The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?

David Wicki-Birchler

International Cybersecurity Law Review
Zeitschrift für Cybersicherheit und Recht

ISSN 2662-9720

Int. Cybersecur. Law Rev.
DOI 10.1365/s43439-020-00012-5

Springer

Int. Cybersecur. Law Rev.
https://doi.org/10.1365/s43439-020-00012-5

The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?

David Wicki-Birchler

Received: 7 July 2020 / Accepted: 2 August 2020

Abstract The Budapest Convention and the General Data Protection Regulation (GDPR)—two Legal Frameworks designed to curb cybercrime. While the Convention on Cybercrime of the Council of Europe, the Budapest Convention, is the only binding international instrument on this issue, the GDPR is globally setting standards in data protection Law. How are the two policies working to curb cybercrime? Cybercrime concerns every person, every company, every authority and every public institution. The fact that the origin as well as the target of the criminal act can be located virtually everywhere around the globe sets a new challenge for lawmakers in their efforts to protect society. The increasing use and importance of the Internet of Things will create new conveniences for the public to enjoy and at the same time provide countless new entry points for hackers to gain access to devices, networks and valuable data, all of which might be abused for criminal intents. The Budapest Convention on Cybercrime plays a crucial role in the fight against cybercrime by setting state of the art principle based criminal law standards and important procedural rules with regard to the provisional storage of data to be potentially used as evidence in prosecuting criminal acts. GDPR is blazing the trail for the appropriate handling of data, and is thereby—albeit from a different starting point—significantly contributing to an improved data security framework and thus efficiently curbing cybercrime.

Keywords Criminal law · Internet of Things · Computer security · Data security · Europe

D. Wicki-Birchler (✉)
Fachstelle Compliance & Datenschutz, Hochschule für Wirtschaft Zürich (HWZ),
Lagerstrasse 5, 8001 Zürich, Switzerland
E-Mail: david.wicki@fh-hwz.ch

Published online: 22 September 2020

1 The development of cybercrime: a challenge for lawmakers

The phenomenon of cybercrime is strongly tied to the rise of computers in both personal and commercial use. This is because the new opportunities of data processing and data exchange, which are the very strength of computers, can be meaningfully used as much as they can be abused unethically and criminally.

In the early 1980s a technocultural phenomenon was captured in a *Time* magazine cover story declaring the personal computer "Machine of the Year" in 1983 [1]. The first generation of personal computers stored data on storage devices such as magnetic tape and/or floppy discs. The exchange of any data was burdensome, and therefore was very limited to essentials, when absolutely necessary. The flow and exchange of data was significantly furthered when companies began to build internal networks using own company servers and central storage devices, which allowed different computers within the firm the access to the same data storage pool.

The creation of internal networks logically started to attract cybercrime, because this allowed a hacker to access data from a large number of computer users by gaining access through the weakest link, often a careless user who paid too little attention to creating a robust password.

While it still was necessary to perform the criminal activity onsite, this emerged when the internet seriously started to be a monumental game-changer both for commercial use as well as across society in general. Because the internet connected internal storage devices, such as servers and hard drives, cybercriminals were able to remotely access, steal and/or alter internal data of companies or municipal authorities. The internet allowed a new way of breaking in electronically from wherever the world wide web granted access.

The nature of cybercrime is about to change dramatically once more with the evolution of the so-called cloud as the new *state of the art* storage system. Whereas the internal servers were traditionally installed and cooled in the basement of companies or public authorities, the storage of data in the cloud happens in server farms of extraordinary sizes. Server farms today consume more than 1.5% of the total electricity in the United States (US) at a cost of nearly $4.5 billion [2]. While the hacker previously needed to break in to the servers located on the premises of the potential victim by electronic means, he now has the opportunity to steal, alter or encrypt data of numerous victims at the same time, provided he can access to the cloud [3], where the data, although technically sub-segregated, is stored [4].

Society is paying a high price for the amenities of the internet, as the cost of cybercrime is estimated to reach $2 trillion dollar by 2019 [5]. While the public enjoys movie streaming, instant messaging and online banking, these achievements have immense capacity to be used unfairly. If cybercrime was a country in this context, it would have been the world's 13th largest economy measured by Gross Domestic Product, just before Australia and Spain. Therefore, regardless of the current technical status, it is most likely that cybercriminals will always try to perform their illegal activity. And for this, they will continue to start with the weakest link in all the safety and security measures, which has remained the same throughout the entire breath-taking technological development: us human beings, making mistakes or taking shortcuts while operating computers.

