ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

Publisher
http://jssidoi.org/esc/home

THE CONCEPT OF A TECHNOLOGY NEUTRAL PAYMENT INSTRUMENT IN CRIMINAL LAW

Renata Marcinauskaitė [1], Tomas Girdenis [2], Marius Laurinaitis [3]

[1,2,3] Mykolas Romeris Law School, Mykolas Romeris University, Ateities st. 20, 08303 Vilnius, Lithuania

E-mails: [1] rennata@mruni.eu, [2]girdenis@mruni.eu, [2] laurinaitis@mruni.eu

Received 18 March 2020; accepted 9 July 2020; published 30 September 2020

Abstract: The development of electronic payment instruments and their online availability constitute important parts of the development of the EU payments market. Individual states adopt different approaches towards interpretation (legal aspects) and types of electronic payment instruments. To encourage sustainable payment services, minimize possible threats, and create favourable conditions for the development of new payment instruments, legislators adopt general legal acts stipulating the legal status of electronic payment instruments. However, the actual interpretation of payment instruments is often narrowed in legal practice, and does not cover payment instruments newly introduced to the market. A new insight into electronic payment instruments corresponding to the latest trends in the market is important in criminal law as well, because crimes related to the use of a payment instrument are common and difficult to investigate. In view of recent changes in payment services (the new Payment Services Directive in 2019), the norms of criminal law stipulating liability for the illegal disposal of electronic payment instruments must reflect circumstances predetermined by today's technological developments. In terms of criminal law, a technologically neutral conception of the payment instrument is necessary, to include a wider range of payment instruments that differ considerably from conventional personalized payment cards. The aim of this article is, therefore, to demonstrate that the current regulation of the Criminal Code of Lithuania lags behind the development of payment instruments, and in order to avoid excessive criminalization it is proposed to narrow the application of Article 214 of the Lithuanian Criminal Code.

Keywords: legal instruments for sustainable payments; payment instrument; criminal law; electronic payments

Reference to this paper should be made as follows: Marcinauskaitė, R., Girdenis, T., Laurinaitis, M. 2020. Conception of a Technology Neutral Payment Instrument in Criminal Law. *Entrepreneurship and sustainability Issues*, 8(1), 917-928. http://doi.org/10.9770/jesi.2020.8.1(61)

JEL Classifications: K10, K14, E42.

Additional disciplines: law

1. Introduction

The first attempt to define an electronic payment instrument was made in 1988 by European Commission Recommendation 88/590/EEC concerning payment systems, and in particular the relationship between cardholder and card issuer. The recommendation aimed not only at defining, but also at legally regulating the new payment services provided in the electronic environment. The recommendation also associated electronic payment instruments with the Payment device, defined as "a card or some other means enabling its user to effect operations, such as:

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

a) electronic payment involving the use of a card, in particular *at point of sale* [emphasis added],
b) the withdrawing of banknotes, the depositing of banknotes and cheques, and connected operations, at electronic devices, such as *cash dispensing machines and automated teller machines* [emphasis added]."

As the market for electronic payment was developing rapidly, the European Commission issued Recommendation 97/489/EC on 30 July 1997, concerning transactions by electronic payment instruments and in particular the relationship between the issuer and holder (hereafter – Commission Recommendation of 1997). The latter recommendation also included innovative electronic payment instruments that allowed the digital storage of the monetary value. This was the first attempt to legally regulate new payment instruments by distinguishing them from conventional remote access instruments (debit and credit cards) used to make electronic payment orders to the credit institution. The Commission Recommendation of 1997 defined an electronic payment instrument as: an instrument enabling its holder to effect transactions including cash withdrawals by means of an electronic payment instrument and the loading (and unloading) of an electronic money instrument, at devices such as cash dispensing machines and automated teller machines and at the premises of the issuer or an institution who is under contract to accept the payment instrument.

Gradually, the market has adopted new payment instruments that fall outside the limits of the present legal regulation because of the specific range of the services they grant (European Central Bank, 2002). The functioning of traditional payment instruments, including credit cards, credit transfer, debit instruments (direct debit and debit cards), and electronic vouchers, has been carefully regulated by legal acts. Meanwhile, modern technologies offer new payment instruments, including prepaid cards, mobile billing, and e-money.

Until 2007, when the Directive of the European Council 2007/64/EC (Payment Services Directive 2007/64/EC; hereafter – PSD 2007) was adopted, the concept of an electronic payment instrument was defined only by the Commission Recommendation of 1997. The amendment of the provisions of the EU Recommendations of 1997, transposed into the Payment Services Directive 2007/64/EC, led to a new definition of an electronic payment instrument that included both the existing and newly developed electronic payment products. A payment instrument was technologically neutrally defined in Article 4 paragraph 23 of the Directive 2007/64/EC (Directive 2007) as: "any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order". This definition therefore comprises a wider range of electronic payment instruments. Prior to 2007, problems used to arise regarding the due identification and acknowledgment of electronic payment instruments stored in workstations (direct non-autonomous electronic payment instruments) as a means of payment, whereas the new concept of an electronic payment instrument extended the definition to include all electronic instruments (autonomous electronic payment instruments and direct non-autonomous electronic instruments). Lithuania first defined an electronic payment instrument in 2003 by amending its Payment Law as follows:

> Electronic payment instruments are remote access instruments of payment and electronic money. The user of an electronic payment instrument (hereinafter referred to as User) is a client of a credit institution granted an electronic payment instrument by the credit institution. Remote access instruments of payment are defined as a means enabling the user to give electronic instructions to the credit institution on the disposal of funds in their account in the credit institution (Law on Payments, 2003).

