

DO DELITO DE DANO E DE SUA APLICAÇÃO AO DIREITO PENAL INFORMÁTICO

TÚLIO LIMA VIANNA

Mestre em Ciências Penais pela Faculdade de Direito
da Universidade Federal de Minas Gerais. Professor de Direito Penal
na Pontifícia Universidade Católica de Minas Gerais.
Assessor Judiciário da 2ª Câmara Criminal do Tribunal de Alçada de Minas Gerais.

SUMARIO: 1. *Prolegômenos* - 2. *Analogia e interpretação extensiva* - 3. *Bem jurídico tutelado* - 4. *Dados informáticos* - 5. *Dados como objeto material do delito de dano* - 6. *Dano informático e divulgação de vírus* - 7. *Dano informático e acesso não autorizado a sistemas computacionais* - 8. *Consumação e tentativa* - 9. *Conclusões* - 10. *Bibliografia*.

1. PROLEGÔMENOS

O crime de dano está previsto no art. 163 do CP brasileiro e sua aplicação na proteção dos dados informáticos tem sido muito discutida em congressos e seminários dedicados ao estudo do Direito Informático no Brasil.

O buslilis encontra-se na palavra *coisa*, utilizada pelo legislador de 1940 para designar o objeto material do delito de dano.

Argumenta-se que, em respeito ao princípio constitucional da legalidade - que veda a analogia como instrumento da criação de tipos -, não se poderia considerar típico um dano a dados informáticos.

Assim, se um agente formatasse um disco rígido sem a autorização de seu legítimo proprietário, com o único intuito de lhe causar um prejuízo, não haveria crime de dano, pois nenhuma "coisa" foi destruída, inutilizada ou deteriorada.

A hipótese reveste-se de grande importância, pois, em suma, esta é a conduta de quem cria e divulga vírus de computador, prática que tem causado grandes prejuízos não só às grandes corporações, mas também a usuários individuais, que, muitas vezes, perdem todas as suas informações armazenadas sobre a forma de dados em seu computador.

Procuraremos demonstrar neste trabalho que é perfeitamente possível a tipificação das citadas condutas como crime de dano sem que haja qualquer ofensa ao princípio constitucional da legalidade.

2. ANALOGIA E INTERPRETAÇÃO EXTENSIVA

Em princípio, cabe-nos determinar se o entendimento do dado informático como *coisa* é uma atividade interpretativa ou integrativa da lei penal.

A interpretação não se confunde com a integração, pois, enquanto esta visa a preencher as lacunas existentes na lei,¹ aquela objetiva tão-somente o correto entendimento da *intentio legis*.

Assim, a analogia não é uma atividade interpretativa, mas sim um instrumento de integração das normas, pois preenche com hipóteses semelhantes as lacunas legais.

No dizer de Heleno Cláudio Fragoso:

"A analogia distingue-se da interpretação, porque constitui um processo de integração da ordem legal, e não meio de esclarecer o conteúdo da norma. Através da analogia aplica-se a lei a hipótese por ela não prevista, invocando-se substancialmente o chamado argumento *a pari ratione*. Há aplicação analógica quando a norma se estende a caso não previsto, mas semelhante, em relação ao qual existem as mesmas razões que fundamentam a disposição legal. A analogia distingue-se da interpretação extensiva, porque nesta não falta a vontade da lei, mas tão-somente a expressão verbal que a ela corresponda" (Fragoso, 1985, p. 87).

Se na integração o intérprete acrescenta à norma elementos previamente não existentes, na interpretação extensiva ele tão-somente revela a *intentio legis* já existente, porém não expressa verbalmente de forma adequada.

"A interpretação extensiva é perfeitamente admissível em relação à lei penal, ao contrário do que afirmavam autores antigos. Nestes casos não falta a disciplina normativa do fato, mas, apenas, uma correta expressão verbal. Há interpretação extensiva quando se aplica o chamado argumento *a fortiori*, que são casos nos quais a vontade da lei se aplica com maior razão. É a hipótese do argumento *a maiori ad minus* (o que é válido para o mais, deve necessariamente prevalecer para o menos) e do argumento *a minori ad maius* (o que é vedado ao menos é necessariamente no mais). Exemplo deste último argumento: se o Código Penal incrimina a bigamia, logicamente também pune o fato de contrair alguém mais de dois casamentos (Manzini)" (Fragoso, 1985, p. 86).

