ARTICLE:

JUDGMENT IN THE CASE OF *K.U. V FINLAND:*

THE EUROPEAN COURT OF HUMAN RIGHTS REQUIRES ACCESS TO COMMUNICATIONS DATA TO IDENTIFY THE SENDER TO ENABLE EFFECTIVE CRIMINAL PROSECUTION IN SERIOUS VIOLATIONS OF PRIVATE LIFE

By **Tuomas Pöysti**

Introduction

The European Court of Human Rights (ECHR) has developed a system of human rights and fundamental rights and freedoms on the basis of the European Convention for the Protection of Human Rights and Fundamental Rights and Freedoms (Convention). The court's case law has opened new dimensions in the material definition of private life as a right to integrity and identity, and in the ways in which private life has to be protected by the domestic legal orders of the Contracting States of the European Convention. The ECHR case law should be compulsory reading for all lawyers specializing in ICT law (information and communication technology law or computer law) and law on electronic evidence. The judgments of the ECHR do not, however, always enjoy the attention they deserve by the specialised lawyers working in fields other than human rights law itself, and certainly not the attention of ITC experts and systems developers.

The ECHR has, in the 2008 judgment of the case of *K.U. v Finland*, further developed its case law concerning the protection of private life – the right to privacy – and the criminal law protection that the Contracting States to the European Convention should give to the right to private life.[1] *K.U. v Finland* is the second judgment during 2008 in applications brought against Finland concerning the positive obligations of the Contracting States to provide for the efficient and effective protection for the right to privacy, and to assure such protection in the context of information and communication systems. The first of these cases, the case of *I. v Finland* of 17 July 2008, concerns the security arrangements on the access to records of sensitive and confidential health data kept by a public hospital.[2] In this judgment, the ECHR stated that it is necessary to have such information security measures in place that provide practical and effective protection to exclude the possibility of unauthorized access from taking place in accordance with the provisions of article 8 of the European Convention of Human Rights. The second of these cases, the case of *K.U. v Finland*, concerns the use of criminal law in the protection of privacy. The ECHR found that the positive obligations of the Contracting States to ensure the protection of private life entailed an obligation to provide law enforcement agencies with the ability to obtain access to dynamic IP addresses and communication data[3] in order to identify a private person who has violated another individual's right to private life.

The ECHR judgment in *K.U. v Finland* contributes to the definition of the balance between the freedom and confidentiality of communications and anonymity over the internet, and the requirements of privacy and limitations of anonymity and confidentiality of communications. This judgment deserves wide international attention, even though it is not a Grand Chamber decision. It opens a new dimension in the case law, and takes position on an issue of interpretation felt particularly important by the court itself. This judgment is also noteworthy in respect of further developments of

[1] *K.U. v Finland, no. 2872/02, 2 December 2008.*
[2] *I. v Finland, no. 20511/03, 17 July 2008.*
[3] *Where the phrase 'communication or communications data' is used, it refers to data that is capable of identifying the sender and recipient of the communication.*

It was claimed in the advertisement that he was looking for an intimate relationship with a boy of his age or older ' to show him the way' .

the obligations of legislators to follow societal and technical developments and amend legislation so as to provide an effective protection, and also to provide for electronic evidence for investigations of alleged violations.

If the judgment in the case of *K.U. v Finland* is set in the wider perspective of the ECHR case law, these requirements seem to go beyond criminal law. The court requires the provisions of a privacy friendly legal, information and communications infrastructure and architecture, which also provides for effective remedies. According to the judgment, an effective and efficient protection of private life and deterrence against violations of private life must be included in the information and communication architecture. The government and the legislator are required to ensure that legislation is up-to-date, and also to ensure that legislation is applicable and effectively applied in practice.

Factual background and the judgment

Material events and legal procedures in Finland

The events in the case of *K.U. v Finland* began on 15 March 1999. On this day, an unknown person placed an advertisement on a dating site on the internet in the name of a 12 year old boy, K.U. The advertisement mentioned the age and year of birth of the boy. It also gave a detailed description of his physical characteristics and a link to his website. This included his picture, and his telephone number, which was correct save for one digit. It was claimed in the advertisement that he was looking for an intimate relationship with a boy of his age or older 'to show him the way'. K.U. became aware of the advertisement when he received an e-mail from a man who proposed to meet him and 'to see what you want'. K.U.'s father requested the police to identify the person who placed the advertisement on the dating site in order to prefer criminal charges. The internet service provider refused to divulge the identity of the holder of the dynamic IP address in question, regarding itself bound by the confidentiality of communications as defined by law.

The police requested the District Court to issue an order to divulge the dynamic IP address and the identity of the holder of the IP address on the basis of the Criminal Investigations Act, Act no. 449/1987 (Esitutkintalaki 449/1987). On 19 January 2001, the District Court refused the order in the absence of an explicit legal provision authorising the court to order a service provider to disclose telecommunications data. According to the decision of the District Court, the Finnish legislation in force at the time allowed the police the right to obtain telecommunication data only in certain offences. The placing of the advertisement in this case would be categorised as a calumny under the Penal Code. The law in force in Finland at the material time did not refer to calumny in the list of offences in which the police had the right to obtain telecommunications data. On 14 March 2001, the Court of Appeal upheld the decision of the District Court. On 31 August 2001, the Supreme Court refused to leave appeal. The prosecutor in charge of the case decided, on 2 April 2001, that the managing director of the internet service provider could not be charged for the violation of the Personal Data Act no 523/1999 because the alleged offence was time-barred.[4]

The application in the European Court of Human Rights

On 1 January 2002, K.U. lodged an application in the European Court of Human Rights against Finland, alleging that the State had failed in its positive obligations to protect the applicant's right to respect for his private life under article 8 of the Convention.

The European Court of Human Rights exercises the

[4] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.95, p. 31-50 was implemented in Finland by Personal Data Act no 523/1999 (Henkilötietolaki 22.4.1999/523). The Personal Data Act is the general data protection statute in Finnish law and it gives effect to the provisions in section 10 of the Constitution of Finland, which requires that protection for personal data shall be provided by law.*

A person convicted of committing an act of calumny against another person by a derogatory statement or by another degrading act faced a maximum term of three months imprisonment if convicted.

highest and final instance jurisdiction on the interpretation of the European Convention on Human Rights. The ECHR assesses whether the law of the Contracting States to the Convention provides guarantees for human rights and fundamental freedoms as they are guaranteed in the Convention. The court focuses on the functioning of the legal order of Member States from the point of view of the protection of human rights.[5]

The ECHR, because it is the final court in terms of protection of the human rights and fundamental rights and freedoms, has an excessive case load. This explains, partly, the time it takes for the court to hear a case. In the case of K.U., the judgment was delivered six years after the application and over eight years after the material events took place. For the development of precedents in the context of the internet and ICT, six years is a very long time. The relevant legislation in the Contracting States has often changed in the meantime. This is also the situation in the case of K.U. However, the reasoning of the ECHR and the requirements it set out are valid and topical.

At the time of the events of the case, section 8 of the Finnish Constitution Act provided that everyone's right to private life is guaranteed. Paragraph 2 of section 8 of the Constitution Act provided for the inviolability of correspondence, telephone calls and other forms of confidential communications. The protection of Privacy and Data Security in Telecommunications Act (Act no 565/1999), which was repealed on 1 September 2004, provided for the protection of the confidentiality of data in relation to transmissions to a particular subscriber connection. Pursuant to section 18 of the Act, the police had the right to obtain data relating to the identity of a person for the purpose of investigating an offence referred to in listed sections of the Penal Code. Calumny was not in the list of the crimes referred to in this Act. The investigations by the police are covered by the Criminal Investigations Act (Act no. 449/1987) and Coercive Measures Act (Act no. 450/1987). At the time of the events of the case, chapter 5a, section 3 of the Coercive Measures Act provided that the police could, upon authorisation of a court, monitor the telecommunications connection in the suspect's possession or otherwise presumed to be in his use, if the information obtained by monitoring could be assumed to be very important for the investigation, and the alleged offence was punishable by imprisonment of not less than four months, or the suspected offence is an offence against a computer system using a terminal device, or a narcotics offence.

Telecommunications monitoring was, thus, allowed in some specific computer related crimes or in serious crimes. At the time of the events, calumny was defined in chapter 27, section 3a of the Penal Code (the provision was inserted to the Penal Code by Act no. 908/1974). A person convicted of committing an act of calumny against another person by a derogatory statement or by another degrading act faced a maximum term of three months imprisonment if convicted. The maximum sentence was four months if the calumny was committed in public or in print or disseminated in writing. Further provisions at that time in relation to chapter 27, section 3a were introduced in 1974 to the Finnish Penal Code as a reaction to the infringement of privacy by the mass media. Other offences against the honour of a person and defamation also had fines as minimum penalty and were not listed as offences in which the monitoring of telecommunications would have been possible.

The processing and publishing of sensitive information concerning sexual behaviour on an internet server without the person's consent was criminalised at the material time as a data protection offence in section 43 of the Personal Files Act (Henkilörekisterilaki 471/1987, criminal provisions were amended by act no 630/1995) and in chapter 38, section 9 of the Penal Code or as data protection violation in section 44 of the Personal Files Act. The publishing of information concerning sexual behaviour could also have caused

[5] *K.U. v Finland, 44.*

liability and a claim for damages in accordance with the provisions of the Personal Files Act. At the material time of the events of the case, the legal position in Finland was that the criminal law did not provide very strong penalties or provide for coercive investigation methods in offences related to moral integrity or other immaterial values. This situation had also been criticized in the legal literature; the criminal law seemed to provide stronger and more comprehensive protection in classic crimes against life and physical integrity and property than in offences against moral integrity or other intangible values.

Since the events of the case, the Finnish law has been changed in many respects. The Constitutional provisions on human rights are substantially the same. The protection of private life is found in section 10 of the Constitution. Freedom of expression, which included a right to receive and send communications, is guaranteed in section 12 of the Constitution. The most significant change is that the Exercise of the Freedom of Expression in Mass Media Act no 460/2003 (Laki sananvapauden käyttämisestä joukkoviestinnässä 460/2003), which entered into force on 1 January 2004. This new act is widely applicable to internet activities. This act also provides access to communications data if the content of a message is of such kind that providing it to the public is a criminal offence. The provisions of section 17 of the Act sets out the conditions of the release of information relating to the identity of the person: a court may order the release of information required to identify a sender of a network message provided that there are reasonable grounds to believe that the contents of the message are such that providing it to the public is a criminal offence. The Act also requires the service provider to keep and record data identifying the sender and the contents of the messages for a certain time in order to ensure the practical implementation of both criminal and civil liability for the contents of the messages.

The general Act on the protection of personal data, the Personal Data Act, provides that a service provider is under a criminal liability to verify the identity of the sender before publishing an announcement on the web.[6] The Coercive Measures Act has been amended by Act no. 646/2003 concerning the definition and conditions of telecommunications surveillance. Disclosure of confidential information about the parties to telecommunications and communications data is only possible in respect of listed serious offences. These are generally offences for which the maximum penalty is at least four years of imprisonment, and certain other crimes including crimes against the functioning of computer systems. Defamation, calumny or the data protection offence in the form of failure of the network service provider to identify the sender of the message in accordance with the provisions of Personal Data Act do not belong to the offences in which a court may authorise surveillance. The Penal Code has been reformed concerning offences against confidentiality of communications and privacy. A new chapter 24 contains offences against privacy. Section 17 in the Exercise of Freedom of Expression in Mass Media Act remains the only provision in Finnish law of the disclosure of dynamic IP addresses or other communications data in cases of unauthorised distribution of information violating individual privacy. The sufficiency of these changes was also discussed shortly by the ECHR, since the Finnish government presented the argument that later legislative changes had rectified some of the alleged defects in the legal framework.

The government's arguments

The response of the Finnish government to the application in the case of *K.U. v Finland* rested on two essential arguments. First, a private individual interfered with the applicant's private life; it was not caused by a public authority. Second, the service provider of the dating service had an obligation to verify the identity of the person who had placed the advertisement. This duty was reinforced by provisions in the Penal Code and Personal Data Act, which made the failure to identify a person a criminal offence, and also established civil damages for the failure to respect the provisions on identity. According to the government, these provisions had sufficient deterrent effect and the State had, thus, taken measures required by the Convention to ensure the protection of private life. The government referred to the ECHR judgment in the case of *X and Y v Netherlands*, according to which the liability in damages could provide a sufficient deterrent effect.[7]

The government also drew attention to the fact that the criminal investigation in the case of K.U. was not successful because of the legislation, whose aim was to protect the freedom of expression and the right to anonymous expression that the fundamental right and freedom entails. The extensive protection to the

[6] *Section 48 of the Personal Data Act.*
[7] *ECHR judgment in the case of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91.*

anonymity of internet messaging, which even covered messages interfering with another person's right to private life, was a mere side effect of the broad and vague concept of message. This definition of the concept of message made it, according to the government, impossible to exclude messages interfering with private life from other messages.

The government argued that the legislation concerning the protection of private life should be assessed in the light of the social context of the time, and that at the material time of the events the rapid increase on the use of the internet was only just beginning. Legislative arrangements undertaken after the material events of the case have, according to the government's argument, further strengthened the protection of private life in respect of the freedom of expression. Legislation thus reflects the legislator's reaction to social development and the need for protection.

The judgment of the court

The ECHR cited and reviewed the relevant Finnish legislation and took note of the legal changes since the events of the case. The court went on to cite relevant international materials, and emphasised the Council of Europe Recommendation No R (95) concerning criminal procedure law connected with information technology and the Council of Europe Convention on Cybercrime of 23 November 2004. The court also reviewed the some of the contents of the European Union Directive 2006/24/EC amending Directive 2002/58/EC, the Directive on Privacy and Electronic Communications, and the EC Electronic Communications Data Retention Directive 2006/24/EC which requires the Member States of the European Union to ensure, amongst other things, that data are available for the purpose of investigation, detection and the prosecution of serious crime in relation to the use of the internet and e-mail communications, such as the address of the subscriber or the registered user to whom an internet Protocol (IP) address is allocated at the time of communication.[8]

The ECHR took particular note of the fact that in the case of K.U., a minor was the subject of an advertisement of a sexual nature. This created a stronger positive obligation on the legislator and other public authorities of a Contracting State to protect fundamental rights and freedoms, even in the relationships between private individuals. The court also pointed out that even though the material events of the case were qualified as calumny under the Finnish law, the case was essentially about the right to private life. The court preferred to assess the events and protection provided by the domestic legal order from that perspective. The situation was aggravated by the vulnerability caused by the relatively young age of K.U. at the time.[9] According to the court, children and other vulnerable individuals are entitled to State protection, in the form of an effective deterrence, from grave types of interference with essential aspects of their private life.[10]

The court reiterated its earlier case law that article 8 of the Convention does not only compel the State to abstain from arbitrary interference by public authorities to private life, but creates positive obligations to ensure the protection of private life.[11] These positive obligations may involve the adoption of measures designed to secure the respect for private life in the sphere of relations of individuals between themselves.[12]

The positive obligations to secure respect for private life extend to the horizontal relations between individuals, and are not only applicable in the vertical relations between individuals and public authorities. The court also recalled its earlier case law, according to which in cases where fundamental values and essential aspects of private life are at stake, efficient criminal law provisions are required.[13]

The court rejected the Finnish government's argument that the mere possibility of a criminal prosecution and the general prevention this possibility was sufficient protection of the right to private life. According to the court, the positive obligations may extend to the effectiveness of a criminal investigation.[14] The court considered that in the case of *K.U. v Finland*, a practical and effective protection required that effective steps be taken to identify and prosecute the perpetrator. In the case of K.U., such protection was not afforded, and

[8] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.*

[9] *K.U. v Finland, 41.*

[10] *K.U. v Finland, 46; the ECHR referred, in respect to this argument, to its judgment on Stubbings and Others v the United Kingdom, 22 October 1996, § 64, Reports 1996-IV.*

[11] *K.U. v Finland, 42. ECHR cited its judgment on the case of Airey v Ireland, judgment of 9 October 1979, Series A no 32, § 32.*

[12] *K.U. v Finland, 43.*

[13] *K. U. v Finland, 43; the ECHR cited its judgments on the case of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91, §§ 23-24 and 27, and the case of August v United Kingdom (dec.), no 36505/02, 21 January 2003 and M.C. v Bulgaria, no 39272/98, § 150, ECHR 2003-XII.*

[14] *K.U. v Finland, 46. The court referred to its earlier case law to judgments on the case of Osman v United Kingdom, judgment of 28 October 1998, Reports 1998-VIII, § 128 and the case of M.C. v Bulgaria, § 153.*

hence there was a violation of right to private life in accordance with the Article 8 of the Convention.[15]

The assessment of the judgment

Substantive and timely topicality of the judgment

Technically, the case concerned conditions of access to the identity of the holder of a dynamic IP address assigned by the internet service provider to a subscriber. The questions concerning preventive surveillance and the storing of communications data is a live issue in many countries. This issue emerges increasingly as a subject in court proceedings. The human rights and fundamental rights and freedoms set limits to the surveillance, storing and use of communications data. The recording and retention of data for the purpose of investigation is, on most occasions, seen as a risk to privacy and other individual rights and freedoms. In difficult cases, the issue is, however, not of only of protecting individual rights against interference by surveillance and data retention, but, rather, of finding a correct balance between various parties and their fundamental rights and freedoms.

The balance between the various rights and liberties based on human rights and fundamental rights and freedoms depends on the context, and the weight given to the various arguments and rights is different depending on each situation. The standards of balancing are created in the legislation. The legislative response, as well as the application of the legislation, is subject to the standards that follow from the protection of human rights and fundamental rights and freedoms and, for the Contracting States of the European Convention, developed mainly by the European Court of Human Rights. The court itself admitted that States and legislators have a margin of appreciation concerning the choice of appropriate ways of ensuring the protection for human rights, but the margin of appreciation is circumscribed by the provisions of the Convention, and the court, in the interpretation of them, must have regard to changing conditions and respond to evolving convergence as to the standards to be achieved.[16]

The ECHR wanted to say that the standards controlling the legislators' use of discretion in ensuring protection are converging and tightening. In Europe, the jurisprudence of the ECHR increasingly determines the limits of the national law and the EC/EU law on electronic evidence. It also acts as a balance between privacy and freedom of expression and anonymity of expression, both in vertical relations between public authorities and individuals, and in horizontal relationships between individuals themselves. For this reason, domestic legislators must have a close look to the evolving jurisprudence of the ECHR.

The content and efficiency of the right to private life

The judgment in the case of *K.U. v Finland* does not bring significant additional elements to the definition of the concept of private life itself. In the judgment, the ECHR rather shortly refers to its already established case law on the matter, particularly to the judgment in the case of *X and Y v the Netherlands*. Private life covers and entails protection of the physical and moral integrity of the person. In the ECHR case law, integrity is also seen as a condition for physical and moral welfare. In the judgment in the case of *K.U. v Finland*, the court underlines the importance for the State to protect the physical and moral welfare of children because of their particular vulnerabilities.[17] The court emphasised the need to protect minors from the inappropriate processing of information concerning sexual behaviour and from approaches of potential sex offenders.[18] In the context of the case of *K.U. v Finland*, it is important also to recall that communications data, traffic data, and the retention of such data falls under the concept of private life in article 8 of the Convention. The ECHR has confirmed this in the judgment in the case of *Copland v the United Kingdom*.[19]

The court sent an important message by recalling that, contrary to the analyses under Finnish domestic law and courts, the issue was not about calumny and criminal investigation within the limits set by the principle of legality, but that the situation in the case should be analysed as concerning the protection of individual integrity and the right to private life. The court analysed the essential issues, and considered the balance between fundamental rights and freedoms from legal technicalities, which the domestic law had been focused upon.[20]

The court's assessment follows its earlier established case law. The ECHR has developed a broad definition of private life, and also underlined the point that the concept is not susceptible to an exhaustive definition. Private life covers, among other things, physical and psychological integrity of a person and several aspects

[15] *K.U. v Finland, 49 – 50.*
[16] *ECHR judgments in the case of K.U. v Finland, 44, and, in the case of Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI.*
[17] *X and Y v the Netherlands, § 22 and K.U. v Finland, 41.*
[18] *K.U. v Finland, 46.*
[19] *ECHR judgment on the case of Copland v the United Kingdom, no. 62617/00, §§ 41 – 44, 3 April 2007.*
[20] *K.U. v Finland, 41.*

of the physical and social identity of a person.[21]

The wide definition of the concept of private life and, consequently, the wide duties of positive protection are also significant with regard to the eventual consequences of the application of the principles laid down in the ECHR case law, including the judgment in the case of *K.U. v Finland*, to the situations likely to arise, for example, in the social media. The social media is one of the environments where violations of privacy and information security similar to the material events in the case of *K.U. v Finland* are likely to arise in the near future for investigation and legal proceedings. The legislation and standard legal interpretations in many countries are not necessarily well adapted to treat with these kinds of problems. The law and the courts sometimes struggle to find a judicial angle from which to approach the violations of individual rights in the context of information and communication networks. In the case of *K.U. v Finland*, the ECHR provides some essential elements concerning legislation and the judicial approach concerning the assessment of the alleged violations of private life and unfair processing of personal information in such contexts of private and social networks.

Private life in the system of the European Convention is a wider concept than the right to informational self-determination, which is at the core of the rights defined by the EC Personal Data Directive 95/46/EC.[22] The wide, integrity-focused approach of the ECHR and the approach emphasising the right to informational self-determination complement each other in defining the elements of protection in the context of electronic communications and ICT systems. Together, these approaches create a powerful legal response to address some of the problems in the current ICT environment.

Non-existent or weak user-identification and authentication of the parties may easily create problems of fundamental rights and freedoms, and particularly the right to the integrity of private life. Personal data legislation can also be used to address these weaknesses. In Finland, identity and authentication have recently been raised as legal problems in the context of the short term, high interest consumer credit available through the mobile telephone, for example by text messaging (SMS). Two problems have become apparent in relation to the use of mobile telephones: loans directed to minors, and the fraudulent use of mobile telephones to purchase goods and services without the consent of the subscriber of the connection. The Data Protection Ombudsman, the national data protection authority, has emphasised the requirements of the EC Personal Data Directive and the Finnish Personal Data Act to properly identify and authenticate such consumer credit transactions.

