. 52–53.

understanding of the limits international law imposes on enforcement jurisdiction.

3.3 THE RELATIONSHIP BETWEEN SOVEREIGNTY AND JURISDICTION

Convention may have us believe that the scope of jurisdiction is determined by the reach of sovereignty. However, few steps can be taken in such a direction without getting tangled in conflicting wisdoms. To bring forward just one illustration; if the scope of jurisdiction is determined by the reach of sovereignty, and sovereignty is delineated by reference to territorial borders, how do we explain recognised forms of extraterritorial jurisdiction, such as jurisdictional claims based on the nationality of an offending party?

More generally, as noted by *Khan*:

> *„[I]n recent years there are increasing signs that the traditional and rather categorical symbiosis between territory and power may no longer lay a legitimate claim for exclusivity. This is hardly deplorable since from an international law perspective, possession and transfer of territory have never been considered an end in itself. L'obsession du territoire of modern States was always meant to serve people, not vice versa."*[28]

All this illustrates that, while there are obvious indirect links between jurisdiction and sovereignty, there is no necessary direct link between these concepts as such. In response to this, some will hasten to drag forward the old argument that jurisdiction ultimately depends on enforcement. However, I seriously question whether people who do so have really thought through the implications of what they then are saying. Surely, we need to distinguish between law, on the one hand, and brute power, on the other hand, even if doing so means that we have to accept (a) that law can be of value even if it cannot be enforced, and (b) that not all enforcement actions are legitimate?

The observations made here as to the relationship between jurisdiction and sovereignty may not have any direct impact on the Google France matter. Nevertheless, they do draw attention to the complexity

[28] See, eg. Khan, D. E. (2012) Territory and Boundaries. In: Bardo Fassbender and Anne Peters (eds.), *The Oxford Handbook of the History of International Law*. Oxford: Oxford University Press, p. 248 (footnote omitted).

of the relevant aspects of international law that must be taken into account by the CJEU.

4. COMITY

To the issues raised above, we may add that both the notion of international comity, and international human rights law can be seen to speak against the crude and simplistic global delisting sought by the CNIL. As to the former, it must be admitted that neither the scope, nor the application, of comity is uncontroversial. In fact, the concept of comity does not lend itself to being easily pinned down. As a result, there are both divergent definitions and divergent views of the value of comity. Here it will have to suffice to note that arguably the most widely used definition would have us view comity in the following terms:

> *„Comity in the legal sense, is neither a matter of absolute obligation on the one hand nor of mere courtesy and good will upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, and to the rights of its own citizens or of other persons who are under the protection of its laws."*[29]

In light of statements such as this, there can be little doubt that the concept of comity may be seen to speak against de-listing order going beyond the European Union.

5. INTERNATIONAL HUMAN RIGHTS LAW

The fact that de-listing orders involve the balancing of different human rights is obvious and need not be elaborated upon. However, one thing that is important to remember is that, as the human rights of non-EU citizens would be affected by the type of orders sought by the CNIL, the CJEU must consider international human rights law; notably the *International Covenant on Civil and Political Rights* (ICCPR), not merely European human rights law. And as was emphasised in the Tallinn Manual 2.0:

> *"restrictions on the right to seek, receive, and impart information pursuant*

[29] Hilton v. Guyot (1895) 159 US 113 (1895), at 164. For a more elaborate discussion of the concept of comity, see, e.g. Briggs, A. (2012) The Hague Academy of International Law, Recueil des Cours, 354 , p. 94.

> *to Article 19 of the ICCPR must satisfy a tripartite test: they must be provided for by law under the clearest and most precise terms possible, foster a legitimate objective recognised by international law, and be necessary to achieve that objective."*[30]

All aspects of this tripartite test may pose a challenge for global delisting orders. Most obviously, it may be difficult to argue that providing the "right to be forgotten" in a situation such as that in Google Spain makes it necessary to delist search results in Fiji, in the Falkland Islands or even in Finland.

6. THE CONCEPT OF "LAGOM"

The above has pointed to the complex international law concepts the CJEU must tackle in adjudicating Google France. But let us now go back in time to the tables of the longhouses in Viking-era Scandinavia. There is a word said to be quite unique to the Swedish language. The word *lagom* means "just enough" or "just right". At least according to folklore, it stems from the phrase *laget om* ("around the team") from the Viking tradition of drinking enough when the drinking horn was passed around, without drinking so much that there is not enough for everyone.

Whether this is the proper origins of the word lagom or not, support for the lagom concept as a guiding principle in Viking drinking etiquette can be found in *Hávamál*. Hávamál is a combination of different poems, attributed to the Norse god Odin, presenting advice for living, proper conduct and wisdom.[31] In Verse 19 we can read Odin's instruction to:

> *"Keep not the mead cup but drink thy measure"*.[32]

I think the concept of lagom – with or without a "divine" origin – is apt indeed to describe how we must approach the issue of Internet jurisdiction. Most obviously, neither excess nor abstinence are acceptable paths forward; that is, emptying the drinking horn before everyone has had a chance to get their fair share would be an insult to their dignity, but a refusal to take part in the drinking would be equally insulting to the dignity of others.

---

[30] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press, p. 202.

[31] Hávamál (2018) [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/

[32] Ashliman, D. L., Bray, O. (2003) *Hávamál* [online] Available: from: http://www.pitt.edu/~dash/havamal.html

Similarly, states should not make excessive jurisdictional claims, as doing so offends the dignity of other states, but equally well, they should not decline to exercise jurisdiction where doing so is called for, as also such inactivity may offend the dignity of other states.

Further, the lagom doctrine incorporates a context-specific proportionality. If the drinking horn is large, or the group of people sharing it small, each member can drink more than if the proportions are in the reverse. In the same manner, jurisdictional claims (and their scope) need to be adjusted to the context. However, the comparison goes further than that. In fact, it is possible to link numerous international law concepts to the lagom doctrine.

Consider the concept of "comity" that clearly can be seen in the requirement of not drinking excessively so as to preclude others from partaking. Or why not the "due diligence" requirement that states must ensure that other states' rights and interests are not violated due to activities over which the first state has jurisdiction; whether we are talking about drinking or about jurisdiction, everyone must partake and claim their share.

In the light of the above, perhaps it can be said to be the case that – at their core – our international law principles on jurisdiction are no more advanced than was the Viking-era drinking etiquette? And perhaps they do not need to be?

7. "LAGOM JURISDICTION"AND THE GOOGLE FRANCE MATTER

Sweden is often described as *landet lagom* (i.e. the country of "lagom") and the lagom attitude can perhaps be detected in the approach taken by the Swedish Data Protection Authority (Datainspektionen) as to "right to be forgotten" delisting:

> *"The DPA's assessment is that the obligation to delete search results means that results must be deleted in such a way that they are not shown when searches are made from Sweden. But, there may be situations where search results must be deleted also when searches are made from other countries. This may be the case if there is a specific connection to Sweden and to the data subject, for example if the information on the webpage which is linked to is written in Swedish, addressed to a Swedish audience, contains information about a person that is in Sweden or if the information has been*

published on the Swedish domain.se", says Martin Brinnen, legal advisor within the Swedish DPA."[33]

This approach is interesting, and the "specific connection" requirement seems to be at least a new phrase (be as it may that it shares commonalities with similar concepts). But the idea that e.g. the use of a Swedish domain – on its own – should determine the scope of jurisdiction seems both naive and misguided.

In any case, it is clear that the *Datainspektionen* has made an attempt to approach the territorial scope of delisting orders in a balanced manner, which stands in stark contrast to the excessive approach taken by its French equivalent (the CNIL). This is important even though further work is needed for the correct balance to be struck. If nothing else, the Datainspektionen has proven the appropriateness of the old Swedish saying that *lagom är bäst*; that is,"lagom is best".

8. CONCLUDING REMARKS

The discussion above has sought to suggest that – at their core – our international law principles on jurisdiction are hardly more advanced or sophisticated than was the Viking-era drinking etiquette, and that arguably they do not need to be. However, the above has also demonstrated something else. The discussion of international law has showcased the complex manner in which we articulate these principles, as well as the degree of lacking consensus as to how we should formulate and approach these principles. And in the light of this, absolutist statements as to what "international law says" in relation to sovereignty and jurisdiction must always be met with a healthy dose of scepticism.

The reality is that international law on sovereignty and jurisdiction is largely a grey-zone populated by conflicting legal rules and principles. Much work lies ahead and in the Google France matter, the CJEU is presented with an interesting opportunity to interpret applicable international law in a manner that helps to steer it in a sensible direction.

But Internet jurisdiction is not just a matter for the courts and other law makers. And it is not just a matter for Internet lawyers. Further, it is not just a matter for the public international law crowd, and it is not just a matter

[33] Datainspektionen. (2017) *The right to be forgotten may apply all over the world.* [online] Datainspektionen. Available from: https://www.datainspektionen.se/press/nyheter/theright-to-be-forgotten-may-apply-all-over-the-world/ [Accessed 4 May 2017].

for those inhabiting the domain of private international law – Internet jurisdiction is a key issue in all of these fields. And, importantly, it is a matter we will only be able to address when the experts from these fields join forces and approach jurisdiction in an open-minded manner.

To this we may add that, addressing Internet jurisdiction is, in fact, a matter for us all — industry, government, courts, international organisations, civil society, and the academic community — to help achieve useful change. Furthermore, those engaged in capacity-building initiatives must recognise that they need to incorporate capacity building in relation to a sound understanding of the jurisdictional challenges and solutions.

Much work lies ahead. But it is crucially important work and we must now turn our minds to these issues to which we, for far too long, have turned a blind eye.

LIST OF REFERENCES

[1] Ashliman, D. L., Bray, O. (2003) *Hávamál* [online] Available: from: http://www.pitt.edu/~dash/havamal.html

[2] Briggs, A. (2012) The Hague Academy of International Law, Recueil des Cours, 354.

[3] CNIL. (2015) *CNIL orders Google to apply delisting on all domain names of the search engine* 12 June. [online] Available from: http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine [Accessed 2 April 2017].

[4] Constine, J. (2017) *Facebook now has 2 billion monthly users… and responsibility.* [online] Techscrunch.com. Available from: https://techcrunch.com/2017/06/27/facebook-2-billion-users/ [Accessed 27 June 2017].

[5] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207-212. Available from: doi: 10.1017/aju.2017.57.

[6] Datainspektionen. (2017) *The right to be forgotten may apply all over the world*. [online] Datainspektionen. Available from: https://www.datainspektionen.se/press/nyheter/the-right-to-be-forgotten-may-apply-all-over-the-world/ [Accessed 4 May 2017].

[7] Endicott, T. (2010) The Logic of Freedom and Power. In: Besson, S. and Tasioulas, J. (eds.) *The Philosophy of International Law*. Oxford: Oxford University Press, pp. 245–259.

[8] Forbes. *The World's Most Valuable Brands.* Forbes.com [online] Available from: https://www.forbes.com/powerful-brands/list/#.

[9] Ginsburg, T. (2017). Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn

Manual 2.0. *AJIL Unbound*, 111, pp. 205–206. Available from: doi: 10.1017/aju.2017.58

[10] Google Inc. v. Commission nationale de l'informatique et des libertés (2017), C-507/17.

[11] Hávamál (2018) [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/

[12] Hilton v. Guyot (1895) 159 US 113.

[13] Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime. (1935) *American Journal of International Law*, 29 Supp 443.

[14] Island of Palmas (1928), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

[15] Judgement of 21 December 2011, The Air Transport Association of America and Others, C-366/10, EU:C:2011:864.

[16] Khan, D. E. (2012) Territory and Boundaries. In: Bardo Fassbender and Anne Peters (eds.), *The Oxford Handbook of the History of International Law*. Oxford: Oxford University Press.