The new concept of the payment instrument specifies that the instrument may be personalized, i.e. linked to a person, and may be used for remote identity verification by the bank or electronic payment service provider. Another important aspect of the concept is that the payment instrument may entail certain procedures. No physical item (a card or an equivalent media) is needed to make a payment – a user name, a password, or a variable password may be enough for identity verification. Such extension of the meaning of payment instrument helped to deal with a previously unresolved problem – whereas formerly payment instruments were understood only as

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

tangible media, such as credit cards and the like, now such instruments may well include biometric data or a mobile phone application subject to party agreement and the availability of relevant technologies. The best and most widely used example of successfully agreed procedures in electronic payment is e-banking, where the user name, the password or generated variable password, and special mobile phone applications or data stored in the phone constitute conventional procedures to initiate and complete payments.

The contemporary Law on Payments of the Republic of Lithuania defines a payment instrument in line with the principle of technological neutrality with no discrimination of issuers (including all financial institutions along with credit institutions). "'Payment instrument' means any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order" (Law on Payments, 2003). This definition has been originally transposed from the new Payment Directive 2015/2366 (hereafter – PSD2). The preamble of Directive PSD2 states that the existing and prospective market players should be granted equal business conditions so as to extend opportunities for new players to enter the market and ensure high-level user security in the use of payment services within the entire European Union. Equal conditions are likely to contribute to the efficiency of the entire payment system, grant a better choice and transparency of payment services, and increase user trust in the payments market.

Personalized devices mentioned in the definition of payment instruments are closely linked to personalized safety features, which are understood as data to be used for user authentication and agreed to by the payment service provider and the user. These features may include a wide range of forms, such as PIN codes, biometric data, or variable algorithm generated values. The PSD2 Directive also specifies the importance of personalized safety features, stating that they have to meet the payment-associated risk level. It is also important to secure conditions for the development of available user-friendly payment instruments, including low risk payments (e.g. contactless payments) that are subject to standard security exceptions independently on whether the payment is done by card or by smart phone. The PSD2 Directive emphasizes the safe use of personalized safety features to reduce the risks of theft and malicious practice. In that sense, user trust in measures granting confidentiality and in the integrity of personalized safety features is essential. Such measures typically include encryption systems based on the use of personal devices, such as card readers or mobile phones, that may be used by the service provider to send encryption data, e.g. text messages or e-mail messages (PSD2 preamble). It is the personal user devices that have actually extended the conventional understanding of the payment instrument, as the user is free to choose the device to store personalized safety features on (data necessary for contactless payment, login code generators, and electronic signature certificates). It has to be presumed that the use of identity verification codes is compatible with the user's duties concerning their payment instruments and personalized safety features (PSD2 preamble). The fact that the Directive associates possession of personalized devices with certain duties of the user is of great importance. Apart from the requirement for the device holder to use their payment device in accordance with the terms and conditions regulating issuance and use of the payment device (which must be objective, non-discriminatory, and proportionate), the user has two major duties (Law on Payments, 2003):

a) The user must immediately report the loss, theft, unauthorized use, or misappropriation of the payment device to the issuer of the payment service provider or an authorized representative of the service provider.
b) On receipt of the payment device, the user must take all possible actions to protect their personalized safety data. The latter, however, constitutes the major challenge to the developer of payment instruments as the user typically prefers simplicity to safety (weak PIN codes, ignored safety requirements, sharing with other people).

Compliance with the latter requirement may protect against unauthorized use of the payment instrument. To meet the requirement, the EU's technological safety standards had to be changed. One of the key solutions was the introduction of the EMV standard in payment cards. EMV is an international technical standard developed by