Under the European Convention, the State has positive duties of protection, which also extend to physical and psychological integrity and the social identity of a person. The judgment in the case of *K.U. v Finland* can be interpreted to mean that legislation and public authorities have an obligation, following from article 8 of the European Convention, to arrange proper identification and authentication in electronic transactions when elements of personal integrity and identity are in question.

A substantial and significant point in the judgment in the case of *K.U. v Finland* is that the ECHR did not accept the wide protection given to the freedom of speech and anonymity of communications in the Finnish law of the time. The court recognised that freedom of expression and the protection of the confidentiality of communication are primary considerations, and that users of the internet must have guarantees for these rights to be respected. At the same time, the ECHR emphasised that the protection of the freedom of expression and anonymity of communications is not absolute, and must yield on occasion to other legitimate interests. The ECHR calls for a balance between various fundamental rights and freedoms and the rights and interests of various parties.

The requirement of a fair balancing between various interests and fundamental rights is strongly present in the case law of the European level constitutional courts in cases concerning access to communication data to establish responsibility and liability in relation to infractions of information-related rights. In the judgment on the case of *K.U. v Finland*, the ECHR clearly underlines that the balance is, in the fist place, for the legislator. The legislator is required to provide the framework for reconciling the various competing claims for protection.[23]

The European Court of Justice recalled the need to balance the various competing claims for the protection of different fundamental rights and freedoms in the judgment in Case C-275/06 *Productores de Música de*

[21] *For a short recollection of the various elements of the concept of private life in the case law of the ECHR, see the ECHR Grand Chamber judgment on case S and Marper v United Kingdom [GC], nos. 30562/04 and 30566/04, § 66.*

[22] *The Directive of the European Parliament and of the Council 95/46/EC of 24 October 1995 on the protection of individuals with regard the processing of personal data and the free movement of such data, OJ L 281, 23.11.1995, p. 31 – 50.*

[23] *K.U. v Finland, 49.*

España (Promusicae) v Telefónica de España SAU, judgment of 29 January 2008.[24] Case C-275/06 concerned, among other things, the interpretation of the EC Directive on Privacy and Electronic Communications 2002/58/EC in relation to the EC Copyright in the Information Society Directive 2001/29/EC and the rules concerning the effectiveness of the protection of copyright and the interpretation of the EU Charter on Fundamental Rights in this context.[25] The ECHR in turn referred to the EC Directive on Privacy and Electronic Communications 2002/58/EC in the arguments in the case of *K.U. v Finland*. The Directive on Privacy and Electronic Communications is, together with the Electronic Communications Data Retention Directive 2006/24/EC, a core part of the EU legislative framework for the protection and access to communications data.

The specific issue in the *Promusicae* case was the access to communications data held by the internet operator in an alleged infringement of copyright. In its judgment, the European Court of Justice underlined the need for the national courts to develop and apply such interpretations of EU Directives and national legislation implementing directives that enable the achievement of a fair and proper balance between various fundamental rights and freedoms. Concerning the interpretation of the EC Directive on Privacy and Electronic Communications, the European Court of Justice stated that neither the Directive on Privacy and Electronic Communications nor the EC Copyright Directives require the Member States to arrange for the retention of communications data in court proceedings that aimed at providing for liability under civil law. Directives do not exclude either form of retention if it is provided in national legislation and leads to a fair balance between various fundamental rights and freedoms, and respects the general principles of law, in particular the principle of proportionality. The European Court of Justice reminded Member States that pursuant to article 15 (1) of the EC Directive on Privacy and Electronic Communications, Member States are allowed to provide for exceptions on the confidentiality of communications data – among other things for the purposes of preventing, investigating and the prosecution of crime.[26]

Both the ECHR and the European Court of Justice, underline the role of the legislator to balance the competing fundamental rights and freedoms in various contexts. Since the context of the judgment of the European Court of Justice in case C-275/06 *Promusicae* was the interpretation of law in pending court proceedings, the ECJ went on to consider further specifications for the method of interpretation and role of the courts. In comparison, the ECHR, in the case of *K.U. v Finland*, considered the appropriateness of the protection given by the legislation at the time. The European Court of Justice went on to explain why EC law, in particular the Directive on Privacy and Electronic Communications, was fairly abstract and provided little direct guidance for a judge in a concrete case, but that this gap has to be filled by the State legislator and the national courts in interpreting the applicable EU and national legislation.[27]

To understand the European law concerning access to communication data, the judgments of the ECHR in the case of *K.U. v Finland*, and the European Court of Justice in Case C-275/06 *Promusicae*, should be read together. Apart from emphasising the role of legislators and the need to balance rights and duties, the European Court of Justice took up the particular role and methods of the interpreting judge and stated that the Union legislator had not provided for the retention of communications data in civil proceedings concerning infringements of copyright. EC Electronic Communications Data Retention Directive 2006/24/EC provides for the storage and retention of data linking a communication to an identity, and traffic data for the purposes of the investigations of crimes. The ECHR considered, in particular, that children, because of their vulnerabilities, require particular protection for the private life and right to physical and moral integrity and right to psychological security. The ECHR stated that sexual abuse of children is unquestionably an abhorrent type of wrongdoing.[28] In the context of sexual abuse, the State legislators should, to enable a fair and proper balance between competing claims for the protection of fundamental rights and freedoms, arrange for access to communication data to allow effective investigation of alleged offences. The assessment in the cases concerning infringement of copyright might be different.

[24] *Judgment of the European Court of Justice (Grand Chamber) of 29 January 2008 in C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU, ECR [2008] I-271.*

[25] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.*

[26] *Judgment of the European Court of Justice in C-275/06 Promusicae, paras 60 - 70.*

[27] *The European Court of Justice has extended this apology for abstract writing style to the EC Personal Data Directive 95/46/EC, see the judgment of the European Court of Justice of 7 May 2009 in Case C-553/07 College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, not yet reported in ECR.*

[28] *ECHR judgment in the case of K.U. v Finland, 49 and also the ECHR judgment in the case of Stubbings and Others v the United Kingdom, 22 October 1996, § 64, Reports 1996-IV.*

The ECHR and the European Court of Justice are right to emphasise the role of the legislator in balancing freedom of expression and the right to confidentiality of communications against the right to effective protection of private life. Legal certainty is improved when the framework for balancing can be read clearly from the legislation. This enhanced role of the legislator also fits well with the principles of democracy.

In practice, however, the ECHR sets very far-reaching duties and obligations on the State legislator, whereas the European Court of Justice seems to be more realistic about the possibilities the EC legislator has in the provision of guidance through abstract, universal norms to all potential conflicts and competing claims for protection in different circumstances that Member States face.[29]

A fairly detailed and far-reaching specification of the role and responsibilities of the Contracting State legislator by the ECHR in ensuring the protection of private life in the changing social and technological context is a very significant point in the judgment on the case of *K.U. v Finland*. The ECHR said the court was sensitive to the argument of the Finnish government that any legislative shortcoming should be seen in the light of its social context at the time. The court stated that it accepted the view of the difficulties involved in policing modern societies. The positive obligations to protect fundamental rights and freedoms should be interpreted in a way that does not impose an impossible or disproportionate burden on the legislator or authorities. The court recalled that another relevant consideration is to ensure that powers to control, prevent and investigate crime are exercised in a manner that fully respects the due process and other guarantees of the fundamental rights and freedoms, including guarantees on which the accused can rely on.[30]

The ECHR requires the legislator to ensure there are clear and well-defined expressions of the outcomes of the balance that must be taken in legislation. But the court also requires the respect of the principle of proportionality, and applies the principle of reasonableness according to which the positive obligations to ensure the protection of private life or other fundamental rights do not make it necessary to take measures that cause a disproportionate burden to the public authorities. The principle of proportionality applied by the ECHR provides that in the horizontal relations between individuals, the positive duties of protection should not create a disproportionate burden to other concerned private persons. These principles are fairly abstract, albeit they are easy to accept as guiding principles of balancing of the benefits, costs and burdens. A significant point in the judgment in the case of *K.U. v Finland*, is that (concurring with earlier case law) the ECHR defined the standards concerning measures that should be considered, and what counts as a disproportionate burden or difficulty in policing. A significant point is that this is, according to the court, a matter ultimately to be assessed by the ECHR from the perspective of the protection of human rights and fundamental rights and freedoms, albeit the legislator of the Contracting State has a margin of appreciation and is required to define the necessary and appropriate measures for the protection of fundamental rights.

The limitation of the State's margin of appreciation by the Convention and the principles laid down in the case law of the ECHR is not a novelty, but well established case law of the court.[31] Noticeable in the judgment in the case of *K.U. v Finland* is the extent of the control exerted by the ECHR over the choices made in State legislation. The court was sensitive to the Finnish government's argument about noting legislative shortcomings in the social context at the time, but the court considered that in 1999, when the material events of the case of K.U. took place, it was well known that the internet could be used for criminal purposes and that a wide-spread problem of the sexual abuse of children existed. The court went further to state that it could not be said that the government lacked the opportunity to put in place a system to protect children from being exposed via the internet. The court considered, thus, that the government of Finland had, in breaching article 8 of the Convention, failed to take measures that could provide practical and effective protection for the applicant's private life by enabling the authorities to identify and prosecute the person who had placed the offensive advertisement on the internet based dating service.[32]

The judgment can be read so that the ECHR places a particular obligation on the government and legislator of a Contracting State to follow societal and technical developments and risks, and to take such effective and practical action that are necessary to protect the human and fundamental rights and freedoms guaranteed by the Convention. The ECHR seems to require an active and systematic approach to learning about social

[29] *European Court of Justice in C-275/06 Promusicae, para 67, and also the judgment of the European Court of Justice in C-553/07 concerning the abstract writing style of the EC Personal Data Directive.*

[30] *K.U. v Finland, 48.*

[31] *The ECHR cited in the judgment in the case of K.U. v Finland its earlier judgment on the case of Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI, on the margin of appreciation see K.U. v Finland, 43 and 44.*

[32] *K.U. v Finland, 48.*

problems and risks to fundamental rights, and to the management of risks to ensure the effective protection of fundamental rights.

The ECHR is certainly right to require such an approach in order to ensure a good level of protection of fundamental rights. This is a significant point for which all governments and legislatures should pay attention to. In many countries, there remain important caveats and items of out-dated legislation in the face of new models of network society and network based communications. Governments and legislatures can only adequately discharge this duty by combining a systematic information and communication technology assessment with a regular general effectiveness assessment of legislation and a review of legislation. The lack of such analyses may be a weak point for several governments. In a legal science perspective, a skills and analyses of ICT law and legal informatics is required.

Use of criminal law in the protection of private life and the requirement of efficient investigations

A significant point in the judgment in the case of *K.U. v Finland* is how far the positive duties for the protection of private life extended in the domain of criminal law. The deterrence by the mere general threat of sanctions was not considered a sufficient protection of private life. Following case law from the judgment in case of *Airey v Ireland*, the ECHR stated that article 8 of the Convention contains not only the negative obligation to refrain from interference with an individual's private life, but also the positive obligation to secure respect for private life in relations between individuals.[33] The Contracting States have a margin of appreciation on the choice of measures, but this margin of appreciation is controlled by the requirements set out in the Convention and developed in the case law of the court. The general requirement for the measures of protection is that they must be efficient. According to the court, this means that in grave acts against private life there should be practical and efficient criminal law measures available.[34] In *K.U. v Finland*, the scope of the acts in which efficient criminal law protection is required was extended to a situation that, according to the court, was not trivial but did not have the same seriousness as some of the situations cited in the earlier case law of the court.[35]

Criminal law is the instance of ultimate state power. Because of the restrictive and punitive character of the criminal law, the use of it and criminal policy is guided by the principle of the last resort (ultima ratio) of criminal law or, the subsidiarity of criminal law, according to which criminal law shall be used only as the measure of last resort when other, morally more acceptable measures are unable to provide sufficient and efficient protection. In several countries, the last resort of criminal law is recognised as a policy principle or policy guideline and in some, for example in Germany and as an application of the principle of proportionality in Finland, it is even recognised as a principle of constitutional law.[36]

In *K.U. v Finland* and in the earlier case law in which the requirement of the efficient criminal law protection is set, the ECHR does not seem to discuss the application of the last resort principle to the situations in the material events of cases. In the judgment of *K.U. v Finland*, the court explicitly rejected the Finnish government's argument that there were other means and remedies available to K.U., and moved on to require practical and efficient criminal law protection.

The court may be too optimistic about the possibilities of criminal law to provide efficient protection for the protection of identity and other essential aspects of private life. On the other hand, the court is right that essential aspects and values of private life need protection by criminal law and thereby recognised as the core values to be protected by the State. The protection of private life and the provision of secure physical, moral and psychological identities can be achieved by attempting to provide for proof of identity and authentication in ICT systems and information networks. Without dispute, there are the essential elements for the feeling of security for individuals.

The ECHR is right to emphasise this aspect and the duties of the State to provide protection against infractions of these rights related to the right to private life. However, the success rate of investigations in crimes conducted through anonymous messages on the internet is limited. This is the case in general in relation to all computer related crime. Pushing the requirements

[33] *ECHR judgments in the cases of K.U. v Finland, 42 and Airey v Ireland, judgment of 9 October 1979, Series A no. 32, § 32.*

[34] *ECHR judgments in the cases of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91, §§ 23-24 and 27 and M.C. v Bulgaria, no 39272/98, § 150, ECHR 2003-XII.*

[35] *K.U. v Finland, 43 and 44.*

[36] *In Germany the principle of last resort, the subsidiarity of criminal law is recognised as a principle in the judgments of the Federal Constitutional Court, see in particular judgment of the Federal Constitutional Court in BVerfGE 39, p. 1 (p.47) and BVerfGE 88, p. 203 (p. 257-258). Principle of last resort is discussed in legal literature in all Nordic (Scandinavian) Countries and it is recognised as policy guideline in the official policy documents of the government concerning drafting of criminal law in Sweden, Norway and Finland. In Finland, the Constitutional Law Committee of the Parliament, which is the highest interpreter of the abstract constitutionality of the proposed Acts of Parliament, requires an assessment if certain conduct is to be penalised and it is necessary for the attainment of the legal good, and the protection required cannot be achieved by other means.*

for criminal law protection too far may be problematic in the view of the last resort principle. Realising this approach in practice may require extensive police measures that may also become problematic in view of the balancing that is required between various rights and claims for protection. The ECHR is not beyond the reasonable limits of criminal law. The court emphasised that in the case of *K.U. v Finland*, the essential concern was the need to protect minors from sexual abuse, and here there are no problems with regard to the principle of proportionality and the principle of last resort of criminal law. However, a cautious reading of the ECHR case law will be needed in order not to widen, without proper thought, the scope of protection under the criminal law without considering alternative measures.

Given the international character of the problem of the sexual abuse of children and the internet, efficient solutions must of necessity be international in scope. This is indirectly recognised by the court, which presents in very a positive light the Council of Europe Convention on Cybercrime as the only wide international instrument that deals with computer and internet-related crime, and which also states that in the assessment of the efficiency of the protection of private life, the court has to take into account the evolving convergence of the standards to be achieved.[37]

Another domain in which problems of the practical effectiveness of user identity have emerged recently is the web-casting and publishing possibilities of the internet, such as YouTube. Such services can be used for anonymous connection, and it has not been possible for law enforcement agencies to identify the perpetrators of violent threats on the basis of the dynamic IP addresses that the publication service providers have disclosed. Traces end at a third country server providing anonymous services.[38] The principles laid down in the ECHR judgment on the case of *K.U. v Finland*, and in the EC Electronic Communications Data Retention Directive 2006/24/EC, or the Council of Europe Convention on Cybercrime, are efficient and effective only if the legislative measures to implement these principles are reasonably global and all countries have law enforcement functions with a sufficient level of integrity and rapidity to offer and provide effective international assistance for investigations.[39] A global problem in the global networks requires a global answer. Although the approach taken by the ECHR is sound and correct, the efficiency of the protection required by the ECHR may still be limited.

An important point in the judgment in the case of *K.U. v Finland* is that the ECHR rejected the Finnish government's argument that civil liability and deterrence caused by the general threat of criminal sanction – the general prevention – gave sufficient protection for private life. The court continued, in *K.U. v Finland*, to develop its case law further, that investigations and prosecution of the crime should be effective in practice, and only this practical effectiveness of criminal investigations provides the necessary level of protection when the physical and moral wellbeing of a child is at stake. The court considered, in particular, that the implementation of practical and effective protection required that effective steps should be taken to identify and prosecute the perpetrator. The overriding requirement of the confidentiality of communications data in the Finnish national law in force at the material time of the events of the case prevented the perpetrator from being identified and thus, also an effective investigation.[40]

A significant contribution of the judgment in the case of *K.U. v Finland* is the requirement of the practical effectiveness of investigations of alleged offences as part of the protection of private life in accordance with article 8 of the Convention. Here, the court went beyond the concept of effectiveness of an individual investigation, but sees success of the investigations in a wider perspective of efficiency of legal protection. The legal order and procedures protecting fundamental rights and freedoms have to be efficient as a system, and they must enable success in individual cases.

The idea of the practical effectiveness of rights and the availability of remedies is not a novelty as such. The practical effectiveness of rights and availability of remedies are, rather, part of the very concept of the rights in the system of the European Convention of Human Rights and in case law of the ECHR. This emphasis on the practical effectiveness has also made the European Convention one of the most successful international systems for the protection of human rights and fundamental rights and freedoms. The law does not remain in books, but the law is of practical protection to individuals.

The ECHR considered, in *K.U. v Finland*, that this general principle of practical effectiveness required the

[37] *K. U. v Finland, 24 and 44; see also ECHR judgment in Christine Goodwin v the United Kingdom [GC], no. 28957/95, § 74, ECHR 2002-VI.*

[38] *This problem has emerged in the investigation of the threats of violence presented trough social media. The aliases behind the dynamic IP addresses assigned by a third country anonymous server have proven to be very difficult to investigate.*

[39] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63. The Council of Europe Convention on Cybercrime, opened for signatures on 23 November 2001, and the Additional Protocol to the Cybercrime Convention adopted in 2003.*

[40] *K.U v Finland, 48 and 49.*

availability of appropriate and efficient means and methods of investigations of alleged crimes and a legal framework that provides the availability of such methods. This will have, if taken seriously and generalised, significant consequences for the law on evidence and access to electronic evidence. The court indicated that it is a requirement for the protection of fundamental rights and freedoms to store and retain electronic evidence, including communications data, and to provide for access to it in police investigations when essential aspects and values of private life are at issue, and the concern is about the protection of children or other persons with particular vulnerabilities. In the light of the case law of the ECHR, the police should also be provided with sufficient resources and expertise to carry out such investigations.

These requirements will add an important additional aspect to the legal and legislative debate about obtaining access to communication data and the surveillance of such data. The storing and retention of communications data is not only a threat to individual rights, on some occasions it is required for the protection of fundamental rights. In the case of *Copland v the United Kingdom*, the court set out some general criteria where access to communications data and communications surveillance may be granted under the European Convention of Human Rights.[41] The *K.U. v Finland* judgment complements this approach well.

The requirement set by the ECHR is a fair one, but not without difficulties in practice. In societies based on the rule of law, the criminal law and criminal justice system exist to protect the individual and his fundamental rights and freedoms. In recent developments, the functioning of the criminal law, criminal procedure and investigations, and the activities of the criminal justice system are increasingly analysed and defined from the perspective of their capacity to protect and respect fundamental rights and freedoms. The judgment in *K.U. v Finland* adds to this development. The Contracting States should, as a consequence, evaluate whether the criminal law and procedure and the law concerning access to communication data and other significant sources of electronic evidence correspond to the test of being able to provide effective practical protection – and beyond that, to guarantee the overall efficiency of the protection of fundamental rights and freedoms. But it is necessary to be cautious about not falling into the fallacy of believing that criminal law and criminal investigations alone could provide sufficient protection for the essential aspects and values of private life.

Effect beyond the criminal law: privacy-friendly information and communication infrastructure

In the case of *K.U. v Finland*, the ECHR required an effective means of identifying the person who placed the advertisement. Indirectly, this requirement means that both the legislation and the information and communication infrastructure, including the ICT architecture, should provide for the reliable identification and authentication of the parties to a communication, and access to past communications data. In the other recent case on private life, where Finland was the responding government and where a violation of the right to private life was also found, the case of *I. v Finland*, the ECHR stated, at 47, that: 'What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place. Such protection was not given here.' In this context, it is necessary to provide for the proper security of IT and archive systems, including the requirement of an effective audit. In *I. v Finland*, the ICT system failed to record who had been obtaining access to and consulting confidential files, access to files was not restricted only to those members of the staff who were responsible for the treatment of a particular individual. These failures were considered to constitute a breach of private life.[42] The judgment in *I. v Finland* makes it clear that the obligations of the State are to ensure that confidential data stored in an ICT system must be held securely; only authorized personnel may be given access to the data, and it should be subject to effective audits. Similar obligations also exist concerning the identity and recording of communications data and the traffic data.

A picture emerges from the ECHR judgments by which the court makes it clear that an information and communication infrastructure and ICT architecture, including the software code and functions, should be designed to protect fundamental rights and freedoms. Proper information and communications security is an essential element of this infrastructure and architecture. Keeping logs and transaction records, secure storage and controlled access to communications identification and traffic data, and reliable and secure identification and authentication of the parties of communications are part of this infrastructure and architecture that emerge

[41] *ECHR judgment in Copland v the United Kingdom, 3 April 2007, no. 62617/00, §§ 45 – 48.*
[42] *I. v Finland, judgment of 17 July 2008, no. 20511/03.*

from the ECHR case law. The court has contributed significantly to providing strong and highly authoritative human rights foundations for the development of the general principles of ICT law, or to the general doctrines and principles of legal informatics, to guide planning and management of information and communication systems and networks. The Contracting State is required to provide a practically effective legal framework for such rights-friendly infrastructure.