[17] Khanna, P. (2016) *These 25 Companies Are More Powerful Than Many Countries.* [online] Foreign Policy. Available from: http://foreignpolicy.com/2016/03/15/these-25-companies-are-more-powerful-than-many-countries-multinational-corporate-wealth-power/

[18] Mann, F. (1996) The doctrine of Jurisdiction in International Law. In: Karl M Meesen (ed.), *Extraterritorial Jurisdiction in Theory and Practice*. Kluwer Law International.

[19] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[20] Ryngaert, C. (2015) *Jurisdiction in International Law*. 2nd edition. Oxford: Oxford University Press.

[21] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press.

[22] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55

[23] Spector, P. (2017). In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223. Available from: doi: 10.1017/aju.2017.56

[24] S.S. "Lotus" (France v. Turkey) (1927) PCIJ Series A, No 10.

[25] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.

[26] Svantesson, D. (2017) *Time for international law to take the Internet seriously.* [online] OUPblog. Available from: https://blog.oup.com/2017/10/international-law-internet/ [Accessed 7 October 2017].

DOI 10.5817/MUJLT2018-1-3

DELICTUAL LIABILITY FOR DAMAGE CAUSED BY FULLY AUTONOMOUS VEHICLES: THE ESTONIAN PERSPECTIVE

by

TAIVO LIIVAK[*], JANNO LAHE[**]

Self-driving vehicles have become a reality. For instance, in the summer of 2017, self-driving buses carried passengers on a designated route in Estonia's capital Tallinn. Regrettably, traffic accidents involving self-driving vehicles have also become a reality. This article focuses on fully autonomous vehicles. The safe and responsible use of fully autonomous vehicles calls for appropriate rules and an appropriate allocation of liability. Above all, fully autonomous vehicles pose a challenge to the law of delict. The article seeks to establish, based on the example of Estonian law, whether the application of delictual liability is affected by the autonomy of a vehicle and, if so, whether related differences are significant, and whether the law of delict needs to be modified in the light thereof. The issues are discussed primarily in the context of Estonian law, but parallels with German law are drawn as well. The conclusions drawn are more or less universal and can be taken into account also in other jurisdictions besides Estonia. The article analyses liability for damage caused by fully autonomous vehicles under general delictual liability, strict liability and product liability.

KEY WORDS

Autonomous Vehicles, Delictual Liability, Product Liability, Self-driving Vehicles, Strict Liability

[*] taivo.liivak@ut.ee, Ph.D. candidate, Tartu University Law School, Estonia.

[**] janno.lahe@ut.ee, Professor of Law of Delict, Tartu University Law School, Estonia; Adviser to the Civil Chamber of the Supreme Court of Estonia.

1. INTRODUCTION

In the summer of 2017, passengers in Estonia's capital Tallinn were carried by self-driving buses in the course of a month-long international pilot project.[1] Although the buses rode along a short route separated from conventional traffic, the test period was a landmark for Estonia, indicating that autonomous vehicles are becoming a reality.[2] Such vehicles are being developed by many established manufacturers as well as new market participants seeking to disrupt not only the transport sector, but also the ways in which vehicles are being manufactured.[3]

In technological terms, this article focuses on fully autonomous vehicles (*autonome Fahrzeuge*)[4] where all persons in the vehicle are merely passengers. Even though one of the main aims of developing fully autonomous vehicles is to improve road safety, traffic accidents involving fully autonomous vehicles cannot be precluded. On the one hand, the laws of physics simply do not allow for halting a vehicle in an instant. On the other hand, a fully autonomous vehicle may find itself in a so-called dilemma situation where it must "decide" which person to harm (for instance, whether to drive off the road and into a tree or hit a child who has run onto the road).[5] This so-called decision depends, above all, on how the software of the vehicle has been programmed.

In order to ensure the safe and responsible use of fully autonomous vehicles, appropriate rules and appropriate allocation of liability is crucial.[6] Vehicles driving in the autonomous mode and autonomous test vehicles

---

1 Government Office EU Secretariat. (2017) *Driverless buses arrive in Tallinn*. [press release] 14 July. Available from: https://www.eu2017.ee/news/press-releases/driverless-buses-arrive-tallinn [Accessed 30 May 2018].

2 In July 2017, the term "self-driving delivery robot" was added the Estonian Traffic Act (TA). It means a partially or fully automated or remotely controlled vehicle which moves on wheels or another chassis that is in contact with the ground, which uses sensors, cameras or other equipment for obtaining information on the surrounding environment and, based on the obtained information, is able to move partially or fully without being controlled by a driver (TA § 2 clause 68^1). The user and the controlling of a self-driving delivery robot was also defined (TA § 2 clauses 68^2–68^3).

3 See, for example, Geistfeld, M. (2017) A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, 105(6), pp. 1615–1616.

4 For a brief overview of the levels of driving automation see Smith, B. W. (2013) *SAE Levels of Driving Automation.* [blog entry] 18 December. Available from: http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation [Accessed 30 May 2018]; SAE International. (2014) J3016. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*. Available from: https://web.archive.org/web/20170903105244/https://www.sae.org/misc/pdfs/automated_driving.pdf [Accessed 30 May 2018].

5 For further information on the dilemma situation see Weber, P. (2016) Dilemmasituationen beim autonomen Fahren. *Neue Zeitschrift für Verkehrsrecht*, (6), pp. 249–254.

have already been involved in as well as caused numerous accidents, including those resulting in fatalities.[7] However, these vehicles were merely semi-autonomous.[8]

When a traffic accident occurs, civil liability issues arise. This article analyses delictual liability that arises or may arise from damage caused by a fully autonomous vehicle.[9] More specifically, the article seeks answers to the following questions: is the application of delictual liability affected by the fact of whether damage has been caused by a conventional motor vehicle or a fully autonomous vehicle; if so, are these differences significant; and does the law of delict need to be modified as a result thereof?

These issues are approached, above all, from the point of view of Estonian law of delict. At the same time, it is quite clear that analogous questions can be raised in many legal systems. In more important matters, comparisons are drawn with the legal rules, case-law and legal writings of the Federal Republic of Germany as a legal system which was the main role model for drafting Estonian civil law following the restoration of Estonia's independence in 1991. The law of delict provisions of the Estonian Law of Obligations Act (LOA)[10] distinguish between general

---

[6] Contissa, G. et al. (2013) Liability and automation: Issues and challenges for socio-technical systems. *Journal of Aerospace Operations,* (2), pp. 79–98. Available from: https://pure.tue.nl/ws/files/3915758/24573390365552.pdf [Accessed 30 May 2018].

[7] See, for example, Marshall, A. and Davies, A. (2018) *Waymo's Self-Driving Car Crash in Arizona Revives Tough Questions.* [online] Wired. Available from: https://www.wired.com/story/waymo-crash-self-driving-google-arizona/ [Accessed 30 May 2018]; Hawkins, A. J. (2018) *Uber 'Likely' not at Fault in Deadly Self-Driving Car Crash, Police Chief Says*. [online] The Verge. Available from: https://www.theverge.com/2018/3/20/17142672/uber-deadly-self-driving-car-crash-fault-police [Accessed 30 May 2018]; Weise, E. and Marsh, A. (2018) *Video Shows Google Self-Driving Van Accident in Arizona*. [online] USA Today, 5 May. Available from: https://eu.usatoday.com/story/tech/2018/05/04/google-self-driving-van-involved-crash-arizona-driver-injured/582446002/ [Accessed 30 May 2018]; Nicola, S., Behrmann, E. and Mawad, M. (2018) *It's a Good Thing Europe's Autonomous Car Testing Is Slow.* [online] Bloomberg. Available from: https://www.bloomberg.com/news/articles/2018-03-20/it-s-a-good-thing-europe-s-autonomous-car-testing-is-slow [Accessed 30 May 2018].

[8] They all had a driver responsible for actively overseeing the behaviour of the vehicle and taking over control. Because of problems with semi-autonomous driving, manufacturers such as, for instance, Ford and Google have decided to skip semi-autonomous driving altogether and aim straight for the highest level of autonomy. See Naughton, K. (2017) *Ford's Dozing Engineers Side with Google in Full Autonomy Push*. [online] Bloomberg. Available from: https://www.bloomberg.com/news/articles/2017-02-17/ford-s-dozing-engineers-side-with-google-in-full-autonomy-push [Accessed 30 May 2018].

[9] Of course, there may be a contract between the injured person and the person operating a fully autonomous vehicle under which damage is suffered (e.g. contract for carriage of passengers). Where damage has been caused by a breach of a contractual obligation, the claim for damages (under Estonian law) must usually be filed on the basis of provisions of contractual liability.

[10] *Law of Obligations Act (võlaõigusseadus) 2001*. SI 2001/81, 487. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/510012018003/consolide [Accessed 30 May 2018].

fault-based delictual liability (§§ 1043–1055), strict liability (§§ 1056–1060) and liability for a defective product (§§ 1061–1067). This distinction largely determines the structure of this article. The possibility to bring a claim for damages based on the provisions of strict liability or product liability does not restrict the right of the injured person (also called a victim, aggrieved person/party) to file a claim based on provisions governing general delictual liability (LOA § 1056(3) and § 1061(5)).

Although damage caused by a fully autonomous vehicle can, in principle, be indemnified by a motor insurance undertaking, the article focuses on the law of delict. The reason lies in the fact that the basis for the insurer's indemnification obligation is, in turn, the liability of the injuring person (in common law, tortfeasor). Therefore, the motor insurance undertaking of the injuring person is required to indemnify damage only where the injuring person (insured person) is liable for it and, in principle, solely to the extent the injuring person is liable towards the injured person.[11]

2. FULLY AUTONOMOUS VEHICLE AS AN INTELLIGENT MACHINE

A system is autonomous to the extent that its behaviour is determined by its own experiences.[12] Intelligence can be described as a way of coping with complexity and uncertainty owing to the ability to be aware of what is happening in the surrounding environment.[13] Thus, a fully autonomous vehicle can be considered an intelligent machine. For the purposes of this article, a fully autonomous vehicle means a whole, i.e. a combination of hardware and software. Thereby the article does not focus on how the vehicle's full autonomy is attained in technical terms, be it based

[11] On the prerequisites for and scope of the liability of an insurer see Lahe, J. (2017) Estland. In: Bachmeier, W. (ed.) *Regulierung von Auslandsunfällen*. 2nd edition. Baden-Baden: Nomos Verlagsgesellschaft, pp. 233–235; Lahe, J., Luik, O.-J. and Merila, M. (2017) *Liikluskindlustuse seadus. Kommenteeritud väljaanne*. Tallinn: Juura, pp. 98–100.

[12] Russell, S. J. and Norvig, P. (1995) *Artificial Intelligence: A modern approach.* New Jersey: Prentice Hall, p. 35.

[13] See, for instance, Sterling, L. and Taveter, K. (2009) *The Art of Agent-Oriented Modeling.* Cambridge: The MIT Press, p. 6. It should be added that artificial intelligence can be defined in various ways, but in essence, these definitions tend to refer to similar phenomena demonstrated by machines. Artificial intelligence can be divided into narrow artificial intelligence (surpasses humans only in specific tasks), artificial general intelligence (human-like abilities) and superintelligence (beyond human abilities). See Russell, S. J. and Norvig, P. (1995) op. cit., pp. 2, 23–28; see also Dickson, B. (2017) *What is Narrow, General and Super Artificial Intelligence*. [online] Tech Talks. Available from: https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/[Accessed 30 May 2018].

on certain predefined criteria which make it capable of "thinking and deciding", on a comprehensive code doing exactly what it is supposed to do, or on some other solution. By and large, it is not of decisive importance from the aspect of delictual liability.

