Crimes contra a Segurança dos Sistemas de Informações da Administração Pública

Hélio Santiago Ramos Júnior

***Resumo*—**O objetivo do presente artigo é dissertar sobre os crimes praticados contra a segurança dos sistemas de informações da Administração Pública que foram inseridos no Código Penal (CP) através da Lei nº 9.983/2000, isto é, o crime de inserção de dados falsos em sistemas de informações da Administração Pública (art. 313-A do CP) e também o crime de modificação ou alteração de tais sistemas sem a devida autorização (313-B do CP). Pretende-se estudar a doutrina e a jurisprudência acerca desta matéria, concluindo, ao final, sobre a necessidade de políticas de segurança da informação em todos os órgãos da Administração Pública.

***Palavras-chave*—**Crimes de informática, Segurança da Informação, Administração Pública.

I. Introdução

A Lei nº 9.983, de 14 de julho de 2000, alterou o Código Penal brasileiro (Decreto-Lei 2.848, de 07 de dezembro de 1940) e, dentre outras coisas, inseriu dois tipos penais no Código Penal, objetivando especificamente a tutela penal da segurança dos sistemas de informações e bancos de dados da Administração Pública.

Neste sentido, restaram tipificados o crime de inserção de dados falsos em sistemas de informações, conhecido como peculato eletrônico, e também o crime de modificação ou alteração não autorizada de sistemas de informações da Administração Pública, respectivamente, nos art. 313-A e 313-B ambos do Código Penal.

É importante mencionar que tanto o art. 313-A quanto o art. 313-B do Código Penal tutela a segurança dos sistemas de informações da Administração Pública e não os sistemas de informações de entidades particulares ou privadas, por isso foram inseridos no Título XI do Código Penal que trata justamente dos crimes contra a Administração Pública.

No primeiro capítulo, será comentado o crime de inserção de dados falsos em sistemas de informações a partir de estudo da doutrina e de pesquisa jurisprudencial acerca da matéria. O mesmo será feito no capítulo segundo em relação ao art. 313-B do Código Penal.

Por último, conclui-se pela necessidade de adoção de políticas de segurança da informação nos órgãos da Administração Pública.

II. O crime de inserção de dados falsos em sistemas de informaçõeS

A. Doutrina

De acordo com o art. 313-A do Código Penal, considera-se crime de inserção de dados falsos em sistemas de informações a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano". A pena atribuída a este crime é de reclusão, de 2 (dois) a 12 (doze) anos, e multa.

Esta norma penal tutela a segurança dos sistemas informatizados e bancos de dados da Administração Pública visando responsabilizar penalmente o funcionário público que, possuindo autorização para acessar o sistema, aproveita-se desta situação para inserir direta ou indiretamente dados falsos, alterar ou excluir dados corretos com a finalidade de obter vantagem indevida para si ou para outrem ou para causar dano.

Assim, "é protegida a Administração Pública, particularmente a segurança do seu conjunto de informações, inclusive no meio informatizado, que, para a proteção de toda a coletividade, devem ser modificadas somente nos limites legais. Daí se punir o funcionário que, tendo autorização para manipulação de tais dados, vem a maculá-los pela modificação falsa ou a inclusão ou exclusão de dados incorretos" (Jesus, 2006, p. 963).

Trata-se de um crime próprio, ou seja, "que exige determinada qualidade ou condição pessoal do agente" (Bitencourt, 2002, p.148). No caso concreto, isto significa dizer que o sujeito ativo deste crime não pode ser qualquer funcionário público, mas somente aquele funcionário autorizado pela Administração Pública para gerir o sistema de informações ou acessar e alterar o banco de dados.

Não obstante o fato de o delito do art. 313-A ser considerado um crime próprio, é possível haver concurso de agentes quando terceiros praticam a conduta descrita no tipo penal em conluio com o funcionário público autorizado o qual vem a facilitar a ação criminosa.