2 The Budapest Convention

The states which are parties to the International Cybercrime Convention have identified modern communication and data processing technologies as a challenge in the fight against computer and cybercrime [6], especially due to the inherently transnational nature of the underlying technology [7, p. 700]. It can be difficult to assess where a criminal act has actually taken place, since data might have been uploaded in one country, the hosting provided in a second country and the victim could be sitting in a third country, while the stolen data was sent to a fourth jurisdiction [8].

The Convention on Cybercrime of the Council of Europe, the Budapest Convention [9], is the first binding international instrument on this issue [7, p. 698]. The preamble of the Budapest Convention describes its intention as follows: A "common criminal policy aimed at the protection of society against cybercrime", and specifically intends "to deter action directed against the confidentiality, integrity, and availability of computer systems, networks and computer data as well as the misuse of such system, networks, and data by providing for the criminalization of such conduct" [10].

2.1 Illegal access (art. 2 CCC)

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right." [...]

Interestingly, the provision further states that a party may require "that the offence be committed by infringing security measures". This corresponds to Art. 5 lit. f GDPR, which sets the standard for appropriate protection [11] of data and is reflected accordingly in cif. 45 of the Explanatory Report to the Convention on Cybercrime [12]. Setting this crime in analogy to the traditional crime of trespassing, this would correspond to obtaining a key for a door, and in fact opening that door, without having proper permission to do so.

2.2 Illegal interception (art. 3 CCC)

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data." [...]

There seems no possibility to intercept any data without getting access first, but here the flow of data from the sender to the recipient will be interrupted and/or deviated [13, p. 540]. This provision aims to protect data privacy and is intended to

mimic the violation of privacy that occurs via wiretaps and recordings of telephone conversations in the physical world [13, p. 540].

2.3 Data interference (art. 4 CCC)

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right." [...]

Is it very important that the action must be both "without right" [12, cif. 62] and "intentionally" [12, cif. 63], because system operators who might negligently interfere with data often would have a right to do so, and normally have no intention to cause any harm. Data interference can be viewed as corresponding to trespass to chattels, but here the subject of the crime is data and not physical items. A common case of data interference is the installation of ransomware in order to blackmail the lawful owner, thereby seeking to extort money from the victim by encrypting files [14, p. 226]. Typically, ransomware is performed in two configurations, either by encrypting some or all documents or files or locking the computer itself to prevent normal usage [14, p. 226].

2.4 System interference (art. 5 CCC)

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

The legal interest of system interference versus data interference is that in Art. 5 CCC the functioning of the system is in focus and not the availability and/or integrity of data [12, cif. 65, 13, p. 542]. Both articles have in common that ransomware is a typical tool to perform the illegal activity. The extortion or blackmailing is not required in either of these to qualify as a criminal act. The interference must be a "*serious hindering without right*" [12, cif. 67–68]. This clarification is of the utmost importance for all maintenance and/or network companies that typically might "interfere" with the functionality of a system by installing updates or bug-fixing but are doing so rightfully.

2.5 Misuse of devices (art. 6. CCC)

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: (a) the production, sale, procurement for use, import, distribution or otherwise making available of: (1) a device, including

a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; (2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, and with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and (b) the possession of an item referred to in paragraphs (1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5." [...]

With the rise of the "Internet of Things", the misuse of devices is becoming even more important than presumably anticipated by the European Council when the convention was adopted. According to the Explanatory Report, the Council intended to penalize in particular the sale, procurement for use, import, distribution or otherwise making available of hacker tools in all forms [12, cif. 71–73]. Today, we enjoy the convenience of operating vacuum cleaners, using lawn-mowing robots remotely and letting the car park itself while we stand on the pavement and watch. These devices may serve hackers as an entry point to a network or simply enable them to misuse devices for improper use. Particularly worthy of note is the misuse of devices that are able to take orders via the user's voice, which could be abused for example as wiretaps.

2.6 Computer-Related forgery (art. 7 CCC)

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible." [...]

The purpose of this article is to fill the gap in criminal law related to traditional forgery, which requires visual readability of statements or declarations embodied in a document, and which did not previously apply to digitally stored data [12, cif. 81]. Because the data referred to in this provision is equivalent to a document with legal effects, the unauthorized input of correct or incorrect data can be compared to the production of a false paper document [12, cif. 83, 13, p. 545]. This article is gaining ever more relevance as we increasingly see legally relevant documentation produced electronically both in the private and in the public sector.

2.7 Computer-Related fraud (art. 8 CCC)

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: (1) any input, alteration, deletion or suppression of computer data,

(2) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

Whereas fraud traditionally consisted of the element of manipulating someone in order to make him transfer goods or money into the perpetrator's custody, the aim of this article is to criminalize undue manipulation in the course of data processing with the intention to effect an illegal transfer or property [12, cif. 86]. Phishing [15] mails, which mimic having a legitimate internal or external sender of emails while containing a request to transfer money, are a common scheme of computer-related fraud.

