artigo de revisão

LEIS, DECRETOS E NORMAS SOBRE GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

LAWS, DECREES AND STANDARDS FOR INFORMATION SECURITY MANAGEMENT IN GOVERNMENT AGENCIES

Wagner Junqueira de Araújo
Doutor em Ciência da Informação pela Universidade de Brasília, Brasil.
Professor do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, Brasil.
E-mail: wagnerjunqueira.araujo@gmail.com

RESUMO: Este artigo faz uma revisão na legislação vigente que aborde temas relacionados com gestão da segurança da informação até Julho de 2012, aplicadas aos órgãos do Governo Federal. Além de uma reflexão dos possíveis impactos provocados pela Lei nº. 12.527, promulgada em novembro de 2011, nas normas e decretos em vigor. O objetivo é que esta revisão venha contribuir para futuras pesquisas sobre o tema na área da Ciência da Informação. Foi verificado na redação dos documentos analisados que termos foram utilizados com definições diferentes. Especificamente na redação do Decreto nº.4.553 e da Lei nº.12.527, apesar de uma Lei se sobrepor a um Decreto, manter textos em documentos normativos oficiais com redações distintas pode gerar confusões ou abrir margens a diferentes interpretações. Também foram constatadas divergências nos prazos e procedimentos para classificação da informação.

Palavras-chave: Segurança da informação – Gestão. Classificação da informação. Administração pública federal. Lei nº.12.527. Decreto nº.4.553.

ABSTRACT: *This paper is a review in Brazilian current legislation that covers topics about information security management until July 2012 and applied to federal government agencies. Besides reflecting the potential impacts caused by Law 12.527. The objective is that this review will contribute to future research on the topic in the area of information science. It was verified in the corpus of the documents examined that same terms have been used with different definitions, in particular in the wording of Decree 4.553 and Law 12.527. Maintain terms in normative documents with different compositions cloud be cause confusion or different interpretations. Were also verified differences in the timing and procedures for information classification.*

Keywords*:* *Information Security Management. Information Classification. Government agencies. Law 12.527. Decree 4.553.*

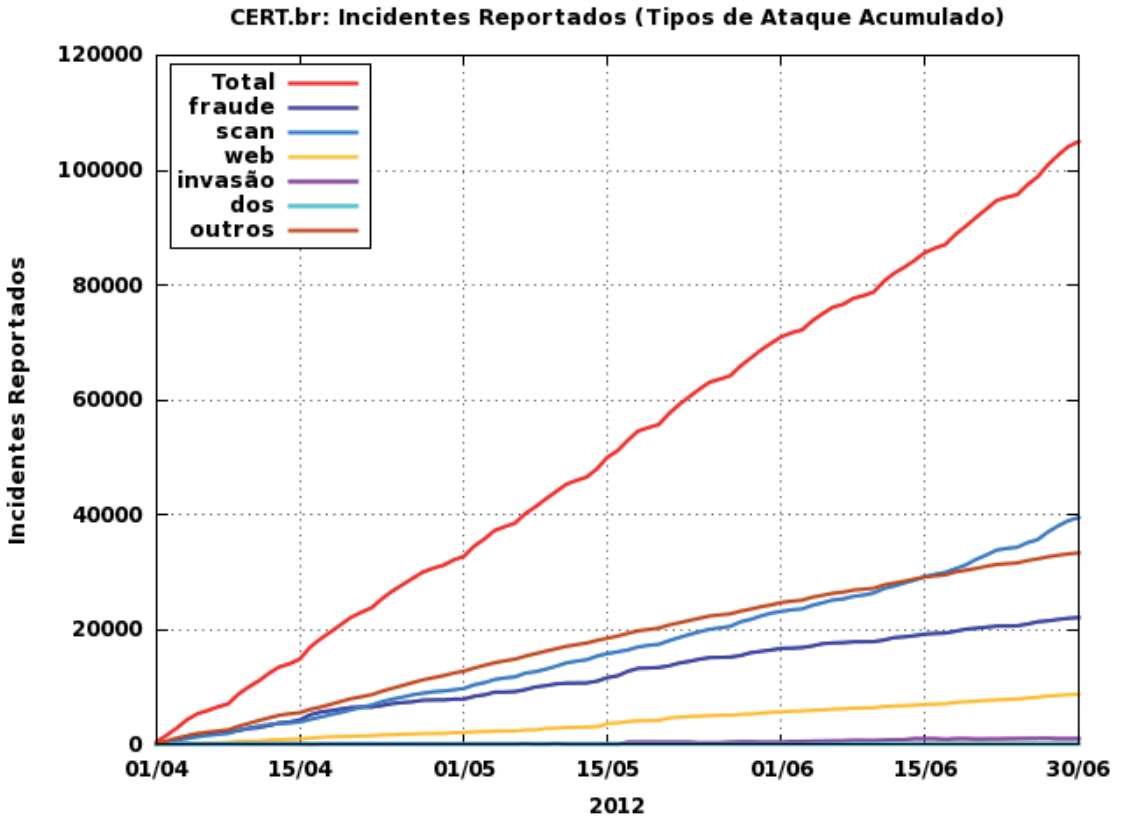
1 Introdução

Ações para segurança da informação acontecem desde tempos mais remotos, Singh (2001) apresenta várias situações na história da humanidade onde determinada informação deveria ser protegida. O autor descreve os esforços para proteger a informação e outros tantos para encontrá-la.