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

Europay, MasterCard, and VISA in 1999. The standard sets safety requirements for any operations performed by chip payment cards and chip card devices, including chip card readers, payment terminals, and automated teller machines. The goal of the EMV standard is to unify the requirements independently across the payment system. The standard is now managed by EMVCo consortium. The EU Single Euro Payments Area (SEPA) project set the requirement for all payment cards issued within the EU to have an EMV standard IC chip along with the magnetic strip on 1 January 2011. The goal of the SEPA initiative is to develop a single area for payments in euros, with no discrimination between national and international payments. Within the SEPA area, credit transfer and direct debit operations in euros are subject to standard payment schemes and the application of uniform terms, rights, and obligations. One of the instruments envisaged by SEPA includes payment cards with integrated EMV standard IC chips. The magnetic strip was deemed unsafe because of the risk of theft of the data necessary for payment initiation stored in the magnetic strip, which could be read without the holder's awareness (by means of various fraudulent schemes). The EMV standard requires a mandatory PIN code to approve payment operations, thus enforcing the user's duty to protect their data. The EMV standard also provides for the use of contactless NFC (near field communication) payment cards, where data necessary for payment initiation are transferred by a radio signal. To improve user convenience, small value payments may be performed with no PIN requirement. Individual countries and financial institutions are free to set limits on transaction sums in view of their customer behaviour and available statistics. The limits typically vary from €12 to €47 (Statista, 2019). NFC payments still retain certain risks, but the user is given the option to choose whether to activate such payments or not. The PSD2 Directive aims to extend the use of user-friendly payment instruments and encourage the development of easy-access user-friendly payment instruments made for low-risk transactions by means of smart phone applications. Generally speaking, a payment instrument is no longer just a payment card or a batch of personalized features necessary to log in to e-banking. In the modern world, payment instruments may already be found in a great deal of personal electronic gadgets. The use of smart phones as payment instruments has been rapidly growing, and they have already become commonplace as payment instruments. Europe has seen an upsurge in wearable payments (a wearable device, for example a ring, bracelet, or smart watch, that has Near-Field Communication (NFC) capabilities). Having linked these items to your debit or credit card, you can pay in the same contactless way (Wearable payments, 2019). Thus, payment instruments have already come to include bracelets, rings, smart watches, or key chains. Surveys reveal that sums paid by means of wearable payments are set to soar in the near future. According to market research and consulting firm Reports and Data, the global wearable device market is expected to grow from $312 billion in 2018 to over $1.1 trillion in 2026 (MasterCard, 2019).

Essentially, payment instruments may not be identified solely as conventional payment cards or remote access instruments, as there is a much wider range of personalized devices in the market that may have the attributes of payment instruments and may be used for payment initiation and completion. In terms of criminal law, it is very important to credibly identify such instruments and their use in order to duly qualify payment associated criminal offences.

Methodologically, this research focuses on the regulation of electronic payment instruments in the EU and Lithuania, and also on the understanding of payment instruments in Lithuanian criminal law. The authors use qualitative research methods, such as the method of textual analysis and the analysis of case law in the field of criminal cases.

2. The Concept of Payment Instruments in Criminal Law

The requirement of criminal law to clearly define the content of payment instruments should be primarily associated with the principles of protection of legitimate expectations, legal certainty, and legal security. It is the aspiration for legal certainty and clarity that implies certain mandatory requirements for legal regulation: "it has to

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

be clear and cohesive, legal norms must be stated clearly and contain no ambiguities" (rulings of the Constitutional Court of the Republic of Lithuania of 13 May 2010, 22 June 2009, 25 December 2008, 26 January 2004 and 30 May 2003). However, in view of the progress and trends in technological development, criminal legal regulation also has to be timely, and the understanding of payment instruments has to correspond to changes in technologies. Having in mind the aforementioned, criminal law needs a concept of payment instruments that is sustainable and, at the same time, reflects modern trends in the financial sector. The harmonization of these two aspects is probably the major issue in safeguarding a cohesive interaction between law (including criminal law) and technologies, i.e. the enforcement of the key provisions of criminal liability alongside the dynamic interpretation of legal norms concerning technological development. Also, interaction between law and technologies at the legislative level should reflect an idea that "[l]aw develops in an evolutionary way, not in a revolutionary way" (Schellekens, 2006).

The need to decide which items contain elements of payment instruments in criminal law is attributable to the fact that Lithuania's Criminal Code imposes criminal liability for the illegal disposal of such instruments. For the sake of accuracy, is has to be mentioned that Lithuania's Criminal Code criminalizes the illegal disposal of: 1) an electronic payment instrument; 2) a misappropriated electronic payment instrument or the data of the identity verification device of the owner of such a payment instrument sufficient to initiate a financial transaction; and 3) an instrument (or instruments) of crime – technical equipment, software, or other means directly intended or tailored to fake or forge electronic payment instruments or their parts. Although the aforementioned elements of crime are included in Article 214 of the Criminal Code as alternatives, they are all, be they data or instruments (tools) of crime, directly related to an electronic payment instrument. An exact definition of the content of a payment instrument is only possible after the identification of what should be deemed an electronic payment instrument in criminal law. The earlier version of Article 214 of the Criminal Code imposed criminal liability for the illegal disposal of fake payment instruments. The provision was changed in 2007 to entrench a much wider concept of an electronic payment instrument, as for a long time the concept of an electronic payment instrument pivoted on Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (hereafter – Decision 2001/413/JHA). Scientific sources used to maintain that payment instruments had certain features: "a material expression and a special purpose – non-cash payments, transfer of money or monetary sums" (Piesliakas & Dvilaitis, 2008). Obviously, this interpretation was similar to the definition provided by Decision 2001/413/JHA, defining a payment instrument as "a corporeal instrument, … enabling, by its specific nature, alone or in conjunction with another (payment) instrument, the holder or user to transfer money or monetary value …, which is protected against imitation or fraudulent use …" (Article 1, paragraph (a)). However, today's interpretation of a payment instrument in terms of criminal law has to be made in view of the fact that the EU adopted Directive (EU) 2019/713 of the European Parliament and of the Council on 17 April 2019, on combating fraud and the counterfeiting of non-cash means of payment, and replacing Council Framework Decision 2001/413/JHA (hereafter – Directive 2019/713). As the scope of application of the directive also includes non-corporeal payment instruments (paragraph 15 of the Preamble), the issue of the content of the electronic payment instrument becomes of key importance.

