

A invasão da privacidade e da honra por meio da internet*

Invasion of privacy and intimacy through the internet

Davi Antunes Pavan**

** Universidade Norte do Paraná (UNOPAR).

Resumo

O presente trabalho tem por objeto a análise do tema “A Invasão da Privacidade e da Honra por Meio da Internet”, abordando seus aspectos formais e materiais, sobretudo de condutas já tipificadas pela legislação vigente na Constituição Federal e no Código Penal, evidenciando o desenvolvimento de novas tecnologias, sendo praticados tais delitos de formas inovadoras, sem perder o objeto delituoso. A internet é atualmente um meio avançado de se obter informações sigilosas devido ao seu alcance, utilizada como meio para prática de crimes. A exposição aborda especificamente os delitos contra a intimidade e a privacidade, fundamentando na doutrina nacional dominante.

Palavras-chave: Internet. Crime. Tipificação. Privacidade. Intimidade.

Abstract

The present work analyzes the theme “Invasion of Privacy and Intimacy through the Internet”, approaching its formal and material aspects, especially conducts already typified by the legislation in force in the Federal Constitution and Criminal Code. It gives evidence of the development of new technologies, showing the practice of such crimes in innovative ways, without losing their wrongful purpose. The Internet is an advanced form of obtaining secret information due to its reach and has been used as a means for the practice of crimes. Based on the dominant national doctrine, this research approached in particular crimes against intimacy and privacy.

Key words: Internet. Crime. Typification. Privacy. Intimacy.

1 Introdução

Verifica-se, ao longo da história do homem, a necessidade e o instinto de superação do seu espaço geográfico, juntamente com a constante preocupação em manter registros sobre suas vidas. Detentor destes sentimentos, retratava diariamente detalhes em pedras, entalhando madeiras, dominando a escrita; finalmente partiu para a conquista do espaço, com a descoberta de novas terras. Contudo, tanto para a escrita, bem como para a superação geográfica, uma importante área também tinha de evoluir, ou seja, a matemática, pois os cálculos seriam de grande importância para tais processos de evolução.

Destarte, eis que a matemática impulsionou todo o avanço tecnológico, inclusive no âmbito da informática. Assim, no século passado, mais precisamente na década de trinta, o matemático britânico Alan Turing demonstrou a possibilidade de uma determinada máquina executar instruções lógicas e armazenar informações; para tanto, utilizaria de um sistema binário, onde o algarismo “1” representaria verdadeiro, enquanto que o algarismo “0”, falso (PAESANI, 2000, p. 22). Todavia, naquele momento, o mesmo não sabia que estava dando subsídios para a criação do

alfabeto dos computadores eletrônicos, a base da linguagem para a qual todas as informações são traduzidas e na qual são armazenadas e utilizadas no interior do computador. (GATES, 1995, p. 37-38).

Na década seguinte, nos Estados Unidos, na Universidade da Pensilvânia, o primeiro computador de grande porte foi criado para resolver problemas balísticos, sendo John Presper Eckert e John W. Mauchly seus inventores. Tal foi chamado de ENIAC (Electrical Numerical Integrator and Calculator), e mais se assemelhava a uma calculadora gigante, tinha 17.468 válvulas de 16 tipos diferentes, ocupava uma sala inteira, pois tinha mais de 30 metros de largura por 3 metros de altura (SILVA, 2003).

Algumas décadas se passaram até que a computação começasse a habituar escritórios e casas; eis que, atualmente, o computador se transformou em uma ferramenta vital de qualquer atividade social, sendo praticamente impossível imaginar qualquer ação humana que prescindia, em todas as suas fases, a era da informática (RAHAL, 2003).

Eis que a Internet dá seus primeiros passos, em 1969, na organização Advanced Research Projects Agency – Rede de Agência de Projetos de Pesquisa

* Artigo redigido sob orientação do professor Junio Cesar Mangonaro (UNOPAR).

Avançada (ARPANET) – nos Estados Unidos (BRASIL, 2000, p. 19)¹.

Desta forma, com o computador e o advento da Internet, surge um novo espaço de interação entre os homens, isto é, os mesmos possibilitaram a criação de um novo mecanismo de comunicação; esse se tornou um meio em que os usuários são livres emissores e receptores de informação.

Contudo, com o alcance cada vez maior de informações, a redução de custos, dentre outras vantagens e facilidades, fez com que, nesse novo espaço, surgissem novas problemáticas e novas situações a serem enfrentadas pelo homem moderno.