2.8 Expedited preservation of stored computer data (art. 29 cif. 1 CCC)

"A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data." [...]

Art. 29 regulates a very important aspect of the prosecution [16, p. 444], which is the access to evidence. It provides that a contracting party may request that data stored by means of a computer system in the territory of the requested contracting party be backed up without delay, and paragraph 3 requires each contracting party to create the legal conditions for this [17]. This is to prevent the data from being modified, removed or deleted during the period necessary for the preparation, transmission and execution of a request for mutual legal assistance to obtain the data [17]. If a state wants to refuse mutual legal assistance in order to preserve evidence in individual cases, this is only permissible under extremely restrictive conditions [16, p. 445]. This procedural provision in the Budapest Convention is absolutely crucial in the fight against cybercrime. Without efficient storage of evidence in a timely manner, the penalization of criminal actions would be extremely challenging to carry out [18].

3 GDPR cybercrime articles

The European Union (EU) Parliament approved the General Data Protection Regulation (GDPR) on April 14th, 2016, and it became legally effective after May 25th, 2018. The introduction of the GDPR left deep traces in the data protection community in Europe and put the topic in the headlines not only for data protection attorneys and specialists, but also for a broader audience. By far, GDPR was the most talked about and feared data protection law in the existence of in the European Economic Area, and arguably even across the entire globe [19, p. 188]. Companies were forced to significantly gear up their processes and set forth or amend existing policies. A rarely observed phenomenon came to light, namely that in the US a law

was largely adopted from Europe, when the Californian lawmaker decided to enact the Californian Consumer Privacy Act (CCPA). Evidently, there are differences [19, p. 191], but it remains obvious that the legislation from Europe was ground-breaking for California.

3.1 Protection requirements (art. 5 cif. 1 lit. f GDPR)

> "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

The GDPR applies a principle-based regulation [20]. This is expedient because methods of cybercrime tend to evolve on a continuous basis, which would most likely make a rule-based cybersecurity regulation outdated before it even became effective. The cybersecurity protection principle as outlined in Art. 5 lit. f of the GDPR and requires appropriate security measures in the processing of personal data by applying qualified technical and organizational precautions [21]. Confidentiality in this context means that the data are exclusively accessible to authorized personnel or departments and technical precautions are set in place to prevent unauthorized access [22]. Those measures shall be reviewed and updated, where necessary. The use of a (complex) password is the most efficient and basic method to ensure authorized access. The current state of art will not only require a password policy detailing periodicity and functional criteria for the composition of the password, but also the addition of two-factor authentication using two separate and independent communication channels to verify the legitimacy of the user.

3.2 Evidencing appropriate protection measures (art. 24 cif. 1 GDPR)

> "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." [...]

Internal control systems, codes of conduct and compliance manuals are well established in large companies. GDPR requirements are setting a new standard for appropriate documentation of lawful data processing. While this might be perceived as not directly impacting cybercrime prevention, the opposite is true: When internal resources are spent and used on scrambling and gathering information about internal work and data flow, this will help tremendously in revealing weak points that consequently will or should be remedied. Hence, lawmakers will force companies to take this task seriously, which will lead to better data protection procedures.

3.3 Risk-based protection measures (art. 32 cif. 2 GDPR)

> "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed."

The GDPR does provide some specific guidance on assessing security risks and identifying which security measures may be appropriate [23, p. 636]. GDPR does not prescribe in detail which security measures need to be taken, but rather demands in general *that* security measures be properly set in place in an appropriate manner [23, p. 636].

3.4 Duty to report breaches (art. 33 GDPR)

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 h after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 h, it shall be accompanied by reasons for the delay." [...]

At first glance, the obligation as set forth by this provision seems to neither help prevent nor efficiently fight cybercrime, since the duty of the notification arises only after a breach was detected. However, this should be considered as a very effective regulation: companies will strive to avoid any notification to authorities for various reasons. They will try to avoid the workload, the fine that might be imposed and—last but not least—they will fear creating a potential reputational risk. It is known that a substantial number of hackers seek first to get into the system of a company, and second try to stay in the system undiscovered. Therefore, an efficient anti-cybercrime system shall not only focus on prohibiting the entrance to the network, but should also incorporate and develop measures to detect intruders already inside, which will significantly enhance the cybersecurity framework.

4 Concluding remarks

Although the GDPR does not mention the Budapest Convention in particular, in Art. 48, the EU legislator intended to require that data transfers pursuant to third country orders shall be conducted under international agreements [24]. Apart from this link, the two agreements take different approaches in the fight against cybercrime. Whereas the Budapest Convention is specifically designed to penalize cybercrime, the GDPR sets forth EU-wide, legally binding standards for data protection. The points of overlap between the Budapest Convention and GDPR is that cybercrime will necessarily be conducted in abusing data in one way or another.