The first consequences of this should be that the functioning of the anonymous servers, that is servers providing a system that aims to make the identity of the parties to communications difficult or impossible, should be critically assessed in all countries. On many occasions, anonymity is compatible with the requirements of fundamental rights and freedoms, but not in all cases. The anonymity of the communications over the internet should be put into a wider and more critical perspective. Secondly and even more significantly, the enforcement of the Data Protection laws requiring confirmation of identity and authentication should be assessed and strengthened, and legislative caveats corrected. Thirdly, legislators have the duty to provide an effective response to the risks to secure identity. The last issue is an old theme in the literature in computer and ICT law – in this, the ECHR has not provided any additional arguments and foundations for such an approach.

Conclusions

The judgment in the case of *K.U. v Finland* is significant, because it requires Contracting States to ensure high quality IT systems are in place in order to provide for the positive obligations of the protection of private life in relations between individuals themselves. In addition, the court also requires Contracting States to have practical and effective legal protection in place, including criminal sanctions, to provide for the protection of private life. This judgment requires governments and legislators to follow societal and technological developments, and to ensure that the legislation in force can provide effective protection. The court extended the principle of practical effectiveness of protection and its implication to require practical effectiveness of investigations to cover electronic evidence and information necessary to identify the perpetrator of the alleged offence. Legislators are required to provide for access to communication data, and governments should ensure the conditions for successful criminal investigations in cases where essential values and elements of private life are at risk. The protection of children against sexual abuse through the internet is essential, because values and elements of private life are in danger, and the right to freedom of expression and anonymity of communications must be over-ridden when dealing with such cases for the benefit of effective investigation. The court has also indirectly defined further general requirements based on human rights and fundamental rights and freedoms concerning the principles of ICT law. In particular it is now necessary (although it has always been so) to consider the implications for security surrounding the identity of parties to communications and the retention of communications data. The ECHR addresses actual and difficult issues relating to crimes occurring in the context of the internet and the need to identify the parties to communications, and also the conditions for success in criminal investigations of serious computer and cyber crime. The ECHR has, in the case of *K.U. v Finland*, contributed to the development of European and international law on electronic evidence and the protection of private life through criminal law.

Dr Tuomas Pöysti is the Auditor-General of Finland, President of the National Audit Office of Finland and Permanent Advisor of the Government Advisory Board for Better Regulation. Dr Pöysti is a Docent of Administrative law at the University of Helsinki, teaches advanced courses on ICT and European criminal law and has an extensive list of scientific publications on information law.

http://www.vtv.fi
tuomas.poysti@vtv.fi

ARTICLE:

BUSINESSES' PERCEPTION OF ELECTRONIC SIGNATURES: AN AUSTRALIAN STUDY

By **Dr Aashish Srivastava**

Introduction

The advent of the internet has transformed the world of commerce. Electronic commerce allows businesses to buy and sell in global markets that are no longer bound by geography or time. Increasingly, governments, businesses and consumers are using information technology and the internet to exchange information, produce, market, buy, sell and even deliver products and services to places virtually unreachable before. Electronic signatures,[1] in particular digital signatures,[2] have been established with the objective to authenticate and facilitate commercial transactions in the electronic environment.

Several initiatives have been implemented over the last decade in order to provide legal recognition to electronic signatures. At a global level, the United Nations Commission on International Trade Law (UNCITRAL) has provided model laws that offer a legislative guide to countries on the framing of their national electronic signature legislation.[3] At a regional level, the Electronic Signature Directive has been enacted by the European Union (EU) in an attempt to ensure consistency and legal validity of electronic signatures across member states.[4] In addition to legislation on an international and regional level, over ninety individual countries have also legislated for the use of electronic signatures. Typically, legislation has taken one of three types of approaches: a minimalist or technology-neutral approach where any technology can be used as an electronic signature provided it satisfies the legal function of a signature;[5] a digital signature or technology-specific approach[6] that recognises the primary use of digital signatures generally to the exclusion of other forms of electronic signature; and a dual approach that provides an evidentiary presumption in favour of validity of an electronic signature if the parties use specific technologies, in particular, digital signatures issued by recognised certification authorities.[7]

In Australia, a technology-neutral legislation was enacted in 1999, the Electronic Transactions Act 1999 (Cth) (ETA).[8] Based on this Commonwealth legislation, States and Territories have enacted similar electronic signature and transaction legislation.[9] The provisions of

[1] *One definition of 'electronic signature' is provided by article 2(a) of the UNCITRAL Model Law on Electronic Signatures 2001 art 2(a), 'as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.'*

[2] *A digital signature is a type of electronic signature, and is described in paragraph 36 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001) as 'created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form'.*

[3] *See UNCITRAL Model Law on Electronic Commerce 1996 and Model Law on Electronic Signatures 2001.*

[4] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12.*

[5] *Most common law countries have adopted the minimalist approach towards legislation. These include the US, the United Kingdom, Canada and New Zealand.*

[6] *The technology-specific approach has also been referred as a prescriptive approach in the literature.*

[7] *The EU Electronic Signatures Directive is a good example of a dual approach. The legislation in China and Singapore are also considered as a dual approach. See Electronic Transactions Act 2004 (China) (for a translation and introduction into English of the Chinese Act, see Minyan Wang and Minju Wang, Translation and Introduction to the Electronic Signatures Law of China, Digital Evidence and Electronic Signature Law Review 2 (2005) 79 – 85, and Electronic Transactions Act 1998 (Singapore).*

[8] *Electronic Transactions Act 1999 (Cth).*

[9] *The state level Acts are: Electronic Transactions Act 2000 (NSW); Electronic Transactions Act 2000 (SA); Electronic Transactions Act 2000 (Tas); Electronic Transactions Act 2000 (ACT); Electronic Transactions Act 2003 (WA); Electronic Transactions (Victoria) Act 2000 (Vic); Electronic Transactions (Queensland) Act 2000 (Qld); Electronic Transactions (Northern Territory) Act 2000 (NT). Note that since the State legislation is essentially the same as the Electronic Transactions Act 1999 (Cth), the discussion in this article is confined to the provisions of the latter legislation.*

' The reluctant take-up of electronic signature tools is slowing down the growth of trade in goods and services via the internet,' asserted a press release, without any evidence.

the ETA are based on the Model Law on Electronic Commerce 1996 (MLEC) which is the first model drafted by the UNCITRAL.

Despite the legislative initiatives at global, regional and national levels to promote the use of electronic signatures, anecdotal evidence and reports in the media indicate that there has been a very slow take-up of the digital signature technology across the world. A progress report on the EU Electronic Signature Directive in 2006 expressed concern with regards to the slow take-up of digital signatures across its twenty-five member states.[10] 'The reluctant take-up of electronic signature tools is slowing down the growth of trade in goods and services via the internet,'[11] asserted a press release, without any evidence. Other countries such as Germany and Thailand have also reported low acceptance of digital signatures in recent years.[12] Some scholars in the field have expressed concern that the culture of the failure to adopt digital signatures by individuals and businesses is hard to change.[13]

Likewise, it has been almost nine years since the ETA has been enacted in Australia, but the use of electronic signatures, particularly digital signatures, has been low.[14] Note that while the legislation was enacted to give an impetus to e-commerce at all levels, digital signatures are mostly used for government on-line services.[15] Anecdotal evidence shows that there has been a low use of digital signature technology among businesses when dealing with other businesses for contracts and commercial transactions, despite the Australian government's effort to promote it as 'a valid form of authentication for enabling and sealing e-commerce transactions'.[16]

Research questions

This led the author to consider a number of questions. Why is there a lack of acceptance of digital signatures by the business community in Australia for entering into contracts and commercial transactions with each other? What could be the likely factors to impede the use of electronic signatures, in particular, digital signature technology in a regulated environment?

The objective of this article is to briefly outline the findings of a comprehensive investigation conducted by the author as part of his doctoral thesis to identify factors that have contributed to the low acceptance of electronic signatures, in particular digital signatures, in the Australian business community. The research was an empirical study relying predominantly on the views and experiences of various groups of people from large country-wide public listed companies in Australia. A sample of 27 participants comprising of heads of the

[10] *Commission of the European Communities, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (Brussels, 15.3.2006, COM(2006) 120 final) http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf.*

[11] *' Electronic signatures: legally recognised but cross-border take-up too slow, says Commission' (IP/06/325, Brussels, 17 March 2006) http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/325&format=PDF&aged=0&language=EN&guiLanguage=en.*

[12] *eGovernment, Take-up of electronic signatures remains low in Germany (2004) epractice.eu (no longer available); Pascale Prud' homme, and Hassana Chira-aphakul, E-Commerce in Thailand: A slow awakening, Thailand Law Forum http://thailawforum.com/articles/e-commerce.html.*

[13] *Heiko Roßnagel ' On Diffusion and Confusion-Why Electronic Signatures Have Failed' in Simone Fischer-Hübner Steven Furnell, Costas Lambrinoudakis, editors, Proceedings of the Third International Conference on Trust and Privacy in Digital Business (TrustBus 2006) 71; Jane K Winn, ' The Emperor New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce' (2001) 37(2) Idaho Law Review 353; Raymond Perry, ' Digital Signatures - Security Issues And Real-World Conveyancing' (2001) 151 New Law Journal 1100. See also in the Australian context, Drugs and Crime Prevention Committee, Parliament of Victoria, Inquiry into Fraud and Electronic Commerce (2004) (180) http://www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf.*

[14] *Drugs and Crime Prevention Committee, Parliament of Victoria, Inquiry into Fraud and Electronic Commerce (2004) 180 http://nla.gov.au/nla.cat-vn3093816.*

[15] *Inquiry into Fraud and Electronic Commerce (2004). The areas in which digital signatures are being promoted are: Australian Customs Service, SPEAR Project run by Land Victoria and EC (Electronic Conveyancing) system, a part of the Land Exchange Program within the Victorian Government's Department of Sustainability and Environment. The latest position is that these projects are currently running at a very small scale. Unfortunately, there is no recent information or reports that are available on these.*

[16] *National Office for the Information Economy, Government Role in B2B E-Commerce (2001) Department of Communications, Information Technology and the Arts www.archive.dcita.gov.au/2001/10/b2b_e-commerce/. The Drug and Crime Prevention Committee report states that digital signatures are used primarily with the ATO and not for other services.*

In general, participants revealed a considerable lack of understanding of the term electronic signature and the legislation governing them.

Information Technology (IT) and legal departments and senior management (SM) executives was used. A series of semi-structured interviews were conducted face-to-face or by telephone. The interviews were then transcribed and analysed by the author using the matrix-based framework analysis approach commonly used in applied policy research.[17] This article first summarises the main findings of the research. It is then followed by a critical discussion, followed by a number of recommendations for measures that may overcome the low use of electronic signatures in the business community.

The main findings

The empirical research demonstrated that there are six potential factors that are likely to have led to a low use of electronic signatures in the Australian business community. These are ignorance or lack of understanding of the technology and the law governing the technology, security concerns, legal obstacles, complexity and confusion, cost concerns, and culture and customs.

Ignorance or lack of understanding

A major finding of this research is ignorance. In general, participants revealed a considerable lack of understanding of the *term* electronic signature and the legislation governing them. Businesses appear to have a limited understanding of the various forms of electronic signature, not to mention digital signature, although they are using a particular form of electronic signature (i.e. e-mails) on a day-to-day basis. Such lack of awareness is identified as the leading reason for businesses' hesitance to use digital signatures.

Ignorance or lack of understanding of the *term* electronic signature

About a quarter of the participants admitted having never heard of the term electronic signatures. Others who were aware of the existence of this term demonstrated very limited understanding of the various forms that electronic signatures take. An electronic signature was generally believed to be a scanned image of a manuscript signature. In addition, there appeared a certain confusion between the term electronic and digital signature. The terms were used interchangeably during the interview process by a few participants.

Ignorance about the legislation

A high degree of ignorance also prevailed among businesses with regard to the legislation governing electronic signatures, in particular the ETA. More than two-thirds of the participants were not aware of the provisions of the ETA and the provisions relating to electronic signatures in Australia. Their lack of awareness emerged from comments such as: 'I don't know what the law is on using electronic signatures;'[18] 'I am not aware of any such law'.[19] On the other hand, those who were aware of the legislation mostly demonstrated a very limited knowledge of the provisions in the ETA. The following responses were noted from participants: 'I am not aware of it being a recognised form;'[20] 'I know there are viable options and there are rules around it but I do not know in great detail;'[21] 'We really haven't gone and explored the wider legal aspect of understanding or where the law sits with

[17] *Note that a five-stage framework analysis method was adopted for analysing the interview data. In stage 1 (familiarisation), the author familiarised himself with the interview transcripts and obtained an overview of the collected data. In stage 2 (identifying a thematic framework) an initial coding was conducted from the issues emerging from stage 1 to set up a thematic framework. The thematic framework at this stage was only tentative and further refining was made at subsequent stages of analysis. In stage 3 (indexing), the initial coding, or in other words the thematic framework, was applied to the data collected through the use of textual codes to identify those segments of the interview transcripts that reflected a particular theme. In stage 4 (charting) specific pieces of data corresponding to a particular theme were identified from the interview transcripts and arranged in charts, with each chart representing a specific theme. After all the indexing and charting were done in accordance with the themes, in the final stage 5 (mapping and interpretation), the key characteristics of the data collected were examined with a view to mapping and interpreting the data set as a whole. The above five steps were carried out with the help of NVivo, a software package well known for the analysis of qualitative data.*

[18] *P2_C02_Legal, Paragraph 31.*

[19] *P12_C07_SM, Paragraph 76.*

[20] *P16_C04_Legal, Paragraph 68.*

[21] *P18_C011_Legal, Paragraph 197.*

it;'[22] 'There are some legislation in 2001, the Electronic Transactions Act or something like that. That is all I remember but I am not deeply familiar with it.'[23] Businesses' lack of awareness and understanding of the legislation appeared to be largely responsible for their lack of appreciation of the different forms that an electronic signature can take. In fact, the research revealed a high level of ignorance at the level of lawyers' and legal advisors. A failure to understand the legislation appears to have potentially weakened businesses' confidence in using electronic signatures.

Security concerns

The research sought participants' views on whether security is an issue with the use of electronic signatures. In general, participants were quite concerned about the security aspect of electronic signatures. The majority of the participants believed that businesses have not embraced the idea of integrating digital signatures into their work environment for a number of security reasons. There were concerns that the technology that currently exists does not provide sufficient safeguards to users. As a result it will be impossible for digital signatures to be used as a secure form of authentication. 'It's very much the insecurity of the whole thing that is why it hasn't been widely accepted,'[24] claimed one participant. Participants were generally concerned that someone could hack into another person's computer system and maliciously use his or her digital signature without the person's knowledge.[25] '[T]he last thing you want for the other party [to the contract] to say is that 'hang on I didn't sign it, that wasn't me, I didn't do it,'[26] remarked a participant.

The security fears expressed by participants were both of technical and legal nature. From a technical standpoint, participants feared that a person could fraudulently use someone else's digital signature and pass it as his own. '[O]nce it's on the computer anyone can access it. ... it's pretty easy to get hold of it if you want to get it,' remarked a legal participant.[27] From a legal stance, participants feared that a plaintiff would not be able to satisfy the court that a forger has forged or affixed his digital signature. As remarked by one of the participants, 'when it comes down to proving, you don't know if this was actually executed by the named person.'[28]

There are three basic ways that digital signatures can be secured, through the use of passwords where a digital signature is stored on the hard disk of a computer; using portable information storage devices (PISDs); and using biometric devices. Issues were raised with all three methods of securing digital signatures.

Hard disk secured with password

The most common form of storage of a digital signature is on the hard disk of a computer.[29] A user wishing to affix his digital signature will use a key board or a mouse (or both) to activate it,[30] and the signature will then be attached to a particular data message. However, the risk is that the same command can be given by anyone else who also has access to that computer, because it is the computer that 'signs' rather than the actual owner of the digital signature. To protect from such risks, the storage of digital signatures on the hard disk of a computer can be secured through the use of a password or PIN. Participants were in general of the view that passwords can adequately protect against unauthorized and malicious access to computers. However, it was also noted that despite password security policies implemented by their organisations' IT department, staff would rarely abide by them. They would often choose passwords that would be easy to guess, or fail to change them at regular intervals as recommended. An IT participant stated:

> When you log into a system you are given a default password. My experience is that fifty percent of the people still have that password so ... anywhere down the track ... I am not sure what we really have to do ... I think if we have to move on to that ... take steps to really follow through on forcing people to change their passwords.[31]

A failure to implement precautionary measures has made digital signatures behind such passwords prone to attack. Therefore, despite the common belief among participants that the storage of a digital signature on a computer could be secured through the use of passwords, their careless attitude towards password use and management made the hard disk an unsafe option for storing electronic signatures.

[22] *P14_C09_SM, Paragraph 123.*
[23] *P21_C012_Legal, Paragraph 10.*
[24] *P8_C05_Legal, Paragraph 114.*
[25] *For example, P15_C010_Legal, Paragraph 63.*
[26] *P2_C02_Legal, Paragraph 88.*
[27] *P24_C015_Legal, Paragraph 55.*
[28] *P6_C04_Legal, Paragraph 76.*
[29] *Especially for Non-Individual digital signature certificates or Organisation digital signature certificates.*
[30] *In the case of digital signature, it is the private key that the subscriber activates to create a digital signature.*
[31] *P18_C011_Legal, Paragraph 124.*

PISDs

Digital signatures can also be stored on PISDs, such as a smart card or a Universal Standard Bus (USB) token (also known as a flash disk). A smart card is amenable to cryptographic implementation and thus enables the subscriber to sign and encrypt a document.[32] A USB token such as a flash disk, however, is not amenable to cryptographic implementation but can conveniently be plugged into the USB port which is available on most computers and laptops.

In general, participants considered the use of PISDs such as smart cards and flash disks to be unsafe. Concerns were raised by participants that PISDs could easily be lost or stolen and used for malicious purposes. '[I]f you lose a smart card who is to decide that someone else cannot read that smart card or use it,'[33] remarked a participant. However, they believed that if the PISD was secured with a password or PIN that would provide adequate security.

Biometric measurements

Apart from passwords and PISDs, another method of securing digital signatures is through the use of biometrics.[34] In this case, instead of using a password or a PISD (or both) to obtain access to his or her digital signature, a subscriber uses a biometric measurement such as fingerprint and retina scan. By using this method, although not perfect, it becomes harder for a malicious attacker to break in and use the signature than any other security mechanisms such as a password or PIN. With the exception of a few operational limitations, participants generally considered biometric measurements to be the most secure method of storing a digital signature. Their perceived views about biometric measurements were reflected in comments such as: 'that's probably a little bit more secure if it's thumb print ... that sounds fairly secure';[35] and 'I guess to crack biometric or fingers or retina or whatever, is not easily accessible to most people'.[36]

The internet and the intranet

The internet, a prerequisite for the usage of digital signature technology, was mostly believed to be insecure, although it was not considered to be a significant deterrent to the use of digital signatures. Those who found the internet insecure made remarks such as: 'I am not sure how safe the internet is ... I have concerns as to the safety of it but that is not to say that I won't use it';[37] and I don't think the internet is completely secure once you are in there it's pretty open and anything can happen'.[38]

However, some participants believed that although a digital signature uses encryption technology and can therefore secure documents traversing over the internet, it is still at risk from hackers because most office computers are connected to the internet or an intranet. According to some participants, the real risk of forgery of a digital signature does not arise primarily from the use of the internet but from fraudulent actions within an organization. As remarked one participant:

> The fraud normally is an internal fraud than transmission fraud and so I think the euphoria of people collecting thousands of cards through siphoning and data out of pay pal and things like that ... yes, a fairly strong imagination.[39]

Legal concerns

Legal concerns associated with electronic signatures were also identified as a potential factor that could contribute to its low use for contracts and commercial transactions. In particular, the lack of admissibility of electronic signatures in the court of law and complexities arising with evidentiary matters when proving authenticity of electronic signatures were raised by participants.

Admissibility of electronic signatures

A high proportion of participants, in particular legal participants, believed that electronic signatures would not be admissible in evidence. Occasionally, their legal advisors would discourage them to use electronic signatures on the grounds of their admissibility in a court of law. A legal participant remarked:

> To the end 2001 I worked on Electronic Data Interchange (EDI) type of contracts. I worked for the IT department but I have to say that apart from the EDI type stuff which never took off no-one was particularly interested in electronic signatures and the lawyer wouldn't either. The lawyer would say, 'look I don't understand all these stuff or the law won't necessarily accept it as evidence or it's too difficult. Just rely on paper or fax or something like that'.[40]

[32] *Johan Borst, Bart Preneel and Rijmen Vincent, 'Cryptography on Smart Cards' (2001) 36(4) Computer Networks 423, 423.*
[33] *P2_C02_Legal, Paragraph 64.*
[34] *Note biometric measurements can also be considered as a form of electronic signature, but are usually used to establish whether the person you are dealing with is the person entitled to the service.*
[35] *P2_C02_Legal, Paragraph 64.*
[36] *P4_C03_Legal, Paragraph 113.*
[37] *P6_C04_Legal, Paragraph 189.*
[38] *P25_C015_IT, Paragraphs 96.*
[39] *P26_C016_SM, Paragraph 57.*
[40] *P1_C01_Legal, Paragraph 61.*

Evidentiary matters

Concerns were expressed about the inconclusiveness of an electronic signature, given there is no physical document that is signed. The general view of the participants was that the law of evidence would struggle to deal with electronic signatures in the absence of original physical documents. Since there is no concept of an original digital object or a signature generated electronically,[41] the concept of primary evidence and secondary evidence cannot be applied in the context of electronic signatures. Views were expressed that courts would require the original document containing the electronic signature to identify the signer. 'The court will always look for an original. There is only one document that is an original and that is the evidence, the primary evidence,' claimed one participant.[42] 'The law very much clings to originals with a signature on it to show that they have been correctly executed between the parties,'[43] remarked another one.

