

CARTÃO DE CRÉDITO E MANIPULAÇÃO DA ASSINATURA DIGITAL

CELESTE LEITE DOS SANTOS*

1 - Introdução

Há pouco mais de trinta anos a elaboração eletrônica de dados invadiu todos os setores da sociedade, provocando verdadeira revolução nos usos financeiros, comerciais e econômicos em geral.

O termo informática nasceu da fusão de informação e automática, entendendo-se como o conjunto de atividades e de noções que resguardam a representação, transmissão, transformação e elaboração automática das informações mediante cálculos eletrônicos. As transformações introduzidas pela informática resguardam hoje os diversos setores da sociedade pós-industrial.

O americano Donn B. Parker, um dos maiores especialistas em "computer crime", cogitou da possibilidade de uma "guerra informática" entre Estados, onde se pode visualizar a tentativa de danificar ou destruir os dados (arquivos ou banco de dados) nos sistemas informativos do inimigo.

As questões mais suscitadas na atualidade referem-se à segurança das informações, nas quais o tema assinatura digital e fraude dos cartões de crédito se insere, dado que o núcleo essencial é justamente a informação.

O grau de virtualidade operativa desses sistemas, ante a ausência de regulação legal, denota a necessidade de o Direito Penal intervir nos crimes informáticos, cumprindo a sua função de instrumento de defesa social que se circunscreve ao denominado "mínimo legal".

Do ponto de vista jurídico, há a necessidade de segurança técnica dos dados, havendo uma tendência à uniformização das legislações dos distintos Estados.

O pano de fundo dessa problemática é a segurança informática, dada a escassa propensão das empresas em investir nesse setor. Por segurança informática deve-se entender todas as medidas e técnicas necessárias para proteger o *hardware*, o *software* e os dados dos acessos não autorizados (intencionais ou não), para garantir a privacidade de eventuais usos ilícitos como a divulgação, modificação ou destruição. A segurança informática se estende à elaboração mesma dos programas de dados e dos arquivos.

Falar em segurança do sistema informativo implica necessariamente em três níveis:

*Advogada, Doutora em Direito pela FADUSP, Especialista em Direito Penal Econômico pela Universidade de Coimbra, Professora das Faculdades Integradas Anchieta e do Curso de Extensão do COGEAE (PUC-SP).

- a) *físico* – isto é, salvaguarda de destruição do centro EDP e de tudo o que interessa à elaboração dos dados;
- b) *lógico* – realizada principalmente via *software*;
- c) *legal* – ou pelo menos controle dos tipos legais.

2 - Direito Econômico

Trata-se de concepção jurídica de caráter político, que subordina as instituições à organização econômica imposta pelo Estado.

O direito econômico não é um ramo do direito caracterizado por seu sujeito, objeto ou características especiais, senão uma transformação dos princípios inspiradores de todo o direito patrimonial a impulsos de um movimento que, frente à ideologia do último século, sobrepõe o coletivo ao individual e o público ao privado¹.

O Direito Econômico é concebido hoje como o conceito normativo que tem por objeto delimitar, preservar e proteger a “ordem pública econômica”, as diretrizes fundamentais dentro das quais devem decorrer as relações e transações de caráter econômico².

2.1. Ordem Pública Econômica

É o conjunto de normas imperativas que se referem à organização econômica do Estado, devendo ser observadas pelas pessoas privadas no exercício de suas atividades econômicas.

Do conceito acima explicitado apreende-se que a organização econômica é a expressão jurídica da ordem econômica fundamental de uma sociedade determinada. No caso da República Federativa do Brasil, adotou-se o *modelo econômico constitucional*³. Desse modo, a Carta Magna disciplina a matéria no Título VII – “Da Ordem Econômica e Financeira”, Capítulo I – “Dos Princípios Gerais da Atividade Econômica”, a matéria nos arts. 170/181.

A opção política do legislador brasileiro está inserta no art. 170 da Constituição Federal, *in verbis*:

Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:

- I – soberania nacional;
- II – propriedade privada;

¹ RUBIO. *Sobre el concepto de Derecho Mercantil*. vol. IV, p. 353.

² HERRERO, Cesar. *Los Delitos Economicos – Perspectiva Jurídica e Criminologica*, p. 33.

³ Preleciona Herrero, C., op. cit., p. 34: “Nos Estados de Direito, estas diretrizes podem estar estabelecidas na Constituição. Nesse sentido, pois, o Direito Econômico teria por objeto o modelo econômico constitucional”.