Considerable advancements have been made in the field of expert systems, which are limited to specific areas of application, including fully autonomous vehicles, which increase the ability of road users to cope with the complexity of traffic. Traffic accidents occur largely due to reasons attributable to humans who fail to cope with such complexity. Fully autonomous vehicles are seen by many as a way to "tame" the complexity of road use and reduce the number of accidents as well as open access to transportation for people who are currently often left out (e.g. the elderly, people with disabilities, etc.).[14]

The six levels of driving automation suggested by a global association of engineers span from no automation to full automation.[15] Full automation means that at all times the automated driving system performs all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.[16] Some argue that, given the ability of fully autonomous machines to make highly consequential decisions in situations that may not be anticipated by their creators, society will need to consider whether existing liability rules will be up to the task of assigning responsibility for the acts they commit.[17]

---

[14] As intelligent machines become more sophisticated in their ability to solve problems, a host of issues arise concerning the moral responsibilities for the acts of intelligent machines sophisticated enough to raise the possibility that they are moral agents and hence morally accountable for their acts (see Himma, K. E. (2009) Artificial Agency, Consciousness, and the Criteria for Moral Agency: What Properties Must an Artificial Agent Have to Be a Moral Agent? *Ethics and Information Technology*, 11(1), pp. 19–29. Available from: https://doi.org/10.1007/s10676-008-9167-5 [Accessed 30 May 2018]. Some even wonder whether intelligent machines should be granted personhood of sorts or be recognised as special-purpose animals or people (see Chopra, S. and White, L. F. (2011) *A Legal Theory for Autonomous Artificial Agents*. The University of Michigan Press., p. 153; Calo, R. (2015) Robotics and Lessons of Cyberlaw, *California Law Review*, 103(3), p. 549.

[15] These levels are not normative, but technical. The elements indicate minimum rather than maximum system capabilities for each level. A particular vehicle may have multiple driving automation features. SAE International. (2014) J3016. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*. Available from: https://web.archive.org/web/20170903105244/https://www.sae.org/misc/pdfs/automated_driving.pdf [Accessed 30 May 2018].

[16] Ibid.

[17] Vladeck, D. C. (2014) Machines without Principals: Liability Rules and Artificial Intelligence. *Washington Law Review*, 89 (1), pp. 117–150. Available from: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1322/89WLR0117.pdf?sequence=1 [Accessed 30 May 2018].

3. GENERAL DELICTUAL LIABILITY FOR DAMAGE CAUSED BY FULLY AUTONOMOUS VEHICLES

Under § 1043 of the LOA[18], a person who unlawfully causes damage to another must compensate for the damage where the person who caused damage is at fault thereof or bears statutory liability for causing the damage. General delictual liability in Estonia is, similarly to general delictual liability under the German Civil Code (BGB),[19] built in three stages. As a general rule, objective elements (*objektiver Tatbestand*) are verified at the first stage: the act of the person who causes damage, damage to the rights of the injured person, and a causal link between them. The second stage views unlawfulness and the third one is the fault of the injuring person.

In the event of damage caused by a fully autonomous vehicle, engaging in traffic may be deemed to be the act of the injuring person. The injured person's legal right that is being violated can, above all, be their life (LOA § 1045(1) clause 1), health (LOA § 1045(1) clause 2) or property (LOA § 1045(1) clause 5). The same applies to damage caused by a conventional motor vehicle. Likewise, establishing a causal link between the act of the injuring person and the damage suffered by the injured person is not special in any way.[20]

At the second stage of the criteria for general delictual liability, the unlawfulness of causing damage is established. Clauses 1–4 of LOA § 1045(2) establish the circumstances that preclude the unlawfulness of causing damage (e.g. consent or self-defence). Where damage is caused by the driver of a conventional motor vehicle, the unlawfulness can alternatively arise from a violation of a protective provision (LOA § 1045(1) clause 7 in combination with a protective provision in the TA[21]) or be based on the general catalogue of causing unlawful damage (LOA § 1045(1) clause

[18] *Law of Obligations Act (võlaõigusseadus) 2001*. SI 2001/81, 487. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/510012018003/consolide [Accessed 30 May 2018].

[19] Bamberger, H. G. et al. *Beck'scher Online-Kommentar zum BGB*. [online] 45th edition, § 823, Rn. 15–41. Available from: https://beck-online-beck-de.ezproxy.utlib.ut.ee/?vpath=bibdata%2fkomm%2fBeckOKBGB_45%2fBGB%2fcont%2fBECKOKBGB%2eBGB%2eP823%2eglI%2egl3%2ehtm [Accessed 30 May 2018].

[20] According to the Estonian legal approach, a causal link is established in two stages. First, the natural cause for damage is assessed (the *conditio sine qua non* test). Next, an assessment of the legal cause for the damage is made by asking whether the purpose of the breached rule was to obligate the injuring person and safeguard the injured person for the specific kind of damage (LOA § 127(2)). See alsoTampuu, T. (2017*) Lepinguvälised võlasuhted (Non--contractual obligations)*. Tallinn: Juura, p. 213.

2 – causing a bodily injury or health damage to the injured person; § 1045(1) clause 5 – infringement of ownership).

In the event of infringement of absolute legal rights such as human life, health or ownership, unlawfulness is based on the harmful effect as such, while it is not important whether the injuring person also violated any obligation. Unlawfulness comes from the wrongfulness of the outcome (*Erfolgsunrecht*).

Establishing unlawfulness merely based on the harmful effect is, however, not an exceptionless rule even in the event of infringing the absolutely protected legal rights. Where an absolutely protected right has been infringed by failure to act or where the harmful effect is a more remote outcome of the conduct of the injuring person, a duty which the latter has breached (*Handlungsunrecht*) must be identified. It may be a statutory duty or the general duty to maintain safety (*generale Verkehrssicherungspflicht*).[22]

While in the event of damage caused by a conventional motor vehicle the unlawfulness of causing damage can usually be derived from harming the injured person's legal right (or, alternatively, also from a violation of the provisions of the TA), it is rather questionable in the event of damage caused by a fully autonomous vehicle. One might argue that, for instance, in a situation where a person is inside a fully autonomous vehicle that causes a traffic accident, the person has not harmed the injured person's legal right by their active conduct. In such an event, the damage caused by the person who was inside the vehicle cannot be deemed to be unlawful owing to the mere harming of the injured person's legal right. In order to hold the person inside the vehicle liable, a duty which the person has breached should be established. Presumably, it cannot be a statutory duty (e.g. under the TA). Thus, the liability of the liable person can be based, above all, on a breach of the general duty to maintain safety. According to Estonian case-law, the general duty to maintain safety and the element of fault are entwined.[23] Thus, when examining if a person has breached

[21] *Traffic Act (liiklusseadus)* 2010. SI 2010/44, 261. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/521122017002/consolide [Accessed 30 May 2018].

[22] According to Estonian case-law, the general duty to maintain safety means a person's duty to make every reasonable effort to ensure that other persons are not harmed as a result of the persons' actions (see Case no. 3-2-1-73-13 (2013) Supreme Court (Civil Chamber), 20 June 2013).

[23] Case no. 3-2-1-73-13 (2013) Supreme Court (Civil Chamber), 20 June 2013.

the general duty to maintain safety, one must substantively assess whether the person has been externally (i.e. objectively) negligent.[24] It has been argued in the context of German law that putting "blind trust" in the autonomous vehicle technology over a long period may constitute a breach of the duty to maintain safety.[25] Under Estonian law, one could partly agree with the opinion. The owner or possessor of a fully autonomous vehicle might be hypothetically criticised for a breach of the general duty to maintain safety where the vehicle is not properly serviced (e.g. software updates have not been made in a timely manner) or where detected errors are not reacted to "maintaining safety" should not usually require more of the owner or possessor.

The fault of the injuring person is the third main criterion of the general delictual liability.[26] The types of fault are negligence, gross negligence and intent (LOA § 104(2)). Negligence is failure to exercise necessary care (LOA § 104(3)). Gross negligence is failure to exercise necessary care to a material extent (LOA § 104(4)). Intent is the will to bring about an unlawful consequence upon creation, performance or termination of an obligation (LOA § 104(5)). In Estonian law of delict, the injured person's fault (incl. negligence) must also be assessed based on the characteristics of the injuring person. Under LOA § 1050(2), the situation, age, education, knowledge, abilities and other personal characteristics of a person must be taken into consideration upon assessment of the fault of the person. Under LOA § 1050(1), the negligence of the injuring person is presumed, i.e. the injuring person who wishes to avoid liability must prove the absence of their fault.

In the event of damage caused by a fully autonomous vehicle, the absence of fault (or a breach of the duty to maintain safety) may be the reason why general delictual liability is not applicable to the owner or possessor of the vehicle (or a person who simply travelled in the fully

---

[24] The Supreme Court explained in its 20 June 2013 judgment in case no. 3-2-1-73-13 that since the general duty to maintain safety means, according to the generally recognised view, a duty of care for the purposes of the legal theory, negligence is one of the forms of fault under LOA § 104(2) and LOA § 1050(1) establishes that a person who unlawfully caused damage is presumed to be at fault, the defendant has the burden to prove that it did not breach the general duty to maintain safety.

[25] Volker, M., Jänich, P. T. and Schrader, V. R. (2015) Rechtsprobleme des autonomen Fahrens. *Neue Zeitschrift für Verkehrsrecht*, 28(7), p. 316.

[26] For a comparative discussion on the fault of the injuring person see Lahe, J. (2013) The Concept of Fault of the Tortfeasor in Estonian Tort Law: A Comparative Perspective. *Review of Central and East European Law*, 38(2), pp. 141–170.

autonomous vehicle at the time of the traffic accident). For instance, if a fully autonomous vehicle causes damage to a third party due to a bug in the control program, one cannot usually argue that the owner or possessor of the vehicle failed to exercise due care or perform the duty to maintain safety. As noted above, the situation may prove different where the vehicle has not been duly maintained or serviced. Nevertheless, it may be concluded that usually it is not reasonable or fruitful for the injured person who has suffered damage caused by a fully autonomous vehicle to bring a claim against the owner or possessor of the vehicle based on provisions governing general delictual liability.

In view of the above, it can be concluded that the injured person's ability to enforce their claim on the basis of general delictual liability is considerably affected by the fact of whether the damage was caused by a conventional motor vehicle or a fully autonomous vehicle. The difference will not create a deep practical issue where the injured person's chances of receiving compensation for damage are sufficiently ensured using other instruments, above all, legislation on strict liability and product liability.

4. STRICT LIABILITY FOR DAMAGE CAUSED BY FULLY AUTONOMOUS VEHICLES

Strict liability is liability for damage caused by a greater source of danger regardless of fault. In case of strict liability, attention is not paid to the act or fault of the injuring person, but it is examined if the harmful effect was caused by the manifestation of a higher risk characteristic of the thing or activity. Thus, being in control of the greater source of danger, the operator of a motor vehicle is liable for the damage caused regardless of whether the operator violated the TA while engaging in traffic or whether the operator was at fault. The causing of damage by a greater source of danger means the emergence of damage as a result of the manifestation of a heightened risk inherent in a thing or activity that constitutes the greater source of danger.[27] As noted by H. Koziol, strict liability means liability for dangerousness.[28] In Europe, the application of strict liability in case of damage caused by a motor vehicle is widespread.

[27] See Case no. 3-2-1-161-10 (2011) Supreme Court (Civil Chamber), 2 March 2011.

[28] Koziol, H. (2012) *Basic Questions of Tort Law from a Germanic Perspective*. Wien: Jan Sramek Verlag, p. 234.