O art. 29, caput, do Código Penal estabelece que quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade. Desta forma,

"nada impede, porém, o concurso de agentes pela participação criminosa, por meio de instigação, ou mesmo a co-autoria, quando a conduta de inserção, alteração ou exclusão é praticada por terceiro" (Mirabete, 2004, p. 313).

No mesmo sentido, "o concurso de pessoas, no entanto, seja co-autoria ou participação, é possível, na modalidade de facilitar, já que nesta o funcionário consente que um terceiro possa adulterar os dados" (Jesus, 2006, p. 964).

A vítima deste crime é o Estado haja vista se tratar de crime praticado contra a Administração Pública, admitindo-se também que o particular possa ser considerado sujeito passivo quando vier a sofrer prejuízo em virtude da prática do crime.

O tipo objetivo do crime de inserção de dados falsos em sistemas de informações abrange as condutas de: inserir dados falsos em sistemas informatizados ou bancos de dados da Administração Pública; facilitar a inserção de dados falsos em tais sistemas por terceiros; alterar indevidamente dados corretos do sistema; e excluir dados corretos do sistema sem a devida autorização. "Trata-se de um tipo misto alternativo, em que a ocorrência de mais um dos núcleos, num mesmo contexto fático, constitui crime único" (Jesus, 2006, p. 964).

O art. 313-A do Código Penal é um crime doloso, que para a sua consumação exige que o agente tenha a vontade de inserir direta ou indiretamente dados falsos, de alterar ou excluir indevidamente os dados corretos do sistema com a finalidade específica de obter vantagem para si ou para outrem ou causar dano.

É considerado um crime formal, pois a sua consumação independe do agente ter conseguido atingir o resultado pretendido. Neste sentido, o crime formal "descreve um resultado, que, contudo, não precisa verficar-se para ocorrer a consumação. Basta a ação do agente e a vontade de concretizá-lo (...)" (Bitencourt, 2002, p. 146).

Para a consumação do crime do art. 313-A do Código Penal é preciso que o agente seja funcionário público autorizado, que pratique a conduta descrita na norma penal e que tenha a vontade de concretizá-la, pouco importando se conseguiu ou não obter o resultado pretendido.

Quando o funcionário autorizado insere dados falsos no sistema de informações da Administração Pública com a consciência de que tais dados são falsos e com a vontade de realizar esta ação para obter vantagem para si ou para outrem ou para causar dano, o crime se consuma a partir do momento em que os dados falsos foram inseridos no sistema de informações, independentemente da obtenção de vantagem ou do dano causado em decorrência da prática do crime.

B. Jurisprudência

Em 2004, o Tribunal de Justiça de Santa Catarina negou provimento a recurso interposto por funcionária pública e por seu comparsa, mantendo a sentença de condenação de ambos, proferida na primeira instância, por violação ao art. 313-A do Código Penal:

Apelação criminal – Inserção de dados falsos em sistema de informações (Art. 313-A do Código Penal) – Autoria e materialidade devidamente comprovadas – Servidora pública que a pedido de seu namorado despachante, inseria dados falsos no sistema do CIRETRAN, liberando os certificados de licenciamento de veículos – Taxas de licenciamento de veículos não recolhidas – Desclassificação para o delito de prevaricação – Condutas que ultrapassam os limites expressos no art. 319 do Código Penal – Diminuição da pena – Arrependimento posterior – Delito praticado por dezessete vezes em continuidade delitiva, demonstrando fragilidade do arrependimento – Aumento que se mostra adequado, considerando o número de reiterações praticadas – Crime praticado em detrimento da Administração Pública – Pena superior a um ano – Perda da função pública – Efeito da condenação – Recursos desprovidos.