III – função social da propriedade;
IV – livre concorrência;
V – defesa do consumidor;
VI – defesa do meio ambiente;
VII – redução das desigualdades regionais e sociais;
VIII – busca do pleno emprego;
IX – tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham a sua sede e administração do país.

Parágrafo único. É assegurado a todos o livre exercício de qualquer atividade econômica, independentemente de autorização dos órgãos públicos, salvo nos casos previstos em lei.

2.2. Direito Penal Econômico

As normas econômicas possuem natureza jurídica diversa, destacando-se:
a) as de caráter administrativo não sancionador – planificação imperativa da economia nacional (Novoa Monreal, 1978);

b) as revestidas de obrigatoriedade em que sua não observância (ilícito administrativo) tem por conseqüência a imposição de sanções de índole administrativa;

c) as que culminam ao seu descumprimento em efeitos puramente punitivos. Este grupo de dispositivos legais constitui o denominado Direito Penal Econômico.

O Direito Penal, entendido como instrumento de defesa social, possui relevância jurídica e social no caso de comprovada inutilidade ou insuficiência de outras sanções.

Desde esse ponto de vista fala-se no princípio da “mínima suficiência”, que se expressa na filosofia jurídica dizendo que o conteúdo da ordem é um fim essencial da comunidade, o que pode acarretar, para sua consecução, graves restrições da liberdade pessoal dos cidadãos; também, por isso, há de praticar-se, unicamente, nos limites do estritamente indispensável, porque a liberdade pessoal tem que ser tutelada como um bem jurídico em si⁴.

Jorge de Figueiredo Dias esclarece:

O lugar da liberdade vem a cobrir-se com a mais radical e originária das realidades: o existir humano; com que se abre à sua investigação um novo campo de possibilidades (para onde, de resto, apontam já quase todas as considerações críticas anteriores): o de a essência da liberdade se cobrir com a peculiaridade irredutível do ser-homem, o de constituir ela, afinal, a originalidade de um modo de ser próprio que, como fundamento oculto, se exprime no homem e na sua obra⁵.

⁴ E. Fortuna. *Manuale di Diritto Penale dell'Economia*, p. 3.

⁵ *Liberdade, Culpa, Direito Penal*, p. 136.

Nessa linha de raciocínio, Klaus Tiedmann preconiza:

É certo que, em muitos sistemas, é mais propriamente a legislação civil e administrativa que se encontram, e muito justamente, em primeiro plano na luta contra a delinquência econômica. Isto é particularmente certo no que afeta a proteção dos consumidores. O direito penal não cumpre, pois, nesta esfera, mais que uma função subsidiária em relação com o direito econômico, o direito comercial ou financeiro. Constitui tão somente a “ultima ratio” reservada aos atos mais graves contra a regulação da vida econômica. Ao mesmo tempo, devido a limitar-se a proteger os valores e interesses fundamentais de uma sociedade determinada, o direito penal reflete, de forma quase negativa, estes valores fundamentais e dirige a opinião pública até a finalidade de criar ou manter certas regras mínimas nas relações e transações econômicas⁶.

Apesar do número e da duração de esforços científicos no direito penal, na criminologia e na política criminal no âmbito das empresas e da vida econômica, os conceitos e os princípios essenciais do direito penal econômico e empresarial não são tão claros no direito comparado. Uma das razões poderia ser o fato de que a maior parte das recentes reuniões científicas sobre o tema tem dirigido seu interesse sobretudo aos problemas criminológicos, a causa de inegável importância atual desses problemas, olvidados durante muito tempo pela criminologia tradicional. (...) Não obstante essas divergências conceituais e terminológicas, o tema do colóquio não deverá em nenhum caso restringir-se aos delitos e contravenções cometidos com ajuda de uma empresa (“corporate crime”). Deverá compreender também os delitos cometidos por particulares contra a ordem econômica (incluindo-se a legislação financeira e social). E, assim mesmo, aqueles atos que pretendem desde sua origem uma finalidade delitativa de conteúdo econômico (“crime as business”). A existência de uma afinidade com o crime organizado não deve impedir o estudo desta parcela particularmente perigosa da criminalidade econômica⁷.

2.3. Conceito de crime econômico

É a infração jurídico-penal que lesa ou põe em perigo a ordem econômica. O conceito de ordem econômica, conforme foi exposto acima, pode variar de acordo com a opção política adotada pelo legislador nos diversos ordenamentos jurídicos.