As Directive 2019/713 states, "[r]ecent years have brought not only an exponential increase in the digital economy, but also a proliferation of innovation in many areas, including payment technologies" (Preamble paragraph 6). New payment technologies are closely related to new payment devices, which become more and more accessible to a massive number of users, grant new opportunities for financial operations, and make the process of payment less complex. As a wide range of activities move into the electronic environment, the impact of new technologies becomes inevitable. However, the rapid development of payment technologies is inseparable from risks emerging in the electronic environment. As "crime follows opportunity" (Clough, 2011), the electronic environment faces a variety of types of fraud involving the use of modern payment instruments. One of the ways to combat fraud is by inflicting criminal liability for the illegal disposal of electronic payment instruments. However, in view of constant technological development, it is essential to regularly reassess whether the present

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

criminalization of illicit acts is up-to-date, and whether the existing legal norms can still be applied to the types of fraud newly emerging in the electronic environment. This issue may also be found in Directive 2019/713 which, *inter alia*, states that "[n]ew payment technologies involve the use of new types of payment instruments, which, while creating new opportunities for consumers and businesses, also increase opportunities for fraud. Consequently, the legal framework must remain relevant and up-to-date against the background of those technological developments" (Preamble paragraph 6). Also, a further insight may be made by assessing the prospects of the development of payment instruments and producing estimations as to whether the notions used in Lithuania's Criminal Code will be applicable to future payment opportunities, which may be forecast in view of trends in the development of payment technologies. Specifically, the question concerns notions describing the content of criminal acts defined in Article 214 of Lithuania's Criminal Code in terms of their applicability to electronic payment instruments emerging in the financial sector.

Presumably, the widespread criminalization of the illegal disposal of electronic payment instruments in Lithuania is predetermined, *inter alia*, by the fact that – implied already in the title of Chapter XXXII of the Criminal Code – such disposal is deemed a serious threat to the national financial system. Specifically, as the judicial practice shows, this threat is to the regulation of the use and disposal of electronic payment instruments intended for non-cash payments (Lithuanian Supreme Court ruling of 24 March 2020 in criminal case No. 2K-77-1073/2020). Justification for the gravity of the crime of illegal disposal of electronic payment instruments may also be based on the provisions of Directive 2019/713, which states that "[f]raud and counterfeiting of non-cash means of payment are threats to security, as they represent a source of income for organised crime and are therefore enablers for other criminal activities such as terrorism, drug trafficking and trafficking in human beings" (Preamble paragraph 1). Since the financial system, as an intermediate link to access and invest in funds, involves financial intermediaries, it is equally important to ensure that "[f]raud and counterfeiting of non-cash means of payment also represent obstacles to the digital single market, as they erode consumers' trust and cause direct economic loss" (Preamble, paragraph 2). In describing the threats posed by the illegal disposal of electronic payment instruments, it is also important to consider a wider range of institutions involved in the functioning of financial markets, instead of associating financial intermediaries merely with financial institutions, i.e. banks. For example, Gai and Kapadia (2019) stated in their analysis of networks and systemic risk in the financial system that "it is likely to become increasingly important to examine network effects across the wider financial system, encompassing insurance companies, investment funds, and other non-bank financial intermediaries". The wider interpretation of the notion of a financial intermediary can also be seen in the judicial practice of Lithuania's courts. For example, in one of the reviewed criminal cases the court stated that the accused illegally disposed of a misappropriated filling station credit card along with the PIN number required to carry out financial operations. As the court identified the illegal disposal of a misappropriated electronic payment instrument along with data of the owner's identity verification, the act was qualified as a crime as described in Article 214 of the Criminal Code (Order of District Court of Klaipėda, Chamber of Klaipėda City of 21 September 2018 in criminal case No. 1-937-795/2018). Lithuania's judicial practice includes cases where an act was qualified as a crime, as described in Article 214 of the Criminal Code, as the accused illegally disposed of a payment card issued by an electronic payment institution licenced by Lithuania's bank along with login data sufficient to initiate a financial transaction (Ruling of District Court of Tauragė, Chamber of Šilutė of 4 October 2018 in criminal case No. 1-512-733/2018). The judicial practice also includes cases where reference to the same article of the Criminal Code was made to qualify the illegal disposal of payment instrument verification data, i.e. login data of an illegally opened account in an electronic payment service company, sufficient to initiate a financial transaction (Ruling of District Court of Vilnius City of 11 January 2018 in criminal case No. 1-371-1034/2018).