Tratando-se de condenação por crime praticado com abuso de dever ou violação de dever para com a Administração Pública, dispensável a indicação dos motivos da decretação por estarem ínsitos na própria fundamentação do convencimento do delito praticado contra a Administração, por serem comuns, devendo a exigência de fundamentação ser específica apenas para os demais casos tratados no art. 92 do Código Penal. (TJSC, Apelação criminal n. 2004.028935-4, de Itajaí, Rel. Des. Solon D'Eça Neves, data do julgado 19/07/2005).

Neste julgado, em síntese, uma funcionária pública, autorizada a lidar com o sistema do Ciretran, e seu namorado foram condenados pelo crime de inserção de dados falsos em sistemas de informações. Ela teria inserido dados falsos no sistema a pedido de seu namorado, digitando no sistema um código de autenticação de pagamento de seguro, entretanto com valor correspondente às taxas de licenciamentos, sem essas estarem recolhidas, com o fim de obter vantagem indevida para si e para o seu comparsa, o qual também foi condenado em virtude de haver participado e instigado a prática do crime.

De acordo com os autos, o esquema funcionava da seguinte forma: "O co-réu, sendo despachante, recebia dos proprietários dos veículos, terceiros lesados, em seu local de trabalho, as quantias que deveriam servir para que efetuasse o pagamento do imposto de propriedade de veículo automotor (IPVA), do seguro DPVAT obrigatório e da taxa de licenciamento de veículo, recolhidas mediante recibo de pagamento expedido pelo banco. Posteriormente, entregaria as guias já pagas à repartição da Polícia Civil, responsável pela expedição dos certificados de registros de licenciamentos de veículos, para então receber os documentos. Ocorre que o co-réu deixava de recolher a taxa de licenciamento de veículo, cujo valor é de R$ 13,00 (treze reais), e encaminhava as guias à co-ré, para que esta burlasse o sistema de automação da Polícia Civil, introduzindo dados falsos e possibilitando que os valores correspondentes às taxas de licenciamentos evidenciassem estar pagos, permitindo a respectiva liberação dos certificados de registro e licenciamento de veículos, obtendo ambos, dessa forma, vantagem indevida".

No ano de 2005, o Tribunal de Justiça do Rio Grande do Sul absolveu, por ausência de provas, um policial civil

acusado pelo Ministério Público estadual de ter praticado o crime previsto no art. 313-A do Código Penal:

Apelação crime. Inserção de dados falsos em sistemas de informações. Art. 313-A, CP. Não é possível concluir que seja o acusado o autor do crime só porque ele seria o único a obter vantagens com a exclusão dos dados Assim, não havendo prova suficiente da participação do réu na prática da infração penal impõe-se a absolvição. (TJRS, Apelação Crime nº 70011793890, Quarta Câmara Criminal, Comarca de Garibaldi, Rel. Des. José Eugênio Tedesco, data do julgado: 18/08/2005).

Neste caso, a denúncia do Ministério Público acusou o réu de ter excluído indevidamente dados dos sistemas informatizados da Polícia Civil com o fim de obter vantagem indevida para si e para sua companheira. Tal vantagem consistiria em retirar do sistema de informações da Polícia Civil dados referentes ao envolvimento do réu e de sua companheira em ocorrência policial ou termo circunstanciado. Entretanto, o réu foi absolvido pelo tribunal em razão da ausência de provas de que o mesmo teria praticado a conduta descrita no art. 313-A do CP.

III. CRIME DE MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMAS DE INFORMAÇÕES

A. Doutrina

O crime de modificação ou alteração não autorizada de sistemas de informações está tipificado no art. 313-B do Código Penal e consiste na conduta de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação da autoridade competente".

A pena aplicável a este crime é de detenção, de 03 (três) meses a 02 (dois) anos, e multa. No entanto, se a modificação ou a alteração resultar dano para a Administração Pública ou para o administrado, a pena é aumentada de um terço até a metade.