2.4. Crimes econômicos praticados através das novas tecnologias de informação⁸

⁶ *Concepto y principios del Derecho Penal Económico – incluida a protección aos consumidores*. Boletim de Informação do Ministério da Justiça da Espanha, n. 248-250 (1981), p. 119.

⁷ Cfr. Klaus Tiedmann, op. cit., p. 118-119.

⁸ Cfr. Carlos M. Romeo Casabona. *La reforma penal ante as novas tecnologias de información*. in: *Informática e Diritto*, 3 (1987), p. 115-118.

Poder-se-ia apontar como crimes econômicos dessa natureza:

a) *fraude informática* – consiste na manipulação de dados informáticos que conduz, na realidade, a uma fraude;

A manipulação da assinatura digital se insere dentro dessa modalidade. Através desse expediente permite-se o conhecimento do número do cartão de crédito, identificação da pessoa signatária, obtenção do número do banco, etc.

b) *espionagem informática* – trata-se de hipótese de “pirataria de programas”;

Apenas a título de ilustração, cumpre ressaltar que existem dois códigos básicos que compõem o programa:

1) *código fonte* – conjunto de fórmulas matemáticas compreensíveis pela mente humana;

2) *código máquina* (ou código objeto) – tradução da linguagem do código fonte para a “linguagem da máquina” de modo que essa se torne operativa.

A pirataria de programas implica na reprodução do código objeto (ou código máquina). Quando visa tão somente decifrar o código fonte, modificando-o, ou não, configura a espionagem informática.

c) *sabotagem informática* – consiste na destruição de programas inteiros; Trata-se da atividade de “hacking” (penetração não autorizada nos sistemas informáticos) e sobretudo da difusão de vírus.

d) *utilização espontânea de computadores alheios*.

Nesta seara, preocupante é a crescente infidelidade dos adeptos do sistema informativo.

Diante desses comportamentos ilícitos, a utilização de preceitos do direito penal tradicional (furto, roubo, fraude, falsificação documental, danos, etc.) é inadequada e objetada pelos doutrinadores, dada a incidência do princípio da legalidade (*nullum crimen sine lege*).

3 - Crimes informáticos e direito legislado

Duas são as técnicas legislativas utilizadas na tipificação dos crimes informáticos: a) objetiva – baseia-se pelo critério do bem jurídico tutelado; b) subjetiva – norteia-se pelo critério da conduta do agente.

3.1. Dinamarca

A Lei nº 284 de 6 de junho de 1984 sobre cartões de crédito, disciplina os sistemas de pagamento com cartão, assim como sistemas de pagamento análogos.

O referido diploma legal determina a aplicação do princípio da subsidiariedade

expressa de seus preceitos. Apreende-se a referida peculiaridade a partir da dicção do legislador, que incluiu normas penais que prevêm penas e interdições nos casos de utilização fraudulenta, porém ressalvando a possibilidade de sua aplicação se outra lei possuir sanção maior.

A Lei nº 229 de 6 de junho de 1985 modificou os arts. 193, 263 e 279 do seu Código Penal, prevendo a hipótese de impedimento ao bom funcionamento dos computadores, o acesso ilegal às informações e aos programas informáticos.

3.2. Estados Unidos da América

a) A primeira lei penal sobre informática foi a *Counterfeit Access Device And Computer Fraud and Abuse*, sendo integrada e substituída em 1996 pela *Computer Fraud and Abuse Act*, publicada em 6 de outubro de 1996 (*Public law 99-474*);

b) Lei federal sobre fraude em cartões de crédito, de 12 de outubro de 1984⁹. Estabelece penas severas no tocante a utilização fraudulenta e falsificação de cartões;

Após a adoção da *Credit Card Fraud Act*, houve uma redução de 50% concretamente entre 1985 e 1986, relativa a perdas por fraude nos cartões de crédito.

c) Lei federal sobre veracidade nas operações de empréstimo¹⁰ - entrou em vigor em 1969 e foi modificada em 1970, 1974 e 1976. Tem por objeto proteger os consumidores nas operações de crédito. Nas seções 12 e 14 regula a emissão e utilização dos cartões de crédito, e também sanciona a utilização ilegal ou fraudulenta de cartões.

3.3. Portugal

A Lei nº. 109 de 17 de agosto de 1991 disciplinou o falso informático, a sabotagem informática, o acesso não autorizado, a interceptação ilegal das comunicações no âmbito dos sistemas informáticos.