It has been argued that in countries where there is no strict liability, the same end result for the injured person is reached with the help of the insurance system or by raising the required standard of care.[29]

Where a motor vehicle causes damage, the easiest solution for the injured person is to build its claim for damages on LOA § 1057, which states that the direct possessor of the motor vehicle is liable for any damage caused upon operating[30] the motor vehicle.[31] Under clause 40 of § 2 of the TA, a power-driven vehicle means a vehicle that is powered by an engine, except for an engine-powered vehicle designated for use solely by a person with reduced mobility, an electric cycle, a self-balancing vehicle, a mini moped, a self-driving delivery robot, an off-road vehicle, a tram and a vehicle with a manufacturer speed of no more than six kilometres per hour. It should be added that the definition of a motor vehicle used in LOA § 1057 is broader than the definition of a power-driven vehicle used in the TA, because under the respective provision of the LOA, for instance, an aircraft is also deemed to be a motor vehicle. Thus, it is obvious that a fully autonomous vehicle can be considered a motor vehicle within the meaning of LOA § 1057.

Under LOA § 1057, only the direct possessor of a motor vehicle can be held liable. Under the Law of Property Act (LPA)[32] § 33(1), a possessor is a person who has actual control over a thing. The second subsection of the same section states that a person who possesses a thing under a commercial lease, residential lease, deposit, pledge or other similar relationship which grants the person the right to possess the thing of another person temporarily is the direct possessor, while the other person is the indirect possessor. According to the case-law of the Estonian Supreme

---

[29] von Bar, C. (2009) *Principles of European Law: Non-Contractual Liability Arising out of Damage Caused to Another*. Munich: Sellier European Law Publishers, p. 703.

[30] Damage is caused upon operating a motor vehicle, above all, when it arises from the purposeful use of the motor vehicle as a motor vehicle in traffic. The slow movement of a vehicle or, in exceptional circumstances, the static status of a vehicle on the road may be considered operating the vehicle (see Case no. 3-2-1-7-13 (2013) Supreme Court (Civil Chamber), 19 March 2013).

[31] In LOA § 1056(1), the application of strict liability is limited to cases where (in the given context, by operating a motor vehicle) the death of a person, a bodily injury or health damage has been caused or where a thing has been damaged. In German law, strict liability relating to a motor vehicle is not provided for in the BGB, but in § 7 of the Strassenverkehrsgesetz (StVG), according to subsection 1 of which the liability of the keeper (*Halter*) of a motor vehicle is not dependent on fault. However, the liability of the driver is fault-based (StVG § 18(1)).

[32] *Law of Property Act* (*asjaõigusseadus*). 1993. SI 1993/39, 590. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/504012018002/consolide [Accessed 7 June 2018].

Court, the liability under LOA § 1057 rests with, above all, the person who has actual control over a motor vehicle regardless of the legal ground or absence thereof. In other words, with the person who controls the vehicle by deciding when and where it moves, bears the related costs and economic risks, and enjoys advantages arising from using the vehicle.[33]

The driver of a motor vehicle is not always deemed to be having actual control over the vehicle. The most common situation in that regard is the performance of employment duties using the employer's motor vehicle. Under LPA § 33(3), a person who exercises actual control over a thing according to the orders of another person in the household or enterprise of the other person is not a possessor. Thus, in the given case LOA § 1057 is not applicable to an employee either.[34] At the same time, the servient possessor may still be liable under provisions governing fault-based delictual liability. As noted above, it would not be an effective option from the point of view of a person who has suffered damage caused by a fully autonomous vehicle, because usually delictual liability would be precluded due to the absence of fault or breach of the duty to maintain safety by the servient possessor. Thus, it may be concluded that, unlike with conventional vehicles, the liability of persons other than the direct possessors is considerably more limited in the event of damage caused by fully autonomous vehicles. It could also be argued that it is a reasonable solution, for an employee should not be held liable for causing damage with a fully autonomous vehicle in a situation where nothing is imputable to the employee regarding the damage caused.

The Estonian LOA also sets out general strict liability.[35] It can be argued with high certainty that a fully autonomous vehicle should be considered a greater source of danger for the purposes of LOA § 1056(2) (at least until the time when technology allows for avoiding accidents entirely). Thus, it

[33] Case no. 3-2-1-7-13 (2013) Supreme Court (Civil Chamber), 19 March 2013.

[34] Varul, P. et al. (2009) *Võlaõigusseadus III. Kommenteeritud väljaanne (Law of Obligations Act. Commented Edition. Vol. III)*. Tallinn: Juura, p. 696.

[35] The first sentence of LOA § 1056(1) states: *"where damage is caused as a result of a danger characteristic of an especially dangerous thing or activity, the person who controls the source of danger is liable for causing the damage regardless of the person's fault."* Under LOA § 1056(2), a thing or activity is deemed to be a greater source of danger where, due to its nature or to the substances or means used in connection therewith, major or frequent damage may arise therefrom even where due diligence expected of a professional is exercised. Where liability for causing damage by means of a source of danger is prescribed by law, it is presumed that the thing or activity constitutes a greater source of danger regardless of the fault of the person who controlled it. It should be noted that there is no general clause on strict liability in Germany. A brief overview concerning discussions on a general clause of strict liability in European law of delict is given in Koziol, H. (2012), op. cit., pp. 236–238.

cannot be precluded that the driver of a motor vehicle who does not qualify as the direct possessor of the vehicle under LOA § 1057 can still be deemed to be in control of the greater source of danger for the purposes of LOA § 1056(1) (the owner of the vehicle who is not the direct possessor could likewise be considered to be in control of the greater source of danger – such need may arise, for instance, in the event of the insolvency of the direct possessor). Even though this view has not yet been confirmed in Estonian case-law, there is substance for such a discussion owing to a decision of the Supreme Court. The court held that a person who is riding a horse but who is simultaneously not the keeper of the animal for the purposes of LOA § 1060 may be deemed to be in control of a greater source of danger under LOA § 1056(1).[36]

The fact that the respective provision contains a list of events where the strict liability of the direct possessor of the motor vehicle does not apply can be seen as the main problem in connection with the application of LOA § 1057. Under LOA § 1057 clauses 1–5, the provision does not apply where:

1) the damage is caused to a thing being transported by the motor vehicle and not being worn or carried by a person in the vehicle;
2) the damage is caused to a thing deposited with the possessor of the motor vehicle;
3) the damage is caused by *force majeure* or by an intentional act on the part of the injured person, unless the damage is caused upon operation of an aircraft;[37]
4) the injured person participates in the operation of the motor vehicle;
5) the injured person is carried without charge and outside the economic activities of the carrier.

[36] Case no. 3-2-1-27-07 (2007) Supreme Court (Civil Chamber), 18 April 2007. The application of the general clause of strict liability (LOA § 1056) may be precluded by the fact that the injured person was somehow related to the greater source of danger. In the same decision, the Supreme Court noted that persons who participate in controlling a greater source of danger, place a greater source of danger under their temporary control or receive gains from controlling a greater source of danger are not, given the principle of good faith, entitled to claim on the basis of provisions governing strict liability that the person controlling the greater source of danger compensate for damage caused to them by the greater source of danger.

[37] The *force majeure* precluding the liability of the person controlling a greater source of danger may be an extraordinary natural phenomenon that assumes the position of the danger emanating from the greater source of danger and the impact of which the person controlling the greater source of danger or the injured person could not and did not have to take into account (Case no. 3-2-1-111-05 (2005) Supreme Court (Civil Chamber), 21 November 2005).

As noted above, in the case of these preclusions it is possible, based on LOA § 1056(3), to apply general delictual liability towards the direct possessor of the motor vehicle, but due to the absence of fault or a breach of the duty to maintain safety, it may prove ineffectual. Thus, at first glance, it may seem as a serious problem.

A closer look at the preclusions set out in LOA § 1057 clauses 1–5 allows for drawing a conclusion that these are unlikely to cause major practical problems also in the context of fully autonomous vehicles. As regards clauses 1 and 2, the injured person should, as a rule, be able to claim damages under contract law.[38] Where damage has been caused by an intentional act or *force majeure* (clause 3), the causal link between the manifestation of a risk inherent in a vehicle and the damage caused to the injured person is broken and the injured person should not be entitled to damages (we would reach the same result also upon application of general delictual liability towards the possessor of a conventional motor vehicle). Where the injured person participates in operating a motor vehicle (clause 4), they usually act on a contractual basis (travelling in a bus or taxi does not qualify as participating in operating a motor vehicle). Thus, claims for damages under contract law are possible.

Perhaps the most problematic one is the preclusion contained in clause 5. If A (the owner of a fully autonomous vehicle) carries B (an acquaintance of theirs) free of charge and outside their economic activities and an accident occurs in which B is injured, the application of LOA § 1057 to A is not possible and fault-based liability would probably be precluded by the absence of A's fault. In such a situation, there may but does not need to be a contract between A and B. It is possible that A was benevolently intervening in another's affairs (*negotiorum gestio*; *Geschäftsführung ohne Auftrag*) when carrying B. In the event where the intervention is justified, the beneficiary can claim damages, but only where the intervener was negligent (LOA § 1022(1)). Thus, the ultimate outcome may be that B cannot claim damages from A under any ground. Yet it can also be argued that this is a fair outcome, because B voluntarily accepted the respective risk. Besides, B will in any event retain the right to claim damages from the manufacturer of the fully autonomous vehicle.

[38] It should be added that, according to the general rule, contractual liability is similarly to strict liability not dependent on fault. The debtor is discharged from liability if the debtor breached a duty or obligation due to *force majeure* (LOA § 103(2)).

5. PRODUCT LIABILITY FOR DAMAGE CAUSED BY FULLY AUTONOMOUS VEHICLES

The issue of product liability is probably more burning regarding fully autonomous vehicles than conventional motor vehicles. In a situation where damage is caused by a fully autonomous vehicle, one can almost always raise the question of a defect of the fully autonomous vehicle. For instance, if the injured person demands that the direct possessor of the vehicle compensate for damage under LOA § 1057, the issue of product liability can usually be raised. This entitles the direct possessor who has compensated the injured person for damage to file a recourse claim against the manufacturer (provided, of course, that the manufacturer is indeed liable) based on LOA § 137(2), which regulates mutual recourse claims of persons that are jointly and severally liable for causing damage.

In the LOA, the rules regulating product liability are set out in §§ 1061–1067.[39] Keeping in mind fully autonomous vehicles, the following can be pointed out as prerequisites for product liability:

1) a legal right of the injured person has been infringed (death, bodily injury or health damage; with certain reservations also infringement of ownership;[40]
2) a defective fully autonomous vehicle has been put into circulation as a product;
3) there is a causal link between the defect of the fully autonomous vehicle and the damage caused to the injured person; and
4) the absence of circumstances precluding product liability.[41]

Under LOA § 1063(1), any movable, including electricity and computer software, is deemed to be a product, even where the movable forms a part of another movable or has become part of an immovable. Thus, both

[39] The rules are based on Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Union* (L 210) 7 August 1985. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1985.210.01.0029.01.ENG [Accessed 30 May 2018] and Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Union* (L 141) 4 June 1999. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/uri=uriserv:OJ.L_.1999.141.01.0020.01.ENG [Accessed 30 May 2018]. Thus, the product liability legislation of the Member States of the EU is largely similar.

[40] LOA § 1061(1) and (2).

[41] LOA § 1064.

the fully autonomous vehicle as a whole as well as, for instance, a computer program that controls the vehicle can be considered a product. By the same token, both the person who manufactured the fully autonomous vehicle as a whole as well as a part of the product (e.g. a computer program) can be considered the manufacturer.[42]

Thus, provided that the prerequisites for liability are met, the injured person can, in principle, file a claim for damages against the person who manufactured the fully autonomous vehicle as well as the persons who made parts thereof. Regardless of the seat of the manufacturer, the injured person can also file a claim against the manufacturer based on the place where the damaging act was committed or the damaging event occurred or based on the place where the damage was suffered.[43]

However, product liability is not absolute. LOA § 1064(1) stipulates that the manufacturer is not liable for damage arising from a product where the manufacturer proves that:

1) the manufacturer has not placed the product on the market;
2) circumstances exist on the basis of which it can be presumed that the product did not have the damage-causing defect at the time the product was placed on the market by the manufacturer;
3) the manufacturer did not make the product for sale or for marketing in any other manner and did not manufacture or market it in the course of the manufacturer's economic or professional activities;
4) the defect was caused by compliance of the product with mandatory requirements in force at the time of placing the product on the market;
5) given the level of scientific and technical knowledge at the time of placing the product on the market, the defect could not be detected.

