CRIMINALIDADE POR COMPUTADOR NA R. F. A.

Pelo Dr. Juiz de Direito
Álvaro de Vilhena de Oliveira e Silva

SUMARIO

1 — INTRODUÇÃO

O desenvolvimento de novas tecnologias contribuiu para o aparecimento de uma nova forma de criminalidade económica. Assim como o aumento de tráfego rodoviário levou o Direito Penal a ter de enfrentar novos problemas, também a introdução e o incremento do uso de computadores na Indústria, Economia, Administração Pública, e sobretudo nas Instituições Bancárias e Companhias de Seguros, veio proporcionar — ao lado de racionalização e progresso — uma oportunidade e simultaneamente um meio para a prática de novos delitos penais.

É assim que surge a Criminalidade por Computador, independentemente do sistema económico-político, porquanto a tendência é para esse tipo de criminalidade aparecer em toda a parte onde forem instalados computadores.

De âmbito adjacente à Criminalidade Económica e de grande interesse nos nossos dias é a actual problemática da utilização por estranhos de máquinas automáticas de pagamento, bem como o extravio e subsequente falsificação e utilização indevida de cartões codificados de crédito, sobretudo em países como os E.U.A., o Japão, a França e a R.F.A.

Ao lado do estudo das causas, montante dos prejuízos, e «milieu» deste complexo campo de criminalidade, devem ser especialmente tratados também os problemas jurídicos respeitantes à própria Criminalidade por Computador, nomeadamente quanto à utilização, por pessoas não autorizadas, de máquinas automáticas de pagamento (Bankomaten).

Trata-se de questões jurídico-penais mas também jurídico-civis pelo que há necessidade de serem discutidas não só a

nível nacional como também a nível internacional a fim de se poder levar a cabo uma reforma das normas legais vigentes.

1.1. CONCEITO DE CRIMINALIDADE POR COMPUTADOR

O conceito de criminalidade por computador abarca todos os comportamentos ilegais penalmente puníveis, que emergem dum processamento automático de dados, ou socialmente prejudiciais pela ilicitude cível em que caem. Isto prende-se, obviamente, com o problema da ameaça da esfera privada dos cidadãos no caso de utilização abusiva de informática. Não obstante isto, nos países mais industrializados a protecção de dados encontra-se legalmente regulamentada havendo sanções para punir tais infracções.

Este tipo de criminalidade atingiu nos últimos anos uma grande extensão a que não é alheio o facto de tanto o programador como o utilizador do computador terem descurado em grande medida o aspecto da segurança.

É sobretudo na actividade bancária que a utilização de computadores se encontra mais desenvolvida, razão porque os riscos de aumento de Criminalidade Económica seriam enormes se se pusesse em prática um serviço de pagamentos sem comprovativos.

Não há ainda uma estatística sobre este tipo de criminalidade porque a Banca tem uma certa relutância em denunciar este tipo de delitos, porquanto a publicidade que se desse dos mesmos, poderia acarretar-lhes a perda da sua boa reputação por um lado, e, por outro lado, a reparação de prejuízos sofridos nem sempre se consegue, mesmo nos casos em que o delinquente é condenado.

1.2. FORMAS DE CRIMINALIDADE POR COMPUTADOR

Excluindo a falsificação de balanços e outros delitos fiscais, pode afirmar-se que dentre os casos até agora conhecidos

há que distinguir quatro grupos de delitos económicos cometidos através de computador.

1.2.1. *As manipulações*

No primeiro plano de uma Criminologia por Computador encontram-se as «Manipulações» que se podem relacionar tanto com a entrada de dados no computador, como com a programação para processamento desses dados.

A manipulação da entrada dos dados no computador bem como a manipulação da saída desses dados é designada por «Manipulação-Input» e «Manipulação-Output», respectivamente.

As falsificações na fase de programação são realizadas na forma de «Manipulações de Programa» e as falsificações na fase de operação, designam-se «Manipulações de Consola».

Vejamos agora um exemplo de «Manipulação-Input». Ficou célebre o caso de um funcionário encarregado do processamento do abono de família numa Repartição da Baviera (R.F.A.). Por meio da utilização abusiva da senha dum outro funcionário, enviou indevidamente suplementos de abano de família — num montante entre 5000 e 10 000 D.M. — para várias contas suas, bem como para contas de familiares.

Como exemplo de «manipulação de Programa» pode dar-se o de um programador numa sociedade anónima alemã. Com o auxílio dum programa especialmente preparado, incluía dados relativos ao vencimento de pessoas fictícias, devendo tais vencimentos ser transferidos posteriormente para a sua própria conta.