3.3. França

A Lei nº 19/88 estabelece o crime de falsificação de documentos informatizados. Todavia, no tocante aos desvios na utilização dos cartões de créditos, nada dispôs.

Em sede de criminalidade informática, a Lei nº 6619 de 5 de fevereiro de 1988 introduziu o novo Capítulo III do Título II do Livro IV do código penal, intitulado

⁹ *Credit Card Fraud Act of 1984 (18 USCS § 1029 [1996])*.

¹⁰ *Truth in Lending Act or Consumer Credit Protection Act of 1968*.

“Algumas infrações em matéria informática”. Assim, foram introduzidos os arts. 462.7 e 462.8 no referido diploma legal.

O primeiro se reveste de particular importância ao punir a *tentativa* para os delitos informáticos previstos nos arts. 462.1, 462.3, 462.4, 462.5 e 462.6 com as mesmas penas previstas para o crime consumado.

O art. 462.8 prevê a participação de uma “associação” formada (ou um acordo estabelecido) com a finalidade de preparar e concretizar um ou mais falsos materiais, de uma ou mais das infrações previstas nos artigos precedentes, e pune com a mesma pena prevista para a infração mesma, ou, no caso de concurso de crimes, com a pena estabelecida para a mais grave das infrações.

3.4. Alemanha

O parágrafo 263 do Código Penal, introduzido pela Lei de 15 de maio de 1986, prevê a figura da “manipulação de computadores”. A referida figura delitiva integra a “utilização não autorizada de dados”, concebida como “modalidade autônoma da ação, destinada a influenciar o resultado de um processo de elaboração eletrônica de dados”.

Hipóteses como reprodução ilícita da senha do cartão de crédito ou outros abusos levados a cabo com cartão magnético roubado ou falsificado encontrariam adequação típica no referido dispositivo.

No tocante aos crimes informáticos em geral, existe uma normativa detalhada e completa. Trata-se, em particular, de uma seção da Segunda Lei relativa à criminalidade econômica, aprovada em 15 de maio de 1996.

A lei em questão prevê hipóteses de espionagem de dados, da falsificação de dados dotados de valor probatório, da alteração dos dados e da sabotagem informática.

3.5. Reino Unido

No tocante ao uso fraudulento de cartões de pagamento se aplica a lei sobre falsificações de 27 de julho de 1981¹¹.

Aplica-se, ainda, a lei sobre prova penal de 1984¹².

Na Inglaterra, o *Computer Misuse Act*, aprovado em 20 de junho de 1990, prevê o acesso não autorizado puro e simples ao material informático com o fim de cometer ou agilizar o cometimento de um futuro crime e a modificação não autorizada no conteúdo de um computador. Com base nesse diploma legal um médico inglês difamado na *Internet* foi ressarcido pelo provedor com a soma de 600 milhões de libras.

¹¹ *The 1981 Forgery and Counterfeiting Act of 1981.*

¹² *The Police and Criminal Evidence Act of 1984.*

3.6. Itália

Em 1990 é publicada a Lei 23 de dezembro de 1993. Possui seu antecedente histórico na Comissão denominada do ministro Vassali de 1989, que adotou o modelo “evolutivo” no tocante aos crimes informáticos. Por esse modelo, modificaram-se as normas já existentes no código penal, estendendo o significado de modo a incluir novos crimes informáticos.

3.7. Suíça

Introduziu em 1996 modificações no seu sistema penal com a finalidade de assegurar uma proteção contra atos encontrados no âmbito da criminalidade informática. Esta lei entrou em vigor em 10 de julho de 1996, modificando-se também dois artigos do Código Penal. Em particular, o crime de fraude informática, estabelecendo : *quem, fornecendo informações não corretas ou incompletas, alterando um programa ou um registro ou modificando, de qualquer outro modo e sem autorização, o resultado de um processo de informação autorizado, de tal modo obtém uma vantagem para si ou ocasiona uma perda para outros sujeitos* (norma inserta na seção 1 do capítulo 9 do Código Penal suíço).

3.8. Grécia

A Lei nº 1800 de 30 de agosto de 1988 introduziu algumas modificações no Código Penal, ao equipar os documentos escritos aos dados contidos na elaboração de documentos eletrônicos, dispondo sobre a “fraude informática”. O tipo penal refere-se à divulgação ilícita dos dados ou programas que contêm dados estatais, científicos ou profissionais ou sigilosos. O referido diploma normativo considera como dados sigilosos aqueles retidos por um sujeito por motivo justificado.