Participants also feared that, unlike a manuscript signature, it was not possible to witness an electronic signature, thus adding another layer of complication. They believed that there is no provision in the law that allows the witnessing of an electronic document, in particular, an electronic signature:

> On certain contracts the execution calls provision for a witness to sign. ... they will then go to the court and testify, 'I saw that authorized officer signing this document.' With an electronic signature I find that very difficult to do.[44]

Finally, electronic signatures were subject to disapproval by participants who claimed that, unlike manuscript signatures, electronic signatures cannot undergo handwriting tests and therefore identifying the actual signatory becomes harder in case of a dispute. Thus, if a person intent on committing a fraud hacks into someone else's computer and fraudulently uses his or her electronic signature to gain an unfair advantage, it would be difficult to convince the court that neither the owner of the computer nor any authorized person used the owner's signature. In contrast, with manuscript signatures, it was asserted that a fraudulent signature can easily be identified with the help of handwriting experts. One participant offered the following comment:

> I think it would be rather difficult showing that or try to prove that there is a probability that someone else could have logged on [with electronic signatures] ... With a manuscript signature often you just need a proof. Someone can bring somebody who knows the signature or you can do handwriting tests.[45]

Complexity and confusion

The general perception among participants was that the use of electronic signatures was complex and confusing. However, these issues were raised mostly in the context of the digital signature while other forms of electronic signature were not necessarily perceived as complex to use. In particular, the digital signature technology was found to involve complicated application programs that would render it unfriendly to use; a complex setting-up process, and a stringent requirement for the recipient organisation to be equipped with a similar technology. The perceived views about the complexity and confusion were reflected in comments such as: 'I suspect that the reason for that [its non-acceptance] is that it is so complex to set up';[46] or 'the big issue is ... that it's a pain in the ass to set something up,' [47] 'You can't do it ... you can't use and communicate with that technology until you establish that the other party has that technology. I guess it adds another level of complication'.[48]

Cost

From the point of view of costs, the expenses involved in educating and training staff was identified as an important factor that could deter the use of electronic signatures. 'There is the cost of educating them as well and we are not interested in doing that';[49] the cost [of electronic signature] includes training and deployment'[50] were typical remarks made by participants.

On the other hand, the cost of obtaining digital signature certificates[51] was not considered to be a disincentive with regard to the use of the technology. Such costs were trivial for participating companies.[52] They claimed that their organisation could easily afford to use the digital signature technology. 'I wouldn't imagine that cost would be prohibitive because big companies would spend a lot more on IT systems,'[53] or 'I don't think cost would be an issue you know, if it make

[41] *Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility, (LexisNexis Butterworths, 2007) 2.20; 4.16-4.35.*
[42] *P1_C01_Legal, Paragraph 77.*
[43] *P18_C011_Legal, Paragraph 68.*
[44] *P6_C04_Legal, Paragraph 76.*
[45] *P18_C011_Legal, Paragraph 228.*
[46] *P1_C01_Legal, Paragraph 19.*
[47] *P1_C01_Legal, Paragraph 28.*
[48] *P22_C013_Legal, Paragraph 82.*
[49] *P5_C03_IT, Paragraph 66.*
[50] *P5_C03_IT, Paragraph 110.*
[51] *A digital signature certificate from an accredited Certification Authority such as VeriSign costs A$130-200 in Australia.*
[52] *Note that because the research confined to large Australian businesses it may be a reason that cost was not an issue. It may be an issue for small businesses.*
[53] *P2_C02_Legal, Paragraph 48.*

things speedier ... I can't imagine it would be costly,'[54] were typical remarks made by participants.

Culture and customs

Another issue raised by a few participants that could inhibit the use of electronic signatures is the culture and custom associated with manuscript signatures. Participants believed that the use of manuscript signatures has become a part of the Australian business culture and custom, and this acts as a significant deterrent to the use of electronic signatures. Relative to an electronic signature, a manuscript signature was considered a 'tried and trusted method of signing documents'[55] for hundreds of years for executing contracts and commercial transactions by the business community. 'A handwritten signature is a cultural thing at the moment,'[56] remarked a participant. 'Things have always been done via pen and paper,'[57] claimed another participant.

Discussion and recommendations

The above section has set out an outline of the various factors that participants identified as potential impediments to the adoption of electronic signature technology. These factors comprise ignorance or lack of understanding of the electronic signature technology and the law governing the technology; security; legal obstacles; complexity and confusion; cost, and culture and customs. Some of these concerns raised are legitimate. For instance, the complex setting-up process of the digital signature technology, the stringent requirement for the recipient organisation to be equipped with a compatible technology or the cost of staff training can result in significant hurdles for businesses. However, several of the concerns raised by participants appear to be unfounded and based on misconceptions.

Ignorance and lack of understanding of the technology was identified as a key impediment to the use of electronic signatures for contracts and commercial transactions in the Australian business community. Because of the lack of awareness, businesses are unable to appreciate the benefits of this technology. It is suggested that they need to recognise that electronic signatures have the capability to enhance their performance and capabilities, and provide them the ease of signing contracts, joint ventures and conduct electronic commerce sitting in front of their computer anywhere in the world.

It is therefore important that resources be provided for training and education programmes for members of staff who are directly or indirectly involved in the use of the electronic signature technology. If the prevailing ignorance, lack of understanding and confusion about the new technology can be addressed, businesses will realise that electronic signatures, in particular digital signatures, can be a secure alternative to manuscript signatures for conducting on-line contracts and commercial transactions. In this respect, the Australian Government Information Management Office (AGIMO) that overlooks the Gatekeeper (which provides accreditation to certification authorities (CAs) to issue digital signature certificates) can play an important role. Other bodies such as the Law Council of Australia (LCA), the Australian Corporate Lawyers Association (ACLA) and the Australian Computer Society (ACS) can also collaborate to promote the use of the technology given its techno-legal nature.

Security concerns were identified as another significant barrier to the use of electronic signatures. In particular, businesses raised concerns with regard to their storage. If electronic signatures are stored properly, their misuse can be minimised. However, participants' views indicated that despite password security policies implemented by their organisation's IT team, staff would not abide by them. Such lackadaisical attitudes towards the use of passwords are in conformity with various studies and surveys that have investigated password security.[58] Such weak passwords can be effortlessly obtained either through the help of social engineering[59] or obtained with the use of software.[60]

On the other hand, replacing passwords with biometric measurements can be a secure option, but is not necessarily a perfect alternative. A computer with an electronic signature stored on its hard disk would most likely be connected at some stage or the other to the internet or an intranet, or both. With the use of either intranet or the internet, there are high risks of remote attacks within an organisation or from a hacker sitting thousands of miles away. Remote attacks can bypass

[54] *P15_C010_Legal, Paragraph 141.*
[55] *P18_C011_Legal, Paragraph 120.*
[56] *P2_C02_Legal, Paragraph 27.*
[57] *P18_C011_Legal, Paragraph 133.*
[58] *Ernst & Young, Global Information Security Survey 2006 at http://www.ey.com/; Steven Furnell, 'Authenticating Ourselves: Will We Ever Escape the Password?' (2005) 3 Network Security 8, 9; Stephen Mason, Electronic signatures in Law, 10.36.*
[59] *For more details on social engineering and password security see Michael E. Whitman, Herbert J. Mattord, Management of Information Security (Course Technology, 2004).*
[60] *Joseph A. Cazier and B. Dawn Medlin 'Password Security: An Empirical Investigation into E-Commerce Passwords and their Crack Times' (2006) 15(6) Information Systems Security 45, 47.*

operating systems security, thereby making any desktop security measures such as biometric measurements, including passwords, redundant.[61] In order to protect electronic signatures from risks associated with the internet or intranet, a possible option is to store them on secure PISDs.[62]

Among all forms of PISD, smart cards appear to be the most secure.[63] However, most participants demonstrated very little understanding of smart cards, particularly the technology associated with them. They were often wrongly believed to be embedded with the magnetic stripe technology, as are most bank credit cards in Australia. Educating the business sector about the technology underlying smart cards might overcome the prevailing ignorance and misunderstanding.[64] To address this issue, the use of biometric measurements may be considered as an alternative to passwords for securing smart cards. While the body is capable of providing several types of biometric measurement, the use of fingerprint has proved itself to be the most suitable technology to date from a security and usability aspect.[65] Thus, it is possible to achieve a higher degree of security by storing a biometric measurement of a fingerprint on the same card that stores a digital signature. A link can be made between the person whose private key is stored on the card and the identity of the person in possession of the card. If such a comprehensive security infrastructure is adopted, digital signatures are protected from malicious acts to the degree that the technology can be considered to be reasonably secure.[66]

Concerns regarding the admissibility of electronic signatures and the evidentiary issues appeared to be another important impediment to the use of electronic signatures in the Australian business community. On the one hand, participants revealed significant ignorance with respect to the law governing electronic signatures in Australia, in particular, the ETA and the law of evidence. The knowledge of lawyers and legal advisors' in this area did not appear to be up-to-date. On the other hand, participants raised some valid arguments with regard to evidentiary matters.

Admissibility concerns raised by participants were in general futile. Both the ETA and the Evidence Act 1995 (Cth) provide rules and guidelines that can be used to prove an electronic signature.[67] Participants' concerns regarding this issue are therefore not exactly tenable. They are mostly characterised by an ignorance of the law underlying electronic signatures. It is arguable that separate provisions on admissibility of electronic signatures in evidence in the ETA would provide more clarity on evidentiary matters related to electronic signatures. On this note, it is useful to point out that the Electronic Communications Act 2000 from the UK, explicitly states that electronic signatures are admissible in evidence in any legal proceedings.[68] The UK Act thus provides a useful model for Australia.

With regard to evidentiary issues, participants expressed concerns about the inconclusiveness of an electronic signature, claiming that there is no actual or original document that is signed. In their contention, the law of evidence would struggle to deal with electronic signatures, because there is an absence of primary evidence.[69] Such views appear to be based on a

[61] *For example, software such as Inspector Copier can remotely back up data from the individual's computer by bypassing the operating system protections.*

[62] *It is possible that electronic signatures stored on a smart card may be susceptible to risks from the internet. This could happen during the process of signing a document, because the smart card is connected to the computer that is in turn connected to the intranet or internet. During this period, a remote attack is possible on the electronic signature. However, since the smart card is in contact with the intranet or internet for only a very short period, this threat is minimal as compared to when electronic signatures are stored on a computer's hard disk which is often connected permanently to the internet or intranet. However, the Network Smart Card can overcome this problem to a considerable extent. See Hong Qian Karen Lu, 'Network smart card review and analysis' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007), 2234-2248 and Joaquin Torres, Antonio Izquierdo and Jose Maria Sierra, 'Advances in network smart cards authentication' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007), 2249-2261.*

[63] *In the past few years smart cards have become more powerful and secure, for which see Bart Preneel, 'A Survey of Recent Developments in Cryptographic Algorithms for Smart Cards' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007) 2223-2233 and Joaquin Torres, Antonio Izquierdo and Jose Maria Sierra, 'Advances in network smart cards authentication' International Journal of Computer and Telecommunications Networking.*

[64] *Note the former federal government was planning to introduce the national identity card that would have used the smart card technology. The intention was to replace a number of existing cards, including the Medicare card and various benefit cards issued by Centrelink and the Department of Veterans' Affairs with the ID card. Had this project been implemented, it would have probably helped users to become familiar with the smart card technology given the broad-based use of Medicare and Centrelink cards. For issues related to such cards see Graham Greenleaf, 'Function Creep – Defined and Still Dangerous in Australia's Revised ID Card Bill' Computer Law & Security Report, Volume 24, Issue 1, 2008, 56-65; Graham Greenleaf, 'Australia's Proposed ID Card: Still Quacking like a Duck' Computer Law & Security Report Volume 23, Issue 2, 2007, 156-166; Margaret Jackson and Julian Ligertwood, 'Identity Management: Is an Identity Card the Solution for Australia?' Prometheus Vol. 24, No. 4. (2006), 379-387.*

[65] *Paul Reid, Biometrics for Network Security (Prentice Hall, 2004) 10.*

[66] *With advances in the smart card technology, it is now possible to have a fingerprint sensor on the smart card itself instead of the computer: 'A standards-based biometric smart card – at what cost?' Biometric Technology Today, Volume 16, Issue 1, January 2008, 3-4; Denis Praca and Claude Barral, 'From smart cards to smart objects: the road to new smart technologies' Computer Networks Volume 36, Number 4, 16 July 2001, 381-389.*

[67] *Sections 8, 9, 10, 11, 12 of the ETA and s 3, 48, 146 of the Evidence Act 1995 (Cth).*

[68] *Electronic Communications Act 2000 (UK) s 7(1).*

[69] *For a discussion on primary and secondary evidence in the context of electronic signatures, see Stephen Mason, Electronic Signatures in Law, 14.10.*

In any event, notaries across the world have taken practical steps to develop techniques to provide for the witnessing the signing of a digital document on a computer with an electronic signature by both the signing party and the notary.

misunderstanding of the current law of evidence. Although the common law position enunciated over 250 years ago was that the best evidence rule[70] (which includes producing original documents containing signatures) should be followed to determine the existence of a signature, this law no longer prevails in the Australian federal and in several state jurisdictions.[71] Because s 51 of the Evidence Act 1995 (Cth) has abolished the common law principles of the best evidence rule for proving a document's contents, the production of an original document is no longer a mandatory requirement to prove a fact. Thus, participants' concerns with regard to the absence of original documents with electronic signatures are unfounded and emanate from their lack of awareness of the current legal position in this regard.

With regard to witnessing the application of a signature, participants feared that unlike manuscript signatures, it is not possible to witness a person affix an electronic signature to a document.[72] Witnessing in the electronic realm has also been described as a complex issue by a few scholars.[73] However, they do not rule out the possibility of witnessing an electronic signature, in particular, digital signatures. Witnesses can use their digital signature to attest an electronically signed document. The witnessing of such documents would require that computers involved in signing the document be technically evaluated to trusted evaluation criteria.[74] In such an environment, the attester would verify the authenticity of the document through the signer's public key and would in turn witness the signatory's signature using his digital signature.[75] In any event, notaries across the world have taken practical steps to develop techniques to provide for the witnessing the signing of a digital document on a computer with an electronic signature by both the signing party and the notary.[76]

The issue of witnessing has been explicitly provided for in a few jurisdictions' legislation. For example, the Electronic Commerce Act 2000 passed in Ireland, provides that electronic signatures can be witnessed electronically provided certain requirements are satisfied. In particular, the main document must specify that it requires witnessing, and the signature of the signatory and the witness must be an advanced electronic signature (that is, a digital signature) based on a qualified certificate.[77] The Electronic Transactions Act 2002 in New Zealand also makes explicit provisions for the witnessing of electronic signatures.[78] A similar provision if inserted in the ETA will eliminate the

[70] *The best evidence rule can be traced back to more than 250 years to the case of Omychund v Barker (1745) 26 ER 15, 33. Lord Harwicke in the case stated that for evidence to be admissible it must be 'the best that the nature of the case will allow'. In other words the contents of a document are only admissible if the party attempting to adduce evidence of the contents is able to tender the original document. Traditionally, this rule has operated to eliminate evidence which has not been the best evidence, such as a copy of a document. This was basically the issue raised by participants when they expressed concerns about the original and copy of a signature. For a detailed understanding of the best evidence rule see Edward W Cleary and John W Strong, 'The Best Evidence Rule: An Evaluation in Context' (1965) 51 Iowa Law Review 825.*

[71] *The States and Territories in which the best evidence rule has been abolished are New South Wales, Victoria, Australian Capital Territory and Tasmania. Note that these States and Territories mirror the Evidence Act 1995 (Cth). See ss 48 and 51 of the Evidence Act 1995 (Cth). The States and Territories in which the best evidence rule are still active are South Australia, Western Australia, Northern Territory and Queensland.*

[72] *Although see the US case of an electronic will, Taylor v Holt CA Tennessee Knoxville 18 August 2003, where the electronic signature of the testator was witnessed by the witnesses, who in turn added their electronic signatures to the document; discussed in Stephen Mason, Electronic Signatures in Law, 10.16.*

[73] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future' (1998) 21(2) University of New South Wales Law Journal 452, 462.*

[74] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future'. A lack of trusted systems may bring into question the legal validity and certainty of such actions.*

[75] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future'.*

[76] *By way of introduction, see the work of the Hague Conference on Private International Law and the e-APP (Electronic Apostille Pilot Program) http://www.e-app.info/.*

[77] *Electronic Commerce Act 2000 (Ireland) s 14.*

[78] *Section 23 of the Electronic Transactions Act 2002 (NZ) specifically entails provisions for witnesses to witness a document using an electronic signature, if: (a) where a signature is being witnessed, that signature is also an electronic signature; and (b) the electronic signature of the witness meets requirements that correspond to those for a primary signature – that is, the electronic signature adequately identifies the witness and adequately indicates that the signature or seal has been witnessed; is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature of the witness is required; and, in the case of a witness's signature on information required to be given to a person, the recipient of the information has consented to the use of an electronic signature rather than a traditional paper-based signature.*

concerns of the Australian business community that electronic signatures and documents cannot be witnessed.

Electronic signatures were also subject to disapproval because they cannot undergo handwriting tests. Participants claimed that unlike manuscript signatures which can be verified using handwriting tests,[79] identifying the actual signatory becomes harder when an electronic signature is used. However, there are other ways of testing whether an electronic signature is genuine and authorized. The operations of the information system from which the signature originated at the time when the signature was created can be used to prove the genuineness of a signature.[80] Further, intrusion detection systems may be used to establish whether the document was signed maliciously by an intruder.[81] This may however require a high standard of information security systems. Nevertheless, this may not necessarily be a foolproof means to identify the actual signatory. In the case of electronic signatures, the identity of the actual signatory will be a matter of inference. Inference may be weak in those cases where the holder of the private keeps his key in a computing platform that cannot be trusted, such as an office or home computer.[82] The inference may be stronger in those cases where better evidence of a signer's identity has been provided through a biometric measurement and a PISD or both.[83]

Some participants claimed that businesses would willingly switch over from the practice of manuscript signature to electronic signatures for endorsing contracts and documents if they received adequate legal advice. Providing adequate legal advice is, however, quite challenging for legal advisors if there are fundamental drawbacks in the electronic signature legislation. A major shortcoming of the ETA is that it does not provide the definition of an electronic signature.[84] This can be rectified if the Act is amended to incorporate the definition of electronic signature and digital signature. Other countries such as Hong Kong have already implemented such changes in their legislation.[85] Similar amendments in the ETA will help the Australian business community and other people that use electronic signatures every day (the PIN on a bank or credit card, the signature at the bottom of an e-mail) understand what an electronic signature represents. Clarity in the legislation is in turn likely to enhance businesses' confidence towards the use of the technology.

Furthermore, section 10 of the ETA (based on article 7 of the MLEC) that deals with the use of signatures in the electronic environment, recognises the validity of electronic signatures under certain terms and conditions without describing what an electronic signature is. In particular, it states that where a Commonwealth law imposes the completion of a transaction through the means of a signature, the use of any method (presumably electronic signature) is valid, provided the method satisfies the following four criteria:

> it identifies the person who made the signature;
> it indicates the person's approval to the contents of the document signed;
> it is as reliable as is appropriate for the purpose for which it is used; and
> the recipient has agreed to the usage of that method.[86]

Clearly, this section is vague and ambiguous, making it difficult to attribute a precise meaning to its provisions, and is the subject of criticism from scholars eminent in the field of electronic signatures. McCullagh and Caelli condemned the legislation on the ground that it does not provide 'any guidance as to what within the electronic commerce environment is or is not a valid electronic signature'.[87] According to Christensen and Low, that 'the method must be as reliable as is appropriate for the purpose for which the information was communicated'[88] is nothing but confusing.[89] What is considered appropriate in the circumstances, argued

[79] *Generally two main aspects of a signature are considered: pictorial representation and the construction of letters. It is common for forgers to focus on pictorial details such as slope, size and spacing but they often fail to copy the way the letters are constructed, such as the direction of the letters. In addition, the signature is also verified on the basis of the attributes of the instrument used to affix the signature such as how smooth the signature has been signed and whether it is jagged or confident. See Stephen Mason, Electronic Signatures in Law, 1.17.*

[80] *Lorna Brazell, Electronic Signatures Law and Regulation (Sweet & Maxwell, 2004), 8-014.*

[81] *Lorna Brazell, Electronic Signatures Law and Regulation, 8-014. Note intrusion detection systems can only detect intrusions but cannot prevent them.*

[82] *Mark Sneddon, Legal Liability and E-Transactions: A Scoping Study for the National Electronic Authentication Council (2000) 3.2, available at http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf.*

[83] *Mark Sneddon, Legal Liability and E-Transactions: A Scoping Study for the National Electronic Authentication Council (2000).*

[84] *Fitzgerald and others argue that ETA is a light-touch legislation because it does not define the electronic signature: Anne Fitzgerald, Timothy Beale, Yee Fen Lim and Gaye Middleton, Internet and E-Commerce Law, (Lawbook Co., 2007) 552.*

[85] *Electronic Transactions (Amendment) Ordinance 2004 (HK).*

[86] *ETA s 10. Note the clause 'the recipient has agreed to the usage of that method' is an extra provision in the ETA as compared to the MLEC.*

[87] *Adrian McCullagh and William J Caelli, 'Non-repudiation in the Digital Environment' (2000) 5(8) First Monday http://firstmonday.org/issues/issue5_8/mccullagh/index.html.*

[88] *ETA s 10.*

[89] *Sharon A Christensen, William Duncan and Rouhshi Low, 'The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures' (2003) 10(4) Murdoch University Electronic Journal of Law http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html.*

Christensen and Low, could be based on the parties' personal preferences and a court's ex-post facto rationalisation of individual approaches, and therefore could vary greatly with no consistent pattern.[90] For example, the appropriateness of an electronic signature may not be the same for a day-to-day ordinary transaction as for complex business transactions involving large sums of money.