No que se refere à objetividade jurídica, "protege-se a Administração Pública, particularmente a incolumidade de seus sistemas de informações e programas de informática, que só podem sofrer modificações ou alterações quando a autoridade competente solicita ou autoriza a determinado funcionário. Por isso, não havendo tal aquiescência, a conduta é punida, tanto mais por se levar em consideração que tais informações, muitas vezes, encerram sigilo e interesses estratégicos do próprio Estado" (Jesus, 2006, p. 965).

Trata-se de crime próprio que, em regra, somente pode ser praticado por funcionário público haja vista a expressa referência a esta qualidade no tipo penal.

É oportuno mencionar que o art. 327, caput, do Código Penal estabelece que, para efeitos penais, considera-se funcionário público quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública; sendo que o §1º deste artigo determina que se equipara a funcionário público quem exerce cargo, emprego ou função pública, em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.

Outro aspecto importante que cabe destacar é que, diferentemente do artigo anterior (art. 313-A) que exige que o funcionário público, autor do crime, seja autorizado pela Administração Pública para operar o sistema, o crime previsto no art. 313-B, por sua vez, pode ser praticado por qualquer funcionário público desde que a modificação ou alteração do sistema de informações ou do programa de computador não tenha sido autorizada nem solicitada pela autoridade competente.

Neste sentido, entende a doutrina:

"Crime funcional próprio, só pode ser praticado por funcionário público no exercício do cargo, sem, no entanto, haver sido autorizado ou obtido solicitação da autoridade competente para a finalidade de alterar sistema de informações ou programa de informática" (Jesus, 2006, p. 965).

"O novo dispositivo trata de crime próprio, sendo o agente funcionário público, esteja ou não autorizado a operar o sistema de informações ou o programa de informática. Nada impede, porém, a participação de terceiro, por instigação ou auxílio material ou moral" (Mirabete, 2005, p. 2335).

Tendo em vista se tratar de crime contra a Administração Pública, o sujeito passivo é o Estado e, como conseqüência, pode ser vítima também o administrado que venha a sofrer prejuízo em virtude da modificação ou alteração do sistema de informações ou programa de informática.

O crime de modificação ou alteração não autorizada de sistemas de informações abrange as condutas de: modificar sistema de informações ou programa de informática; e alterar sistema de informações ou programa de informática.

Há uma discussão doutrinária no sentido de verificar se tais verbos possuem ou não o mesmo significado, não obstante a esta divergência, pode-se considerá-los como sinônimos na medida em que se pode dizer que, de fato, toda alteração gera uma modificação no sistema de informações ou no programa de informática.

Damásio Evangelista de Jesus argumenta que não se trata de verbos idênticos "já que modificar pretende-se a dados que dizem respeito à estrutura do sistema (de dados) ou ao programa de informática. Já o alterar vincula-se a informações contidas no sistema ou no programa. Ponderamos que a colocação de dois núcleos tão parecidos teve a finalidade de não deixar dúvidas aos intérpretes e aplicadores da norma penal. Trata-se de um tipo misto alternativo, em que a concretização de mais de um dos núcleos, num mesmo contexto fático, constitui crime único" (Jesus, 2006, p. 965).

O art. 313-B do Código Penal se caracteriza como um crime doloso, isto é, exige-se que o funcionário público tenha a intenção de modificar ou alterar sistema de informações ou programa de informática da Administração Pública sem autorização da autoridade competente.

Trata-se de um crime de mera conduta, ou seja, basta que o agente pratique o comportamento descrito na norma penal para a sua consumação. No caso, o crime se consuma com a

simples modificação ou alteração do sistema de informações ou do programa de informática desde que a conduta seja praticada sem que haja autorização ou solicitação da autoridade competente.

Neste sentido, "consuma-se o crime previsto no art. 313-B com a modificação ou alteração total ou parcial do sistema de informações ou do programa de informática, independentemente de haver ou não prejuízo efetivo para a Administração Pública ou terceiro. Se este ocorrer, o crime será qualificado" (Mirabete, 2005, p. 2.336).