Destarte, se advogássemos a tese de que o art. 163 do CP pudesse ser interpretado como "destruir, inutilizar ou deteriorar coisa alheia ou *dados informáticos*", estaríamos defendendo a analogia.

Se, porém, admitirmos que os dados informáticos são "coisas", não haverá analogia, mas sim interpretação extensiva, pois a *intentio legis* é evitar um dano patrimonial, seja ele praticado em objetos tangíveis ou não.

Não se está, pois, acrescentando novo conteúdo à lei, mas sim evidenciando um novo significado da palavra "coisa" impossível de ter sido previsto pelo legislador de 1940, mas certamente contido na norma.

- (1) "Interessante exemplo da lógica da integração é uma brincadeira em que alguém conta um caso aparentemente sem sentido e o resto do grupo tenta deduzir um fator que tornaria a situação lógica por meio de perguntas que só podem ser respondidas com sim, não ou irrelevante. Vejamos: um homem entra num bar, pede um copo d'água. O garçom dá um tiro para o alto, ele agradece e vai embora. À primeira vista parece uma situação totalmente absurda, sem a menor coerência. As primeiras perguntas mais desviam a atenção do que guiam para o caminho correto: - O tiro matou alguém? - Não. - O garçom trouxe a água para ele? - Não. Porém, depois de algum tempo, as perguntas fundamentais são feitas: - O homem estava com sede? - Não. - Mas ele pretendia beber a água: - Sim. Após uma meia hora, alguém, num momento de iluminação, solta a frase reveladora: - Ele estava com soluços! E o problema está solucionado (Com o perdão do trocadilho)" (Vianna, 1998, p. 253-254).

3. BEM JURÍDICO TUTELADO

O bem jurídico penalmente tutelado no delito de dano é o patrimônio, que deve ser entendido como conjunto de bens de valor econômico, valor utilidade e valor afetivo para seu proprietário.

Se a vítima tem armazenada, em papel ou em formato digital, uma tabela em que catalogou o número de manchas nas asas de inúmeras espécies de borboletas, possivelmente estes dados não terão valor econômico (quem iria comprar isso?), mas certamente terão um valor utilidade para a vítima que levou anos realizando tal pesquisa.

Por outro lado, caso a vítima tenha as cartas - ou os e-mails - de seus ex-namorados guardados e seu companheiro atual, num momento de ira, destrua todas estas mensagens, certamente haverá crime de dano, pois, não obstante a inexistência de valor econômico ou utilidade, há aqui um claro valor afetivo para a vítima.

Obviamente o agente deve ter plena consciência de que o bem danificado tem valor para a vítima. Nos casos de valor econômico isto é bastante óbvio para o autor, mas quando se trata de valor utilidade ou valor afetivo, muita vez pode o agente não imaginar que aquele bem tenha alguma importância para a vítima. Nesta hipótese, caso danifique a coisa, não poderá ser penalmente punido, pois agiu em erro de tipo, uma vez que lhe faltava o elemento cognoscitivo do dolo.

Vale lembrar ainda que o valor da coisa tem de ser significativo, caso contrário aplicar-se-ia o princípio da insignificância, que exclui a própria tipicidade penal em respeito ao princípio da lesividade, corolário natural do Estado Democrático de Direito constitucionalmente previsto.

4. DADOS INFORMÁTICOS

Dados são informações representadas em forma apropriada para armazenamento e processamento por computadores.

Ainda que em sua maioria estas informações estejam na forma de texto, sendo, pois, compostas de palavras, as informações são representações da mente humana que podem abranger os cinco sentidos: uma foto, uma música, um perfume, um sabor, um beijo.

Os computadores, se comparados à mente humana, no entanto, são máquinas muito simples e não conseguiriam reconhecer as complexas representações criadas pelo homem. Assim, criou-se um artifício pelo qual todas as informações são passadas aos computadores na forma de presença ou ausência de corrente elétrica.