In the same vein, Mason argued that the reliability test is unrealistic. According to him, if the parties to a contract have agreed in good faith on a particular technology and have acknowledged that the contract is authentic and valid, the court should not question its authenticity and validity on the grounds of reliability. 'There should be no need for any court to take the matter any further,' remarked Mason.[91]

The lack of clarity in the provisions relating to signatures in the electronic environment is a major drawback in the ETA and other jurisdictions whose electronic transactions laws are based on the MLEC. It would indeed be hard for legal advisors to advise businesses to use electronic signatures with such loose, imprecise and ambiguous provisions in the laws. Note that post MLEC, two other set of laws, the Model Law on Electronic Signatures 2001 (MLES) and the Convention, have been drafted by the UNCITRAL that address the drawbacks in the initial model law but to date the ETA has not been amended accordingly.

The complexity of the electronic signature, in particular digital signature, was regarded as another hindrance to the use of electronic signatures by participants. However, the complexity of the technology can also optimistically be regarded as an attribute. Seen from a different perspective, due to its complex nature, digital signatures can only be used by authorized people who have acquired an expertise or training in this respect. Thus, the complexity of the technology can potentially enhance its security by restricting its use.[92]

It appears that much of businesses' confusion with electronic signatures arises from an ignorance or lack of understanding of the technology. The electronic signature technology, in particular digital signatures, is not necessarily as complex as it is perceived. This perceived complexity is often the result of poor understanding and lack of information.

Economically, the expense involved in educating and training staff was identified as an important deterrent towards the use of digital signatures by participants. However, businesses may reconsider that the use of digital signatures may justify the expenses involved in their use, because of the slightly greater security. Although in the short run they may incur certain expense in terms of training and educating their staff, the long run it is possible that the gains might outweigh the expenses.

Conclusion

This article identifies the potential reasons underlying Australian businesses' hesitance to use electronic signatures, in particular digital signatures, for contracts and commercial transactions in a fast developing and regulated e-environment. It also provides some useful suggestions to overcome the low use of the technology in the business community. While legislative and technological shortcomings are identified as being important factors that can make businesses hesitant to adopt electronic signatures, the perception of people in business are often not supported by reference to the actual legislation or to the technology underlying electronic signatures. Rather, there is significant evidence of Australian businesses' lack of awareness and understanding of electronic signatures and the associated legislation, despite a regulatory framework to facilitate their use. It is unlikely that any perfection of either electronic signature technology or the legal environment for electronic signatures will see a greater use by the business community of such signatures until knowledge of these things becomes more pervasive.

Dr. Aashish Srivastava is in the Department of Business Law and Taxation, Monash University, Australia. His doctoral thesis comprised an empirical research on the lack of acceptance of electronic signatures by the Australian business community. His research interests include legal issues in electronic signatures, e-government, internet security and cyber crimes.

aashish.srivastava@buseco.monash.edu.au

[90] *Sharon A Christensen, William Duncan and Rouhshi Low, ' The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures'.*

[91] *Mason's argument is in the context of article 7 of the Model Law on Electronic Commerce 1996, which can also be applied to ETA because s 10 of the ETA is a replication of article 7 of the model law. Stephen Mason, Electronic Signatures in Law, 3.18.*

[92] *Some commentators consider digital signatures to be the most secure form of electronic signature, although a number of companies in Russia bear witness to having large sums of money removed from their bank accounts by an unknown unauthorized third party, who obtained the private key of the company, and then initiated the transfer of the money without the authority or knowledge of the company, for which see Olga I. Kudryavtseva, ' The use of electronic digital signatures in banking relationships in the Russian Federation' , Digital Evidence and Electronic Signature Law Review, 5 (2008) 51 – 57 and Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П, Digital Evidence and Electronic Signature Law Review, 5 (2008) 149 – 151.*

ARTICLE:

CIVIL LAW LIABILITY FOR UNAUTHORIZED WITHDRAWALS AT ATMs IN GERMANY

By **Assistant Professor DDr. Gerwin Haybäck**

The liability for unauthorized withdrawals at automatic teller machines (German: Geldautomat; Austria: Bankomat) (ATMs) and point of sale terminals (POS) is caused by the manipulations of unauthorized third parties, sometimes because of the incautious behaviour of the cardholder, where the loss of a card is exacerbated as a result of the PIN being recorded with the card in some way. The bank may also refrain from taking precautions, such as providing an effective shield to terminals, refusing to record a transaction with the use of video or CCTV,[1] and failing to provide for increased program code and internet safety. The aim of this article is to discuss what can be considered a fair allocation of risks. It deals with system security and different methods exercised by criminals in order to detect the personal identification number (PIN). The prima facie evidence granted in favour of the bank is a controversial issue discussed in relation to substantive law and case law.[2]

Introduction

The first time a card holder may become aware that an unauthorized transaction might have occurred at an ATM or POS, is when they notice an unknown debit posting on their current account.[3] Accordingly, the card holder will probably inform the card issuer that the posting is an unknown withdrawal against their account, and the debit should be refunded.

The card issuing bank, on the other hand, will probably respond by pointing out that only the card holder knew the PIN, which can be four numbers (as in the UK for instance) or four or five numbers (as in Germany for instance). This means it is assumed that the card holder has complete control over the card (also known as bank card, payment card, bank customer card, debit card). The card issuer may well reach the conclusion that either the card holder must have withdrawn the respective amount at the ATM, or they authorized a third person so to do, or they were so negligent as to permit an unauthorized third person to obtain possession of the card and PIN. Where the card holder loses control over their PIN or card, or both PIN and card, it may be that third persons have obtained the card and discovered the PIN, then they attempt to remove as much cash as possible before the card is retained. Whatever happens, the law of evidence and how the pleading are drawn up will be of great importance in establishing which party is put to proof to prove their case.

Occasionally, a criminal will obtain possession of several charge or credit cards, and within a short period of time, the maximum amount is removed because the criminals know that the card is blocked only after two (or more) hours.[4] The card issuer notices the theft only after some time.[5] Consequently, the ATM card is frequently blocked too late. Therefore, it is important to establish

[1] *Although a video recording of a transaction does not prove anything if the ATM clock and video clock are not synchronized, for which see a murder case where the wrong people were arrested in the USA in Stephen Mason, editor, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 3.20-3.22.*

[2] *Prima facie evidence in Germany is similar to a presumption in English jurisprudence.*

[3] *See in detail Gerwin Haybäck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich (Neuer Wissenschaftlicher Verlag GmbH Nfg KG, 2008), 45 and following.*

[4] *See the report: 'Bankomat: Kartensperre schützt nicht' ('ATM: Card blocking does not protect'), available at: http://www.klartext.at/downloads/presse/bankomat kartensperre nuetzt nicht.PDF.*

[5] *Note by editor: card issuers purport to have mechanisms in place to detect fraud of this nature, so if a card issuer fails to implement the mechanism where large amounts are removed from an account that is not within the normal spending patter of the card holder, the fault may be with the card issuer, not the card holder. Fraud detection is a pattern recognition problem and it can be carried out either using expert systems where people write the rules, or training a system by providing data, and for it to establish the rules. However, detecting fraud is far more complex. It is necessary to consider what types of fraud are known, then to be alert to a change in fraud patterns that avoid the previous patterns, then when new patterns are detected, the new patterns must be countered. It is necessary to understand that in attempting to detect fraud, the early cases of a new type of fraud may not be detected for some time. A significant problem when dealing with allegations that a customer is responsible for a withdrawal from an ATM, is that nobody in this field will explain what they are looking for, or publishes any analysis on how good they might be at identifying patterns of fraud.*

criteria for the distribution of risks and charges between the contracting parties. The allocation of risks concerning the damages caused by third parties is of importance, especially if the offender is unknown or has no assets when caught and successfully prosecuted. On the one hand the card holder is obliged to use the two components (card and PIN) together. On the other hand, the card holder always has to keep the two components strictly separated for security reasons. The most frequent attacks are to manipulate an ATM, or to create a cloned card. Occasionally, criminal energy focuses upon discovering secret numbers.

Concerning the substantive law of contract, it is necessary to determine the duties of care the card holder is required to comply with. Second, consideration must be given to the standard of care and security that should be the responsibility of the credit services sector. This article primarily deals with the security of the PIN system. In addition, the question of liability concerning the PIN (as the present electronic instrument of identification) is discussed. The analysis deals with the liability for damages in civil law, not criminal law.

Liability and the German EC system

The German EC ATM system is a participant of the European Europay ATM system and the Global Maestro system.[6] There arrangements permit transnational withdrawals at ATMs and POS payments for goods and services. When the EC card (including the Maestro logo as well as the electronic cash logo) is used at an ATM, a legal transaction takes place within the single mandate between the card holder and the card issuer. In accordance with section 665 of the German Civil Code (Bürgerliches Gesetzbuch), these mandates comply with the authority to make a payment from the account of the card holder:

> § 665 Abweichung von Weisungen
>
> Der Beauftragte ist berechtigt, von den Weisungen des Auftraggebers abzuweichen, wenn er den Umständen nach annehmen darf, dass der Auftraggeber bei Kenntnis der Sachlage die Abweichung billigen würde. Der Beauftragte hat vor der Abweichung dem Auftraggeber Anzeige zu machen und dessen Entschließung abzuwarten, wenn nicht mit dem Aufschub Gefahr verbunden ist.
>
> Section 6654[7]
>
> Deviation from instructions
>
> The mandatary is entitled to deviate from the instructions of the mandator if he may assume in the circumstances that the mandator would approve of such deviation if he were aware of the factual situation. The mandatary must make notification to the mandator prior to such deviation and must wait for the decision of the latter unless postponement entails danger.

The EC card is a payment (debit) card, in accordance with the provisions of section 676h of the German Civil Code. Subsequently, the card issuing bank is entitled to demand reimbursement of expenses for use of a payment card only where it was not abused by a third party. Apart from the possibility of excluding claims for expenses, there still remain the card issuer's claims for damages against the card holder, in accordance with the general regulations (sections 280 and 281 of the German Civil Code).

Risks associated with the PIN

Methods to detect the PIN

As the result of the experience with ATM systems at the time of writing,[8] it is known that taking cash out of a bank account at ATMs is much safer than relying on the cheque guarantee card system.[9] Experienced criminals can forge a signature in such a way that the average recipient of a cheque cannot discover the deception.[10]

An unauthorized withdrawal using the correct PIN is a forgery, although it follows that the PIN itself can be only correct or incorrect. Card issuers fail to understand this logic, and therefore it is incorrectly assumed that

[6] *The agreement was concluded between the Federal Association of the German Volksbanken and Raiffeisenbanken, the Federal Association of the German Banks, the German Sparkassen- and Giroverband as well as the Federal Association of Public Banks of Germany (all of them incorporated societies), in force from 1 December 2003; see Karsten Schmidt, Zu E. Bankkartenverfahren; 1. Vereinbarung über das deutsche ec-Geldautomatensystem, in: Münchener Kommentar zum HGB (Handelsgesetzbuch is the Commercial Code), 2nd edition, (beck on-line, 2009).*

[7] *Translation taken from http://bundesrecht.juris.de/englisch_bgb/index.html.*

[8] *The history of the eurocheque system is covered in Ewald Judt and Alfred Scholz, 35 Jahre Geldausgabeautomat – 20 Jahre Bankomat in Österreich, ÖBA (2000) 839.*

[9] *For contributions that deal with the advantages and disadvantages of the eurocheque system, see Ewald Judt, Der eurocheque: 1968 – 2001 – ein Nachtrag, ÖBA (2003) 136; fundamentally Gerwin Haybäck, Zur Risikoverteilung bei Euroscheckfälschung, ÖBA (1997) 251.*

[10] *Michael Bucher, Die Risikoverteilung bei der Benutzung elektronischer kartengesteuerter Zahlungssysteme, (P. Lang, 1992), 180; Günter H. Roth, Grundriß des österreichischen Wertpapierrechts, Wien: Manz, 2nd edition (1999) 85 and following: checking the signature on forged EC cheques.*

Where a third person obtains the PIN, it is assumed that the card holder has been engaged in careless behaviour, despite the ease by which a PIN can be obtained by a third person.

the card holder has a duty of care to prevent the passing of the PIN to third persons. Where a third person obtains the PIN, it is assumed that the card holder has been engaged in careless behaviour, despite the ease by which a PIN can be obtained by a third person. The PIN is the most important identifier of the (authorized) card holder at ATMs and POS terminals. Card holders are contractually bound to keep the PIN safe, and are not entitled to inform anybody voluntarily of the PIN.[11] This requires a discussion as to how a third person is able to detect the correct PIN. The three most frequent causes are breach of secrecy, spying to obtain the PIN, and guessing the PIN.

Breach of secrecy

The card holder has a contractual duty to take care of their card and PIN. The issue is to establish what those duties might be. Both the prevailing opinion as well as the conditions for the use of the Maestro Card oblige the card holder to keep his PIN confidential and never pass the PIN to others.[12] In particular, the PIN must not be noted on the card or otherwise stored together with it, even in an altered form.[13] Should the card holder keep the Maestro card and code close together, they undermine an important component of the Maestro safety system.[14]

In 1999, it was held by the Local Court in Hamburg that keeping the EC card in the hip pocket of a pair of trousers (without carrying the secret number) was not regarded a grossly negligent violation of the duty to care.[15] 'Saving the EC components separately'[16] means keeping them in different boxes, pieces of furniture and locked drawers,[17] or in different pockets of items of clothing.[18]

The Local Court in Kassel has determined that it is extremely careless behaviour to keep a note of the PIN in an address book together with the ATM card.[19] Such behaviour is in conflict with the strict duty of secrecy stipulated in the conditions for the use of the Maestro Card, in accordance with the prevailing case law. This method of concealing the PIN is well-known by criminals.[20] However, in the opinion of Professor Udo Reifner, such behaviour cannot be considered unreasonable. It is usual for a person to make a permanent record of the PIN for the purposes of an aid to memory. Further, he also approves the transmission of the PIN to persons of trust.[21]

Nevertheless, if the card holder fails to notice the loss of an ATM card by taking money out or placing money, account statements, and the ATM card carelessly into the pocket of a coat or jacket, such behaviour is considered as grossly negligent, in accordance with a decision by the District Court at Halle.[22]

The requirement of isolating the card in a safe is out of touch with everyday life. On the one hand, the card holder acts grossly negligently if he is absent for three or four hours while leaving the card and the PIN on the

[11] *In contrast, concerning to the duty of secrecy, the card holder only has to afford a reasonable, i.e. conventional duty of care (in German: 'zumutbar', what can be expected of an average card holder). Full particulars are discussed by Stefan Werner in Thorwald Hellner and Stephan Steuer (editors), Bankrecht und Bankpraxis, (2008) Rz 6/1463.*

[12] *Although informing others of the PIN seems to be practiced in particular between family members, nevertheless the prevailing opinion is strictly against any transfer of the PIN, for which see Franz Häuser and Lutz Haertlein, E. Bankkartenverfahren, in Münchener Kommentar zum HGB, 2nd edition, (beck on-line 2009) Rn E 33 and following; likewise Ernst Heymann, Norbert Horn, and Peter Balzer, Handelsgesetzbuch (Commercial Code), 2nd edition, (2005) section 372 annex; Adolf Baumbach, Wolfgang Hefermehl, and Matthias Casper, Wechselgesetz, Scheckgesetz, Recht der kartengestützten Zahlungen, 23rd edition (2008) Rn 36; Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1264, 1269; Viola Russenschuck, Die Auszahlung von Bargeld an Automaten nach deutschem Zivilrecht (2002) 75 and following; for dissenting views, see Christian Hofmann, Schadensverteilung bei Missbrauch der ec-Karte, WM (2005) 441, 444 and Professor Dr. Udo Reifner, Die Haftung des Kontoinhabers bei Missbrauch seiner Bankomatkarte durch Dritte, BB 1912, 1918.*

[13] *Stefan Werner, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen PIN, BKR (2004) 50.*

[14] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1264, 1269.*

[15] *Local Court Hamburg, VuR (1999) 88.*

[16] *BGH WM (2000) 2421, 2422.*

[17] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269, referring to District Court Essen, WM (1988) 493 and District Court Hanau, ZIP (1995) 559.*

[18] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269, referring to Local Court Hannover WM (1996) 2013.*

[19] *Local Court Kassel, I D 5. b – 1. 95 WuB, Pfeiffer.*

[20] *Local Court Kassel, WM (1994) 2110; see Stefan Werner in: Thorwald Hellner and Stephan Steuer (editors), Bankrecht und Bankpraxis, (2008) Rz 6/1470; Horst Ahlers, Die neuen Bedingungen für ec-Karten, WM (1995) 601, 607; dissenting Hartmut Strube, Haftungsrisiken der ec-Karte, WM (1998) 1210 and following.*

[21] *Professor Dr. Udo Reifner, Die Haftung des Kontoinhabers bei Missbrauch seiner Bankomatkarte durch Dritte, BB (1989) 1912 and following.*

[22] *District Court Halle, WM (2001) 1298.*

In order to provide for the safety of the maestro system, the credit services sector promotes the physical shielding of the front of ATMs, as well as a nationwide development of video control at each ATM.

desk in his flat,[23] or if he keeps both components in a folder.[24] However, the card holder is entitled to physically carry the card as well as the PIN. On the other hand, the PIN must not be written down on the card or otherwise stored together, to avoid a thief obtaining the PIN if the card is stolen.

In what is known at the 'Hospital case', the court made high demands on the safe keeping of the card and PIN. It was determined that keeping the card with the PIN (camouflaged as a four-digit telephone number) was a grossly negligent contributory cause that allowed a third party to obtain unauthorized access to the account. The card holder was not exculpated by putting both components (card and code) into a solid strong box in a locked sick room. It is a matter of fact that a hospital is considered an unsafe location where the theft of such items cannot be excluded.[25]

The cumulative effect of judicial pronouncements indicates that it is necessary to keep the components (card and PIN) strictly separated, even in private rooms. According to a recent judgement of the Federal Court of Justice of Germany (Bundesgerichtshof, BGH), the customer does not act grossly negligent if they keep the card and PIN in different rooms of a flat, and, as a result, unauthorized, abusive withdrawals follow.[26] Within the domestic arrangements of a family home, it is not necessary to take measures against theft between family members where the relationships between family members are in good order, and if the card issuer does not request special protective measures to be put in place caused by any specific circumstances the family might find themselves in. Examples where the card issuer might consider that there are special circumstances that require additional consideration for security are flat-sharing communities or residential homes where family members are not present.

In a recent judgment of the Higher Regional Court of Düsseldorf, it is considered to be grossly negligent if a purse containing the card is placed in a shopping trolley in a department store.[27]

Observing the PIN by third parties

It is possible to differentiate between active and passive observation of the PIN.[28] The most common method is passive observation, such as looking over someone's shoulder, especially at ATMs in busy places or at POS terminals in supermarkets. Criminals will go to the length of renting flats across from ATMs for this purpose. Thus, they take possession of different PINs by using binoculars, telephoto lens, mini-spy-cameras, or by transmitting the PIN to an external personal computer where the ATM has been manipulated by the criminal to obtain the PIN when the PIN is entered into the ATM.

In order to provide for the safety of the maestro system, the credit services sector promotes the physical shielding of the front of ATMs, as well as a nationwide development of video control at each ATM.[29] On the other hand, the card holder is obliged to take reasonable precautions. If the card holder takes cash out of the bank account at ATMs, or makes payments at POS terminals, they have to stay away from the next customer, protect the number pad, and such like.[30]

It is possible to fabricate a clone of the card and take cash out of the victim's bank account at an ATM in a foreign country if a criminal obtains sufficient information from the card and knows the correct PIN.

[23] *District Court Frankfurt 1. December 1992, 2/13 ol 98/92.*
[24] *Higher Regional Court of Nürnberg WM (1989) 405; Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz 6/1470.*
[25] *District Court Bonn, NJW-RR (2000) 1415.*
[26] *Federal Court of Justice of Germany, NJW (2001) 286.*
[27] *Higher Regional Court of Düsseldorf, BKR (2008) 41.*
[28] *Professor Dr. Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR (1997) 121, 124; Professor Dr. Manfred Pausch, Die Sicherheit von Magnetstreifenkarten im automatisierten Zahlungsverkehr, CR (1997) 174.*
[29] *Various authors demand an obligation of the banks to provide an area-wide video control of ATMs, see Professor Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR 1997, 121 (123); Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz &/1481.*
[30] *Professor Dr. Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR (1997) 124; Werner Schindler, Die neuen PIN-Nummern der ec-Karten, NJW-CoR (1998) 223, 226; Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz 6/1469.*

The information, but not the PIN, can be obtained from the magnetic stripe on the reverse of the card. From 1982 on in Germany, detectors for an anti-fraud feature known as the Moduliertes Merkmal (MM code) began to be installed in ATMs, in order to provide protection from cloned cards.[31] The MM code consists of two components, one stored on the magnetic stripe, and one hidden within the material of the card. The MM code is verified by the ATM with a cryptographic operation that is performed to check that the component of the MM code on the magnetic stripe corresponds to the one hidden on the card. The correct hidden component of the MM code cannot be calculated from the information recorded on the magnetic stripe alone. It is also necessary to have a cryptographic key, which is stored in the MM code detection unit. ATMs in Germany include a special MM detection unit and sensor to read and verify the MM code, although cash machine manufacturers are not permitted to obtain access to or service the unit.