2 A Proteção à Intimidade, à Vida Privada, à Privacidade

2.1 Conceitos e Diferenciações

Em 1948, a Assembléia Geral das Nações Unidas estabelece por meio de um documento intitulado Declaração Universal dos Direitos do Homem os direitos de liberdade além das fronteiras físicas dos Estados e os meios de proteção aos mesmos (DECLARAÇÃO..., 2005).

Esse documento é de suma importância, haja vista que nele se encontram proteções inerentes à vida privada, à luz do art. 12:

Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo homem tem direito à proteção da lei contra tais interferências ou ataques. (RAHAL, 2003, p. 30).

Por seu turno, o art. 11 da Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), promulgada pelo Decreto nº 678, de 06-11-92, dispõe que “toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade” (RAHAL, 2003, p. 30).

A acuidade de tais direitos eleva-se na medida em que a autonomia da vida privada passa a ser ameaçada em decorrência das novas modalidades de invasão científica e tecnológica.

Nesse sentido, a Constituição da República de 1998 corroborou invioláveis nos dizeres do artigo 5º, X, “a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado do direito à indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 2004).

Rahal (2003, p. 32) reza “[...] que a inovação constitucional teve direta relação com a publicidade inerente à mídia, ao exercício da liberdade de informação e às inovações tecnológicas”.

Entretanto, várias são as denominações utilizadas no que tange ao direito à intimidade, quase sempre equivalente ao direito à privacidade e à vida privada. Todavia, consoante Moraes (2004, p. 208), em sua obra Direito Constitucional, nos ensina que:

a intimidade relaciona-se às relações subjetivas e de trato íntimo da pessoa, suas relações familiares e de amizade, enquanto a vida privada envolve todos os demais relacionamentos humanos, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo, etc.

Contudo, o mesmo dispositivo em comento (art. 5º, X) declara invioláveis a honra e a imagem das pessoas. Por honra, entende-se “o conjunto de qualidades que caracterizam a dignidade da pessoa, o respeito dos cidadãos, o bom nome, a reputação”. A inviolabilidade da imagem da pessoa “consiste na tutela do aspecto físico, como é perceptível visivelmente” (SILVA, 2001, p. 208).

Todavia, o direito à preservação da honra e da imagem, no entender de SILVA (2001, p. 208) não se coaduna propriamente ao direito à privacidade e à intimidade, haja vista que “constituem, pois, objeto de um direito, independente, da personalidade”.

Por oportuno, é de bom alvitre distinguir a honra subjetiva, que se traduz no apreço próprio, na estima a si mesmo, da honra objetiva, que é a consideração para com o sujeito no meio social. Por derradeiro, fala-se em honra comum, peculiar a todos os homens, e em honra especial ou profissional, “que é aquela referente a determinado grupo social ou profissional, cuja sensibilidade, às vezes, se reveste de contornos diversos da média” (MIRABETE, 2003, v. 2, p. 154).

3 A Privacidade e a Honra à luz do direito na era digital

Feitas tais considerações, passa-se a abordar a tutela penal frente aos direitos e garantias previstos no artigo 5º, X da Carta Magna.

Ademais, diante do todo exposto, eis que o presente tema será abordado em duas vertentes, quais sejam: A primeira diz respeito à privacidade no que tange a invasão por meio da Internet com o auxílio do computador. Quanto a segunda, abordar-se-ão as questões ligadas à injúria, à calúnia e à difamação, ou seja, ofensa à honra.

3.1 Da Privacidade

Araújo e Nunes Júnior (2001, p. 109), ensina que, por privacidade,

deve-se entender os níveis de relacionamento social em que o indivíduo habitualmente mantém oculto ao público em geral, dentre eles: a vida familiar, as aventuras amorosas, o lazer e os segredos dos negócios. Assim, dentro dessa esfera teríamos demarcado o território próprio da privacidade, formado por relações marcadas pela confidencialidade.

Embasando-se em René Dotti (1981 apud RAHAL, 2003, p. 31), tem-se que a “intimidade se caracteriza

¹ Os mesmos solicitaram ao seu Departamento de Defesa que elaborassem e construíssem um sistema de transmissão de dados, cuja principal função fosse a de que um computador pudesse se comunicar com outros de tal sorte que as informações transmitidas não ficariam armazenadas numa só máquina, em caso de destruição, ou no caso de um dos troncos (caminho pelo qual trafega o sinal eletrônico) estar obstruído, à procura por outro se daria automaticamente para substituir àquele, haja vista que, naquele momento, a principal preocupação dos Norte-Americanos era com um possível ataque militar soviético, em virtude da Guerra Fria.

como a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais”, ou seja, “este é um direito negativo, pelo qual cada um permita ou não que se exponham fatos, detalhes, características de sua intimidade”.