In defining the concept of a payment instrument in criminal law, an important factor is the principle of technological neutrality. The implementation of the principle, including in criminal law, may help to avoid the limitations that may arise in the application of legal norms due to certain technological aspects involved: "[t]he benefit of technological neutrality based on the rationale of sustainability would be that it makes regulation 'time-

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

proof'" (van der Haar, 2007, p. 23). Having analysed various aspects of the aforementioned principle, it becomes obvious that the requirement to maintain technological neutrality can only be met by properly stating the content of the notion. As I. M. van der Haar states, "lawmakers would need to adhere to a more functional definition, meaning a definition solely relying on functional concepts, thereby leaving out all references to technologies" (2007, p. 23). The importance of functions and the most common features – not the specific types of technologies – have also been emphasized by P. Ohm: "[t]ech-neutral provisions refer to technology in general, vague, open-textured terms that specify purposes, effects, functions, and other general characteristics" (2010). In interpreting electronic payment instruments in criminal cases of the illegal disposal of electronic payment instruments, in line with the principle of technological neutrality, the priority should be given to the intent of the instrument and the functions of the technology chosen for financial operations instead of the technology itself. Such a priority would allow safeguarding a sufficiently sustainable understanding of an electronic payment instrument and help to avoid possible loopholes in criminal law caused by changes in technology. The importance of technological neutrality in view of the development and dissemination of technologies is also hinted at in Directive 2019/713. This Directive notes that modern payment instruments granting the user new opportunities may be used for fraudulent purposes; therefore "the legal framework must remain relevant and up-to-date against the background of those technological developments, on the basis of a technology-neutral approach" (Preamble, paragraph 6). The provisions of the preamble of the Directive reflect, *inter alia*, the notions included in Directive 2019/713. For instance, a non-cash payment instrument is defined as "a non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange" (Article 2, paragraph (a)). As can be seen from Directive 2019/713, a non-cash payment instrument is described by means of abstract, technologically neutral notions such as *device, object, or record*, primarily focusing on the features' indication of their intent and functions – the instrument has to *enable the holder or user to transfer money or monetary value.* As digital economics rapidly develops and introduces more and more innovations, the definition of payment instruments given in Directive 2019/713 has envisaged opportunities to apply it not only to existing payment technologies, but to prospective ones as well.

The concept of an electronic payment instrument is not explicitly specified in the Lithuanian Criminal Code, leaving the interpretation of its content at the discretion of the courts tasked with the responsibility of deciding in their hearings whether an illegally disposed instrument contains features of an electronic payment instrument. Having reviewed the judicial practice of the Lithuanian Supreme Court, it becomes clear that one of the sources helping to identify the content of a payment instrument in criminal hearings is Lithuania's Law on Payments. For example, the Lithuanian Supreme Court ruling of 24 March 2020 in criminal case No. 2K-77-1073/2020 notes that "'payment instrument' means any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order", which is fully compliant with the frequently referred to provisions of the Law on Payments. It is equally important that such an understanding of a payment instrument in criminal law fully complies with the requirements of the principle of neutrality, applicable, *inter alia*, to the terminology used in legal acts. Here, it is necessary that "[technologically] neutral regulation appears to have three main aims: futureproofing, online and offline equivalence, and encouraging the development and uptake of the regulated technology" (Reed, 2007).

To decide if the aforementioned technologically neutral concept of a payment instrument and its data helps to deal with practical problems likely to arise in the qualification of crimes, a survey of Lithuania's judicial practice has been conducted. The survey summarized 158 rulings of district courts in the period of 2018–2020, which stated that the accused committed, *inter alia*, a criminal act as described in Article 214 of the Criminal Code, besides other crimes (see Table 1).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

Table 1. Object of the crime as described in Article 214 of the Criminal Code in Lithuania's judicial practice

Object of the crime	Identified cases	Percentage (%)
A misappropriated genuine corporeal electronic payment instrument	106	67
Misappropriated non-corporeal payment instrument verification data, sufficient to initiate a financial operation	41	26
Data of a misappropriated genuine electronic payment instrument, sufficient to initiate a financial operation	7	4
A fake corporeal electronic payment instrument	3	2
Possession of technical equipment and software intended or tailored to fake electronic payment instruments.	1	1