As informações digitais - ou dados - podem representar qualquer informação humana através de uma seqüência ordenada de zeros e uns, sendo que o 0 (zero) representa a ausência de correntes elétricas no circuito e o 1 (um) representa sua presença.²

(2) Evidentemente foi necessária a criação de uma tabela que correlacionasse cada uma das letras do alfabeto humano a uma seqüência de zeros e uns inteligíveis pela máquina. Assim, *verbi gratia*, a letra A passou a ser representada pelo código 01000001, a B por 01000010, a C por 01000011 e assim sucessivamente, de forma tal que toda palavra humana pudesse ser entendida como uma seqüência de passagem ou ausência de corrente elétrica. As imagens, por outro lado, foram divididas em milhares de linhas e colunas e cada um dos pontos formados pela interseção destas linhas e destas colunas, x1, x2, y1, y2, passou a ser representado pela passagem ou ausência de corrente elétrica. Evidentemente todos estes dados são processados em velocidades incríveis, razão pela qual muita vez não nos damos conta da complexidade em que se baseia o sistema digital.

Estes dados podem ser armazenados em diversos meios físicos. Nos discos rígidos e nos disquetes estas informações são armazenadas na forma magnética, sendo que a presença de corrente magnética representa o 1 (um) e sua ausência representa o 0 (zero). Em CDs, DVDs, sejam eles de dados, músicas ou filmes, estas informações digitais também são representadas na forma de dados, sendo que o 1 (um) indica a reflexão do laser pelo CD/DVD e o 0 (zero) a sua não-reflexão.

Ontologicamente não há qualquer distinção entre um CD de áudio e um CD-ROM, assim como não há qualquer distinção entre um DVD-ROM e um DVD de filmes. Em todos eles há uma seqüência gigantesca de 0 (zeros) e 1 (uns) que o aparelho decodificador irá transpor para informações humanamente inteligíveis.

5. DADOS COMO OBJETO MATERIAL DO DELITO DE DANO

Tanto as fitas K7 como as VHS armazenavam informações por meio magnético, ainda que de forma analógica e não digital. Assim, a exposição destas fitas a um ímã poderia causar a perda completa das informações nelas armazenadas, ainda que posteriormente fosse possível gravar novos dados na fita.

Suponhamos então que Tício, utilizando-se de um ímã e com o claro propósito de causar um prejuízo a Mévio, danifique a fita VHS na qual está gravada a cerimônia de seu casamento.

Certamente não houve um prejuízo patrimonial propriamente, pois é possível que, com um pouco de sorte, Mévio ainda possa gravar alguma nova informação naquela fita.

O dano causado por Tício não foi, pois, ao continente, mas ao próprio conteúdo da fita, isto é, às informações nela armazenadas. A tipicidade do crime de dano é evidente, pois Tício produziu a perda de uma informação que possuía grande valor afetivo para Mévio.

Ainda que se pudesse cogitar na aplicação do princípio da insignificância como excludente da tipicidade da conduta em razão do baixíssimo valor da fita virgem, impossível seria desconsiderar o imenso valor afetivo das informações nela armazenadas.

Uma "coisa" é uma fita virgem. Outra "coisa" é uma fita gravada. Trata-se de uma constatação de senso comum, mas que muitos estudiosos do Direito Informático parecem não perceber.

Da mesma forma, se Tício, com o uso de um ímã, intencionalmente danifica um disquete de Mévio, no qual estão armazenados seus trabalhos escolares, estará cometendo a conduta típica de dano, não pela perda do disquete, mas pela perda dos dados nele armazenados.

A hipótese torna-se um pouco mais sutil se Tício, em vez de utilizar-se de um ímã, coloca o disquete de Mévio em um computador e emite um comando para que ele seja formatado.

Ora, o dolo de Tício é exatamente o mesmo. Do ponto de vista objetivo, por outro lado, a conduta também é idêntica, diferindo-se tão-somente pelo instrumento utilizado para produzir o dano. No primeiro caso utilizou-se de um ímã. No segundo, de um computador. Ambos, o ímã e a controladora do disquete, através de um processo magnético, apagaram as preciosas informações de Mévio armazenadas no disquete.

Está clara, mais uma vez, a tipicidade do delito de dano, pois uma "coisa" é um disquete com trabalhos escolares gravados e outra "coisa" é um disquete virgem.