Os sistemas de programação de dados à distância, que têm vindo a aumentar de importância nos últimos anos, são uma variante especialmente interessante e cheia de sucesso das técnicas de manipulação a que se vem aludindo: o computador está ligado através da rede telefónica ou de energia eléctrica ao programador de dados de modo que o delinquente pode realizar as suas manipulações em sua casa com o seu próprio terminal sem ter necessidade de se introduzir na empresa lesada.

Como exemplo típico dum caso destes, conta-se o de um estudante americano que, nos anos 70, por meio de ligação à rede telefónica pública, alcançou o computador da «Central Pacific Telephon Corporation» conseguindo que lhe fossem fornecidas gratuitamente mercadorias no montante de cerca de 1 milhão de dólares.

1.2.2. *A Espionagem por Computador*

A espionagem no âmbito da utilização dos dados é favorecida pelo facto destes estarem armazenados num compartimento o mais acanhado possível e poderem sem mais nada ser transmitidos para utilização noutro computador.

Lembre-se por exemplo o caso das fórmulas químicas altamente confidenciais, das têmperas dos metais, até das fórmulas dos perfumes, dos dados científicos, etc.

Daqui resulta a utilização do conteúdo de dados armazenados por pessoas não autorizadas, isto é, o furto de dados. Acrescente-se que a utilização de programas de computador por pessoas estranhas requer já um apreciável «know-how».

Cabe ainda referir que as possibilidades de «Espionagem de Programação de Dados» não são utilizadas apenas na Espionagem Económica das Empresas, mas também na Espionagem Política por parte de Estados estrangeiros, nomeadamente pelos seus Serviços Secretos.

1.2.3. *A Sabotagem da Programação de Dados*

Tanto pelo montante dos prejuízos como pelo modo como são cometidos, há que referir os casos de sabotagem no domínio da programação de dados.

Estes casos de sabotagem são favorecidos por falta de segurança nos centros de processamento e pela ausência dos contrôles suficientes nas aplicações informáticas e consistem na alteração ou apagamento dos dados armazenados nos ficheiros magnéticos do computador da Empresa ou Instituição.

1.2.4. *O «Furto de Tempo»*

O designado «furto de tempo» representa mais um caso de criminalidade por computador e consiste na utilização não autorizada das instalações de processamento de dados por colaboradores infiéis ou por terceiros estranhos aos serviços, com a finalidade de fazer trabalhos estranhos à Empresa ou Instituição.

2 — A UTILIZAÇÃO ABUSIVA DE MÁQUINAS AUTOMÁTICAS DE PAGAMENTO (BANKOMATEN)

Os novos «Straftatbestände» da «Burla por Computador» propostos pelo art. 2.º da Lei Contra a Criminalidade Económica (WikG-Wirtschaftskriminalitätgesetz) podem também resolver um outro problema que resulta de uma especial utilização de técnicas informáticas no domínio da Banca: o uso indevido por terceiros não autorizados dos designados cartões codificados de crédito (Codekarte).

As máquinas automáticas de pagamento instaladas nos E.U.A., no Japão, na França, na Suíça, e desde há muito também na R.F.A., dão aos clientes dos Bancos, que dispõem de um cartão codificado de crédito, a possibilidade de levantar uma vez por dia uma determinada quantia em dinheiro.

Para impedir o uso ilegal destes cartões por terceiros, todos os sistemas de máquinas automáticas de pagamento existentes na R.F.A., prevêem que o cliente além de ter de introduzir o cartão codificado na ranhura da máquina (Bankomat) necessite ainda de marcar o número secreto que está gravado na banda magnética do respectivo cartão. Só no caso de o número introduzido na máquina automática de pagamento (A.T.M.), na terminologia inglesa, coincidir com o que está gravado magneticamente no cartão codificado, o «Geldautomat» entrega a importância solicitada.

A fim de evitar que os clientes possam levantar dinheiro com o cartão de crédito codificado mais de uma vez por dia em diversas máquinas automáticas de pagamento desse Banco,

tanto na R.F.A. como noutros países, utilizam-se certas medidas de segurança, sendo a mais eficiente a que consiste numa ligação directa permanente de todas as máquinas automáticas de pagamento, de modo a permitir o conhecimento do saldo da conta e informar dos diversos movimentos efectuados. Todavia, este sistema não é utilizado devido aos elevados custos que acarretaria.

Os sistemas usuais prevêem que a máquina automática de pagamento, simultaneamente com a entrega de dinheiro, registe magneticamente no cartão codificado a data e a importância do levantamento efectuado (1).