3.9.1. Conselho da Europa

Em 1989 foram elaborada uma lista mínima e uma lista facultativa a serem adotadas pelos países membros da Comunidade Européia na prevenção e repressão dos crimes informáticos:

A) Lista mínima

- a) fraude informática;
- b) falso informático;
- c) dano dos dados ou programas informáticos;

d) acesso abusivo a um sistema ou rede informática;
e) interceptação abusiva de comunicações;
f) reprodução abusiva de programas informáticos protegidos pela lei;
g) reprodução não autorizada de uma topografia (isto é, do circuito de um microprocessador n. d. r.).

B) Lista facultativa

a) alteração dos dados ou programas informáticos;
b) espionagem informática;
c) utilização não autorizada de um computador;
d) utilização não autorizada de programas informáticos protegidos pela lei.

4 - Cartão de crédito

4.1. Conceito

O cartão de crédito é um documento nominativo legitimante, intransferível, cuja finalidade é permitir ao usuário beneficiar-se com as finalidades de pagamento pactuadas com o emissor e as resultantes do contrato celebrado entre este e o provedor do bem ou serviço requerido por aquele¹³.

O cartão de crédito é emitido em favor do usuário, e é o documento indispensável para executar o rol de direitos que surgem da relação trilateral conformadora sobre a base da celebração dos contratos: a) entre a emissora com a pessoa a quem se lhe entrega; b) entre a emissora e o comerciante¹⁴.

4.2. Uso criminoso do cartão de crédito

Geralmente, o uso delitivo do cartão de crédito é efetuado por terceiros não intervenientes na relação jurídica. Sem embargo, existem hipóteses de convivência tanto de titulares como de proprietários de estabelecimentos aceitantes e/ou empregados dos mesmos, como dos próprios emissores, não pessoalmente, senão sempre em virtude da infidelidade de seus empregados ou colaboradores.

A) Hipóteses de uso abusivo pelo titular¹⁵:

a) configura-se o delito de fraude a obtenção de cartão de crédito com o propósito de realizar compras por um montante que excederia a possibilidade de

¹³ FARINA, Juan M. *Contratos Comerciais Modernos*, p. 601.

¹⁴ Idem, *ibidem*, p. 601.

¹⁵ Amadeo, CNCRimCorr, sala VI, 31/7/85, *in*: *Tarjeta de Crédito*. JA, 1987-IV-1059 e ss.

pagamento;

b) existe um ardil inicial, que permite a realização do aproveitamento patrimonial mediante a utilização do cartão de crédito muito acima do permitido, se o certificado apresentado era o suficiente equívoco como a induzir a um decisivo erro sobre o saldo regular e de um bom nível;

c) a adulteração do cartão de crédito, para ocultar sua caducidade aos comerciantes do local em que se adquire mercadoria, configura uso de documento privado adulterado em concurso ideal com fraude.

B) Conduta do comerciante¹⁶

Comete o crime de fraude mediante uso de documento privado falso (arts. 172 e 292, Código Penal Espanhol) o comerciante que falsifica formulários de crédito fazendo figurar uma compra inexistente e inserindo os dados dos titulares de cartões de crédito, e os negocia por um preço inferior ao que figura neles¹⁷.

C) Conduta de terceiros

O cartão pode funcionar como forma de realização direta do crime ou como meio para a realização da atividade delitiva. Em qualquer caso estaremos diante de delitos patrimoniais.

Poder-se-iam apontar como hipóteses de uso criminoso do cartão de crédito, independentemente da qualificação penal dos mesmos:

a) meio de pagamento de coisas ou serviços em estabelecimentos públicos;

b) sacar dinheiro da conta vinculada ao cartão, através de caixas automáticos, etc.

O apoderamento de fato do cartão de crédito pode ser considerado pelo direito penal tradicional como furto, fraude ou apropriação indébita, segundo a modalidade comissiva. A regra do concurso de crimes (art. 69 a 71 do Código Penal Brasileiro) pode ser aplicada quando essa atividade punível por si só encerra outra ação constitutiva do crime, como a extração de dinheiro de um caixa automático, com cartão indevidamente possuído pelo sujeito.

A diversidade de funções que hoje se assinalam aos cartões nas relações normais do comércio (instrumentos de pagamento, instrumentos de crédito, instrumentos de garantia, instrumentos de acreditação, etc.) dá idéia do complexo elen-

¹⁶ Idem ibidem, pp. 1059 e ss.