O crime será qualificado quando a modificação ou a alteração resultar dano para a Administração Pública ou para o administrado, circunstância em que a pena aplicada será aumentada de um terço até a metade, nos termos do parágrafo único do art. 313-B do Código Penal.

B. Jurisprudência

No ano passado, em outubro de 2006, o Tribunal Regional Federal da 4ª Região negou provimento a recurso de apelação interposto por um estagiário do Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul (UFRGS) condenado pelo crime de modificação ou alteração de sistemas de informações:

Apelação criminal. Art. 313-B e Art. 327, § 1º, ambos do Código Penal. Modificação e alteração não autorizada de sistema de informação da UFRGS. Processo administrativo disciplinar realizado no âmbito da universidade. Réu confesso. Prova testemunhal uníssona. Materialidade e autoria comprovadas. Dano demonstrado. Condenação.

As provas colhidas no Processo Administrativo Disciplinar realizado no âmbito de Universidade, posteriormente ratificadas integralmente em juízo, são aptas a ensejar condenação.

O réu que, na condição de bolsista (estagiário) do Centro de Processamento de Dados da UFRGS, desempenha função pública é, para fins penais, equiparado a funcionário público.

Para a configuração do delito tipificado no art. 313-B do CP é irrelevante o prejuízo, o qual, se ocorrer, poderá ensejar a causa de aumento de pena prevista no parágrafo único do mencionado artigo.

No caso de resultar dano para a Administração ou para o administrado, incide a majorante prevista no parágrafo único do art. 313-B, ainda que o prejuízo não seja de natureza patrimonial.

Apelação desprovida. (TRF 4ª Região, Apelação Criminal nº 2005.71.00.016873-9/RS, Rel. Des. Federal Maria de Fátima Freita Labarrère, publicado no D.J.U. de 11/10/2006).

No caso, o aluno bolsista confessou que utilizou a senha de um funcionário para ter acesso ao sistema informatizado de controle de dados da UFRGS para alterar o conceito em disciplinas e o vínculo de cursos de graduação, de forma que se considerou estarem comprovadas a autoria e a materialidade do crime.

O réu alegou que o crime foi praticado tão somente com o objetivo de adquirir conhecimentos a respeito do funcionamento do sistema alterado, entretanto este argumento foi contestado pelo Ministério Público Federal que o denunciou, tendo em vista que as alterações foram realizadas de forma contínua por um período de 8 (oito) meses, bem como se constatou que o réu alterou seus conceitos (notas) em disciplinas por diversas vezes.

Mesmo o réu sendo bolsista contratado pela Fundação de Apoio da Universidade Federal do Rio Grande do Sul (FAURGS), entidade de direito privado, por exercer função pública junto ao Centro de Processamento de Dados da UFRGS, foi equiparado à condição de funcionário público, nos moldes do §1º do art. 327 do Código Penal.

Portanto, o Tribunal Regional Federal da 4ª Região manteve a decisão do juízo de origem que condenou o réu pelo crime de modificação ou alteração de sistemas de informações ou programa de informática, reconhecendo que se trata de crime de mera conduta, que independe de prejuízo para a sua consumação, sendo que uma vez constatado prejuízo para a Administração Pública ou para o administrado, o crime passa a ser qualificado, com aumento da pena nos termos do parágrafo único do art. 313-B do CP.

IV. Proteção Jurídica dos Sistemas de Informações da Administração Pública na Sociedade em Rede

A proteção jurídica dos sistemas de informações dos órgãos da Administração Pública é fundamental para que seja possível responsabilizar penalmente o agente que atentar contra a segurança de tais sistemas.

Em 2006, um hacker, identificado como “Lady Diana”, invadiu o sistema de informática do governo do Estado do Rio Grande do Norte e modificou as páginas iniciais de diversos órgãos vinculados ao Poder Executivo.