Uma outra estratégia de segurança consiste em os movimentos efectuados serem regularmente verificados através duma central de máquinas automáticas de pagamento de modo que, no caso de levantamentos reiterados, movimentações estranhas de contas, ou outras irregularidades, seja transmitida imediatamente a todas as máquinas automáticas de pagamento uma ordem para bloqueamento do respectivo cartão.

Por outro lado, impõe-se a uniformização das medidas de segurança das diferentes Instituições Bancárias a fim de evitar que o portador do cartão faça levantamentos nas máquinas automáticas de pagamento do Banco onde não possui conta.

O uso ilegal de cartões de crédito codificados (Codekarte) que frequentemente se observa no estrangeiro, consiste — além do levantamento reiterado de somas de dinheiro e de utilização de contas a descoberto — sobretudo no uso indevido, por terceiros, desses cartões perdidos pelos seus titulares, ou mesmo furtados.

De facto, o delinquente que encontra ou furta um cartão codificado de crédito, vai tentar através de truques telefónicos, chantagem ou meios mais sofisticados, conhecer o número secreto gravado magneticamente nesse cartão para depois o

---

(1) Este é também o sistema utilizado entre nós, que foi iniciado em Maio de 1983 pelo B.P.A. e que gradualmente começa a ser utilizado pela generalidade dos Bancos.

poder utilizar nas máquinas automáticas de pagamento fazendo aí levantamentos de somas de dinheiro.

3 — OS MEIOS PREVENTIVOS DA CRIMINALIDADE POR COMPUTADOR

E em razão dos eventos delituais que esquematicamente atrás se enunciaram que as áreas tecnológicas e organizativas vêm ensaiando sistemas de prevenção e meios de segurança da mais diversa ordem que poderão também em síntese resumir-se em três grupos:

3.1. SEGURANÇA FISICA DOS ESPAÇOS

Neste grupo se inclui desde a protecção física e vigilância dos locais de instalação de equipamentos aos locais de armazenagem de dados até às classificações de segurança das áreas só penetráveis por pessoas a quem corresponda igual grau atribuído de garantia de fidelidade e sigilo.

3.2. SEGURANÇA TECNOLÓGICA

Nesta área incluem-se desde os sistemas de protecção e auto-protecção dos equipamentos contra fraudes, até à compartimentação estanque das diversas áreas de técnicas interventoras desde o «in-put» ao «out-put», de modo a que a imiscibilidade de funções garanta a diminuição do risco de acesso aos processos acabados ou aos dados armazenados por técnicos de diversas áreas do processo global de tratamento informático.

3.3. SEGURANÇA DE PESSOAS

Ainda que eventualmente não possa falar-se para já de uma «jurisdicionalização» de estatuto semelhante ao que, por

exemplo, distingue o cidadão comum do funcionário judicial, que pode manejar processos no exercício das suas funções, ou do estatuto do guarda prisional, que tem acesso a espaços que o comum das pessoas não pode ter em qualquer hora do dia, já, contudo, na prevenção da chamada criminalidade por computador se vêm desenhando sistemas de classificação das pessoas por graus de segurança em termos de, certa áreas e certos tipos de informação ou dados, só poderem ser acessíveis a pessoas com perfil e história pregressa previamente clivada em termos de garantia contra o uso abusivo ou a utilização de dados, programas ou equipamentos, afora ou para além dos fins a que estão especificamente destinados, seja quanto aos seus titulares, seja quanto aos resultados da operacionalidade de tais sistemas.

4 — A PUNIBILIDADE DESTE TIPO DE DELINQUÊNCIA NA R.F.A.

A Criminalidade por Computador diz respeito normalmente a objectos não corpóreos como o segredo negocial, o know-how» ou outras informações. Não é pois de admirar que os «Tatbestände» tradicionais, apenas parcialmente e por uma mera casualidade, possam abranger este tipo de moderna delinquência, razão pela qual o legislador alemão ocidental previu a introdução de dois novos «Straftatbestände» (delitos penais).

4.1. A SANÇÃO DO «FURTO DE TEMPO»

O caso de «furto de tempo», isto é, a utilização abusiva das instalações de processamento de dados, não cabe em nenhum dos delitos penais contra a propriedade ou contra bens, puníveis pelo Direito Penal da R.F.A.: o «furtum usus», previsto e punido pela alínea *b*) do art. 248.° do Código Penal Alemão (StGB), respeita apenas a delitos especiais: o furto de bicicletas e de automóveis.

Também o furto de energia eléctrica, previsto e punido pela alínea *c*) do art. 248.° do mesmo Código, se não pode aplicar ao «furto de tempo» porque não é utilizado um determinado condutor como sucede no caso de subtracção de energia.