Additionally, the producer of a raw material or a part of a product is not liable for damage where the producer proves that the defect of the raw

[42] LOA § 1062(1) clause 1.

[43] Section 94 of the *Code of Civil Procedure (CCP) (tsiviilkohtumenetluse seadustik)*. 2005. SI 2005/26, 87. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/506022018001/consolide [Accessed 7 June 2018]. In Estonia, injured parties do not usually bring claims against manufacturers. To date, the Supreme Court is yet to make its first decision based on product liability legislation.

material or part was caused by the construction of the finished product or the instructions given by the manufacturer of the finished product (LOA § 1064(2)).

Upon holding the manufacturer liable for damage caused by defects of a fully autonomous vehicle or parts thereof, the key question is, above all, how to apply LOA § 1064(1) clause 5. In other words, how extensive will be manufacturers' chances of proving that a defect of the product could not have been detected based on the scientific and technical level at the time. Too extensive application of this exception cannot be deemed reasonable regarding defects of fully autonomous vehicles, because otherwise the product liability legislation would largely lose its meaning in the context of new technologies.

Similarly to strict liability, the manufacturer can be held liable based on general delictual liability in a situation where product liability is precluded (LOA § 1061(5)). Where product liability rules are not applicable, for instance, because of LOA § 1064(1) clause 5, this fact allows the manufacturer to easily prove that it was not at fault regarding the damage and still be discharged from liability.

It can be argued that there are no differences of principle when it comes to the application of product liability provisions based on whether damage has been caused by a fully autonomous vehicle or a conventional motor vehicle. However, it cannot be precluded that in the case of fully autonomous vehicles the courts are more eager to apply the preclusion of liability arising from LOA § 1064(1) clause 5 in order not to impede technological development.

6. DIVISION OF LIABILITY IN THE EVENT OF MUTUAL DAMAGE

An important special problem in connection with fully autonomous vehicles may be the question of how to divide liability in a situation where a fully autonomous vehicle and a conventional motor vehicle have caused mutual damage.[44] In Estonian law, there is no separate legal rule for division of liability in the event of mutual damage caused by motor

[44] Where mutual damage has been caused by two fully autonomous vehicles, it should be possible to rely on the general rules applicable to situations involving mutual damage caused by two conventional motor vehicles.

vehicles.[45] However, the ultimate damages can be adjusted based on a general rule that regulates the reduction of damages (LOA § 139(1)), which states that where damage is caused in part by circumstances dependent on the injured person or due to a risk borne by the injured person, the amount of damages is reduced to the extent that such circumstances or risk contributed to the damage.[46]

The LOA is based on the idea according to which persons who have caused mutual damage with motor vehicles are (above all, based on LOA § 1057) fully liable for causing damage to each other in the first step, but the damages payable by either one of them can be adjusted on the basis of LOA § 139(1), i.e. the damages payable can be reduced because of the share of the injured person in causing the damage. Under LOA § 139, on the one hand, the circumstances arising from the motor vehicle operational risk and, on the other hand, circumstances characterising the behaviour of the drivers can be taken into account upon reducing the damages.[47]

The reason for taking into account the motor vehicle operational risk (*Betriebsgefahr*) lies in the understanding that once a person already engages in traffic using a motor vehicle (i.e. enters a dangerous situation), alone this fact is a sufficient ground for reducing the damages to a certain extent. In the framework of the operational risk, one can distinguish between the general operational risk and a special operational risk. The circumstances affecting the general operational risk include, for instance, the mass, dimensions, speed of movement, roadworthiness and safety equipment of the vehicle. Thus, the risk arising from a heavy truck may be considerably higher than the risk arising from a moped. A special operational risk means the objective nature and dangerousness of a specific

[45] Unlike in, for example, German law where, under StVG § 17, the obligation of multiple keepers of motor vehicles to compensate for damage caused to a third party depends on the circumstances of the accident, above all, on which person mainly caused the damage. Under StVG § 17(2), the principle set out in subsection 1 also applies upon division of mutual liability between keepers of motor vehicles where damage has been caused to a keeper of a motor vehicle involved in the accident. The respective provisions also apply where the damage has been mutually caused by a motor vehicle and a trailer, a motor vehicle and an animal, and a motor vehicle and a train (StVG § 17(4)).

[46] Special problems arise where more than two motor vehicles have been involved in causing damage. On such a situation see Bachmeier, W. (2010) *Verkehrszivilsachen*. 2nd edition. München: C. H. Beck, pp. 72–77.

[47] Case no. 3-2-1-7-13 (2013) Supreme Court (Civil Chamber), 19 March 2013. The same criteria are followed upon division of liability also in German law. See Säcker, F. J., Rixecker, R. and Oetker, H. (2012) *Münchener Kommentar zum Bürgerlichen Gesetzbuch. Band 2. Schuldrecht. Allgemeiner Teil*. 6th edition. München: Verlag C. H. Beck, p. 528.

manoeuvre. Thereafter, upon reducing the damages, it is important to also assess the behaviour of the persons who were involved in the accident, above all, whether they failed to exercise due care and disregarded the traffic rules.[48]

On the basis thereof, the extent of reduction of both parties' damages is established.[49] If the share of one person was higher in causing the accident, it must be taken into account upon reducing the damages on the basis of LOA § 139(1).[50]

According to the opinions established in Estonian case-law, the damages must be presumably reduced 50 % in a situation where both drivers breached the requirements for safe road use established in the TA and their share in the traffic accident was, given their behaviour as well as the operational risks emanating from their vehicles, more or less equal.[51] By way of exception, the damages can be reduced to the minimum or be precluded in a situation where it has been established that the accident was caused solely by a severe mistake of one person, as a result of which the other person who did not break the rules, could not reasonably avoid the accident.[52] In certain events, the share of the drivers involved in a traffic accident may also remain unknown. § 139 of the LOA is also applied where it is not proven that either person breached the traffic rules. In such an event, the basis for reducing the damages is the operating risks arising from the vehicles.[53]

---

[48] Case no. 3-2-1-7-13 (2013) Supreme Court (Civil Chamber), 19 March 2013.

[49] In German law, *Haftungsquoten*. For a detailed discussion of the case-law regarding liability quotas see Grüneberg, C. (2007) *Haftungsquoten bei Verkehrsunfällen. Eine systematische Zusammenstellung veröffentlichter Entscheidungen nach dem StVG*. 10th edition. München: Verlag C. H. Beck.

[50] Case no. 3-2-1-64-15 (2015) Supreme Court (Civil Chamber), 26 November 2015.

[51] In German case-law, liability is divided 50-50 in the case of an equal operational risk and fault. For further information see Grüneberg, C (2007), op. cit.

[52] Case no. 3-2-1-64-15 (2015) Supreme Court (Civil Chamber), 26 November 2015. Likewise, according to German case-law a person is discharged from the obligation to compensate for damage in the case of an unpreventable event (*unabwendbares Ereignis*). See Hentschel, P. (2003) *Strassenverkehrsrecht. Beck'sche Kurzkommentare.* 37th edition. München: Verlag C. H. Beck, pp. 227–231. Where the fault of a person is the overwhelming reason for the accident, it may eliminate the operational risk emanating from the other person's vehicle (Säcker, F. J., Rixecker, R. and Oetker, H. (2012), op. cit., p. 562). In general, a road user can rely on the fact that the other road user does not intentionally commit a severe breach of the traffic rules (Ibid., p. 537).

[53] Case no. 3-2-1-64-15 (2015) Supreme Court (Civil Chamber), 26 November 2015. According to the case-law established in Germany, the liability quota of either person is 50 % in such case. See Greger, R. (2007*) Haftungsrecht des Strassenverkehrs*. 4th edition. Berlin: De Gruyter Recht, p. 619.

In the case of fully autonomous vehicles, one must first decide how to assess the size of their operational risk. On the one hand, one could argue that the operational risk of fully autonomous vehicles should be higher than that of conventional vehicles, because they are merely controlled by a computer program and a human basically lacks the opportunity to "correct" the program's errors. On the other hand, it could be argued that the operational risk of a fully autonomous vehicle should be considered smaller, because such vehicles do not cause damage due to human error and refrain from causing damage in so far as possible according to the laws of physics. For instance, it may happen that upon manifestation of a risk the breaking distance of a fully autonomous vehicle is considerably shorter, because the program is able to initiate breaking with virtually no reaction time.

With fully autonomous vehicles it is not possible to take into account the driver's behaviour (whether the driver violated the traffic rules). Therefore, it seems that the operational risk of fully autonomous vehicles must be assessed based on rules different from those applicable to conventional motor vehicles. For example, while damages are usually reduced by approx. 20–30 % based on the operational risk,[54] there will likely be a need to deviate from this principle regarding fully autonomous vehicles and deem the operational risk of a fully autonomous vehicle to be higher than usual. This question is important because the reduction of the damages of one party to an accident affects the reduction of the damages of the other party. Presumably the ultimate result must be damages that do not exceed 100 % in total, i.e. if it has been identified that the damages of one party must be reduced to 40 %, those of the other must be reduced to 60 % in general.

When a fully autonomous vehicle, due to a programming error or otherwise, causes damage to an injured person who did not breach the traffic rules or was not negligent, the injured person's damages could be reduced only to the extent of the operational risk arising from their vehicle (20 % for instance, and therefore, the damages of the owner of the fully autonomous vehicle should be reduced presumably 80 %). Where a fully autonomous vehicle has caused damage in a way that in the case of a conventional vehicle would mean a severe mistake of the driver

[54] Säcker, F. J., Rixecker, R. and Oetker, H. (2012), op. cit., p. 562.

(e.g. driving onto the intersection while the traffic lights prohibit it), the damages of the owner of the fully autonomous vehicle should be reduced to zero and the damages caused to the injured person should be compensated for in full. Thus, the operational risk of the fully autonomous vehicles should be considered 100 % in such event. If the damages of the owner of the fully autonomous vehicle were reduced by merely 20–30 % in such an event, it would lead to a clearly unfair result for the other party involved in the traffic accident.

Finally, it may be argued that even though the fair division of liability in the event where damage is caused by a fully autonomous vehicle calls for certain adjustment of the practice of application of LOA § 139, it is not a complicated task upon shaping case-law. At any rate, there are no rules in Estonian law, which would prevent the courts from reaching a fair and just result upon division of liability in the described situations.

7. CONCLUSIONS

Fully autonomous vehicles will be put into daily operation soon. This scenario must also be taken into account in legislative drafting and case-law. As noted in the introduction, traffic accidents caused by semi-autonomous vehicles have become a reality. Thereby the main question is whether traditional rules of the law of delict adequately regulate liability for damage caused by fully autonomous vehicles. This question will arise in all countries where fully autonomous vehicles are introduced.

It can be argued that the application of delictual liability is affected by the fact of whether damage is caused by a conventional motor vehicle or a fully autonomous vehicle. Above all, it is expressed in the impossibility to apply the general fault-based liability towards the owner or possessor of a fully autonomous vehicle. The reason lies in the fact that usually the owner of a fully autonomous vehicle cannot be reproached for negligence or a breach of the duty to maintain safety. The difficulty of applying fault-based liability upon damage caused by a fully autonomous vehicle is universal and should also concern other legal systems besides Estonia. However, there is no reason to consider this a serious problem in practice, provided that the injured person is guaranteed damages based on provisions governing strict liability.