Source: the authors' research

The results of the survey reveal that the vast majority of cases of illegal disposal of electronic payment instruments are attributable to misappropriation and possession of a genuine electronic payment instrument (67%). The disposal of misappropriated bank cards (including contactless) was probably most typical However, when considering whether an electronic payment instrument as specified in Article 214 of the Criminal Code may be of a non-corporeal nature, it has to be noted that the survey revealed several cases of the illegal disposal of payment instrument verification data of the owner of a misappropriated non-corporeal electronic payment instrument, sufficient to initiate a financial operation (26%). Such cases were mostly associated with the illegal acquisition of data sufficient to perform a financial operation in e-banking. As Lithuania's Supreme Court states, such data constitute personal electronic identity data, provided by the bank under a bank account contract stipulating the terms and conditions of the use of the account (Lithuania's Supreme Court ruling of 10 October 2013 in criminal case No. 2K-389/2013). Since the initiation of financial operations in e-banking is of a specific nature, criminal cases of the latter category relate to the illegal disposal of identity verification codes and login passwords (for example: the ruling of District Court of Kaunas, Chamber of Kaunas of 6 February 2019 in criminal case No. 1-576-573/2019; the ruling of District Court of Vilnius City of 5 March 2018 in criminal case No. 1-184-270/2018; and the ruling of District Court of Alytus, Chamber of Druskininkai of 6 September 2018 in criminal case No. 1-982-182/2018). It also has to be noted that the provisions of Article 214 of the Criminal Code state that payment instrument verification data (including e-banking data) are deemed to be objects of the crime described in the same article of the code only in cases where they are sufficient to initiate a financial operation. Another aspect of the aforementioned criminal cases that is important for our analysis is that courts allow a wider approach to the concept of an electronic payment instrument by attributing to it the potential to have more than merely material characteristics. Lithuania's Supreme Court notes in its judicial practice that "all monetary operations are carried out in e-banking by means of human-written computer programs. Instead of direct liaison, the client communicates with the bank via an electronic system. The system is designed to receive instructions and perform operations only when correct user identification codes are submitted" (Ruling of Lithuania's Supreme Court of 9 October 2001 in criminal case No. 2K-682/2001). The way financial operations are performed predetermines the absence of any links between the use of electronic channels (e.g. the internet of e-bank) and the corporeal payment instrument. In such cases, the notion of an electronic payment instrument also entails "an electronic system of rendering bank services via the Internet along with certain procedures applicable for payment initiation and agreed between by the payment service provider and the payment service user" (Marcinauskaitė, 2019). As Laurinaitis notes, the best example "illustrating procedures agreed in electronic payment and widely used in Lithuania is e-banking, where a user name, a password and password cards constitute conventional procedures of payment initiation and completion" (2015). A similar interpretation may also be observed in the judicial practice that has been reviewed. For example, in one criminal case the court arrived at the conclusion that, apart from other punishable acts, the accused illegally acquired and kept electronic payment instrument verification data, namely e-banking login data. Such data were considered by the court to be payment instrument verification data attributable to an electronic payment instrument – the e-banking system of the specific bank – and therefore sufficient to initiate a financial operation (ruling of District Court of Kaunas, Chamber of Kaunas of 2 August 2018 in criminal case No. 1-2663-917/2018).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

Analysis of the judicial practice demonstrates that amendments to the Criminal Code made in 2007 which identify electronic payment instruments as possible objects of crime provided opportunities for their wider interpretation, extending the notion of an electronic payment instrument to include both corporeal and non-corporeal means of payment. This aspect is of particular importance in view of the fact that Directive 2019/713 aims at entrenching the non-corporeal nature of payment instruments in criminal law. In view of the fact that today's judicial practice interprets the notion of payment instruments in accordance with the comparatively broad and technologically neutral definition laid down in the Law on Payments, Article 214 of the Criminal Code will continue to be applicable to future technologies as the payment instrument remains identifiable not by its form, but by its functioning as a means of payment (i.e. it provides the possibility to transfer money or monetary value or to initiate a payment operation).

Having analysed the provisions of Directive 2019/713, one can note several relevant aspects in the context of criminal responsibility for the illegal disposal of electronic payment instruments. For instance, criminal responsibility should be primarily provided for the illegal disposal of payment instruments subject to special protection against counterfeiting and misappropriation. In view of this, the issuance of specially protected payment instruments should be encouraged (Preamble, paragraph 12). Since an instrument is only deemed as a payment instrument on the condition that it actually ensures the possibility of initiating and completing a payment operation, "unlawfully obtaining a mobile payment application without the necessary authorisation should not be considered as an unlawful obtainment of a non-cash payment instrument as it does not actually enable the user to transfer money or monetary value" (Preamble, paragraph 8). Such conditions are relevant in regard to criminal law as an *ultima ratio* remedy. Criminal acts involving the illegal disposal of specially protected payment instruments that can actually initiate and complete a financial operation may be qualified in accordance with the objective criteria as gravely dangerous, and seriously threatening the financial system. Consequently, criminal penalties may be inflicted upon individuals for such acts. Finally, as Directive 2019/713 lays down, sanctions should not be imposed for the legal use of the payment instrument (Preamble, paragraph 13). The judicial practice of Lithuania's Supreme Court maintains that criminal responsibility, provided for in Article 214 of the Criminal Code, can only be inflicted for the

> unlawful acquisition, storage, transfer or handling of payment instrument verification data sufficient to initiate a financial operation. It is also important in this respect that in the presence of consent by the owner or an authorized user of the payment instrument to specific acts of a third party (e.g. to the use of the payment instrument for the purpose of a limited sum financial operation), such acts of the third party are not usually deemed illegal under Article 214 of the Criminal Code (Lithuania's Supreme Court ruling of 24 March 2020 in criminal case No. 2K-77-1073/2020).