A utilidade que a primeira "coisa" tinha não existe mais. O dano se deu, pois, na modalidade de inutilizar coisa alheia.

6. DANO INFORMÁTICO E DIVULGAÇÃO DE VÍRUS

A palavra vírus deriva do latim e significava originariamente:

" 1. Suco (das plantas). 2. Baba, peçonha (dos animais). 3. (Em geral) Veneno, peçonha. 4. Mau cheiro, cheiro fétido" (Ferreira, p. 1.228).

O termo acabou sendo usado pelas Ciências Biológicas para designar diminutos agentes infecciosos, visíveis apenas ao microscópio eletrônico, que se caracterizam por não ter metabolismo independente e ter capacidade de reprodução apenas no interior de células hospedeiras vivas.

Os vírus informáticos, à semelhança de seus homônimos biológicos, também são capazes de causar graves danos a seus hospedeiros, em geral um disquete ou um disco rígido.

Se, nos seres vivos, os vírus agem comandados por uma seqüência de ácidos nucleicos que são injetados na célula da vítima, nos computadores os vírus são uma seqüência pré-ordenada de 0 (zeros) e 1(uns) que obrigam o computador a realizar uma série de funções não desejadas por seu proprietário.

Suponhamos então que Tício, em vez de utilizar-se de um imã ou da formatação por meio de um computador, prefira infectar o disquete de Mévio com um vírus capaz de obrigar o computador de Mévio a formatar os dados nele armazenados na próxima sexta-feira 13.

Mais uma vez, a conduta é absolutamente típica. O dolo é idêntico ao das condutas anteriores, pois a intenção de Tício é a de apagar os dados armazenados e causar um prejuízo a Mévio. Objetivamente, também há uma inutilização por meios magnéticos dos dados.

O que diferencia esta hipótese dos casos precedentes é tão-somente o momento do resultado, que nos primeiros exemplos dá-se logo em seguida aos atos executórios e aqui só ocorre em data futura pré-determinada pelo agente.

Conclui-se, pois, que, quando alguém divulga um vírus de computador, objetivamente está emitindo comandos para que no futuro o próprio computador da vítima inutilize os dados armazenados, seja em um disquete, seja, mais comumente na atualidade, em um disco rígido.

7. DANO INFORMÁTICO E ACESSO NÃO AUTORIZADO A SISTEMAS COMPUTACIONAIS

O acesso não autorizado a sistemas computacionais é ainda conduta atípica no Direito Penal brasileiro, mas pode, muita vez, servir de instrumento para a prática do crime de dano.

Se Tício, com seu computador conectado à Internet, obtém por meios ilícitos acesso a uma página na Internet e altera seu conteúdo, colocando no ar uma página de protesto, *verbi gratia*, estará, por meio de um acesso não autorizado, praticando crime de dano.

É necessário demonstrar, porém, que aquela página possui um valor para a vítima, o que em páginas comerciais é demasiadamente óbvio. Os anúncios que deixam de ser exibidos e as vendas que não se concretizam por ter sido o site desfigurado por si so demonstram os prejuízos econômicos da vítima.

Em uma página que preste informações sobre as condições climáticas, tráfego etc, o valor utilidade é claro, caracterizando-se também o crime de dano.

Em páginas pessoais, o valor sentimental da página para a vítima deverá ser levado em conta, mormente se a vítima não tinha cópia (*back-up*) dos documentos danificados.

8. CONSUMAÇÃO E TENTATIVA

O crime de dano é material e consuma-se no momento do resultado.

Na maioria absoluta dos casos analisados, o resultado se dá logo em seguida aos atos de execução, não gerando, pois, maiores problemas na análise da tentativa.

O dano praticado através de vírus de computador, porém, só se consuma muito tempo após a prática do último ato executório, razão pela qual merece uma análise mais acurada.

A simples criação de um vírus de computador não é punida pelo Direito Penal brasileiro. Trata-se de fase preparatória do delito de dano informático e, como tal, não pode ser punida, pois, se o agente não divulgar o vírus, o dano não se concretizará.

O início da execução do crime de dano realizado através de vírus informáticos se dá no momento em que o agente disponibiliza por qualquer meio o vírus a outrem.