The fight against cybercrime was not the primary goal of GDPR, but rigorous implementation of the above-mentioned security measures would significantly contribute to the efficient containment of criminal activity in the Internet. The technical and/or organizational measures to prevent criminal behavior in the first place, followed by appropriate security measures as required by the GDPR, in combination with a harmonized criminal justice regime and meaningful storage of evidence in transnational criminal proceedings, are expedient and a desirable measure to curb cybercrime, notwithstanding, naturally, our own self-responsibility as private and/or business users of the Internet.

Funding Open access funding provided by University of Applied Sciences in Business Administration Zurich HWZ

References

1. Nooney L, Driscoll K, Allen K (2020) From programming to products: Softtalk magazine and the rise of personal computer user. Inf Cult 55:106
2. Gandhi A, Das R, Harchol-Balter M, Lefurgy C (2009) Optimal power allocation in server farms. In: SIGMETRICS/Performance'09 Seattle, WA, June 15–19, 2009
3. Morscher L (2011) Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht. ZBJV 147:216–217
4. Park Y (2016) Up in the cloud. A with Honors Projects, p 2 (Famous example of a hacked cloud was the incident when Apple's iCloud server was hacked and private pictures of several celebrities were exposed to the public.). https://spark.parkland.edu/ah/175
5. Clark MA, Espinosa JA, Delone WH (2020) Defending organizational assets: a preliminary framework for cybersecurity success and knowledge alignment. In: Proceedings of the 53rd Hawaii International Conference on System Sciences, p 4283
6. Federal Supreme Court of Switzerland (2015) Decision 141 IV 108, p 122
7. Clough J (2014) A world of difference: the Budapest convention on cybercrime and the challenges of harmonisation. Monash Univ Law Rev 40(3):700
8. Weissbrodt D (2013) Cyber-conflict, cyber-crime, and cyber-espionage. Minn J Int Law 22(2):368
9. The Budapest Convention on Cybercrime (2001) T.I.A.S 131, E.T.S. No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Accessed 6 July 2020
10. The Budapest Convention on Cybercrime, Preamble Section 9. https://rm.coe.int/1680081561
11. Buchholtz G, Stentzel R (2018) Comment On Art. 5 Gdpr. In: Gierschmann S, Schlender K, Stentzel R, Veil W (eds) Kommentar Datenschutz-Grundverordnung, vol 23. Bundesanzeiger Verlag, Köln
12. Council of Europe (2001) Explanatory report to the Budapest Convention. https://rm.coe.int/16800cce5b. Accessed 6 July 2020
13. Van Dine A (2020) When is cyber defense a crime? Evaluating active cyber defense measure under the Budapest Convention. Chic J Int Law 20(2):540
14. Kansagra D, Kumhar M, Jha D (2015/2016) Ransomware: a threat to cyber security. IJCSCS 7:226
15. United States Court of Appeals, Eighth Circuit (2014) Choice escrow & land title, LLC v. Bancorpsouth bank. 754 F.3d 611
16. Isenring B, Maybud RD, Quiblier L (2019) Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick. SJZ 115:444

17. Swiss Federal Council official comment on the approval and implementation of the Budapest Convention into Swiss Law. https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf. Accessed 6 July 2020 (p. 4731)
18. Schwarzenegger C (2002) Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 – Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses. In: Donatsch A, Forster M, Schwarzenegger C (eds) Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag. Schulthess, Zürich, p 310
19. Antokol J (2018) GDPR and data protection in the US. Digma: 188
20. Black J, Hopper M, Brand C (2007) Making a success of principles-based regulation. Law Financial Mark Rev: 194
21. Schmitz B (2018) Datenschutzrechtliche Grundsätze. In: Moos F, Schefzig J, Arning M (eds) Die neue Datenschutzgrund-verordnung mit Bundesdatenschutzgesetz 2018, vol 39. De Gruyter, Berlin/Boston
22. Weichert T (2020) Grundsätze für die Verarbeitung personenbezogener Daten. In: Däubler W, Wedde P, Weichert T, Sommer I (eds) EU-DSGVO und BDSG – Kompaktkommentar, 2nd edn. vol 68. Frankfurt am Main
23. Burton C (2018) Comment on Art. 32 Gdpr. In: Kuner, Bygrave, Docksey, Drechsler (eds) The EU general data protection regulation (GDPR)—A commentary. Oxford, p 636
24. Kuner C (2018) Comment on Art. 48 Gdpr. In: Kuner, Bygrave, Docksey, Drechsler (eds) The EU general data protection regulation (GDPR)—A commentary. Oxford, p 835