Logo em seguida, argumentava-se que a conduta deste indivíduo estaria tipificada pelo art. 313-B do Código Penal. Entretanto, tratou-se de uma informação equivocada.

Conforme se verificou nos capítulos anteriores, os artigos 313-A e 313-B, ambos do Código Penal, são crimes próprios que somente podem ser praticados por funcionário público, seja individualmente ou em concurso com outros agentes.

A prática de invadir sistemas de informações e modificar páginas da internet é conhecida como *defacement* ou desconfiguração. Neste caso, o que acontece é que o hacker explora falhas e vulnerabilidades da rede, fazendo alterações nas páginas iniciais de órgãos da Administração Pública, sem possuir nenhuma autorização ou vínculo com a mesma.

Em relação ao funcionário público autorizado, evidentemente não é necessário que ele seja um hacker, grande conhecedor das ciências da computação, para praticar tais crimes porque possui livre acesso ao banco de dados ou ao sistema de informações da Administração Pública.

De qualquer forma, mesmo não possuindo autorização, o funcionário está dentro da organização o que facilita consideravelmente a prática do crime, já que se aproveita da confiança que possui em relação ao órgão público no qual trabalha.

Diferentemente do funcionário público, o hacker não possui

este vínculo funcional com a Administração Pública, utilizando tão somente os seus conhecimentos e habilidades para modificar páginas, seja de instituições públicas ou privadas.

Assim, nesta hipótese, como não se verifica a possibilidade deste ser equiparado a funcionário público, tal indivíduo que vem a modificar páginas da web de órgãos da Administração Pública somente poderá ser responsabilizado pelo crime do art. 313-A ou 313-B do Código Penal se o praticar em participação ou co-autoria com funcionário público, o que, na prática, dificilmente ocorrerá.

Diante deste cenário, fica evidenciada a necessidade de proteção jurídica dos sistemas de informações da Administração Pública perante terceiros, pois nem sempre o ordenamento penal vigente consegue tutelar de forma eficaz os interesses e bem jurídicos aos quais se dispôs a proteger.

Frise-se que, de início, o projeto de lei que deu origem à Lei nº 9.983/00 objetivava a responsabilização penal dos funcionários públicos autorizados que inseriam dados falsos no sistema de informações da Previdência Social visando à obtenção de vantagem indevida para si ou para outrem.

Entretanto, houve uma alteração ainda na fase de tramitação do projeto de lei que lhe deu origem para que fosse possível a sua aplicação a todos os sistemas de informações e bancos de dados da Administração Pública.

A necessidade de tutela penal visando à proteção dos sistemas de informações da Administração Pública perante terceiros se tornou mais evidente com o advento da internet e de um fenômeno conhecido como governo eletrônico.

Pode-se conceituar o governo eletrônico como "uma infra-estrutura única de comunicação compartilhada por diferentes órgãos públicos a partir da qual a tecnologia da informação e da comunicação é usada de forma intensiva para melhorar a gestão pública e o atendimento ao cidadão. Assim, o seu objetivo é colocar o governo ao alcance de todos, ampliando a transparência das suas ações e incrementando a participação cidadã" (Rover, 2005, p. 55).

Além da transparência e da publicidade, há também o princípio constitucional da eficiência administrativa que foi inserido no caput do art. 37 da Constituição Federal pela Emenda Constitucional nº 19/98 e que serve de argumento para justificar a informatização e modernização da Administração Pública.

Trata-se de princípios constitucionais que trouxeram a necessidade de utilização da internet como um meio para tornar o governo mais eficiente e mais próximo do cidadão. Neste sentido, "a Lei nº 9.755, de 16 de dezembro de 1998, ao dispor sobre a criação de homepage na Internet, pelo TCU, para divulgação dos dados e informações, criou a norma jurídica necessária para o cumprimento do previsto no art. 37 da Constituição Federal brasileira, no que diz respeito aos princípios da transparência e da publicidade nesse novo modo de organização da sociedade e do Estado" (Olivo, 2004, p. 175).