¹⁷ No Brasil, a conduta configura o crime de uso de documento falso (art. 304 do Código Penal) em concurso com o crime de falsidade ideológica (art. 299 do Código Penal). Todavia o crime-meio (falsificação) restaria absorvido pelo crime-fim (uso de documento falso), porém há entendimentos doutrinários divergentes a respeito. Cumpre ressaltar que as condutas supra-citadas estão dispostas no Título X – “ Dos Crimes Contra a Fé Pública” de nosso diploma punitivo.

co de possíveis condutas ilícitas e abusivas relacionadas com as mesmas.

Todavia, o uso do cartão de crédito com **manipulação do sistema ou rede de comunicações** escapa do mero uso do mesmo. O cartão é utilizado fraudulentamente, porém neste caso não é o objeto principal do delito, mas apenas um meio posterior ou anterior àquele, idôneo para desfrutar do ato delitivo.

Trata-se de hipótese de **fraude informática**, segundo qualificação da doutrina penal moderna.

5 - Assinatura digital

A assinatura digital é elemento desconhecido no Direito: firma fotostática, mecânica. Trata-se de evolução dos meios através dos quais se emitem vontade e promessas.

Cumpra a mesma função das firmas (assinaturas) manuais. É de se ressaltar que nos ordenamentos jurídicos, os Códigos Civis ou Comerciais, via de regra, não possuem um capítulo dedicado à firma manual. De outra parte, o art. 225 do Novo Código Civil atribui valor probatório pleno à assinatura digital, na hipótese de ausência de impugnação pela parte a quem for exibido o documento.

A assinatura digital vem sendo utilizada há vinte anos sem expressa previsão legislativa. A esse respeito preleciona José Henrique Barbosa Moreira Lima Neto:

Concluindo, não restam dúvidas que ainda que sem um disciplinamento específico, como ocorre com os cartões de crédito, o meio eletrônico vem legitimado por um uso reiterado. O emprego do meio eletrônico em atividades comerciais, por exemplo, através de práticas repetidas, deverá transformá-lo em verdadeiro uso comercial.¹⁸

A firma digital pode ser utilizada em entornos fechados ou abertos (*internet*). No primeiro caso, a mensagem de dados circula por um entorno que utiliza os sistemas SWIFT, BOLERO, EDI. No segundo caso, embora atribua-se as mesmas funções, esta possui faces distintas, podendo ser inserir no contexto de um negócio jurídico celebrado entre empresários (B2B) ou entre empresário e consumidor (B2C).

Quando a firma digital é utilizada entre empresários, o objeto jurídico protegido não é propriamente o conteúdo, mas a segurança de que a mensagem não se perca nem se altere durante o percurso, pois as partes são previamente conhecidas (EDI).

A principal função da assinatura é a atribuição da mensagem de dados de quem está celebrando o contrato, pois as pessoas não se conhecem. A relevância

¹⁸ José Henrique Barbosa Moreira Lima Neto, *Aspectos jurídicos do documento eletrônico*, p. 8. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1780>. Acesso em 18 de março de 2003.

da identificação e atribuição no comércio eletrônico é dada por uma função de segurança. Busca-se em primeiro lugar a identificação das partes (essa ênfase não é necessária no entorno fechado, pois as partes já se conhecem). Na hipótese de relações de consumo, o uso do cartão de crédito com sua senha satisfaz a segurança da mensagem durante o trajeto. A assinatura serve para assegurar as partes que estão celebrando o contrato, pois estas não se conhecem (v. g., um cliente que compra uma máquina fotográfica busca qual o vendedor eletrônico que oferece o melhor preço).

A assinatura eletrônica equivale funcionalmente à assinatura manual, sendo largamente utilizada no comércio eletrônico.

Cerca de quinze países já disciplinaram a firma eletrônica, excluindo do princípio da equivalência funcional: negócios jurídicos de imóveis; família e filiação; a atividade do notário (a assinatura eletrônica nunca equivale funcionalmente à assinatura manual do notário).

A segurança que a assinatura digital pretende proporcionar é antes de tudo jurídica, visando ao seu reconhecimento nos tribunais. Todavia, para a obtenção desse efeito deve ser efetuada através de uma tecnologia compatível, ou seja, aquela que não seja facilmente “burlável” ou “pirateável”.