The prevailing case law indicates that it is considered as grossly negligent behaviour where the customer fails to realize the loss of the card by taking money out, then putting the money, account statements, and card into a coat pocket. The same consequences apply where the customer does not protect the number pad.[32] Generally, the card holder has to take reasonable care. The mere fact that the offender knew about the PIN is not sufficient to prove the card holder's breach of his duty to care.[33] In other reported cases, the chance of observing a different secret number is mentioned, but was excluded in the case under consideration.[34] On one occasion, the District Court in Berlin formally criticized the lack of safety screening devices. In this case, the criminals had detected the secret number and thereupon pursued the card holder through Berlin. In the view of the court, the card holder is not at fault if she does not pay attention to people around during the time it takes to make the withdrawal.[35]

To this end, Dr. Tilman Hoppe proposes the following: 'First of all, the banks as well as the participants of the POS system are requested to redesign the conditions in such a way that is not possible to spy out the PIN. Especially, the screen of the key pad at POS terminals in trade seems inadequate in case of large crowds. It should be taken into consideration whether the identification of the customer is carried out as it is the case with the POZ system.'[36] Hoppe draws the conclusion that the bank is obliged to prove that the respective ATM is not protected at best. Measures of improving the shield of the number pad are required, especially in superstores.[37]

It is debatable whether Hoppe's proposal is acceptable: 'to deliberate about whether in trade the identification of the customer should take place as it is the case with the POZ system.'[38] This comment is in conflict with a long experience in providing for the security for withdrawals at ATMs in comparison with those of the eurocheque system. With good cause, the eurocheque as well as the (former) POZ system were suspended (in 2001, respectively in 2007), because it was easy to forge the manuscript signature but impossible to detect whether the correct secret number, if used, was used by the card holder, and not an unauthorized third party. The PIN system is arguably much more secure than payment instruments using the signature to authorize the customer, because of the cryptographic controls in place.[39] Since 2006, the credit services sector has refused to accept the risks of forgery in connection with the POZ system based on the manuscript signature of the customer.[40]

In 2003, the Local Court in Dortmund reached the conclusion that there is no empirical deduction providing that the card holder must have caused unauthorized withdrawals from an ATM in a grossly negligent way, where they retained the card with the PIN, or noted the PIN on the card where it was stolen from a rucksack.[41] In contrast to the view of the Higher

[31] *Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 292, 294. Concerning the risk of forging bank cards in Austria, see Gerwin Haybäck, Haftungsfragen bei Totalfälschung der ec-Karte, wbl (1999) 56.*

[32] *District Court Halle, WM (2001) 1298.*

[33] *Local Court Buchen VuR (1998) 42. The risk of observing the PIN is not mentioned in the following: District Court Hannover, WM (1998) 1223; Local Court Dinslaken, WM (1998) 1126; Local Court Osnabrück, WM (1998) 1227; Local Court Charlottenburg, WM (1998) 1224.*

[34] *Local Court Wildeshausen, WM (1998) 1128; District Court Bonn, WM (1995) 575; Local Court Frankfurt, CR (1998) 723.*

[35] *District Court Berlin, ZBB (1999) 85.*

[36] *In German, Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 88 (93) proposes: 'Zunächst sind die Banken wie auch die Teilnehmer am POS-Verfahren im Handel gehalten, die Bedingungen bei der Eingabe so zu gestalten, dass ein Ausspähen nicht möglich ist. Besonders der Sichtschutz der Eingabetastaturen im Handel erscheint im Falle unübersichtlichen Gedränges allzu dürftig. Es wäre dringend zu überlegen, ob im Handel die Legitimation des Kunden nicht ausschließlich durch Unterschrift geschehen sollte, wie bisher schon im sogenannten POZ-Verfahren.'*

[37] *Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 88 (93).*

[38] *POZ system means point of sale without guarantee of payment by using EC card plus a manuscript signature (without a PIN); Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 93, referring to Ulrich Häde, Die Zahlung mit Kredit- und Scheckkarten, ZBB (1994) 33, 41.*

[39] *Gerwin Haybäck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich, (2008) II.D.3, p 96 and following; to EC liability Gerwin Haybäck, ÖBA (1997) 256 and following.*

[40] *Stating that the former POZ system was 'highly susceptibel (in German: "anfällig") to misuse': Wolfgang Gößmann, § 68: ec-Kassen und POS-System (Point-of-Sale). GeldKarte, in: Herbert Schimansky, Hermann J. Bunte, and Hans-Jürgen Lwowski, Bankrechts-Handbuch, Bd 1, 3rd edition (2007) marginal number 12, 13.*

[41] *Local Court Dortmund, BKR (2003) 912.*

Regional Court of Frankfurt,[42] most of the cases show that obtaining the secret number is not to be considered as absurd and only a theoretical possibility.

According to a recent decision of the Austrian Supreme Court (OGH), the card holder is not liable for withdrawals caused by unauthorized third parties where he keeps the card and PIN safe. In this case, the card holder took out 90 Euro from an ATM. When doing so, he not aware that he was being observed by an unknown person. The card holder protected the key pad against observation from behind with the upper part of his body. After the withdrawal, the customer put the money and the card into a wallet, and the wallet into the main pocket of his rucksack, which he then placed on his back. He was followed by the thief, who stole the card in the underground. When the card holder noticed the theft, he initiated the block of the card. However, 310 Euro (the original 90 Euro plus a further withdrawal of 310 Euro meant the maximum of 400 Euro maximum was reached because that was the maximum for any withdrawal a day) were withdrawn by an unauthorized third person. The Austrian Supreme Court (OGH) decided that the card holder did not breach his duty of care. It was determined that he was not obliged to take additional measures against criminals, such as protecting the key pad with the second hand or shielding it from lateral observation. In contrast to the court of appeal, who considered it as negligent behaviour because of the fact that the card holder had worn the rucksack on his back and had therefore lost the sight of the zip, the Austrian Supreme Court stated in this case that the safekeeping of the card enclosed in the main pocket of the card holder's rucksack was performed according to his duty to care. As a consequence, the bank lost the appeal.

As a result, the court drew the conclusion that it is sufficient to put a purse into a closed rucksack that is worn on the back, and to protect the number pad with the upper part of the body, even if the purse and card disappear from the customer's sight.[43]

Guessing or calculating the PIN

At the time of implementation of the ATM PIN system, it was only considered an academic question whether unauthorized third parties were able to find out the PIN, because of the marginal probability of 0,03 per cent.[44] It is generally accepted that the Data Encryption Standard (DES), which was applied until the end of 1997, was considered cryptographically secure.[45] Randomizing the code using conventional means was considered impossible. In 1992, the Higher Regional Court of Berlin considered the PIN code secure, in reference to statements of the Federal Office for Security and Information Technology. Regarding the guessing or randomizing the PIN code at that time, the Federal Office acted on the assumption of 72 quadrillion alternatives.[46]

However, this judgment was overturned by the rapid development of the semiconductor technology. In 1994, experienced criminals would have required 1900 years to find out a PIN. Three years later, they would only have needed 96 days, shortly after only 19 days, since 1999 no more than 24 hours.[47] Thereafter, a decision of the Higher Regional Court of Hamm initiated a serious discussion as well as major doubts about the cryptographic safety of DES used until the end of 1997. In this now famous case, the court refused to grant a prima facie evidence in favour of the bank. It was possible that the criminal could have decoded the PIN by using the data recorded on the ATM card. As a consequence, the customer won the case.[48]

As a result, the cryptographic system was updated and replaced by the Triple Data Encryption Algorithm (TDEA). New, regionally generated PINs have been distributed, and an on-line network has been established.[49] Thus, the credit services sector improved the safety of the system against external attacks. Nevertheless, several judgments in favour of the card

[42] *Higher Regional Court of Frankfurt, WM (2002) 2101.*

[43] *The 'Rucksack' decision of 2 February 2007, in: ÖBA 2007/1424 (OGH). Consenting Georg Graf, Wer haftet beim Bankomatkartenmissbrauch? Anmerkungen zu einem aktuellen OGH-Urteil sowie den Auswirkungen des Transparenzgebotes auf die Auslegung von AGB, ÖBA (2007) 531 and following.*

[44] *The Higher Regional Court of Berlin (German: Kammergericht), case: WM (1992) 729, relied on a statement from the Federal Office for Security and Information Technology (Bundesamt für Sicherheit in der Informationstechnik) for this figure of the margin of probability.*

[45] *Concerning the safety of the PIN cp. Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 292 and following. Referring to the former DES PIN system, see the US study at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf: A DES key consists of 64 binary digits (0s or 1s) of which 56 bits are randomly generated and used directly by the algorithm.*

[46] *Federal Office for Security and Information Technology (Bundesamt für Sicherheit in der Informationstechnik). For the judgment mentioned above, see Higher Regional Court of Berlin, WM (1992) 729.*

[47] *The detailed report of 19 January 1999 is available at: http://www.heise.de/tp/deutsch/inhalte/te/1771/1.html.*

[48] *Higher Regional Court of Hamm, NJW (1997) 1711 and following. To the safety of the former PIN system, sceptically Professor Dr. Werner Schindler, Ec-Karten: Wie sicher ist die PIN-Nummer?, NJW-CoR (1997) 284; Hans-Jürgen Stenger, Zur Kritik an der Annahme einer Errechenbarkeit einer PIN, CoR (1997) 363 and following.*

[49] *Hartmut Strube, Haftungsrisiken der ec-Karte, WM 1210 (1998). In respect of the question of the safety of the PIN, see Johannes Köndgen, Die Entwicklung des privaten Bankrechts in den Jahren 1999-2003, NJW (2004) 1288.*

holder were delivered.[50] For example, the Local Court at Duisburg reached the conclusion that PIN codes could be decoded by ordinary card readers. Even the RSA-155-Code (512-bit numbers in the code have about 155 decimals) used in internet transactions (SSL protocol) was cracked. Although it is admitted that some withdrawals at ATMs are performed by using stolen payment cards, this does not necessarily imply grossly negligent behaviour on the part of the customer.[51]

On the other hand, there are still decisions in favour of the prima facie evidence of ATM withdrawals that either the card holder has withdrawn the money, or he has not kept the secret number safe.[52] The Higher Regional Court of Hamm mentioned several methods of manipulation, such as card reader, frequency of certain number combinations, switching off the 'faulty operation counting function' in the card by technical manipulation,[53] and others. However, in Germany, off-line systems have not been in use since 1997.[54] From that time on, the prima facie evidence could not be countered by the possibility that criminals discovered the PIN.[55] The Federal Court of Justice of Germany felt confident that the security architecture of the Triple Data Encryption Algorithm (TDEA) system practiced since 1997 is safe. For this reason, the court has imposed significant demands on the customer whenever the latter has attempted to counter the prima facie evidence in favour of the bank.[56]

Prima facie evidence in favour of the bank – a controversial issue

In contrast to other payment instruments, such as the cheque, specific problems of evidence arise from the ATM PIN system, because of the anonymous communication process. If it is impossible to find out who executed the withdrawal at issue, it is necessary to begin the investigation with what is meant by a legally performed electronic payment process. If the bank was legally obliged to furnish full proof, it would result in insoluble difficulties.

The prevailing judicial opinion is that the prima facie evidence is granted in favour of the bank. This is proper evidence which is equated to formal evidence. The prima facie evidence comes into action in case of formal and typical events. According to experience, the circumstances of the case must either indicate only one cause or one definite process.[57] Exercising prima facie evidence is based on the assertion that the decoding of the PIN is impossible at short notice. The prima facie evidence rests upon the mutable experience of life, as well as technological progress.

Therefore, the use of the EC (ATM) card in connection with the PIN establishes the ground for prima facie evidence that either the card holder himself withdrew the respective amount at the ATM, or enabled the unauthorized withdrawal by grossly negligent behaviour.[58] Regarding unauthorized transactions caused by third parties, the customer is required to report abnormal events described in a plausible, precise, and substantial manner, should he intend to counter the prima facie evidence. In accordance with the provisions of section 670 of the German Civil Code, only where the customer succeeds in reporting such evidence in substance, will a claim for disbursement not be granted to the bank:[59]

§ 670 Ersatz von Aufwendungen

Macht der Beauftragte zum Zwecke der Ausführung des Auftrags Aufwendungen, die er den Umständen nach für erforderlich halten darf, so ist der Auftraggeber zum Ersatz verpflichtet.

Section 670

Reimbursement of expenses

If the mandatory, for the purpose of performing the

[50] *Local Court Hamburg, VuR (1999) 88; Local Court Frankfurt, WM (1999) 1922; Higher Regional Court of Stuttgart, NJW-RR (2002) 1274.*

[51] *Local Court Duisburg, JurPC Web-Dok (1999) 197, Abs 1 – 15; cracking the RSA-155-Code, see http://igw.tuwien.ac.at/fit/2001/fit05/sicherheit/der_rsa_algorithmus.html.*

[52] *District Court Stuttgart, WM (1999) 1934; Local Court Dinslaken, WM (1998) 1126, referring to: Local Court Hannover, WM (1997) 1207; Local Court Wuppertal, WM (1997) 1209, against Higher Regional Court of Hamm, NJW (1997) 1711. Likewise the side proceeding of this case, see District Court Darmstadt VuR (2000) 357; Rolf Aepfelbach and Gerd Cimiotti, Zur Sicherheit des ec-Kartensystems, WM (1998) 1218 and following.*

[53] *The Federal Office for Security and Information Technology considered the possibility of switching off the 'faulty operation counting function' in the card by technical manipulation as an 'annoying issue', for which see Werner Schindler, Die neuen PIN-Nummern der ec-Karten, NJW-CoR (1998) 223, 224.*

[54] *Stefan Werner, Anscheinsbeweis und Sicherheit des ec-PIN-Systems im Lichte der neuen Rechtsprechung, WM (1997) 1516.*

[55] *Local Court Frankfurt, NJW (1998) 687; Local Court Osnabrück, WM (1998) 1127.*

[56] *Federal Court of Justice of Germany, NJW (2004) 3623; expressively confirmed two years later, Federal Court of Justice of Germany, NJW (2007) 593.*

[57] *Federal Court of Justice of Germany, NJW (1996) 1828; (1997) 528. Taking of evidence in the view of the experts, cp. Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 297.*

[58] *District Court Köln, WM (1995) 976; Local Court Diepholz, WM (1995) 1919; Local Court Schöneberg, WM (1997) 55; Local Court Hannover, WM (1997) 64; Local Court Frankfurt, WM (1995) 880; Local Court Wuppertal, WM (1997) 1209; Local Court Hannover, WM (1997) 1207; Local Court Charlottenburg, WM (1997) 2082; Stefan Werner, Beweislastverteilung und Haftungsrisiken im elektronischen Zahlungsverkehr, MMR (1998) 232 and following; Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269.*

[59] *Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 89; BGH NJW (1979) 1964; BGH WM (1979) 417.*

mandate, incurs expenses that he may consider to be necessary in the circumstances, then the mandator is obliged to make reimbursement.

This may be the case if the card holder has demonstrably not been at the place of the events (that is, at the physical location of the unauthorized withdrawal at the ATM or POS terminal) at the time in question; if the ATM card was lost before the withdrawal; if a video recording suggests another conclusion, or if fingerprints on the retracted card are not those of the customer, or a manipulated faulty operation counter are detectable.[60]

Further, the ATM journal is of importance. The case law indicates that the correct documentation of a single payment by the ATM journal tape is considered as prima facie evidence that the ATM has paid out money in the amount of the documented sum.[61] In case an ATM does not dispense money at all or dispenses out too little, this may be a fault that is documented by the ATM journal. Time, place, sum, denomination, and data input are documented exactly, although it is possible but rather difficult to destroy the data of the ATM journal. The authenticity of a card is checked by the modulated feature (MM-Modul) in the ATM corresponding with the chip on the card. The module on the card is read by the bank, and data is exchanged between the card and the bank, and if this data is accepted by the bank, it provides sufficient evidence to the satisfaction of the bank to infer that the customer's card is physically in the ATM. This evidence is considered to be prima facie evidence that the customer's card was inserted in the ATM, and acts to demonstrate that a third person cannot have inserted a duplicate EC card in the terminal.

Given such evidence, it is for the customer to verify why atypical events are to be taken into consideration.[62] The jurisprudence concerning the prima facie evidence makes clear that, regarding electronic means of payment, there is a close connection of prima facie evidence and system security.[63] If prima facie evidence is to be accepted lawfully, it is necessary to assume the security of the system is functioning correctly.

The customer cannot merely carry out his duty to report the theft of a card and any subsequent misuse as a matter of fact. He is also required to make clear what the abnormal events are, and to described them.[64] As mentioned above, the Higher Regional Court of Hamm did not grant a prima facie evidence to the bank in 1997.[65] The court did not exclude the possibility that an unauthorized third person could have been able to find out the PIN by guessing or calculating it. This judgment is now in the minority, because it acts on the assumption that only the card holder knew the correct PIN, and the use of the correct PIN was not sufficient to prove the card holder's breach of his duty of care.[66]

Position of the Federal Court of Justice (BGH) and subsequent case law

Thereafter, the Federal Court of Justice of Germany decided a case in favour of the bank, in which a third person having stolen the payment card took 1000 Euro out of the ATM.[67] Considering the application of the 128 bit Triple Data Encryption Algorithm (TDEA) in 1997, the prima facie evidence suggested the fact that the thief noticed the PIN only because the card holder was negligent by keeping the secret number together with the ATM card. It was concluded that the claimant must have violated her duty of care by having recorded the PIN on the card or stored the latter together with the PIN. The Federal Court of Justice of Germany refused the alternative explanation of decoding the PIN, because this would be mathematically impossible. Although at the time of this case, there was no evidence put forward to indicate the code had been cracked. In the view of the court, purely theoretical possibilities to find out the PIN are not sufficiently suitable to disable the prima facie evidence. The result means there is no reason to obtain evidence regarding the system security. Obtaining the PIN by observation is only considered as a 'different' cause where the card is stolen in close connection with the respective ATM, at the same time the PIN was entered. In this instance, the card holder was not able to substantiate such circumstances.

In the view of Stefan Werner, the Federal Court of

[60] *Michael Bucher, Die Risikoverteilung bei der Benutzung elektronischer kartengesteuerter Zahlungssysteme, (Verlag P. Lang, 1992), 302.*

[61] *Herbert Schimansky, Hermann-Josef Bunte and Hans-Jürgen Lwowski, Bankrechts-Handbuch, (3rd edition, Verlag C. H. Beck München, 2007), 13-14.*

[62] *Gerwin Hayböck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich, (2008) 156 and following.*

[63] *Stefan Werner, Beweislastverteilung und Haftungsrisiken im elektronischen Zahlungsverkehr, MMR (1998) 234 and following.*

[64] *Local Court Schöneberg, WM 66 (1997); Local Court Hannover, WM 64 (1997); Local Court Wuppertal, WM 1209 (1997); District Court Hannover, WM 1123 (1998); District Court Bonn, NJW-RR 815 (1995). In general Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1270.*

[65] *OLG Hamm, NJW (1997) 1711.*

[66] *Local Court Buchen, VuR (1998) 98; similiar District Court Frankfurt, VuR (1997) 423; District Court Frankfurt, VuR (1998) 162; District Court Dortmund, CR (1999) 556. Against it, the bank won the case, because the customer did not succeed in demonstrating the practical alternative of guessing or randomizing the PIN, Local Court Flensburg, VuR (2000) 131. Likewise: District Court Köln, WM (2001) 852.*

[67] *Federal Court of Justice of Germany, NJW (2004) 3623; consenting Jan Christian Eggers and Andreas Goerth, Die Haftung des Bankkunden für unbefugte Abhebungen mittels ec-Karte und PIN – BGH, NJW (2004) 3623; BGH JuS (2005) 492.*

The correlation between the theft of the card and the unauthorized withdrawals as mentioned by the Federal Court of Justice is somewhat ambiguous.

Justice stated that, at least if a card and PIN are used promptly at an ATM, the prima facie evidence argues for the fact that the card holder has noted the PIN on the card or stored it with the card. Certainly, this argument only applies if different causes regarding the misuse can be excluded, according to the experience of life.[68] This judgement was criticized by Christian Hofmann inasmuch as it has 'discharged the bank from responsibility although the bank is able to battle against failure of the payment system.'[69] Rightly, the Institute of Financial Services (Hamburg) emphasized the significant problems for the customer to counter the prima facie evidence under the prevailing circumstances.[70]

The correlation between the theft of the card and the unauthorized withdrawals as mentioned by the Federal Court of Justice is somewhat ambiguous. The prima facie evidence is granted to the bank at the expense of the card holder where the PIN is entered and at the first attempt at withdrawal succeeds within one hour after the theft of the card. This time is short, hence the explanation that the thief was able to decode the PIN by using technical instruments is excluded.[71]

The Federal Court of Justice of Germany confirmed the prevailing case law in a class action[72] initiated by a consumer advice centre.[73] In this case, a number of consumer claims of card holders were transferred to the Consumer Advice Centre of Nordrhein-Westfalen. By transferring the minor claims of 19 participants, a total of 13,500 Euro was claimed, due to cards being used by unauthorized third parties. The Federal Court of Justice decided that the Advice Centre of Nordrhein-Westfalen was a rightful claimant. In the interests of the consumer as well as for the public benefit, the judicial assignment for collection was considered to be necessary because it produces a more effective enforcement than any individual action. This is the case if there are circumstances preventing a person with the right to initiate an action, for example in the case of disproportionately high costs of the proceedings, or a high risk of litigation, or of practical problems of law enforcement.[74]

In this decision, the Federal Court of Justice confirmed the previous case law concerning the distribution of the burden of proof in case of misuse of stolen EC cards. The alternative of observing the PIN by a third party as a 'different' cause that only comes into question if the EC card was stolen and where it can be shown that it coincided with entering the PIN by the card holder at an ATM or POS terminal. The court convincingly emphasized the limits of the prima facie evidence. It is not possible for a customer to challenge a bank effectively until the safety standard of the electronic payment system is no longer granted to be authentic or genuine.

Conclusion

The distribution of risks between the EC card holder and the bank in case of unauthorized withdrawals at ATMs or POS terminals caused by third parties is closely connected with the safety standard of the electronic payment system. Despite the prevailing assertions of the safety of the system, courts always have to question if the current system grants a sufficient safety standard in order to apply the prima facie evidence in favour of the bank.