Exemplos desta nova realidade são a declaração de imposto de renda pela internet, o uso do pregão eletrônico nas compras públicas, a informatização do processo judicial através da Lei nº 11.419, de 19 de dezembro de 2006 dentre outros.

Os fenômenos do governo eletrônico e da Administração Pública em rede justificam a necessidade de uma adequada tutela penal para os sistemas de informações dos órgãos públicos perante terceiros visando à proteção e segurança jurídica de tais sistemas em face dos crimes de informática.

Assim, está em tramitação o projeto de lei substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003 que, dentre outras coisas, pretende inserir o art. 339-A no Código Penal tipificando a conduta de "acessar indevidamente rede de computadores, dispositivo de comunicação ou sistema informatizado". É caracterizado como um crime de mera conduta, ou seja, basta o agente praticar o acesso indevido para consumar o delito,

O projeto substitutivo também define, no art. 339-C, inciso III, o conceito de sistema informatizado para fins penais como: "o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador, ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente".

Independente da constatação ou não da necessidade de uma tutela penal mais adequada para o caso concreto envolvendo a segurança dos sistemas de informações de entidades públicas, percebe-se que há uma necessidade constante de adoção de políticas de segurança da informação em todos os órgãos da Administração Pública.

Neste sentido, o Tribunal de Contas da União elaborou cartilha contemplando as melhores práticas em Segurança da Informação para serem utilizados na Administração Pública.

Por fim, é oportuno mencionar também que o Decreto nº 3.505, de 13 de junho de 2000, instituiu a Política de segurança da Informação nos órgãos e entidades da Administração Pública Federal, estabelecendo como alguns pressupostos básicos a criação, desenvolvimento e manutenção de mentalidade de segurança da informação; capacitação científico-tecnológica do País para o uso da criptografia na segurança e defesa do Estado; e, conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

REFERÊNCIAS

[1] C. R. Bitencourt, *Manual de Direito Penal*: parte geral. vol. 1. 7.ed. São Paulo, SP: Saraiva, 2002, 744 p.

[2] "Lady Diana invade sites de repartições do Estado". In: *Diário de Natal*. Natal, terça-feira, 14 de novembro de 2006. p.6. Disponível em: < http://pesquisa.dnonline.com.br/document/?view=13006>. Acesso em: 10 set. 2007.

[3] Brasil. Tribunal de Contas da União. *Boas práticas em segurança da informação*. Brasília: TCU, 2003. 70 p.

[4] C. Delmanto et al. *Código Penal comentado*. 6.ed. Rio de Janeiro, RJ: Renovar, 2002, 1100 p.

[5] D. E. de Jesus. *Código penal anotado*. 17.ed. atual. São Paulo: Saraiva, 2006. 1181 p.
[6] J. F. Mirabete; R. N. Fabbrini. *Manual de direito penal*. parte especial. v.3. 19.ed. arts.235-361. São Paulo: Atlas, 2004.
[7] J. F. Mirabete. *Código Penal interpretado*. 5.ed. São Paulo: Atlas, 2005. 2700 p.
[8] L. C. C. de Olivo. *A Reglobalização do Estado e da Sociedade em Rede na Era do Acesso*. Florianópolis: Fundação Boiteux, 2004. 221 p.
[9] A. J. Rover. "Governo eletrônico: uma introdução". In: *Anais da II Conferência Sul-Americana em Ciência e Tecnologia Aplicada ao Governo Eletrônico*. Ijuris: Florianópolis, 2005. pp. 53-64.

Hélio Santiago Ramos Júnior é bacharel em Direito pela Universidade Federal de Santa Catarina (UFSC), mestrando em Engenharia e Gestão do Conhecimento EGC/UFSC. Membro do Grupo de Pesquisa Informática Jurídica, Direito e Tecnologia CNPQ/UFSC.