Conclusions

It can be concluded that Lithuania's legal acts define a payment instrument in line with the principle of neutrality, with no discrimination between issuers – comprising all possible financial institutions and including a wide range of payment instruments. However, the problem of identifying specific payment instruments is still frequently encountered in practice. As a result, the concept of an electronic payment instrument as an object of a crime is not strictly defined in Lithuania's Criminal Code, leaving enough space for its wide interpretation. The technologically neutral nature of Lithuania's legislation has ensured the opportunity for an electronic payment instrument to be identified in criminal law not by its form, but according to the functions it performs.

During recent decades, conventional payment instruments have transformed considerably to become completely different from their former equivalents in terms of their form and their system. Today's instant electronic payments are done by means of completely novel payment instruments, where personalized safety data are no longer stored in IC cards as they have been replaced by smart devices such as mobile phones, smart watches, and bracelets. In the context of criminal law, these new types of instruments may be acknowledged as electronic

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 1 (September)
http://doi.org/10.9770/jesi.2020.8.1(61)

payment systems, and as the object of a crime where the act in question indicates the intentional illegal disposal of a specially protected payment instrument that can initiate and complete a financial operation. At the same time, it is essential to prove that the culprit had the direct intention to misappropriate the item specifically as a means of payment.

Directive PDS2 aims to extend the use of user-friendly payment instruments and encourages the development of easy-access, user-friendly payment instruments integrated into mobile or wearable devices. Despite this, Lithuania's judicial practice, particularly in criminal law, is often faced with the specific practical problem of the identification of such instruments, as they are often mistaken for ordinary items because of a failure to identify the elements of their integrated payment functions.

References

88/590/EEC: Commission Recommendation of 17 November 1988 concerning payment systems, and in particular the relationship between cardholder and card issuer. *OJ L* 317, 24.11.1988, 55–58. http://data.europa.eu/eli/reco/1988/590/oj

97/489/EC: Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (Text with EEA relevance). *OJ L* 208, 2.8.1997, 52–58. Retrieved from http://data.europa.eu/eli/reco/1997/489/oj

2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. *OJ L* 149, 2.6.2001, 1–4. Retrieved from http://data.europa.eu/eli/dec_framw/2001/413/oj

Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. *Criminal Law Forum*, *22*(1–2). https://doi.org/10.1007/s10609-011-9133-5

Constitutional Court of the Republic of Lithuania ruling of 30 May 2003, case No. 21/2003. Retrieved from https://www.lrkt.lt/en/court-acts/search/170/ta1244/content

Constitutional Court of the Republic of Lithuania ruling of 26 January 2004, case No. 3/02-7/02-29/03. Retrieved from https://www.lrkt.lt/en/court-acts/search/170/ta1254/content

Constitutional Court of the Republic of Lithuania ruling of 24 December 2008, case No. 09/06-30/06-01/07-30/08. Retrieved from https://www.lrkt.lt/en/court-acts/search/170/ta1426/content

Constitutional Court of the Republic of Lithuania ruling of 22 June 2009, case No. 16/07-17/07-20/08. Retrieved from https://www.lrkt.lt/en/court-acts/search/170/ta1284/content

Constitutional Court of the Republic of Lithuania ruling of 13 May 2010, case No. 04/08-11/08. Retrieved from https://www.lrkt.lt/en/court-acts/search/170/ta1495/content

Directive (EU) 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance). *OJ L* 319, 5.12.2007, 1–36. Retrieved from http://data.europa.eu/eli/dir/2007/64/oj

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC. *OJ L* 337, 23.12.2015, 35–127. Retrieved from http://data.europa.eu/eli/dir/2015/2366/oj

Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. *OJ L* 123, 10.5.2019, 18–29. Retrieved from http://data.europa.eu/eli/dir/2019/713/oj

District Court of Alytus, Chamber of Druskininkai ruling of 6 September 2018 in criminal case No. 1-982-182/2018. Retrieved from https://e-teismai.lt/byla/80360532108014/1-982-182/2018

District Court of Kaunas, Chamber of Kaunas ruling of 2 August 2018 in criminal case No. 1-2663-917/2018. Retrieved from https://eteismai.lt/byla/260978209221727/1-2663-917/2018

District Court of Kaunas, Chamber of Kaunas ruling of 6 February 2019 in criminal case No. 1-576-573/2019. Retrieved from https://e-teismai.lt/byla/145209209297222/1-576-573/2019

District Court of Klaipėda, Chamber of Klaipėda City order of 21 September 2018 in criminal case No. 1-937-795/2018. Retrieved from https://eteismai.lt/byla/182262923524827/1-937-795/2018?word=vks%20kaunas

District Court of Tauragė, Chamber of Šilutė ruling of 4 October 2018 in criminal case No. 1-512-733/2018. Retrieved from https://eteismai.lt/byla/91553969772732/1-512-733/2018

District Court of Vilnius City ruling of 11 January 2018 in criminal case No. 1-371-1034/2018. Retrieved from https://eteismai.lt/byla/63547702678501/1-371-1034/2018

District Court of Vilnius City ruling of 5 March 2018 in criminal case No. 1-184-270/2018. Retrieved from https://eteismai.lt/byla/145636416590795/1-184-270/2018