[68] *Stefan Werner, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen PIN, BKR (2004) 504 and following. Critically: Hartmut Strube, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen persönlichen Geheimzahl, BKR (2004) 497, 501 and following: ' The technical dispute concerning the PIN system, also a legal issue, will go on.' ,In Der technische Disput über das PIN-System, nicht eben ein urjuristisches Thema, wird also weitergehen' : BKR (2004) 501.*

[69] *Christian Hofmann, Schadensverteilung bei Missbrauch der ec-Karte, WM (2005) 441, 449 'den aus der Verantwortung entlassen hat, der Sicherheitslücken des Systems bekämpfen kann.'*

[70] *Institute of Financial Services (Hamburg) (Institut für Finanzdienstleistungen) (Hamburg), VuR (1998) 256.*

[71] *Local Court München, BKR (2005) 39.*

[72] *For that purpose, on 27 November 2008, the European Commission issued a Green Paper ' On Consumer Collective Redress' , Brussels, 27.11.2008 COM (2008) 794 final; Georg E. Kodek, Sammelklagen für Verbraucher: Ein neues Grünbuch der EU, ecolex (2009) 185.*

[73] *Consumer Advice Centre of Nordrhein-Westfalen (Verbraucherzentrale Nordrhein-Westfalen).*

[74] *Federal Court of Justice of Germany: NJW (2007) 593, 595 et seq. Likewise: Higher Regional Court of Frankfurt, Keine Anhaltspunkte für Sicherheitsmängel des PIN-Verschlüsselungssystems, MMR (2008) 473; Higher Regional Court of Karlsruhe 06. 05. 2008 - 2 O 16/07, BeckRS 15410 (2008).*

Further improvements to the security architecture of ATMs and POS terminals should be achieved. This refers, for example, to an effective shielding of the number pads, video control, increased program code and internet safety. The traditional magnet strips have to be replaced by highly effective computer chips. It is time for a world-wide improvement and the introduction of a secondary form of authentication, such as a biometric measurement of the fingerprint or other biometric measurements, such as user authorization with an iris scan.[75] For this purpose, several appropriate projects, such as 'FairPay', are provided by the German Research Centre for Artificial Intelligence.[76] To this end, banks, software developers as well as university departments dealing with the internet and safety technology, should work together.[77]

The costs may be high – but safety, particularly in the electronic age, is worth its price, especially if it ameliorates the anguish and suffering that people have to go through when money is taken from their bank account with authority.

Gerwin Haybäck, Dr. phil., Dr. iur, Assistant Professor at the Department of Business Law, University of Salzburg, Austria, is an author of several publications in the field of civil (consumer) law, commercial law, and intellectual property law. In April 2009 he won the Leopold Kunschak Scientific Award.

gerwin.haybaeck@sbg.ac.at
http://www.uni-salzburg.at/HWR/haybaeck.gerwin

[75] *Guiseppe Parziale and Reingard Riener-Hofer, Biometrie: Begriff und Diskussionsstand, juridikum (2004) 79; this study was influenced by the USA entry and visa requirements imposed by after 11 September 2001.*

[76] *German Research Centre for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz) at http://www.dfki.de/web/forschung/projekte?pid=103.*

[77] *Manfred Leber, Fair Pay – Sicherheit im elektronischen Zahlungsverkehr, CR (2000) 492.*

ARTICLE:

BANK CARD FRAUD IN SPAIN[1]

By **Ricardo M. Mata y Martín** and **Antonio Mª. Javato Martín**

Technological progress over the last two decades, in combination with the opening up of international borders across the internet that has further developed human and commercial relations, have led to the appearance of new payment systems in the form of bank cards. These instruments may be used at commercial shopping centres, at the network of cash dispensers, and now, with the development of telecommunications networks, in the context of the internet. The mass use of cards as a means of payment inevitably gives rise to a significant amount of fraud. The legal treatment of fraud under criminal law involving bank cards requires penalties to be set for the ways in which these categories of offenses may be committed, and which may be applied under these circumstances: conventional fraud, computer fraud and burglary or housebreaking.

Introduction

At present, electronic telecommunication networks may also be applied to payment systems. These technological advances mean that the most extensively used are the multiple versions of the bank card. The dynamics of economic globalization will, in turn, expand modern payment systems even further.

Naturally, as an effective instrument in commercial relations, the new payments systems are subject to a more or less complete set of legal regulations, which in certain situations requires the implementation of criminal legislation. For such legislation to be effective, it is essential to study and to define the elements that constitute the offences that may be applied to these still relatively novel acts. This article considers the issues relating to the fraudulent use of bank cards, because of the scale of their use – it is significant and the most widely used means of payment, even greater than cash payments – and their specific regulation.

As this article will demonstrate (and the work that this article is taken from), there is no specific provision in Spanish criminal law relating to the use of bank cards as a means of payment, except in the case of misrepresentation. As a means of payment in a criminal context, it is necessary to distinguish between the use of the bank card at commercial establishments, for payment over telecommunications networks, and card abuse at automatic cash dispensers (ATM). Finally, the fraudulent use of banks cards can imply the application of some types of criminal offence related to misrepresentation.

Payment in person at commercial premises

In this part, cases are considered in which a card held in the name of an individual is used without that person's consent as a means of payment at a commercial establishment from which a product or service is acquired, in such a way that the salesperson accepts the payment under the belief that the real card holder is in fact present. Doctrine[2] and jurisprudence[3] has implicitly equated this method of impersonation with the conventional offence of fraud, as regulated under article 248.1 of the Codigo Penal (Penal Code), which states that:

> Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Fraud is committed by whoever, for personal benefit,

[1] *This paper forms part of the research into Electronic means of payment - Proyectos de Investigación sobre Medios electrónicos de pago VA111/04 (Programa General de Apoyo a Proyectos de Investigación de la Junta de Castilla y león) and SEJ2004-03704 (Planes Nacionales I+D/I+D+I, del Ministerio de Educación y Ciencia). Abbreviations (where used): CP: Código Penal/Penal Code; LOPJ: Ley Orgánica del Poder Judicial/Organic Law on Judicial Power; TS: Tribunal Supremo/Supreme Court; STS: Sentencia del Tribunal Supremo/Judgment of the Supreme Court; ATS: Auto del Tribunal Supremo/Order of the Supreme Court; SAP: Sentencia de la Audiencia Provincial/Judgment of the Provincial Court; RJ: Aranzadi (Repertorio de Jurisprudencia del TS)/Collection of Supreme Court Jurisprudence; ROJ: Repertorio Oficial de Jurisprudencia/Official Collection of Jurisprudence; CENDOJ: Centro de Documentación Judicial. Consejo General del Poder Judicial/Centre for Judicial Documentation General Council of Judicial Power; RGDP: Revista General del Derecho Penal/General Journal of Criminal Law.*

[2] *Jesús Fernández Entralgo, 'Falsificación y utilización fraudulenta de tarjetas electrónicas' in Tarjetas bancarias y Derecho penal. Cuadernos de Derecho Judicial, VI-2002, 58.*

[3] *See, amongst others, STS of 30-10-2003 -La Ley Juris 2004,10845-; STS 21-1-2003 La Ley Juris 2003, 1269-.*

From the perspective of the need for 'engaño bastante (sufficient deceit)' in the description of the offence, and in accordance with the general prerequisites of the modern principle of objective accusation, it is necessary that certain self-protection procedures be complied with in carrying out the payment correctly.

practices sufficient deceit to the extent that they mislead another, inducing the latter person to make an act of disposal to his own detriment or to that of a third party.[4]

Criminal deception under Spanish law requires, in the first place, deceitful conduct on the part of the offender (in this case the presentation of a card thereby affirming both an apparent ability to pay and sufficient solvency). The deceit practiced by the active subject must be sufficient to lead another party to be misled (the seller is misled into thinking that they are dealing with the person to whom the card was issued, and trusts in the solvency of the legitimate card holder, but is not in fact dealing with the person to whom the card was issued). The erroneous situation in which the other party is placed leads to an act of disposal (the transfer of goods or the provision of services by whoever receives the payment), which causes a loss for that person or for a third party (the seller, the card issuer or the card holder, according to whoever is liable to cover the costs of the amount that is defrauded). From the subjective point of view, the offender must act with an economic interest in mind and with the sole aim of personal enrichment.

In recent years, it has also been made clear that there is an obligation on the receiver of the payment to comply with certain procedures when accepting payment. From the perspective of the need for 'engaño bastante (sufficient deceit)' in the description of the offence, and in accordance with the general prerequisites of the modern principle of objective accusation, it is necessary that certain self-protection procedures be complied with in carrying out the payment correctly.[5] In cases where the card is presented as a form of payment at a commercial establishment, the basic procedure requires that the seller satisfy themselves that the person in possession of the card is the person to whom the card was issued, and should also check the expiry date of the card.

This tendency has been accepted in modern jurisprudence, which has consistently failed to apply the legal definition of fraud and has punished the offence, where applicable, solely as misrepresentation, under circumstances in which the victim of the deceit failed to act with due diligence that is expected in commercial practice when verifying the identity of the subject. A good example of the approach taken by the judiciary is the STS of 3 June, 2003,[6] which declared as abnormal the act of paying with a stolen bank card belonging to a person of the opposite sex, because the sales person made no effort to verify the identity of the card holder, not even to establish whether the person that presented the card was a man or a women, such that the deceit could not be qualified as sufficient to be held as a causal factor that helped to cause the economic transfer.[7]

As well as conventional fraud, the offence of misrepresentation of a commercial document (article 392 of the CP) may be considered, where the manuscript signature of the actual card holder is forged by another person on the sales receipt issued by the bank card reader. Similarities will occur between both categories of criminal offence. As much is established in the Agreement of the 2nd Chamber of the Supreme Court (Sala 2ª del Tribunal Supremo) dated 18 July 2007, subsequently applied in the Judgment of 19 July 2007 (nº 451/2007), in which the accused, a Romanian national, entered a jeweller's shop in the locality of

[4] *The penalty established for the crime of conventional fraud ranges from a six-month to a three-year prison term (article 249). This same penalty also applies to computer fraud.*

[5] *Jesús María Silva Sánchez in Pablo Salvador Coderch and Jesús María Silva Sánchez Simulación y deberes de veracidad, (Civitas, Madrid, 1999), 98 and following, 387; Francisco Muñoz Conde, 'De la llamada estafa de crédito' in RGDP 9, 2008, Iustel, 2 and following; Mercedes Pérez Manzano, 'Acerca de la imputación objetiva de la estafa', in Hacia un Derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann, (BOE, Madrid 1995), 285 and following.*

[6] *Nº 807/2003 Actualidad Penal. Nº43. 17 - 23 November 2003, 2310 and following. Along the same lines, supported by the same judgment, the SAP of Barcelona of 25 January 2007, which deals with practically identical circumstances (a card bearing the name of a woman fraudulently used by a man).*

[7] *The failure to notice the gender of a person reflects on the accuracy of the observations about the accuracy of a manuscript signature, as noted in Stephen Mason, Electronic Signatures in Law, (2nd edition, Tottel, 2007), 1.2, footnote 1.*

Tavernes Blanques (Valencia) where she made purchases to a value of 1,399 euro and 860 euro, paying for these purchases with the credit card of another person. To do so, she presented the Swiss National Identity Card of the legitimate holder of the credit card, but which bore the photograph of the accused. Subsequently, the accused signed the sales receipts imitating the signature of the legitimate cardholder. This decision followed and endorsed the comments made in earlier judgments made by the same judicial organ. However, if the card reader finally fails to authorize the attempted payment once the card had been swiped and in such a way that the perpetrator was finally unable to sign the sales ticket, it would amount to an attempt to falsify a commercial document (STS 25-6-98 nº 882/98). In the 1998 judgment, (STS 882/1998 25 June), the following ruling was made where the accused entered a jeweller's shop in Barcelona, and expressed an interest in buying a watch. To pay for it, the accused handed over a Master Card to the sales assistant in the name of a United States citizen, together with the legitimate passport of the US citizen. The accused had replaced the photograph of the passport holder with his own photograph. When the sales assistant requested authorization from the bank, it was refused via the POS (Point-of-Sale) terminal. The accused did not, therefore, place a false signature on the sales ticket. In view of the above, the accused handed over a second card (Visa), which had been cloned, which enabled him to pay for the watch. With respect to the first card, the Supreme Court considered it as an attempted misrepresentation of a commercial document.

As regards aiding and abetting misrepresentation, the TS has made it clear that where more than one person practices deceit in a commercial outlet by purchasing goods or services with another person's card, it does not matter which of those accused actually signs the sales slips; they are all guilty of misrepresentation, because the offence does not solely consist of having signed the sales receipt. Thus, the guilty parties are all those who benefit from the proceeds of the crime where there is a joint decision to commit the crime (STS de 26-5-2002 nº 661/02).

The bank card and remote payments

As the technical possibility of making remote payments with cards became more widely used without the need for the physical presence of the card holder, certain problems have arisen that have affected the law. Electronic procedures, especially over the internet, have facilitated remote commercial transactions that are normally settled with payment made by means of the electronic transfer of the data stored on a card.

The prevailing jurisprudence provides that the deceit at the heart of criminal deception is necessarily of a personal nature. It may only arise as the result of a direct relation between two people. Likewise, the error must also be a consequence of the deceitful act being of a psychological nature, which is only possible where there is close personal proximity.[8] Due to these assumptions, classic or conventional estafa (fraud) is, in such circumstances, impossible. Thus, when the new Penal Code was approved in 1995, the legislator included a different set of circumstances for computer-aided criminal deception (article 248.2). Given the personal nature of deceit and error under Spanish law, no references were made to them in article 248.2. In their place, it was provided that there must be a prerequisite of manipulating computer data. The subject must achieve the unauthorized disposal of an asset through the manipulation of computer data. Property assets are thus construed as objects, the manipulation of which will affect their value in such a way as eventually to cause loss to the property of a third party. The transfer implies that accountable assets pass initially to the property of the offender, and that the effect is to cause actual loss.

The offence of electronic fraud describes the circumstances relating to fraudulent payments made over the internet, in which the offender uses a cloned card or the information obtained from a legitimate card to obtain goods or services using the card details of another person, thereby causing an innocent person to be charged for the payment. The broad concept of computer manipulation basically corresponds to that proposed by Romeo,[9] in the sense of a wrongful modification of the result of an automated process at any of the stages of computer processing or programming with the aim of personal benefit and causing loss to a third party.

An alternative to this broad concept of computer manipulation has arisen with the Judgement of Malaga Criminal Court nº 3 of 19th December, 2005.[10] The court excluded the input of inappropriate data into the

[8] *A detailed presentation may be found in M. L. Gutierrez Francés, Fraude informático y estafa (Ministry of Justice 1991), 336 and following, and Ricardo M. Mata y Martín Los delitos de estafa convencional, esstafa informática y robo en el ámbito de los medios electrónicos de pago, 57. Jurisprudentially, STS nº 533/2007 of 12 June Id Cendoj: 28079120012007100455: and STS 369/2007 of 9 of May Id Cendoj: 28079120012007100374.*

[9] *C.M. Romeo Casabona, Poder informático y seguridad jurídica, (Madrid 1987), 47.*

[10] *ARP 2006/43.*

information system as an element of electronic fraud. The case refers to acts in which the defendants:

> ... puestos previamente de común acuerdo en fecha 28 de noviembre del 2000 a través de la página www.tododvd.com de la empresa Red Fénix Sistemas, SL realizaron el pedido de un reproductor de DVD marca Pionner modelo 530/535 con precio de venta 438 ? a nombre de Luis Pedro, ... y realizando el pago con la tarjeta VISA núm. NUM006, de la que era titular un tercero ajeno a los hechos, quien no había autorizado a los acusados a utilizarla.
>
> ... having previously come to a common accord on 28th November 2000, they placed an order in the name of Luis Pedro... on the Red Fénix website www.tododvd.com for a Pioneer brand DVD player model 530/535 at a sale price of €438 and made payment for it with a VISA card number NUM006, which belonged to a third party unconnected with the facts, who had not authorised its use by the accused.

The court only considered the subject-matter of this form of fraud in terms of the actions affecting the existing data (alteration, modification, deletion) in the system, and not the fact that the data provided, although correct, was not provided with the authority or agreement of the actual person whose data was used:

> Por ello no cabe incluir la conducta de los acusados en el párrafo segundo del art. 248 del Código Penal pues los mismos no manipularon sistema o programa informático alguno sino cuando se les solicita el número de una tarjeta bancaria para cargar en la cuenta asociada a la misma el importe de la compra efectuada designan el número de una tarjeta de la que no es titular ninguno de los acusados y es en la creencia de que todos los datos introducidos en la página web al hacer el pedido del reproductor de DVD son correctos por lo que la empresa Red Fénix SL, procede a hacer la entrega de dicho aparato en el domicilio indicado al hacer el pedido.
>
> It is for this reason that the conduct of the defendants is not to be included in the second paragraph of art. 248 of the Penal Code, as the latter did not manipulate the system or the computer programme in any way, but when they were asked for the number of a bank card against which to charge the said amount to the associated bank account, they inputted the number of a card that was not held in any of their names. It was in the belief that all the correct data was inputted into the web page when the order for the DVD player was placed that led the firm Red Fénix SL to proceed with the dispatch of the said device to the address they specified when the order was placed.

Were such a distinction to be upheld, all such conduct involving the introduction of misappropriated data to make purchases over the internet would be excluded from the category of computer fraud, offences which even today are being punished under that criminal category, as applied by the Supreme Court. Thus, STS of 20.11.2001 points out that computer manipulation:

> bien puede consistir en la alteración de los elementos físicos, de aquellos que permiten su programación o por la introducción de datos falsos
>
> may either consist in the alteration of physical elements, or of those that allow it to be programmed or by inputting false data.

To date, the jurisprudence has only dealt with circumstances referring to the use of credit cards and bank passwords, although in the case of on-line banking, there are no decisions, or at least none that the authors have found, that refer to payment by mobile telephone and what is known as electronic money. Thus, for example, the Judgment of the Provincial Court of the Balearic Islands num. 30/2005 (Section 2º) of 14 of April 2005, convicted a person for computer or electronic fraud that used personal passwords without the authorization of the account holder to make multiple transfers using the Línea Oberta de la Caixa website to accounts held by the banks of Banesto and La Caixa.

A peculiarity arises in this field, with regard to electronic fraud in association with a commercial outlet. It is a question of the circumstances under which the offender in various ways manages to persuade the owner or employee of an outlet to facilitate an irregular payment. Normally, the offer involves a half share of the benefits obtained from the sales in exchange for collaboration. This circumstance is dealt with, for example, in STS num. 2175/ 2001 of 20 November 2001. Specifically, it refers to an employee of a firm who was responsible for sending out credit cards to their owners and who appropriated a card and proceeded to a sales outlet, where, according to the testimony of the sales

assistants, he used it to make purchases, which were subsequently charged to the card holder's account. The TS upholds the similar nature of the offence described in article 248-2 as:

> quien aparenta ser titular de una tarjeta de crédito (...) y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado.
>
> whosoever appears to be the holder of a card (...) and acts in collusion with whoever inputs the data into the machine, thereby making it possible for it to work automatically is using an artifice so as to register as the owner of the bank card at the bank terminal by inputting the owner's data to obtain funds without the consent of the party incurring the loss.[11]

At other times, that the offender creates a fictitious commercial entity by requesting a Point-of-Sale (POS) terminal with which to commit the fraud. Thus, in the trial leading to the Judgment of the Provincial Court of Valencia of 2-11-1999[12] (num. 4/1999), various individuals by mutual accord considered installing a POS terminal for a fictitious business, and by making use of the terminal and credit cards stolen from their owners (which they possessed in great number), made fictitious transactions, thus obtaining the money from the transactions. The Provincial court appreciated the existence of a continuing offence of electronic fraud and the continuing offence of the falsification of commercial documents.

The use of credit cards in ATMs by thieves

There is yet another area in which the fraudulent use of bank cards takes place: at ATMs owned by banks that enable people to us the facilities offered at any hour of the day. These systems have also prompted the illicit use of bank cards, usually to obtain quantities of cash from cash dispensers. The emergence of such new attacks[13] lacked specific provisions in relation to the offence set out in the Penal Code. However, the response from the judges was to analyse the offence in relation to the physical layout of the ATMs. To begin with, the cash dispensers were placed in an enclosed space that required the same bank card to gain entry. This led the courts to define the offence as burglary using false keys.[14]

With the approval of the Penal Code of 1995, the legislator understood that the solution proposed by the courts made it possible to consider a card as a false key, and amended the definition of false keys with the inclusion of a final paragraph which sought to establish a comparison between a magnetic stripe and false keys:

> A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas y los mandos o instrumentos de apertura a distancia.
>
> For the purposes of the present article, both cards, whether magnetic or perforated, and remote control opening devices or instruments are considered keys (article 239 in fine).

This treatment constitutes consolidated case-law;[15] although the reservations expressed in legal doctrine are not, it appears, altogether dismissed by the amendment to the legislation. In these cases, the application of the specific provision in the final paragraph of article 239 has normally led to charges of 'robo con fuerza (burglary)' in criminal proceedings, without entering into some of the more debateable points that might complicate an appraisal of the actual offence of burglary or housebreaking.[16]

On this point, it is worth pointing out that the provision clearly states that it is to be considered 'for

[11] *See also STS of 26 June 2006 (RJ 2006, 4925). At the Provincial Court level, similar criminal behaviour to those set out here may be appreciated, for example, in the SAP of Granada of 10/11/2006 (ROJ: SAP GR 2008/2006), and in the SAP of Alicante of 27 November 2007 (ROJ: A 2931/2007).*

[12] *ARP 1999/4239, consulted on the Aranzadi Westlaw Database.*

[13] *This class of criminal offence appeared in the second half of the 1980s as a consequence of the proliferation of automatic cash dispensers by banking entities. Enrique Bacigalupo Zapater, 'Utilización Abusiva de Cajeros automáticos por terceros no autorizados' in Poder Judicial, Número Especial IX: Nuevas formas de delincuencia, 85 and following; A.M. Javato Martín, 'Análisis de la Jurisprudencia Penal en Materia de Medios Electrónicos de Pago', in Los medios electrónicos de pago. Problemas jurídicos (Ricardo Manuel Mata y Martín and Antonio María Javato Martín), Comares, Granada, 2007, 375.*

[14] *The crime of burglary (articles 237 and following of the CP) consists in the misappropriation of goods using methods assessed as housebreaking or breaking and entering, which includes the use of false keys.*

[15] *On all these, STS of 22 January 2004, nº35/2004 (Supreme Court Sentence 22nd of January, 2004), EDJ 2004/8295 that rectifies the criteria of the Provincial Court of Madrid that in judgements that led to convictions for theft and not burglary due to it not having taken into account that the cash dispenser from which the money was withdrawn was situated in a booth which would have been opened, or that it would have been necessary to open a door or gate with the magnetic stripe.*

[16] *For further detail on this problem, see Ricardo M. Mata y Martín, Los delitos de estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago. (Aranzadi 2007), 142 and following.*

the purposes of the present article', that is, in the case of burglary using false keys, which means it is necessary to provide all of their general features, specifically that force must be used 'para acceder al lugar donde éstas se encuentran (to gain entry to the place where these are found)' (article 237). The provision in question refers to devices or instruments for remote 'opening', which brings us back to the specific context of burglary, which could also be applied to this category of offence. Furthermore, the keys in the Spanish Penal Code are considered false when they are used to open a lock in the normal way in order to allow entry into an enclosed space. However, the cards used in cash dispensers do not have to have previously facilitated access to an enclosed space, and in addition, they involve other aspects that go beyond the definition in the Code of a false key as being merely an opening device.