Em breves palavras, “poderíamos ilustrar a vida social como um grande círculo, dentro do qual um menor, o da privacidade, em cujo interior seria aposto um ainda mais constricto e impenetrável, o da intimidade” (ARAÚJO; NUNES JÚNIOR, 2001, p. 109).

No que concerne ao *nomen juris* genérico dos delitos que afrontam interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos, ou seja, os denominados *hardwares*, bem como redes de computadores e programas de computador, conhecidos por *softwares*, não há um consenso, tendo sido mais utilizada a denominação crimes de Internet.

Tal fenômeno, isto é, os crimes informatizados, surgidos no final do século XX, assinalam todas as modalidades de conduta ilegais realizadas mediante a utilização de um computador, conectado a Internet, que vão desde a movimentação de contas bancárias, pirataria de programas de computador, violação de sistemas de telecomunicação, tanto de pessoas jurídicas, tais como empresas, até mesmo de pessoas físicas, no que diz respeito à invasão de computadores domésticos. Todas essas condutas revelam

uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas. (FERREIRA, 2000, p. 209).

Tais condutas criminosas são de dimensões mundiais, e por serem cada vez mais preocupantes, clama-se por definições. Para a Organization for Economic Cooperation and Development (OECD), o crime cometido por meio de computador é “qualquer comportamento ilegal, aéutico ou não autorizado envolvendo processamento automático de dados e / ou transmissão de dados” (ARAS, 2005); assim,

podendo implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou o uso não autorizado de computadores e redes. (ARAS, 2005).

Quanto à classificação dos crimes informatizados, a classificação mais aceita é a propugnada por Hervé Croze e Yves Bismuth (1986 apud FERREIRA, 2000), os quais distinguem duas categorias:

- a) os crimes cometidos contra um sistema de informática, seja qual for a motivação do agente;
- b) os crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática.

Primeiramente, depara-se com os delitos de informática propriamente ditos, isto é, a figura do computador é utilizada não apenas como meio, mas também como meta, tendo como escopos de tais comportamentos o

próprio computador, seus periféricos, os dados e ainda o sustentáculo lógico da máquina, bem como as informações ali depositadas. Quanto ao segundo caso, trata-se de utilizar o computador apenas como meio de execução na consecução do crime-fim.

Nos dizeres de Gomes (2000), os cybercrimes se dividem em: crimes contra o computador; e crimes por meio do computador, sendo neste o instrumento do fato típico e antijurídico hábil para atingir a *meta optat*, ou seja, a utilização do computador ligado à rede mundial de computadores, indevidamente, servirá de meio para a consumação do crime.

Aras (2005) preleciona que “os criminosos eletrônicos, ou ciberdelinquentes, já foram batizados pela comunidade cibernética de *hackers*, *crackers* e *phreakers*”.

No que tange aos primeiros, em geral, são simples invasores de sistemas, que atuam por espírito de rivalidade, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais, bem como computadores domésticos. Os *crackers*, por seu turno, são os “*hackers* aéuticos”. Invadem sistemas para adulterar programas e dados, furtar informações, valores e prejudicar pessoas. Praticam fraudes eletrônicas e derrubam redes informatizadas, causando prejuízos a vários usuários e à coletividade.

Por derradeiro, os *phreakers* são especialistas em fraudar sistemas de telecomunicações, principalmente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros.

Convém salientar que, no “mundo cibernético”, há essas diferentes designações com relação aos sujeitos e o *modus operandi*. Todavia, para a grande maioria das pessoas, a palavra *hacker* serve para designar o criminoso eletrônico de um modo geral, isto é, ao se ouvir falar em crime digital, logo se está diante de um ciberdelincente.

No âmbito doméstico, cita-se o uso de *sniffers* e a utilização de *cookies*. *Sniffers* são programas intrusos que servem para vasculhar a intimidade de internautas, ao passo que os *cookies* (“biscoitos”, em inglês) são também códigos programados para aderir ao disco rígido do computador que acessa um determinado *site*, e se prestam a colher informações pessoais do usuário. Nesse grupo, também estão os programas Cavalos de Tróia ou *Trojan Horses*, que abrem brechas de segurança em sistemas, permitindo a instalação de uma espécie de janela virtual no computador da vítima e que pode ser aberta ao alvitre do *hacker* para fins ilícitos, sendo esse um dos meios mais simples de invasão a um computador doméstico, tendo como exemplo de tal programa o vulgarmente B.O. ou “*Back Orifice*” cujo grupo criador foi o intitulado “*Cult Of Dead Cow*”.