Por outro lado o «Tatbeständ» de infidelidade, previsto e punido pelo art. 266.° do mesmo diploma (StGB), que pressupõe tanto uma certa margem de actuação do delinquente como também um prejuízo para o ofendido, só pode utilizar-se em circunstâncias especiais.

Na realidade, não se trata precisamente de um (pequeno) uso abusivo de corrente eléctrica, mas sim de uma utilização abusiva do computador, da qual resulta para o delinquente um considerável enriquecimento.

O «furto de tempo» assemelha-se, pois, a um furto de uso como o previsto e punido na alínea *b*) do art. 248.° e na alínea *a*) do art. 265.°, ambos do Código Penal Alemão (StGB), sendo certo que até agora ainda não existe um preceito que o puna autonomamente pelo que a maior parte das vezes permaneceu impunível.

4.2. A SANÇÃO DA SABOTAGEM DE COMPUTADOR

Todas as acções de sabotagem na esfera da programação de dados são previstas e punidas pelo art. 303.° do Código Penal Alemão.

Com efeito, a opinião dominante considera a alteração ou apagamento de dados nos ficheiros magnéticos dos computadores como um dano material.

Se bem que o bem jurídico protegido pelo art. 303.° do Código Penal Alemão não seja de todo idêntico no caso de sabotagem de computadores, o certo é que é assim que o direito vigente pune a actuação desse tipo de delinquentes.

4.3. A SANÇÃO DA ESPIONAGEM POR COMPUTADOR

Tanto o «furto de tempo» como a espionagem por computador levantam interessantes problemas tanto para o Direito Penal como para o Direito Civil.

Mas o fulcro da discussão hoje em dia é a protecção da propriedade intelectual dos programas de computadores e isto porque actualmente a doutrina alemã é unânime em considerar que a protecção dos programas dos computadores só raramente pode fazer-se através do Direito das Patentes.

A doutrina alemã dominante entende que a programação de dados de computador representa uma criação espiritual pessoal, nos termos do § 2.º do art. 20.º do Código dos Direitos de Autor (UrhRG) e que a sua protecção se encontra assegurada pelas disposições penais da Lei da Concorrência Desleal (UWB) que punem a revelação do segredo negocial e empresarial: arts. 17.º, 18.º e 20.º

4.4. A SANÇÃO DAS MANIPULAÇÕES DE COMPUTADOR

Os problemas da Criminalidade por Computador, especificamente de Direito Penal, resultam sobretudo das Manipulações de Computador.

A problemática penal da Criminalidade por Computador concentra-se nos delitos contra a propriedade (especialmente Burla e Infidelidade) e nos delitos de Falsificação (Falsificação de documentos e de apontamentos técnicos), sendo irrelevante o «erro de computador» devido a falha humana.

A programação de um computador exige consideráveis conhecimentos técnicos e assim, no caso de manipulações levadas a efeito por funcionários experientes e altamente qualificados, entende a doutrina alemã que as «Manipulações Input» caiem no domínio do art. 263.º do Código Penal Alemão, que prevê e pune o crime de burla.

Já quando se trata de manipulações de computador levadas a efeito por funcionários auxiliares, tem a jurisprudência alemã dos Tribunais de 1.ª Instância tendido para considerar esses

casos como delitos de infidelidade, por existir uma certa margem de discricionaridade, caindo na previsão do art. 266.º do mesmo diploma.

Aos casos de falsificação de documentos registados magneticamente tem sido aplicado o n.º 3 do art. 268.º do mesmo Código.

5 — CONCLUSÃO

Pode dizer-se que a punição dos crimes por computador nem sempre é assegurada pelo Direito Penal da R.F.A.

Por esse motivo um projecto de Lei contra a Criminalidade Económica, publicado em Junho de 1982, propôs a introdução de dois novos «Straftatbestände»: a «Burla por Computador [qualificando-a no artigo 263.º do Código Penal Alemão pela adição de uma alínea, alínea a)] e a «Falsificação de Dados Computadorizados revivificando a previsão do artigo 269.º do Código Penal Alemão e repondo este preceito em vigor mas com previsão específica quanto a dados computadorizados.

Desapareceriam assim as principais lacunas do Código Penal Alemão, no que respeita à luta contra a Manipulação de Computadores.

E em Portugal, *quid juris?*

6 — RESUME

La Criminalité par Ordinateur a pris un très grand essor das les pays industrialisés, notamment aux E.U.A., au Japon, en France et en R.F.A., et a frappé surtout l'Industrie, l'Economie, l'Administration Publique et les Institutions Bancaires et Compagnies d'Assurances.