In reality, the very nature of this type of offence relates to a fraudulent act, to which the conventional offence of fraud as defined under Spanish law does not apply, because of the absence of personal deceit that is required by legal doctrine and judicial precedent. In addition, beyond any possible use as an opening device, the purpose of the card is, naturally, to be used in the exercise of a right to credit or to withdraw funds through the financial entity – based on the pre-existing legal contract between the card holder and the issuing entity – which by using the PIN, the issuer obtains sufficient evidence to assure itself that the legitimate holder of the card wishes to initiate a transaction in the ATM.

Judgment of the TS of 9 May 2007

Showing some sensitivity to the reasoning set out above, the recent judgment of the TS of 9 May 2007 moves away from what is accepted as consolidated jurisprudence and considers it possible to include the improper use of bank cards at automatic cash dispensers within the definition of computer fraud as defined in article 248.2.[17]

The factual circumstances to which the judgment refers concerned a group that was dedicated to copying credit cards and to making fraudulent use of them for the purposes of personal profit. To do so, they used a procedure known as 'skimming' consisting of the substitution of a magnetic band on an original or new credit or debit card for data on an existing one which they surreptitiously obtained by means of card readers. Having created forged cards, they used these in commercial establishments – presenting forged documents to identify themselves as the owners of the cards, and to withdraw money from the bank account of the customers whose data they had stolen.

They also used the procedure known as 'la siembra (sowing)', which consists in obtaining the victim's PIN number and credit card by placing somebody at a suitable distance from a card holder at a cash dispenser to observe the PIN, and to distract him in such a way that he loses sight of the card when it is returned by the machine, by which time it is removed and replaced by another card. The victim does not notice the switched bank card until he uses it to carry out further operations. The bank cards obtained in this way are used to withdraw money from cash dispensers; when these became invalid because they have reached the preset maximum withdrawal limit, they are used as a resource to manufacture other cards with which to carry out further operations.[18]

A number of criticisms have been made by legal commentators on the inclusion of these circumstances within the offence of burglary (absence of access into an enclosed space, lack of consent to hand over the goods), yet the judgment upholds the definition of the facts as elements of computer fraud. The Spanish High Court have established that the offender, by inputting the PIN or secret number of the stolen card into an ATM, is dishonestly identifying himself to the bank as the rightful owner of the card, thereby prompting the bank to transfer an amount of money voluntarily. Such an identification

> ... ha de ser considerada bajo la conducta de manipulación informática a que se refiere el tipo de la estafa del art. 248.2 CP
>
> ... has to be considered as behaviour that amounts to manipulation of computer data to which the category of fraud defined under art. 248.2 Penal Code refers.

This interpretation is supported, in the words of the Spanish High Court, by the Council Framework Decision

[17] *Note that is the sole judgment of the TS pronounced in this direction. Formerly, some decisions by the High Court (STS 185/2006) pronounced in favour of the solution of computer fraud although in a hypothetical or merely dialectical manner, as the category of crime in article 248.2 of the Penal Code has not been the subject of the accusation.*

[18] *For more descriptions of similar attacks, together with additional case law from across the world, see Stephen Mason, editor, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 4.04-4.15.*

The courts have begun to move away from the criteria they initially upheld, and begun to punish such conduct as counterfeiting of legal tender.

of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment,[19] because article 3, relating to offences and computers, covers the following:

> Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally:
>
> performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by:
>
> - without right introducing, altering, deleting or suppressing computer data, in particular identification data, or
>
> - without right interfering with the functioning of a computer programme or system.

The defining characteristics of data manipulation as provided for in article 3 includes identification by means of a secret number or PIN.

Counterfeiting and the alteration of cards

The treatment of counterfeiting and the alteration of cards in case law has varied over time. In the Penal Code of 1973, and in the absence of specific regulation, bank cards were accorded the status of a mercantile document. As a consequence, the creation of a cloned card by forgery and the manipulation of legitimate cards were subsumed under the articles dedicated to this type of counterfeiting, as determined by the Supreme Court in its judgment of 3 December 1991.[20]

Greater difficulties were involved in the assessment, alteration or manipulation of the magnetic stripe on the card, as the element that it incorporates is difficult to equate with the concept of a document. The problem was corrected in the Penal Code of 1995, which provides an extensive and broad concept of a document under article 26 that now covers magnetic stripes on cards. However, the specific consideration of credit and debit cards as money in article 387 of the New Penal Code will raise questions over such an approach to the problem in case law. The courts have begun to move away from the criteria they initially upheld, and begun to punish such conduct as counterfeiting of legal tender. An especially controversial point is the alteration of the magnetic stripe, as the Penal Code of 1995 decriminalised the conduct previously defined as alteration of legal tender, such that the card that has been manipulated can only be compared in a rather laboured way to the category of offence in article 386-1, which is the manufacture of money, understood as the creation of new money by counterfeiting legal tender.

The Supreme Court has put an end to debate on the question through the Acuerdo del Pleno no Jurisdiccional de la Sala Segunda (Agreement of the Non-Jurisdictional Full Court Session of the Second Chamber) issued on 28-6-2002. It opted to subsume alterations to the magnetic stripes of an authentic card under the offence of counterfeiting, putting forward the following argument:

> ... las tarjetas de crédito o débito son medios de pago que tienen la consideración de 'dinero de plastic', que el artículo 387 del Código penal equipara a la moneda, por lo que la incorporación a la 'banda magnética' de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el art. 386 del Código penal.

[19] *2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment OJ L149, 2.6.2001, p. 1–4.*

[20] *Emilio Manuel Fernández García and Juana López Moreno, 'La utilización...', in Cuadernos de Derecho Judicial VI-2002, 81.*

... credit and debit cards are means of payment that are considered 'plastic money', which article 387 of the Penal Code equates with money, such that the incorporation of data obtained in a fraudulent manner on the 'magnetic stripe' of one of these instruments of payment constitutes a process of production or preparation that should included under art 386 of the Penal Code.

This view was later be confirmed by a Judgement of the Supreme Court num. 948/2002 (Criminal Chamber) of 8th July,[21] in which the Supreme Court proceeded to differentiate between the behaviour in question and computer fraud. The reform of Organic Law 15/2003 has endorsed the criteria of the Spanish Supreme Court, by reintroducing the alteration of legal tender as a form of criminal offence in article 386 of the Penal Code. Likewise, the judicial interpretation of the concept of money was also extended to 'las demás tarjetas que puedan utilizarse como medios de pago (the other cards that may be used as means of payment)' (cash card and such like).

The classification of falsifying electronic bank cards as a crime of counterfeiting legal tender is open to criticism from two points of view. First, from the point of view of punishment, a very harsh sentence in the case of counterfeiting legal tender (a prison term of between 8 to 12 years, article 386 Penal Code) would be applied to circumstances that are much less serious, such as forgery of an isolated card or the mere possession of a forged card to use it as an instrument of payment. Second, from the point of view of authorization by virtue of article 65. b. LOPJ, the competency to judge these facts falls on the Audiencia Nacional (National Court) with a specialized jurisdiction covering terrorism and organized crime, which appears to be questionable.[22]

Hence, the Supreme Court has subsequently modified its general doctrine in the AATS of 18 February 2004[23] and 21 April 2004,[24] insofar as it identifies two types of circumstances:

a. The forgery of the card (alteration or manipulation of its magnetic stripe) and possessing forged credit cards for making purchases or distribution constitute counterfeiting of money and the competent court is therefore the Audiencia Nacional (High Court).

b. Mere possession of one or various forged cards for their use as an instrument of payment are subsumed under the offence of falsification of mercantile documents and thus do not amount to the counterfeiting of money that comes under the jurisdiction of the Audiencia Nacional.

The European Community perspective

There is an interest in a more effective assurance of security for the means of payment that may clearly be seen in the international context, especially respecting electronic payments. In this respect there are two areas of action of great importance for criminal regulation, the Cybercrime Convention of 2001 and various actions of the European Union.

The Convention on Cybercrime, drawn up in Budapest in 2001, deals with the complex problem of computer crime in the international context. Among its proposed measures, it includes the harmonization of punishable acts linked to computing that should be the subject of criminal offences in the signatory countries. The Convention establishes various groups of infractions that should be incorporated into national legislation and which it classifies into four broad categories of illicit offences. Among these, in a second group of behaviours, the Convention refers to computer crimes, which include computer-related forgery and computer-related fraud. Computer fraud (article 8) refers to the input, alteration, deletion, or suppression of computer data or any interference with the functioning of a computer system, with a view to procuring an economic benefit for oneself or for another person.

Furthermore, especially from European Union institutions, the importance of payment systems has been highlighted, which have a bearing on the criminal legislation of the Member States. In reality, the perspectives of the European Union are not strictly penal, but aim to guarantee and to stimulate economic activity, consumer protection and, to some extent, to prevent and deal with organized crime. However, through certain community measures that have an effect on domestic criminal legislation, it proposes the criminalization of certain conduct and other measures with the aim of protecting this means of payment. Thus,

[21] *Nº 948/2002 in Actualidad Penal. Nº45. 2 al 8 de diciembre de 2002, p. 3141 and following.*

[22] *Carolina Villacampa Estiarte, ' La falsificación de medios de pago distintos del efectivo en el Proyecto de Ley Orgánica de Reforma del CP de 2007: ¿respetamos las demandas armonizadoras de la Unión Europea?' , in Diario La Ley, nº 6994, 22 of July, 2008, 3 and following.*

[23] *Id Cendoj: 28079120012004200356.*

[24] *Id Cendoj: 28079120012004200586. See also on this point ATS 10-3-2004, Id Cendoj: 28079120012004200420; of 1-4-2004, Id Cendoj: 28079120012004200545, of 7-12-2004 Id Cendoj: 28079120012004202326.*

the European Union has not ceased to show concern and to adopt measures to prevent illicit acts with what it refers to as 'non-cash means of payment'.[25]

In view of the importance that is given to electronic commerce for the future economic development of the zone, various initiatives have been taken, each having a greater degree of definition and penetration. Thus, the Commission, on 16th April 1997, in a Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'A European Initiative in Electronic Commerce' COM(97)157, proposed that certain actions be defined and set in motion aiming to maximise the advantages of the new technology involved in electronic commerce. The Council also invited Member States to set up awareness-raising campaigns and training on practical improvements, and to create transparent consultation mechanisms with the aim of drawing up the legal framework and the specific actions for the promotion of this type of commerce. Finally, it called on European regulatory bodies to draw up more efficient working methods with a view to ensuring interoperability and to respond to consumer needs.

Subsequently the Communication from the Commission to the European Parliament, to the Council, to the Central European Bank and to the Economic and Social Committee on 'A Framework for action on combating fraud and counterfeiting of non-cash means of payment' was approved. The Communication approved by the Commission, on 1st July (COM (1998)395) is in response to the proposal from the Council of Europe on June 1997, in which the Commission examined the question of fraud and counterfeiting in relation to all non-cash means of payment, including electronic payments, which means it will encompass facts relating to conventional criminal activity and facts relating to the use of the new technologies.[26] The Communication proposes a two-pronged plan in the strategy to prevent and deal with fraud.

The first point is a Joint Plan of Action directed, on the one hand, at ensuring that frauds referring to all non-cash means of payment are categorised as criminal offences and made punishable through effective, proportionate and dissuasive sentences in all Member States and, on the other hand, at setting up appropriate mechanisms for cooperation that will enable the effective prosecution of the crimes. To that effect, classes of behaviour are described which are considered advisable to classify as criminal offences, whatever the means of payment might be. The following in particular are included among the offences listed: theft or the forgery of a means of payment, the possession of altered or counterfeited means of payment, the use or acceptance of a payment in full knowledge of the facts with the aid of a forged or stolen means of payment. The second point of the action plan against fraud presents various preventive measures to be studied by all interested parties (payment card schemes, issuers, card users, and competent authorities). Thus, from the standpoint of prevention, it is thought that one of the Communication's objectives is to urge operators to adopt more effective protection measures for the payment instruments that they manufacture.

The concern of Community institutions for the success of the information society, as a prerequisite for growth, competitiveness and employment opportunities, is expressed in the Communication from the Commission on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime-COM(2000) 890 FINAL. The Communication considers different initiatives with respect to a wide range of objectives that comprise part of the Information Society, which aim to improve information infrastructures as a way of preventing and dealing with computer crime. In reference to the Lisbon summit of March 2000, it underlines the importance of a transition to a competitive, dynamic, knowledge-based economy as well as to the centrality of information infrastructures in present-day economic life, on which society increasingly depends, while noting, at the same time, that these technologies may be used to commit and to facilitate criminal activities. Security measures must focus on adapting to these new forms of criminality.

This makes the ever-greater proximity of computer crime to the new categories of organized crime very clear. Associated criminality increasingly involves a greater number of offences among which computer fraud is increasingly apparent. The community institutions stated as much at the Tampere Summit, in October 1999, at which high-Tech crime was included in a list of areas in which a special effort had to be made to agree on definitions, types of offences and common sanctions. All these points are contained in recommendation 7 of the strategy of the European

[25] *On this matter, see Lafuente Sánchez, R. Los servicios financieros bancarios electrónicos, (Tirant lo Blanch 2005), 337, and Francesco Buffa, "Moneta digitale e tutele". Commercio elettronico e tutela del consumatore a cura di Giuseppe Cassano (Giuffré 2003), 178 and following.*

[26] *Lafuente Sánchez, R., Los servicios financieros bancarios electrónicos (Tirant lo Blanch 2005), 337.*

Union for the new millennium on prevention and control of organized crime, adopted by the JHA Council in March 2000.

An important impetus was given with the approval by the Commission of a Framework Decision in matters concerning non-cash means of payments. Indeed, the Framework Decision, together with other instruments of the European Union, will be greatly heeded in the reform of the Penal Code proposed in the Draft Law of 2006. In accordance with the provisions of article 34 of the Treaty on European Union (the former article K.6), the proposal was to replace the joint action proposed by the Commission in its Communication of 1 July 1998, on combating fraud and counterfeiting of non-cash means of payment with a Framework Decision. Equally, the Proposal for a Framework Decision also had as its aim the inclusion of legislative changes that have been enacted since the approval of the Communication. Thus the Council Framework Decision of 28 May 2001, relating to the fight against fraud and the counterfeiting of non-cash means of payment, is intended to complete a series of measures already adopted by the Council with the same aim. For the purposes of the Framework Decision, means of payment are considered to be all corporeal instruments except for legal tender, the specific nature of which is to allow, by itself or with another instrument, the holder or user to transfer money or a monetary value, and which is protected against counterfeiting or fraudulent use. This description precludes not only money in cash (banknotes and legal tender) but also electronic money in its strictest sense that has no material presence.

The objective of the Framework Decision continues to be that of ensuring, on the one hand, that all fraud with non-cash means of payment becomes an offence subject to effective penalties in all Member States and, on the other hand, that mechanisms are created for cooperation between Member States and between services and public or private bodies with the objective of successfully prosecuting such offences. In the Framework Decision, any fraud involving a non-cash means of payment is considered a criminal offence punishable by effective, proportionate and dissuasive sentences throughout the Member States of the Union.

With respect to the criminal conduct, the approach of the Framework Decision is to avoid resorting to categorical definitions already strictly defined in the criminal law of the Member States, because it varies by country. Thus, the Framework Decision limits itself to drawing up a list of different intentional behaviours that should be considered criminal offences throughout the Union. Different behaviours are defined according to whether they are primarily concerned with the actual instrument of payment or the counterfeiting of instruments of payment, and whether it is a question of one or more payments or of the clearing system used to execute, collect, process, or settle payment transactions. Thus, it includes:[27]

a. theft or misappropriation of an instrument of payment,

b. the alteration or counterfeiting of an instrument of payment with a view to its fraudulent use,

c. receiving, obtaining or transporting, sale or transfer to another person or possession of instruments of payment that have been misappropriated or altered or counterfeited for fraudulent use, and

d. fraudulent use of a means of payment that has been stolen, misappropriated, altered or counterfeited.

Offences that will also be subject to prosecution are those using computers to make or cause a transfer of money or monetary values that lead to unauthorized loss of property, with the intention of procuring economic benefit through the unauthorized inputting, alteration, suppression or deletion of computer data – especially personal data, or unauthorized interference in the operation of a computer system or programme. Other criminal offences include the manufacture, receipt or transfer of computer programs and other devices prepared for the commission of the former offences.

With respect to the nature of the penalties to be adopted in this field, it is envisaged that the list of conducts be categorised as criminal offences throughout the Member States. As a consequence, Member States should establish criminal penalties for these offences, according to whether they are committed by natural or by legal persons. The expression that is so well liked in EU documents reiterates that the penalties must be effective, proportionate and dissuasive. They will not necessarily imply prison terms, except for the most serious cases for which extradition can be justified. The Member States enjoy a certain leeway when defining the seriousness of an offence and the nature and severity of

[27] *Francesco Buffa, 'Moneta digitale e tutele' in Commercio elettronico e tutela del consumatore (Editor Giuseppe Cassano) (Giuffré 2003), 179-80.*

the applicable penalties.[28]

Finally, as the work of the Commission on these means of payment has continued, a further Communication was issued from the Commission.[29] The Commission considers that cooperation between all the agencies involved is a fundamental principle in order to prevent and deal with fraud in an effective manner. In fact, greater cooperation is desirable between public authorities and the private sector in the Member States. With the aim of ensuring an effective exchange of information at a European level, the Commission stated that clarification of community and national legislation in the field of data protection is needed in the area of fraud prevention.

The draft reform of the Penal Code

The economic significance of payment systems and the high volume of fraud drew the attention of the legislator to this field, and particularly the attention of the criminal legislator. Hence, the Draft Law to reform the Penal Code of 15 December, 2006,[30] is intended to amend criminal regulation of these matters. It sought to add a specific element to the field of frauds under article 248: the use of bank cards or related data. The draft law fell into abeyance as the legislative term came to an end, but parts of it may be found in the programme of criminal measures for the present legislature, and in any case, it points to the way in which possible criminal reforms may be introduced in this field.

In a general way, the Explanatory Memorandum of the draft law goes a long way to justifying its proposals on the basis of the commitments and obligations that European integration implies for the criminal justice system. Among the areas subject to community harmonisation is that of the means of payment, which lies behind the new regulation. The Explanatory Memorandum of the project points out that:

> La causa central que explica su acotado alcance ha de ser buscada fundamentalmente en los compromisos y obligaciones que la integración europea suponen para la justicia penal en toda su dimensión penal, procesal, judicial y policial. La importante vertiente del derecho penal ha venido recogiendo al paso de su aparición cuantas orientaciones comunes, plasmadas en los diferentes instrumentos jurídicos de la Unión Europea, determinaban modificaciones u adiciones al Código penal, y eso explica buena parte de las alteraciones del Código. Pero además, en los últimos años, especialmente a partir del Tratado de Ámsterdam en 1997, el llamado Tercer Pilar fortaleció la importancia de hacer efectiva la cooperación policial y judicial en materia penal, lo cual exigía necesariamente la armonización o aproximación de las leyes estatales en materia penal, y por esa razón se han ido produciendo Decisiones marco sobre un amplio catálogo de problemas penales, Decisiones que empujan a una necesaria similitud de las formulaciones de delitos y responsabilidades en los derechos internos.

The central reason that explains its highly defined scope is to be found in the commitments and obligations entailed by European integration for criminal justice in all of its dimensions, be they criminal, procedural, judicial or police related. This important vector of criminal law has brought together many common perspectives since its emergence, expressed in the different legal instruments of the European Union, which determined modifications and additions to the Penal Code, and these explain a good part of the amendments to the Code. But in addition, in recent years, especially since the Treaty of Amsterdam in 1997, the so-called Third Pillar strengthened the importance of ensuring effective police and judicial cooperation in criminal matters, which necessarily required the harmonisation or approximation of State laws on criminal matters, and for that reason Framework Decisions have been drafted in response to a wide range of criminal problems, Decisions that work towards a much-needed similarity in the formulation of offences and liabilities in domestic rights.

Committing fraud through the use of misappropriated

[28] *For an incomplete treatment of how some Member States have implemented the various EU Directives (that nevertheless runs to over 450 pages), see a paper by Stephen Mason, ' The implementation of Community regulations in national legislation: IT offences in the strict sense of the word and offences committed using IT' , prepared for a judicial seminar entitled: Investigation, Prosecution and Judgment of Information Technology Crime: Legal framework and criminal policy in the European Union, held for judges and public prosecutors specializing in dealing with cybercrime, organized within the framework of the European Judicial Training Network, (Tuesday 25 November 2008 to Friday 28 November 2008 at the Hôtel Jean de Bohême, Durbuy, Belgium), and available as a free download from http://www.stephenmason.eu/training-for-lawyers/judicial-training/.*

[29] *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment {SEC(2004) 1264} (Text with EEA relevance)/* COM/2004/0679 final */.*

[30] *http://www.congreso.es.*