An analysis of Estonian law of delict allows for drawing a conclusion that, in most cases, the injured person can file a claim under LOA § 1057

against the direct possessor of the fully autonomous vehicle, regardless of their fault. If the direct possessor proves insolvent, general strict liability might be of help, for it allows for holding, for instance, the owner of the fully autonomous vehicle who is simultaneously not the direct possessor of the vehicle liable as a person in control of a greater source of danger. The application of LOA § 1057 is indeed restricted in the events specified in clauses 1–5, but these preclusions do not considerably affect the injured person's position. In the case of the preclusions, the injured person may have the right to claim damages under contract law (clauses 1, 2 and 4). In circumstances described in clause 3 of § 1057 of the LOA (the injured person's intent or *force majeure*), the injured person is clearly not entitled to damages. It is debatable whether the preclusion contained in clause 5 of § 1057 of the LOA (carrying the injured person free of charge and outside economic activities) is justified with regard to fully autonomous vehicles.

As for the application of provisions governing product liability, there are no fundamental differences based on whether damage arises from a defect of a fully autonomous or conventional motor vehicle. The fair and just division of liability for mutual damage caused by a fully autonomous vehicle and a conventional motor vehicle is possible without amending the law in force.

Thus, the Estonian example illustrates that the safeguarding of the rights of the injured person is not considerably influenced by whether the damage has been caused by a fully autonomous vehicle or a conventional motor vehicle. The traditional law of delict is largely able to safeguard the injured person regardless of the fact that fault-based liability cannot usually be applied regarding fully autonomous vehicles. However, the importance of product liability legislation may start to play a more important role in that regard. Therefore, there is no urgent need to amend the law of delict in the anticipation of fully autonomous vehicles. By and large, this conclusion should also apply to other countries where the structure of the law of delict resembles that of Estonia.

However, it cannot be precluded that in countries that have not introduced strict liability for damage caused by motor vehicles or where the preclusions of strict liability are considerable, the rules of the law of delict may need some modification. There would be no practical need for it in a situation where the insurance system guaranteed the injured person

compensation also in a situation where the injuring person was not liable for the damage.

LIST OF REFERENCES

[1] Bachmeier, W. (2010) *Verkehrszivilsachen*. 2nd edition. München: C. H. Beck.

[2] Bamberger, H. G. et al. *Beck'scher Online-Kommentar zum BGB*. [online] 45th edition, § 823, Rn. 15–41. Available from: https://beck-online-beck-de.ezproxy.utlib.ut.ee/?vpath=bibdata%2fkomm%2fBeckOKBGB_45%2fBGB%2fcont%2fBECKOKBGB%2eBGB%2eP823%2eglI%2egl3%2ehtm [Accessed 7 June 2018].

[3] Calo, R. (2015) Robotics and Lessons of Cyberlaw, *California Law Review*, 103(3), pp. 513–563.

[4] Case no. 3-2-1-111-05 (2005) Supreme Court (Civil Chamber), 21 November 2005.

[5] Case no. 3-2-1-27-07 (2007) Supreme Court (Civil Chamber), 18 April 2007.

[6] Case no. 3-2-1-161-10 (2011) Supreme Court (Civil Chamber), 2 March 2011.

[7] Case no. 3-2-1-7-13 (2013) Supreme Court (Civil Chamber), 19 March 2013.

[8] Case no. 3-2-1-73-13 (2013) Supreme Court (Civil Chamber), 20 June 2013.

[9] Case no. 3-2-1-64-15 (2015) Supreme Court (Civil Chamber), 26 November 2015.

[10] Chopra, S. and White, L. F. (2011) *A Legal Theory for Autonomous Artificial Agents*. The University of Michigan Press.

[11] *Code of Civil Procedure (tsiviilkohtumenetluse seadustik)* 2005. SI 2005/26, 87. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/506022018001/consolide [Accessed 7 June 2018].

[12] Contissa, G. et al. (2013) Liability and automation: Issues and challenges for socio--technical systems. *Journal of Aerospace Operations,* (2), pp. 79–98. Available from: https://pure.tue.nl/ws/files/3915758/24573390365552.pdf [Accessed 30 May 2018].

[13] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Union* (L 210) 7 August 1985. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/uri=uriserv:OJ.L_.1985.210.01.0029.01.ENG [Accessed 30 May 2018].

[14] Dickson, B. (2017) *What is Narrow, General and Super Artificial Intelligence*. [online] Tech Talks. Available from: https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/ [Accessed 30 May 2018].

[15] Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Union* (L 141) 4 June 1999. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1999.141.01.0020.01.ENG [Accessed 30 May 2018].

[16] Geistfeld, M. (2017) A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, 105(6).

[17] Government Office EU Secretariat. (2017) *Driverless buses arrive in Tallinn*. [press release] 14 July. Available from: https://www.eu2017.ee/news/press-releases/driverless-buses-arrive-tallinn [Accessed 30 May 2018].

[18] Greger, R. (2007) *Haftungsrecht des Strassenverkehrs.* 4th edition. Berlin: De Gruyter Recht.

[19] Grüneberg, C. (2007) *Haftungsquoten bei Verkehrsunfällen. Eine systematische Zusammenstellung veröffentlichter Entscheidungen nach dem StVG*. 10th edition. München: Verlag C. H. Beck.

[20] Hawkins, A. J. (2018) *Uber 'Likely' not at Fault in Deadly Self-Driving Car Crash, Police Chief Says.* [online] The Verge. Available from: https://www.theverge.com/2018/3/20/17142672/uber-deadly-self-driving-car-crash-fault-police [Accessed 30 May 2018].

[21] Hentschel, P. (2003) *Strassenverkehrsrecht. Beck'sche Kurzkommentare*. 37th edition. München: Verlag C. H. Beck.

[22] Himma, K. E. (2009) Artificial Agency, Consciousness, and the Criteria for Moral Agency: What Properties Must an Artificial Agent Have to Be a Moral Agent? *Ethics and Information Technology,* 11(1), pp. 19–29. Available from: https://doi.org/10.1007/s10676-008-9167-5 [Accessed 30 May 2018].

[23] Koziol, H. (2012) *Basic Questions of Tort Law from a Germanic Perspective*. Wien: Jan Sramek Verlag.

[24] Lahe, J. (2013) The Concept of Fault of the Tortfeasor in Estonian Tort Law: A Comparative Perspective. *Review of Central and East European Law*, 38(2), pp. 141–170.

[25] Lahe, J. (2017) Estland. In: Bachmeier, W. (ed.) *Regulierung von Auslandsunfällen*. 2nd edition. Baden-Baden: Nomos Verlagsgesellschaft.

[26] Lahe, J., Luik, O.-J. and Merila, M. (2017) *Liikluskindlustuse seadus. Kommenteeritud väljaanne*. Tallinn: Juura.

[27] *Law of Obligations Act (võlaõigusseadus)* 2001. SI 2001/81, 487. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/510012018003/consolide [Accessed 30 May 2018].

[28] *Law of Property Act (asjaõigusseadus).* 1993. SI 1993/39, 590. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/504012018002/consolide [Accessed 7 June 2018].

[29] Marshall, A. and Davies, A. (2018) *Waymo's Self-Driving Car Crash in Arizona Revives Tough Questions.* [online] Wired. Available from: https://www.wired.com/story/waymo-crash-self-driving-google-arizona/ [Accessed 30 May 2018].

[30] Naughton, K. (2017) *Ford's Dozing Engineers Side with Google in Full Autonomy Push*. [online] Bloomberg. Available from: https://www.bloomberg.com/news/articles/2017-02-17/ford-s-dozing-engineers-side-with-google-in-full-autonomy-push [Accessed 30 May 2018].

[31] Nicola, S., Behrmann, E. and Mawad, M. (2018) *It's a Good Thing Europe's Autonomous Car Testing Is Slow*. [online] Bloomberg. Available from: https://www.bloomberg.com/news/articles/2018-03-20/it-s-a-good-thing-europe-s-autonomous-car-testing-is-slow [Accessed 30 May 2018].

[32] Säcker, F. J., Rixecker, R. and Oetker, H. (2012) *Münchener Kommentar zum Bürgerlichen Gesetzbuch. Band 2. Schuldrecht. Allgemeiner Teil*. 6th edition. München: Verlag C. H. Beck.

[33] SAE International. (2014) J3016. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*. Available from: https://web.archive.org/web/20170903105244/https://www.sae.org/misc/pdfs/automated_driving.pdf [Accessed 30 May 2018].

[34] Smith, B. W. (2013) *SAE Levels of Driving Automation.* [blog entry] 18 December. Available from: http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation [Accessed 30 May 2018].

[35] Sterling, L. and Taveter, K. (2009) *The Art of Agent-Oriented Modeling.* Cambridge: The MIT Press.

[36] Russell, S. J. and Norvig, P. (1995) *Artificial Intelligence: A modern approach*. New Jersey: Prentice Hall.

[37] *Strassenverkehrsgesetz (StVG) (Road Traffic Act)* 2003. SI 2003/310, 919. In German.

[38] Tampuu, T. (2017) *Lepinguvälised võlasuhted (Non-contractual obligations)*. Tallinn: Juura.

[39] *Traffic Act (liiklusseadus)* 2010. SI 2010/44, 261. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/521122017002/consolide [Accessed 30 May 2018].

[40] Varul, P. et al. (2009) *Võlaõigusseadus III. Kommenteeritud väljaanne (Law of Obligations Act. Commented Edition. Vol. III)*. Tallinn: Juura.

[41] Vladeck, D. C. (2014) Machines without Principals: Liability Rules and Artificial Intelligence. *Washington Law Review*, 89 (1), pp. 117–150. Available from: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1322/89WLR0117.pdf?sequence=1 [Accessed 30 May 2018].

[42] Volker, M., Jänich, P. T. and Schrader, V. R. (2015) Rechtsprobleme des autonomen Fahrens. *Neue Zeitschrift für Verkehrsrecht*, 28(7), pp. 313–318.

[43] von Bar, C. (2009) *Principles of European Law: Non-Contractual Liability Arising out of Damage Caused to Another*. Munich: Sellier European Law Publishers.

[44] Weber, P. (2016) Dilemmasituationen beim autonomen Fahren. *Neue Zeitschrift für Verkehrsrecht*, (6), pp. 249–254.

[45] Weise, E. and Marsh, A. (2018) *Video Shows Google Self-Driving Van Accident in Arizona.* [online] USA Today, 5 May. Available from: https://eu.usatoday.com/story/tech/2018/05/04/google-self-driving-van-involved-crash-arizona-driver-injured/582446002/ [Accessed 30 May 2018].

<<< ARTICLES

REVIEWS >>>

DOI 10.5817/MUJLT2018-1-4

PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES. TIMAN, T.; NEWELL, B. C.; KOOPS, B.-J. (EDS.)*

by

JAKUB MÍŠEK**

Timan, T.; Newell, B. C.; Koops, B.-J. (eds.). (2017) Privacy in Public Space: Conceptual and Regulatory Challenges. Cheltenham: Edward Elgar Publishing, 315 p.

Privacy in Public Space is the eighth contribution in the Elgar law, technology and society series, published by Edward Elgar Publishing. The book is a collective monograph consisting of 10 chapters written by different authors, divided into two parts. Overlaying theme of the book is a challenge for privacy in public spaces that was brought by technological advancements. The book does not elaborate on privacy issues of online or virtual environment. The chapters are strictly focused on the technology--based intrusions of privacy in the actual physical world. Chapters in the first part, called *Philosophical and Empirical Insights*, are generally more theoretical and try to take new approaches in debating the topic. On the other hand, chapters in the second part, named *Law and Regulation*, describe specific legal problems, often comparing European and American way of regulation. The chapters are accompanied by an introduction (written by the editors)[1] and conclusion (written by Timan Tjerk)[2], which aims to bind the whole book together and provide a unifying frame.