Parmi les diverses formes de cette criminalité on peut distinguer: les manipulations, l'espionnage por ordinateur, le sabotage dans la programmation des données et le vol du temps.

Dans l'activité bancaire de ces pays s'est répandu l'utilisation des G.A.B. (Guichets Automatiques de Billets) ce qui a contribué au développement d'une nouvelle sorte de délinquance qui consiste, soit à l'utilisation abusive d'une Carte Codifiée de Crédit (Codekarte) appartenant à un tiers, soit à l'utilisation par le légitime titulaire de ladite Carte dans une dépendance bancaire où il ne possède pas de compte, ou encore l'utilisation d'un compte à découvert.

La punition de ces délinquants entraîne d'énormes difficultés dûes au fait que le législateur de la plupart de ces pays n'a pas encore introduit dans leur législation pénale les tous nouveaux «Straftbestände» et par conséquance il en résulte des lacunes.

On peut dire qu'en R.F.A. ce problème se trouve presque résolu puisqu'un projet de loi de Juin 1982 a proposé l'introduction de deux nouveaux Straftatbestände: «l'Escroquerie par Ordinateur» — punissable par l'alinéa *a*) de l'article 263 du Code Pénal — et «la Falsification des Données d'Ordinateur» — punissable par l'article 269 dudit Code.

Mais malgré cela la punition de ces délinquants n'est pas toujours assurée en R.F.A.

Et au Portugal, quid juris?

7 — ZUSAMMENFASSUNG

Die Computerkriminalität hat ein sehr grosses Ausmass in Industrieländern, besonders in den Vereinigten Staaten, Japan, Frankreich und in der Bundesrepublik Deutschland angenommen und vor allem die Industrie, die Wirtschagt, öffentliche Verwaltung, die Kreditanstalten und Versicherungsgesellschaften getroffen.

Bei den verschiedenen Formen dieser Kriminalität kann man folgende unterschieden: Manipulationen, Computerspionage, Sabotage bei Datenverarbeitung und «Zeitdiebstahl».

Im Bankwesen der obengenannten Ländern hat sich die Benutzung des Bankomaten eingebürgert, was zur Entwicklung

einer neuen Form von Kriminalität beigetragen hat, die entweder in der missbräuchlichen Benutzung der Codekarte eines Dritten besteht, oder in der Benutzung dieser Codekarte durch ihren Eigentümer, jedoch in einer Bankfiliale, wo er kein Konto besitzt, bzw, bei einem Konto ohne Deckung.

Die Bestrafung dieser Straftäter bringt grosse Schwierigkeiten mit sich die aus der Tatsache hervorgehen, dass der Gesetzgeber in den meisten angeführten Länder alle diese neuen Straftatbestände noch nicht in seiner Strafrechtsgesetzgebund aufgenommen hat und folglich Lücken bestehen.

Man kann sagen, dass in der Bundesrepublik Deutschland dieses Problem fast gelöst ist da ein Gesetzentwurf von Juni 1982 die Aufnahme zweier néuer Straftatbestände vorgeschlagen hat: den «Computerbetrug», strafbar nach Absatz (a) des § 263 des Strafgesetzbuches und die «Fälschung gespeicherter Daten», strafbar nach § 269 desselbes Gesetzbuches.

Dennoch ist die Bestrafung dieser Straftäter in der Bundesrepublik Deutschland noch nicht immer gewährleistet.

Und in Portugal, *quid juris?*

8 — BIBLIOGRAFIA

EDP Analyze — Computer Fraud and Embezzlement, Vol. 11, n.° 9 — Setembro 1973.

Gillis — Fraude et Sécurté Informatique — Conferência proferida em Paris em 25 e 26 de Novembro de 1982, no Séminaire International sur les Instruments d'une Informatique plus sûre.

Gropp — Die Codekarte: der Schlüssel zum Diebstahl — Juristenzeitung, 1983.

Kraus / Mac Gahan — Computer Fraud and Countermeasures — 1979.

Parker — Crime by Computer, 1976.

Rohner — Computerkriminalität — strafrechtliche Probleme bei «Zeitdiebstahl und Manipulationen, 1976.

Schroth — Der Diebstahl mittels Codekarte, Neue Juristische Wochenschrift, 1981.

Sieber — Computerkriminalität und Missbrauch von Bankomaten, in Zeitschrift für Wirtschafts — und Bankrecht — n.° 49, Dezembro 1983.

Tiedemann — Wirtschaftsstrafrecht und Wirtschaftskriminalität, 1976 — 2 Band.