European Central Bank. (2002). E-Payments in Europe – The Eurosystem's Perspective. Retrieved from https://www.ecb.europa.eu/pub/conferences/shared/pdf/epayments.pdf

Gai, P., & Kapadia, S. (2019). Networks and systemic risk in the financial system. *Oxford Review of Economic Policy*, *35*(4), 586–613. https://doi.org/10.1093/oxrep/grz023

GlobeNewswire. (12 March 2019). Wearable Payments Devices Market to Reach USD 1121.01 Billion By 2026. Retrieved from https://www.globenewswire.com/news-release/2019/03/12/1752029/0/en/Wearable-Payments-Devices-Market-To-Reach-USD-1121-01-Billion-By-2026.html

Laurinaitis, M. (2015). *Elektroninių pinigų teisinis reguliavimas [Legal regulation of electronic money]* (Doctoral dissertation, Mykolas Romeris University). Retrieved from https://repository.mruni.eu/handle/007/14384

Law on the Approval and Entry into Force of the Criminal Code of the Republic of Lithuania, 26 September 2000, No. VIII-1968 (As last amended on 21 November 2017, No. XIII-791). Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/28b18041843311e89188e16a6495e98c?positionInSearchResults=0&searchModelUUID=5a098314-89b7-4643-a9e5-02151f3b103a

Law on Payments of the Republic of Lithuania, as amended on 5 June 2003, No. IX-1596. *Valstybės žinios,* 2003-06-27, No. 61-2753. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/TAIS.211757?jfwid=-1819orfczc

Marcinauskaitė, R. (2019). *Nusikalstamos veikos elektroninėje erdvėje: elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje*. Vilnius: Mykolo Romerio universitetas.

MasterCard. (28 November 2019). *Wearable payments are taking off across Europe: eightfold increase in transactions in just a year* [Press release]. Retrieved from https://newsroom.mastercard.com/eu/press-releases/wearable-payments-are-taking-off-across-europe-eightfold-increase-in-transactions-in-just-a-year/

Ohm, P. (2010). The argument against technology-neutral surveillance laws. *Texas Law Review*, *88*(7), 1685, 1687–1700.

Piesliakas, A., & Dvilaitis, V. 2008. Elektroninės mokėjimo priemonės kaip Baudžiamojo kodekso 214 ir 215 straipsniuose numatytų nusikalstamų veikų dalyko, samprata [Electronic payment instrument as an object of Articles 214 and 215 of the Criminal Code]. *Jurisprudencija*, *11*(113), 100–106.

Schellekens, M. H. M. (2006). What holds off-line, also holds on-line? In B. J. Koops, A. M. B. Lips, J. E. J. Prins, & M. H. M. Schellekens (Eds.), *Starting Points for ICT Regulation: IT & Law; No. 9* (pp. 51–75). The Hague: TMC Asser Press. Retrieved from https://ssrn.com/abstract=952275

Statista. (2019). Contactless card limits in Europe (2019) as of January 2019, by country. Retrieved from https://www.statista.com/statistics/971686/contactless-card-limits-in-europe-by-country/

Supreme Court of Lithuania ruling of 9 October 2001 in criminal case No. 2K-682/2001.

Supreme Court of Lithuania ruling of 10 October 2013 in criminal case No. 2K-389/2013. Retrieved from https://eteismai.lt/byla/48287863512745/2K-389/2013

Supreme Court of Lithuania ruling of 24 March 2020 in in criminal case No. 2K-77-1073/2020. Retrieved from https://eteismai.lt/byla/51432793036133/2K-77-1073/2020

Van der Haar, I. M. (2007). Technological neutrality; What does it entail? *SSRN Electronic Journal*. TILEC Discussion Paper No. 2007-009. https://dx.doi.org/10.2139/ssrn.985260

Renata MARCINAUSKAITĖ is a lecturer at Mykolas Romeris University Law School. Her doctoral thesis focuses on the issues of interpretation and qualification of criminal offences against the confidentiality of electronic data and information systems. The major areas of her research interests are cybercrime, the issues of the qualification of these criminal offences, and jurisdictional problems in cyberspace.
ORCID ID: https://orcid.org/0000-0002-9978-1200

Tomas GIRDENIS is an associate professor at Mykolas Romeris University Law School. He obtained a PhD degree in law from Mykolas Romeris University in 2011 (the topic of his PhD thesis was related to multiple offenses in Lithuanian criminal law). His research interests include criminal law and sentencing.
ORCID ID: https://orcid.org/0000-0002-4638-1414

Marius LAURINAITIS is an associate professor at Mykolas Romeris University. He was granted a PhD in law at Mykolas Romeris University in 2015 (the PhD thesis was published under the title Legal Regulation of Electronic Money). He is an executive editor of the international scientific research journal *Intellectual Economics*. His research interests include IT law, law of privacy and personal data protection, electronic identification law, electronic payments law, and electronic money. As a researcher, he has taken part in a variety of EU and national scientific projects.
ORCID ID: https://orcid.org/0000-0002-2926-9260