Destarte, sempre existe um elemento de insegurança jurídica presente nessa relação dada a possibilidade de ser interceptada, lida, modificada no mundo da *internet*. *Mutatis mutandis*, a assinatura manual pode ser falsificada. Nesse ínterim, resta ao Direito Penal, no exercício de sua função de mínimo vital, tipificar a matéria.

O próximo passo desses instrumentos é a utilização da senha (número de identificação pessoal, PIN). Trata-se de instrumento que oferece maior segurança em relação à mensagem de dados firmada eletronicamente. Porém, é facilmente vulnerável, embora seja mais segura que a assinatura digital ou e-mail. Pode ser utilizado através do sistema da chave única ou dupla chave (do emissor da mensagem e do destinatário da mensagem, podendo ser pública ou privada).

Na chave única (sistema simétrico) o destinatário aplica a chave do signatário e a mensagem é decifrada. O referido mecanismo é composto por cerca de 120 dígitos, sendo que uma máquina mais potente leva dias para decifrá-los. O inconveniente é a necessidade do envio da mesma de forma separada para cada destinatário. A possibilidade de um terceiro não autorizado ter acesso à mesma é considerável.

A tecnologia dominante é a da chave dupla (sistema assimétrico). Há uma chave para fechar a mensagem e outra para abri-la. A chave da assinatura é privada do signatário. A chave pública é transmitida ao destinatário da mensagem de dados.

A chave pública ampara-se em um certificado de assinatura pelos prestadores de serviço de certificação (ou autoridade de certificação – nos países em que a matéria foi disciplinada; porém não são autoridades públicas).

O prestador de serviço de certificação administra a chave pública e a chave privada, ou seja, possui um repertório público das chaves públicas de seus clientes. Caso a chave pública não coincida com a chave privada, a mensagem não se abre.

Desse modo, a assinatura não é uma identificação aposta no final do documento, mas uma combinação de dígitos única e irrepetível.

Pode-se apontar ainda as hipóteses de biometria ou assinatura biométrica: se baseia em caracteres biológicos do destinatário, suscetível de identificação (v. g. , íris do olho, impressão digital, odor, etc). A assinatura biométrica significa aplicar os caracteres biométricos a mensagem de dados. O único inconveniente desse método é o de que não é passível de reposição, como se faz com outras chaves.

5.1. Formas de acesso ao PIN contra a vontade do titular

a) obtenção do escrito onde o titular o tenha anotado, seja por roubo, furto do mesmo, cópia, etc.;

b) comunicação oral mediante engano do agente do crime, que chama o titular fazendo-se passar por empregado do emissor, que precisa do PIN para confeccionar um novo cartão para o titular, a quem acaba de subtrair o cartão;

c) manipulação do sistema, especialmente da memória do computador ao qual está conectado o próprio caixa automático, por exemplo, obtendo mediante analisadores a decodificação dos dados durante a sua transmissão pela rede;

d) comunicação a um empregado do emissor para que colabore com o ato criminoso, etc.

5.2. Funções da assinatura eletrônica

a) *autenticação* – consiste na identificação e atribuição da mensagem de dados, bem como a informação contida nela.

Implica na identificação do destinatário e atribuição do conteúdo da mensagem, de forma que não possa ser repudiada pelo signatário.

É o mesmo efeito que cumpre a firma autógrafa.

Trata-se de função relativa, pois é feita por semelhança.

b) *privacidade*

A assinatura digital permite decodificar a mensagem, o nome e outros dados do assinante.

Através desse expediente impede-se o conhecimento dos dados que circulam decodificados (criptografados) no entorno aberto, impossibilitando o acesso ao número do cartão de crédito, à identificação da pessoa e do banco.

c) *integridade*

A tecnologia utilizada pela assinatura digital deve explicitar qualquer abertura ou alteração na mensagem de dados firmados entre signatário e destinatário.

A lei européia exige que as três condições acima sejam satisfeitas pelas assinaturas avançadas.

5.3. Manipulação da assinatura eletrônica

Ao obter uma determinada assinatura digital através da manipulação do sistema ou rede de comunicações, o agente obtém todas as informações necessárias para a consecução de posteriores fraudes de cartão de crédito. Desse modo, o cartão de crédito utilizado fraudulentamente não é o objeto principal do delito, mas apenas um meio posterior àquele.

É de se ressaltar que o acesso aos dados que compõem a assinatura digital não é um acesso físico, mas eletrônico ou telemático.