Desta forma, vislumbra-se que os direitos à intimidade, bem como à privacidade, estão a cada dia mais vulneráveis a sofrer ofensas por meio da Internet, tendo em vista que a tecnologia crescente garante *hackers* de programas específicos para lhe possibilitar ações delituosas e com sucesso, pois a gama de ataques faz com que os meios de defesa, muitas vezes, se tornem inúteis e até mesmo obsoletos.

Contudo, faz-se necessário ressaltar que muitos usuários ainda não estão totalmente preparados para navegar com segurança, na maioria das vezes, por desinformação ou por se tratar de pessoas leigas em informática. Assim, não instalam programas de defesas, bem como tomam medidas simples de proteção, o que facilita ataques à integridade dos mesmos, tendo seus dados e informações devassados e espalhados pelo cybermundo.

3.2 Da Honra

Trata-se agora da honra objetiva, tutelada pelo Código Penal Brasileiro (Decreto-lei 2848/40) à luz dos crimes de calúnia e difamação (artigos 138 e 139, respectivamente), e da honra subjetiva, no que concerne ao crime de injúria (artigo 140). Todavia, semelhante previsão pode ser encontrada na Lei 5.250/67, Lei de Imprensa, nos artigos 20, 21 e 22, respectivamente.

De maneira pueril, Rahal (2003, p. 32) ensina que “os primeiros delitos atingem a ‘honra exterior’ das pessoas, o sentimento manifestado nas relações exteriores de cada um. Já a injúria atinge a ‘honra interior’”.

É de salutar importância asseverar que o Código Penal, em seu artigo 141, inciso III, aumenta a pena em um terço, quando o crime é cometido “na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria”. Em tais casos, o dano normalmente é maior, contudo não se exige a ocorrência desse resultado, por se tratar de um crime formal, isto é,

não há a necessidade de realização daquilo que é pretendido pelo agente, e o resultado jurídico previsto no tipo ocorre ao mesmo tempo em que se desenrola a conduta, havendo separação lógica e cronológica entre a conduta e o resultado.[...] Por isso, são chamados de crimes de consumação antecipada. (MIRABETE, 2002, v. 1, p.134).

A *exceptio veritatis* é admitida pela legislação no que diz respeito aos institutos tratados acima, pois não são direitos absolutos; assim, eis a conveniência estabelecida pelo ordenamento jurídico para provar a verdade ao fato jurídico imputado.

Neste íterim, quando se tratar de ofensa divulgada em salas de bate-papo (*chats*) ou *sites*, o aumento de pena previsto no artigo 141, III, do Código Penal, será aplicado, haja vista que nestes casos propalar a ofensa é bem mais fácil.

Por seu turno, em se tratando de e-mail com destinatário específico ou a conversa “reservada” em *chats* (recurso que alguns provedores disponibilizam em salas de bate-papo impedindo o acesso de terceiros a conversas dos internautas que se utilizam de tal recurso), o ilícito não se torna o conhecido por várias pessoas, assim não desafiam o aumento de pena do mencionado artigo. Porém,

dúvida poderá surgir nos casos nos quais a ofensa for irrogada em e-mails encaminhados a vários destinatários, situação na qual as demais circunstâncias do caso é que indicarão a aplicabilidade ou não do aumento de pena em questão. (RAHAL, 2003, p. 33).

É necessário salientar que, diante dos crimes de calúnia e difamação, Mirabete (2003, v. 2, p. 157) assevera que “consuma-se o crime quando qualquer pessoa, que não a vítima, toma conhecimento da imputação, ou seja, quando ela é ouvida, lida ou percebida por pessoa diversa do sujeito passivo”.

Todavia, no que tange ao crime de injúria, a recíproca não é verdadeira, uma vez que somente “se configura no momento em que a ofensa chega ao conhecimento do próprio ofendido” (RAHAL, 2003, p. 32).

Nesse sentido, ofendida a honra ou a dignidade de alguém estará, ainda que um e-mail tenha sido enviado do ofensor para o ofendido.

Muitas vezes, ao navegar em salas de bate-papo, tanto pelo modo “visitante” (possibilidade de apenas visualizar o conteúdo de conversas estabelecidas por pessoas que não se utilizam do modo “reservado”, já explanado retro), como usuário apto a participar de diálogos, depara-se com muitas figuras enviadas por usuários que expressam gestos de baixo calão, bem como palavras reles, verdadeiras ofensas à honra daqueles que a recebem.