* This review was created with the support of Masaryk University Grant No. MUNI/A/1015/2017.

** jkb.misek@mail.muni.cz, Ph.D. candidate and lecturer at the Institute of Law and Technology on Masaryk University, Brno, the Czech Republic.

1 See p. 1–15 of the book.

2 See p. 269–290 of the book.

The biggest problem of the publication, and in my opinion the only major problem of it, is that this binding and framing together does not really work well. The book is a mosaic of ideas and topics. Some of them are more prominent (like a notion of wearing masks which is a main theme of chapters 2 and 7, but can be found also in others[3], or accenting of the necessity of thinking about privacy in a specific context), some of them appear only to disappear and be absent for the rest of the book (human geography approach as is presented in the chapter 1). That is problematic for two reasons. Firstly, because of this issue, many questions remain unanswered. For example, it might be very interesting to read more about the mentioned human geography context, because the first chapter is only an introduction to the topic. However, next chapters do not follow up on that, but offer new themes and thought-provoking ideas concerning privacy in public. Absence of more thorough elaboration on specific issues leads to a certain disappointment. Secondly, it is not clear, why are these specific chapters (and topics they present) parts of the book or what is their role within it. Why were these specific texts chosen? Was that just because they were good on their own, or was there a higher intent? It is interesting that almost a third of the publication consists of texts which were previously published somewhere else (chapters 8[4], 9[5] and 10[6]). There are chapters which present a brand-new approach to understanding of privacy (e.g. chapter 1), chapters which summarise current state of knowledge (chapter 6) and chapters which look into the future and try to predict next development (chapter 10). Tjerk writes in the Conclusion that

> *"The common denominator in this book is that this data gathering happens in public space."*[7]

[3] E.g. part 3.1 of chapter 4 (pp. 98–101) where the author writes about self-protection measures for ensuring one's privacy in public space.

[4] The chapter is an abridged and updated version of paper Froomkin, A. M. (2015) Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, 67(5), pp. 1713–1790.

[5] Parts of the chapter come from Scherr, A. E. (2013) Genetic Privacy and the Fourth Amendment: Unregulated Surreptitious DNA Harvesting. *Georgia Law Review*, 47(2), pp. 445–526.

[6] Original version was published as Jones, M. L. (2015) Privacy without Screens & the Internet of Other People's Things. *Idaho Law Review*, 51(3), pp. 639–660.

[7] See p. 274 of the book.

All of the chapters truly fit into this description, most of them are interesting and bring good critical insights, but they just do not interplay between each other.

Because of this problem, the book is in fact closer to conference proceedings than to a monograph. It might not be a problem if the reader has adequate expectations.[8] However, chapters, or more precisely papers, present in the book are generally worth reading as the authors managed to bring forth interesting ideas and they discussed them properly.

In following paragraphs there are described in more detail four chapters which in my opinion were most interesting and show well width of topics and approaches present in the book. In chapter 2, named *Hidden in a plain sight*, Michael Nagenborg focuses on

> *"philosophical perspective on the usage of masks in the context of resistance to surveillance"*[9].

Nagenborg in his historical-philosophical analysis starts from the perspective that a mask is a tool used both for hiding (and obtaining anonymity as an individual) and recognizability (and obtaining identity as a member of a group). In this meaning the masks were used in ancient Rome, as well as in classic Shakespearean theatre and most recently during mass protests and civic uprisings (good examples are Anonymous masks in the shape of famous Guy Fawkes's mask or *pasamontana* used by the members of the Zapatistas movement). An interesting twist is brought by new technologies, especially mass surveillance of public places that is made possible thanks to a system of different types of cameras (e.g. long-distance CCTV, wearables etc.). In this context, Nagenborg mentions specific kinds of masking for which he uses the word *camouflage*[10]. It

> *"aims for making faces unreadable to machines by exploiting some of the underlying assumptions of face-recognition algorithms."*[11]

This technique uses a highly stylized make-up and hair styling, so the automatic system cannot recognise the face as a face. As the author

---

[8] The back cover of the book states that its content is created by multiple authors with different approaches so in this matter the book tries to set the expectations right.

[9] See p. 49 of the book.

[10] See p. 58 of the book.

[11] Ibid.

correctly mentions, this action is not helpful against human eyes; on contrary it brings attention to the wearer. However, this can be understood as a clear act of communication by which the wearer claims that she does not want to be automatically identified. We can see there a parallel with the "do not track" principles we meet in the context of online privacy.

In the book, there is a number chapters that provide a good comparative study of differences in legal regulation in Europe and in the United States. One of them is chapter 7 (*Covering up: American and European approaches to public facial anonymity after SAS v. France*) by Angela Daly, which is also directly connected with chapter 2, because it is concerned with right to cover one's face when being in public spaces. Daly analyses decision of the European Court of Human Rights in *SAS v. France*[12], in which the Court decided that prohibition of wearing of clothing designed to conceal one's face in public places does not violate basic human rights guaranteed by the Convention. Even though in this case was disputed wearing of Muslim face veils, the wording of the act in question is much broader and thus it applies on *"any facial covering worn for any motivation"*[13]. Unfortunately, as the author correctly mentions, the question of surveillance was not raised during the proceedings and thus it was not part of a balancing test. Daly then compares European regulation with anti-mask laws in the US. She explains different contexts of creation of such laws and what different outcomes would have similar situations. The writing is very clear and comprehensible, pointing out important facts. Unfortunately, the author did note use this opportunity to address the problem from the practical position of anti-surveillance camouflage. She mentions this only briefly in one paragraph at the very end of the chapter, saying that the solution is not clear, but that

> *"the SAS v. France decision does not seem to give a solid fundamental rights basis to using identity-obscuring techniques in Europe."*[14]

This is a missed opportunity. The chapter is a practical legal analysis, the author prepares ground that can be used for following argumentation

[12] Judgment of 1 July 2014, S.A.S. v. France, application no. 43835/11. Available from: http://hudoc.echr.coe.int/eng?i=001-145466

[13] Ibid; see p. 167 of the book.

[14] Ibid; see p. 182 of the book.

concerning allowance of anti-surveillance camouflage and then she decides to leave the questions open without even attempting to answer them.

A. Michael Froomkin in chapter 8 (*Privacy Impact Notices to address the privacy pollution of mass surveillance*) provides another interesting comparison of the European and US law when he tries to find a regulatory method which would be applicable in the US to combat mass surveillance. His starting point is that for number of reasons the US legislator will never accept European system, which might not be perfect, but is currently better suited for solving this issue. Froomkin therefore proposes that a possible way in the US might be to take inspiration from the local environmental protection regulation. Companies which conduct such surveillance should have a new duty to create in certain situations *Privacy Impact Notices* which will help to inform people about their data and their value. There are two points I would like to mention. Firstly, the author offers a list of data processing types which are categorically excluded from this duty. Some of the types are very specific (e.g. sporting events or surveillance of persistent protest) and from European point of view this is quite surprising, because regulation based on more abstract rules using a purpose as a regulatory cornerstone is much more flexible with maintaining of the same effect (in abovementioned examples the same purpose can be e.g. journalism). Secondly, connecting privacy data protection with environmental protection confirms the idea that personal data protection is (at least in part) a non-distributive right (a public good).[15]

Meg Leta Jones in chapter 10 (*The Internet of other people's things*) also compares European and American approaches to the privacy law and regulation of public spaces. Her chapter is focused on the near future, in which most of the screens of devices will be replaced by tangible, ambient computing. With that will be threatened one of the basic premises of personal data and privacy protection – informed privacy self--management. Leta Jones cites Daniel Solove and other authors and reminds the reader that even now, when we have screens with information available, is this concept problematic, at least. However, disappearance of screens will dissolve even this little basic justification. The author sees this as an opportunity, because the change is so big that it might create a new technological momentum, a phase during which a new technological

[15] For more information, in Czech, see Polčák, R. (2012) *Internet a proměny práva.* Praha: Auditorium, p. 342.

standard is set. If we are careful, the new standard can be designed in a way that it can overcome flaws of informed consent concept. Meg Leta Jones argues well what is needed to be done and is optimistic about the future. It is a really good paper, highly recommended to read.

The other chapters continue in the trend of very broad span of both thematic and methodological approaches. As examples can serve abovementioned chapter 1[16], in which Bert-Jaap Koops and Maša Galič take as a starting point human geography, chapter 4[17], in which Karsten Mause uses law and economics approach, and chapter 5[18], where Julia M. Hildebrand elaborates on the concept of "privacy bubbles" in the light of law and humanities approach.

Privacy in Public Space offers several interesting chapters (papers) in which authors provide insights from different fields and areas connected with privacy and publicity. The editors did a good work in selecting papers present in the monograph. Unfortunately, the chapters are not very connected together. If they were, the book would be more compact, more balanced and might have been even better in general, because the unanswered questions, which remained now, might have their answers there. However, in spite of that, the book contains a richness of information and for that it can be recommended.

LIST OF REFERENCES

[1] Froomkin, A. M. (2015) Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, 67(5), pp. 1713–1790.

[2] Jones, M. L. (2015) Privacy without Screens & the Internet of Other People's Things. *Idaho Law Review*, 51(3), pp. 639–660.

[3] Judgment of 1 July 2014, S.A.S. v. France, application no. 43835/11. Available from: http://hudoc.echr.coe.int/eng?i=001-145466

[4] Polčák, R. (2012) *Internet a proměny práva.* Praha: Auditorium, 392 p.

[5] Scherr, A. E. (2013) Genetic Privacy and the Fourth Amendment: Unregulated Surreptitious DNA Harvesting. *Georgia Law Review*, 47(2), pp. 445–526.

[16] The name of the chapter is *Conceptualizing space and place: lessons from geography for the debate on privacy in public*.

[17] The chapter is called *A politico-economic perspective on privacy in public spaces*.

[18] The chapter is named *Visually distant and virtually close: public and private spaces in the Archives de la Planete (1909-1931) and Life in a Day (2011)*.

DOI 10.5817/MUJLT2018-1-5

LEGAL PERSONHOOD: ANIMALS, ARTIFICIAL INTELLIGENCE AND THE UNBORN. KURKI, V. A. J.; PIETRZYKOWSKI, T. (EDS.)*

by

JAN ZIBNER**

Kurki, V. A. J.; Pietrzykowski, T. (eds.). (2017) Legal Personhood: Animals, Artificial Intelligence and the Unborn. Springer International Publishing, 158 p.

In 2017, Springer's *The Law and Philosophy Library*[1] was expanded by a next work in the philosophy of law which focuses on the theoretical research of a legal personhood in the context of chosen entities. The topic of legal personhood is discussed in a highly theoretical way which adds a huge potential to the book itself. Especially since animals, artificial intelligence (AI) and the unborn shall form the core of the research. However, the result remains slightly behind its potential. This review will describe briefly the content of the book selected into three parts (see below) and evaluate these parts separately following the individual descriptions.

Discussion of the legal personhood in the selected context is crucial when considering the question of an AI in the area of law. Nowadays, AI represents a significant challenge to the law because of the multiple options of its operation. For example, considering its role in copyright, an AI might be a principal element in the chain of creating the works. Following that, some part of the doctrine tries to understand the AI as an author. The problem is that the understanding of the AI is still prevailing in its own object-oriented form. However, the role of an AI as a subject of legal

* The review was written within the project PrF/08/2018: *"Conceptualization of the Artificial Intelligence"*.

** jan.zibner@mail.muni.cz, Ph.D. student at the Institute of Law and Technology on Masaryk University, Brno, the Czech Republic.