Procurou-se fazer uma descrição hipotética do crime de manipulação de firma eletrônica¹⁹.

5.3.1. Sujeito ativo

a) entornos fechados (EDI) – parte interveniente na relação jurídica.

b) entornos abertos (*internet*) – qualquer pessoa.

5.3.2. Sujeito passivo

a) entornos fechados (EDI) – parte interveniente na relação jurídica.

Em outros termos, o empresário que tenha relações comerciais com outro empresário conhecido (sistema B2B).

b) entornos abertos (*internet*) – qualquer pessoa.

5.3.3. Objeto material

O objeto material dos crimes informáticos *latu sensu* é o denominado bem informático. Trata-se de bem incorpóreo com características de direito real, ou seja, de inerência do direito bem que representa o objeto, de *jus in re propria*. Apresenta-

¹⁹ Já que não se encontra tipificação legal específica em nossa legislação pátria. Já se ressaltou a inadequação do uso das figuras penais tradicionais, dado que o mesmo ofende o princípio da legalidade (*nullum crimen, nulla poena sine lege*).

se também como defesa dos direitos garantidos na Constituição da República Federativa do Brasil.

O tema está inserto na Constituição portuguesa de 1976 de forma expressa no art. 35 e na Constituição espanhola de 1978 nos arts. 18 e 105.

No crime de fraude de firma eletrônica aposta na utilização de um cartão de crédito na formação de um contrato, o objeto material não é o cartão de crédito (cartão de plástico ou dinheiro de plástico como denominam os autores), mas a **informação** contida nele. Em outros termos, o objeto material do delito são os dados que se traduzem na denominada firma digital, qualquer que seja a tecnologia empregada.

5.3.4. Objeto jurídico

O objeto jurídico é a segurança das informações nas relações econômicas.

6 - Conclusão

A proteção das informações que circulam no meio eletrônico é um bem digno de tutela penal, no exercício de sua função de “mínimo vital”.

A inadequação dos dispositivos penais vigentes frente a essa nova forma de criminalidade (“computer crime”) conduz à reflexão. Uma suposta adequação típica do crime de assinatura eletrônica com os crimes de falsificação previstos no Título X – “Dos Crimes Contra A Fé Pública” do Código Penal Brasileiro implicaria em uma afronta ao princípio da legalidade.

7 - Bibliografia

ANIYAR DE CASTRO, L. *Criminología de la reacción social*. Maracaibo, Instit. de Criminología de la Facultad de Derecho de la Universidad de Zulia, 1977.

BARCELÓ, Rosa Julia. *Comercio electrónico entre empresarios. La formación y prueba del contrato electrónico (EDI)*. Valencia, Tirant lo blanch, 2000.

BERISTAIN, A. & NEUMAN, E. *Criminología y dignidad humana (Diálogos)*. Buenos Aires, Edit. Depalma, 1989.

CALARA, María del Carmen Geta-Alonso y. *El pago mediante tarjetas de credito*. Madrid, Lasuy, 1990.

DIAS, Jorge de Figueiredo. *Liberdade, Culpa, Direito Penal*. Coimbra, Coimbra Editora LTDA, 2ª ed., s/d.

DOLAN, John F. *Secured Transactions and Payment Systems*. Boston, Little Company, 1995.

FARINA, Juan M. *Contratos comerciais modernos*. Buenos Aires, Astrea de Alfredo y Ricardo Depalma, 1997.

FORTUNA, E. *Manuale di Diritto Penale dell'Economia*. Padova, Casa Editrice Dott. Antonio Milani, 1988.

FRANCO, Alberto Silva. *Crimes Hediondos*. São Paulo, Revista dos Tribunais, 4ª ed., 2000.

GAWALDA, Cristian. *Les Cartes De Paiment Et De Crédit*. Paris, Éditions Dalloz, 1994.

HERRERO, Cesar Herrero. *Los Delitos Economicos – Perspectiva Juridica e Criminologica*. Madrid, Secretaria General Técnica. Ministerio do Interior. Subdirección General de Estudios, 1992.

LAURET, B. Y. Gauthier. *Droit Pénal des affaires*. Paris, Ed. Económica, 1990.

LOZANO, Pablo Luiz Nuñez. *La Tarjeta De Credito*. Madrid, Consejo Economico e Social, 1997.

ZAGAMI, Raimondo. *Firma Digitale E Sicurezza Giuridica*. Verona, Casa Editrice Dott. Antonio Milani, 2000.