Ainda *hackers*, ao se aproveitar da vulnerabilidade de páginas de Internet, bem como computadores domésticos, invadem-nos e deixam mensagens afrontando a honra de indivíduos ou grupos, expondo em *sites* a terceiros que acessarem naquele momento.

Pelo exposto, é evidente que tais atitudes são casos explícitos de ultraje, passíveis de oferecimento de queixa-crime, nos termos do artigo 145 do Código Penal.

4 Conclusão

Consoante o exposto, não se pode confundir direito à honra com direito à intimidade: “o primeiro, como visto, consiste na visão que a própria pessoa tem de sua dignidade pessoal e o reflexo dessa em olhos alheios” (RAHAL, 2003, p. 32). A idéia de transgressão da honra provém da noção de dignidade, deste modo, está se diante da intimidade, ou seja, a pessoa se furta à exposição.

Neste contexto, os direitos à privacidade e à honra são protegidos à luz da Carta Magna no que diz respeito aos direitos fundamentais dos cidadãos, todavia não o são por meio de lei ordinária.

Destarte, momentaneamente, tal lacuna tem sido preenchida com o uso da interpretação analógica, isto é, os cybercrimes são embasados em tipos penais “genéricos”, ou seja, enquadrando-se na norma penal existente.

Sendo assim, a sociedade clama pela criação de uma lei ordinária ou tipos penais específicos visando tutelar tais direitos mencionados, tidos como fundamentais, passando a reprimir de forma severa condutas delituosas que possam vir a denegri-la.

Referências

ARAS, V. *Crimes de Informática: uma nova realidade*. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=2250>>. Acesso em: 27 fev. 2005.

ARAÚJO, L.A.D.; NUNES JÚNIOR, V.S. *Curso de Direito Constitucional*. São Paulo: Saraiva, 2001.

BRASIL, A.B. *Informática jurídica: o ciber direito*. Rio

de Janeiro: Ciberlex, 2000.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Disponível em: <<http://www.senado.gov.br/sf/legislacao/const/>>. Acesso em: 29 maio 2004.

CORRÊA, G.T. *Aspectos jurídicos da internet*. 2. ed. São Paulo: Saraiva, 2002.

CULT of Dead Cow. Disponível em: <<http://www.cultofdeadcow.com>>. Acesso em: 26 ago. 2004.

DECLARAÇÃO Universal dos Direitos Humanos. *Wikipédia*: a enciclopédia livre. Disponível em: <http://pt.wikipedia.org/wiki/Declara%C3%A7%C3%A3o_Universal_dos_Direitos_Humanos>.. Acesso em 26 maio 2005.

FERREIRA, I.S. A criminalidade informática. In: LUCCA, N.; SIMÃO FILHO, A. (Coord.). *Direito e internet*: aspectos jurídicos revelantes. Bauru: Edipro, 2000. p. 207-237.

GATES, B. *A estrada do futuro*. São Paulo: Companhia das Letras, 1995.

GOMES, L.F. *Atualidades Criminais (1)*. Disponível em: <<http://www.direitocriminal.com.br>>. Acesso em: 29 fev. 2005.

MIRABETE, J.F. *Manual de Direito Penal*. 18. ed. São Paulo: Atlas, 2002. v. 1.

_____. *Manual de Direito Penal*. 20. ed. São Paulo: Atlas, 2003. v. 2.

MORAES, A. *Direito Constitucional*. 15. ed. São Paulo: Atlas, 2004.

PAESANI, L.M. *Direito de informática: comercialização e desenvolvimento internacional do software*. 4. ed. São Paulo: Atlas, 2000.

RAHAL, F. Vírus, direito à intimidade e a tutela penal da internet. *Revista do Advogado*, São Paulo, n. 69, p. 25-36, maio 2003.

SILVA, J.A. *Curso de Direito Constitucional Positivo*. 19. ed. São Paulo: Malheiros, 2001.

SILVA, R.C.L.. *Direito Penal e sistema informático*. São Paulo: RT, 2003.

Davi Antunes Pavan*

Graduando em Direito (UNOPAR).

e-mail: <davi.pavan@pop.com.br>

* **Endereço para correspondência:**
Avenida Rio de Janeiro 932 – Apt. 1001 – CEP 86.010-150 Londrina,
Paraná, Brasil.