1 For more information about this series see: https://www.springer.com/series/6210

relationships – considering development of its capabilities and exploitation – is not anymore just wishful thinking.[2] Therefore it is necessary to examine the most basic principles and concepts in the context of an AI, including legal personhood.

The book itself consists of ten chapters by various authors and is logically divided into three parts. *Part One* conceptualizes the legal person and personhood *per se*, so that it establishes a theoretical background of the book. *Part Two* applies this theoretical concept of legal personhood to the non-personal subjects of law, such as animals, things and "machines". This part represents a more practical part of the book and its most valuable section trying to answer some important normative questions. Finally, *Part Three* discusses legal personhood in the view of bioethics and biolaw. In general, this part discusses the depersonalization and extraction of personhood from the human nature on the one hand and on the other hand it highlights the role of human rights. As a result, the book provides a unique and global assessment of legal personhood. Moreover, each chapter is followed by a special list of references which is very beneficial for the narrow focus and better insight to authors' researches, instead of the final list of references common to all the chapters.

As it was stated before, Part One, *"Identifying the Legal Person"*, discusses legal personhood purely in its theoretical sense and attempts to explain a historical context and background of the legal personhood idea. The development of the concept and its understanding are described in a very detailed way.[3] This part also refers to fundamental international documents on human rights and reflects the biological and ideological, as well as philosophical meaning of personality, personhood and other related terms. The first chapter, *Brożek: "The Troublesome 'Person'"*, highly relies on Engelhardt's position distinguishing people and persons.[4] Brożek strictly points out the criterion of humanity, consciousness and psychology when dealing with the legal personhood.[5] The second chapter, *Naffine:*

[2] The author of this review is dealing with the artificial intelligence as a technological challenge to copyright where an AI is analysed in a context of copyright with emphasis on its possible authorship of copyrighted works. For an AI as an author of such works, it is needed in the first instance to shift from its position as pure object of legal relationship to the position of subject. However, such shift is dependent on granting the (un)limited legal personhood to the AI.

[3] See especially p. 4–6 of the book.

[4] See p. 3 of the book.

[5] See p. 8 et seq. of the book.

"Legal Persons as Abstractions: The Extrapolation of Persons from the Male Case", does not deny any of previous atatements and broadens the knowledge with placing the person to the structure of the legal relationship as an analytical unit of the subject position.[6] Naffine discusses the legal fiction of personhood[7] and notices that individuals tend to be understood as mental and physical units.[8] Following that, it could be a question of whether the model of universal personhood is enough, or not, because of the role of gender.[9] Finally, the third chapter, *Lindroos-Hovinheimo: "Private Selves – An Analysis of Legal Individualism"*, concentrates on the position of legal personhood within the legal setting of EU law, emphasising the individuality and privacy issues. Lindroos-Hovinheimo divides the understanding of legal personhood into two groups, as a legal artifice and an ontological God-given nature.[10] In this context, legal personhood is connected to the area of privacy and personal data, and with the relation to *Solove's* taxonomy of privacy it is analysed there.[11] This EU--centric part brings out the inherent connection of privacy and personality; establishing their relevancy and need the for further analysis as the requirement for the legal subjectivity.[12]

The theoretical determination of personality and legal personhood in this part of the book is indeed brilliantly done. It perfectly helps to understand the discussed matter in a clear and concise manner. There could only be just one objection and it lies in better linking between theory and practice. This shortcoming may either be caused by the form of the book, or by the highly philosophical conception of the chapters.

Part Two, *"Persons, Animals and Machines"*, forms the core of the book as a practice-oriented discussion of legal personhood in the case of persons, animals and machines in three selected chapters. This part starts with analyzing the importance of the legal systems. The first chapter, *Pietrzykowski: "The Idea of Non-personal Subjects of Law"*, is based on reflection over purpose of the legal systems. These systems have been constructed as exclusively human creations and though they might still serve solely for

---

6 See p. 16 of the book.
7 See p. 16 et seq. of the book.
8 See p. 20 of the book.
9 See p. 25 of the book.
10 See p. 30 of the book.
11 See p. 32 et seq. of the book.
12 See p. 44 of the book.

the humans.[13] Following that, the idea of non-personal subjecthood is described within the discussion of the traditional dualism of persons (personhood) and things (thinghood) as well as their place in more or less complex legal relationship.[14] When talking about that, the personhood is sometimes being divided into personhood of human beings and juristic entities.[15] Furthermore, an effort is made to explain animal personhood in the context of human rights as well,[16] or the idea of deriving the legal personhood from the ability to feel and suffer which could help to recognize the personal and non-personal subjects of law.[17] This chapter ends with recommendations, controversies and warnings of granting the legal personhood to some entity, which is not a living human being, without proper analysis.[18] Next chapter, *Kurki: "Why Things Can Hold Rights: Reconceptualizing the Legal Person"*, focuses on an analysis of right-holding persons, and the development of such a concept.[19] There is an emphasis on Western jurisdictions regarding the fundamentals of paradigmatic natural persons,[20] the duties of legal persons, and their capacity to hold rights.[21] The main idea of this chapter is that the problem lies not in the unacceptability of granting the legal personhood to other entities but rather in the unimaginability of such a shift for many jurists. It is done by underlining the role of consciousness while there is a plethora of research indicating non-human animals can be conscious.[22] The situation is compared to slaves and their social role in history when the law established a special category for them.[23] This part of the book is concluded with the chapter, *Michalczak: "Animals' Race Against the Machines"*, where the idea of personhood for an AI is evaluated. Ethical questions are thoroughly described[24] as well as the apparent resemblance between AI's and an undeveloped child's intelligence, whereby brain activity is mooted

[13] See p. 49 of the book.
[14] See p. 51 et seq. of the book.
[15] See p. 54 of the book.
[16] See p. 57 et seq. of the book.
[17] See p. 58 of the book.
[18] See p. 60 et seq. of the book.
[19] See p. 71 of the book.
[20] See p. 74 of the book.
[21] See p. 82 of the book.
[22] See p. 80 of the book.
[23] Ibid.
[24] See p. 92 et seq. of the book.

as a relevant criterion for granting of personhood to AI.[25] There is also established a parallel between animals and AI through the conceptual and pragmatic argument which highlights the impossibility of animals to be granted with the legal personhood.[26] Following that, the legal subjectivity of software agents is analysed in the same way.[27] The chapter is concluded by describing the wartime and peacetime (trading) scenarios of AI subjectivization.[28]

This part should have been the most valuable part of the book. Nevertheless, I find it quite vague and half-empty when considering the possible extent of discussed topic; especially in the part dealing with the AI. While the question of personhood is adequately analysed as it relates to persons and animals, the AI problematics not so much. The arguments discussing the subjectivization of AI are well structured. However, there is missing further differentiation of AI's legal personhood, its limitations and discussion on the needs for the shift of comprehension that is required given the growing influence and importance of AI. When analysing the legal personhood of AI, it is not enough to focus only on ethical problems. It requires analysis of the fundamentals of personhood and their application to AI. The next problem lies with the conclusions of the chapters which are very broad and lack further elaboration of related ideas.

Part Three, *"Humanity, Personhood and Bioethics"*, summarizes the theory of legal personhood and argues the question of legal personhood in the case of non-personal entities in a view of bioethics, biolaw and other ethically problematic disciplines. The chapter, *Palazzani: "Person and Human Being in Bioethics and Biolaw"*, highlights the role of bioethics and "personism"[29]. It shows the utilitarian and libertarian theory of personality and their importance.[30] Palazzani states the personhood as the real condition for existence based on the ontological argument of sensitivity, rationality and will of the individuals.[31] Following chapter, *Silva: "From Human to Person: Detaching Personhood from Human Nature"*, appeals to human nature and its

[25] See p. 94 of the book.
[26] See p. 94 et seq. of the book.
[27] See p. 96 et seq. of the book.
[28] See p. 99 et seq. of the book.
[29] See p. 105 of the book.
[30] See p. 106 et seq. of the book.
[31] See p. 110 of the book.

crucial role. Silva here states that such nature can never be abound although there are apparent expanding efforts.[32] The chapter warns of the dangers of depersonalisation and highlights the purpose of the biological constitution and equity in that sense as possible clues for assessment.[33] Next, there is the chapter *Barbosa-Fohrmann et al.: "Are Human Beings with Extreme Mental Disabilities and Animals Comparable? An Account of Personality"*. This chapter is focused on the description of how the personal identity is created.[34] At this point, the role of *Kant's* idea of substantial self is criticized.[35] Barbosa-Fohrmann et al. are also dealing with vulnerability as a fundamental feature of humanity when talking about differences between humanity and animality.[36] Finally, the chapter, *Bielska-Brodziak et al.: "Is Sex Essential for Personhood? Being 'Halfway Between Female and Male' From the Perspective of Polish Law"*, discusses the question of gender and its role in the question of legal personhood. Bielska-Brodziak et al. analyse the question of sex from the biological and legal point of view.[37] The determination of the biological sex is described with a plethora of links to literature.[38] It is stated that determination of gender in a birth certificate could be sometimes problematic, especially for those who suffer from gender dysphoria or similar conditions.[39] By way of contrast Bielska-Brodziak et al. also present the possible pitfalls the absence of a birth certificate would present.[40]

This last part of the book highlights ethical problems and appeals to humanity. Concerning that, there is nothing to reproach because expanding the impact of legal personhood necessarily has ethical connotations. Still, this area could be considered more broadly. There are a lot of examples used in this part but only from the human or animal kingdom, while excluding the area of an AI (and machines). Yet, it is an AI that is so controversial and could serve as a clear example of whether it is right or wrong to grant legal personhood to something or somebody else than mankind. Furthermore, the final chapter feels out of place with the rest

[32] See p. 114 et seq. of the book.
[33] See p. 119 of the book.
[34] See p. 128 of the book.
[35] See p. 136 of the book.
[36] See p. 132 of the book.
[37] See p. 143 et seq. of the book.
[38] See p. 145 of the book.
[39] See p. 149 of the book.
[40] See p. 151 of the book.

of the book, as there are no obvious connections to the analysis of legal personhood in case of animals, AI or the unborn. The chapter focuses on disorders of sex development and incongruence between biological sex and sex assigned at birth. Instead of that, it might be more helpful to provide some summary, resumé or final remarks on before-mentioned knowledge, some recapitulation and drawing conclusions.

In conclusion, the book brings together general knowledge of legal personhood and comprehensively examines various levels of humanity and other entities. The way the book is structured into coherent – though quite independent – chapters helps to orientate in individual aspects of the problematics as well as to essentially illustrate such theoretical material. On the other hand, the division into distinct chapters impacts the consistency of the text possibly caused by limited choose of legislations of individual authors. It could benefit from short conclusions tieing ideas together between each part or as a final conclusion section. The book is very valuable when dealing with the legal personhood in the theoretical essence with emphasis on humanity, animals and unborn. However, the issue of AI is not dealt with in an exhaustive manner, even though it should have been one of the crucial parts of the book according to its luring title. Individual chapters may only serve as edification of all the crucial aspects of legal personhood which needed to bear in mind when talking about AI. The book shall be thus read by – and recommended to – those who are eager for deepening of their legal personhood knowledge base in the general way as well as from different angles. It may be helpful for those who are looking for a strong argumentation background. Unfortunately, for those longing for further AI analysis, the book could leave them simply unsatisfied, because the problematics of legal personhood in the case of AI could be analysed much more deeply.

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2017 Partner

Wolters Kluwer ČR, a. s.
www.wkcr.cz

Cyberspace 2017 Partner

Zákony pro lidi.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

Cyberspace 2017 Media Partner

PRÁVNÍ PROSTOR.CZ
www.pravniprostor.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeall (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/CitationguideMUJLT.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES

LIST OF REVIEWS