Se Tício infecta um disquete com um vírus de computador e o oferece a Mévio alegando tratar-se de um excelente jogo de computador, haverá o início de execução do crime de dano.

Se Tício dolosamente envia um e-mail infectado com vírus a Mévio, haverá início de execução do crime de dano.

Se Tício disponibiliza em sua página na Internet um vírus de computador, alegando tratar-se de um excelente programa, haverá também o início da execução de crime de dano.

Em todos estes casos o vírus tornou-se acessível à vítima por meio de uma conduta dolosa de Tício.

A consumação do delito dar-se-á no momento do resultado, isto é, quando o vírus praticar o dano nos dados da vítima.

Se a vítima, porém, jamais executar o vírus, haverá a tentativa, pois, não obstante o agente ter praticado todos os atos de execução, o crime não se consumou por circunstâncias alheias à sua vontade.

9. CONCLUSÕES

O crime de dano previsto no art. 163 do CP brasileiro é perfeitamente aplicável à tutela dos dados informáticos, sendo completamente prescindível a criação de um novo tipo penal para tal fim. Trata-se de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal.

A proteção patrimonial dos dados não se limita a seu valor econômico, pois a *intentio legis* é proteger todo o patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor utilidade e do valor afetivo que porventura tenha a coisa.

A divulgação de vírus informáticos com intenção de dano pode ser punida como tentativa de dano, caso o resultado não se concretize, ou como dano consumado, caso o resultado naturalístico venha a ocorrer efetivamente.

10. BIBLIOGRAFIA

- DELMANTO, Celso, DELMANTO, Roberto, DELMANTO JÚNIOR, Roberto. *Código Penal comentado*. 4. ed. Rio de Janeiro: Renovar, 1998. 961 p.
- FERREIRA, Antônio Gomes. *Dicionário de Latim-Português*. Porto: Porto Editora, s/d. 1.240 p.
- PRAGOSO, Heleno Cláudio. *Lições de direito penal: a nova parte geral*. 8. ed. Rio de Janeiro: Forense, 1985. 491 p.

- _____. *Lições de direito penal: parte especial: arts. 121 a 212 do CP*. Rio de Janeiro: Forense, 1983. 615 p.
- MACHADO, Cynthia Semíramis F. "Software e privacidade: uma defesa do código-fonte aberto na preservação do direito constitucional à vida privada". In: CERQUEIRA, Tarcísio Queiroz, IRIARTE, Erick, PINTO, Márcio Morena (Coords.). *Informática e internet: aspectos legais internacionais*. Rio de Janeiro: Esplanada, 2001.
- MAXIMILIANO, Carlos. *Hermenêutica e aplicação do direito*. 16. ed. Rio de Janeiro: Forense, 1997. 426 p.
- MIRABETE, Júlio Fabbrini. *Código Penal interpretado*. São Paulo: Atlas, 1999. 1.972 p.
- VIANNA, Túlio Lima. *Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais*. Rio de Janeiro: Forense, 2002.
- _____. "Hackers: um estudo criminológico da subcultura cyberpunk". In CERQUEIRA, Tarcísio Queiroz, IRIARTE, Erick, PINTO, Márcio Morena (Coords.). *Informática e internet: aspectos legais internacionais*. Rio de Janeiro: Esplanada, 2001.
- _____. "Cibernética penal". *Boletim do Instituto de Ciências Penais*, Belo Horizonte, ano 2, n. 16, p. 4-6, jun. 2001.
- _____. "Dos crimes pela internet". *Revista do CAAP*, Belo Horizonte, ano 5, n. 9, p. 367-385, 2000.
- _____. "Dos crimes por computador." *Revista do CAAP*, Belo Horizonte, ano 4, n. 6, p. 463-491, 1999.
- _____. "Prolegômenos à hermenêutica jurídica". *Revista do CAAP*, Belo Horizonte, ano 3, n. 4, p. 243-263, 1998.
- ZAFFARONI, Eugênio Raul, PIERANGELI, José Henrique. *Manual de direito penal brasileiro - Parte geral*. 2. ed. rev. e atual. São Paulo: Ed. RT, 1999. 888 p.