Em tempos mais recentes, é comum nos depararmos com notícias sobre vazamento de informações sigilosas, conforme pode ser constatado nos relatos de Ribeiro (2007); ou em O Globo (2012). Estes exemplos foram selecionados com cuidado em um universo de casos que são publicados quase que diariamente. O primeiro relata o vazamento de informações de contribuintes da base de dados da Receita Federal do Brasil, o segundo se refere a problema semelhante, mas sobre informações de uma CPI (Comissão Parlamentar de Inquérito) conduzida no Senado Federal. O que demonstra que mesmo organizações governamentais em diferentes esferas estão suscetíveis a estes problemas.

Segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (BRASIL, 2012a) somente no período de abril a junho de 2012 cerca de 80.000 ataques foram registrados. Estes registros são computados por meios de notificações voluntárias e refletem os incidentes ocorridos em redes e reportados espontaneamente ao CERT.br. A figura 1 ilustra este cenário.

Figura 1 – Total acumulado por tipo de ataques reportados.



Fonte: www.cert.br

Cada tipo de ataque é descrito conforme indicado:

> dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
>
> invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
>
> web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
>
> scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles..
>
> fraude: qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro. Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
>
> outros: notificações de incidentes que não se enquadram nas categorias anteriores. (BRASIL, 2012)

Os problemas de vazamento de informações, ou quebra de sigilo em organizações públicas são recorrentes. Entretanto, há tempos o Governo Federal brasileiro vem implementando procedimentos para gestão da segurança da informação com vistas a minimizar tais problemas. Grande parte destas ações está registrada em normas, decretos e Leis.

Este artigo faz uma revisão na legislação vigente até Julho de 2012 e uma reflexão dos possíveis impactos provocados pela Lei nº.12.527 promulgada em novembro de 2011 e que entrou em vigor em maio de 2012. O texto desenvolvido foca nas legislações aplicadas aos órgãos públicos federais, pois a Lei nº.12.527 afeta estas entidades. Apesar da segurança da informação ser uma preocupação antiga, ainda é um tema pouco explorado como objeto de pesquisa pela Ciência da Informação - CI, fato que foi constatado ao se consultar a biblioteca de teses e dissertações digitais - BDTD do IBICT em 22 de março de 2012, quando uma consulta com o termo "segurança da informação", para trabalhos depositados nos últimos cinco anos, teve como resposta a indicação de 51 trabalhos, sendo apenas sete trabalhos desenvolvidos em Departamentos de Pós-graduação em CI. O objetivo deste artigo é que esta revisão venha contribuir para futuras pesquisas sobre o tema na área da CI.

2 Leis, decretos e normas em segurança da informação

O Brasil não possui uma Lei única para tratar a "segurança da informação", mas no conjunto de sua legislação, várias podem se aplicadas ao tema, conforme apresentado por Vieira (2008).

Em tempos da informação virtual, a preocupação com os crimes de roubo ou vazamento de informações digitais ou sua divulgação em canais digitais é constante. Um exemplo claro dessa situação são as publicações do portal WIKILEAKS (wikileaks.org) que expõem informações sigilosas de governos do mundo todo.

Para combater este tipo de problema o governo Brasileiro promulgou a Lei nº.9.983, de 14 de julho de 2000 em que o artigo 313-A trata da inserção de dados falsos em sistema de informações e o 313-B da modificação ou alteração não autorizada de sistema de informações.

> Art. 313-A. 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: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.(BRASIL, 2000b)

A Medida Provisória nº.2.200 de 28 de Junho de 2001 que Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências. Somam-se a estes, dois Decretos, o nº.3.505 de 13 e junho de 2000 que "institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal" e o nº.4.553, de 27 de dezembro de 2002 que

> dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

Sendo que este último vai necessitar de revisão na sua redação pela Presidência da República, conforme será discutido no próximo tópico deste artigo.

Além dos dois Decretos, foram identificados duas Instruções Normativas, uma da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão e outra do Gabinete de Segurança Institucional da Presidência da República. Também foram localizadas 14 normas complementares, conforme indicado no Quadro 1.

Quadro 1 – Relação de instruções normativas e normas sobre segurança da informação

Instruções Normativas Normas	Ementa
Instrução Normativa Nº 4 - SLTI/MPOG, de 12 de novembro de 2010	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 Nov 2010- Seção 1)
Instrução Normativa GSI Nº 1, de 13 de junho de 2008	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.(Publicada no DOU Nº 115, de 18 Jun 2008- Seção 1)
Norma Complementar nº 02/IN01/DSIC/GSIPR	Metodologia de Gestão de Segurança da Informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1)
Norma Complementar nº 03/IN01/DSIC/GSIPR	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1)
Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1
Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1)
Norma Complementar nº 06/IN01/DSIC/GSIPR	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1)
Norma Complementar nº 07/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 86, de 7 Maio 2010 - Seção 1)

... continuação do quadro 1

Instruções Normativas Normas	Ementa
Norma Complementar nº 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1)
Norma Complementar nº 09/IN01/DSIC/GSIPR	Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 222, de 22 Nov 2010 - Seção 1)
Norma Complementar nº 10/IN01/DSIC/GSIPR	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 11/IN01/DSIC/GSIPR	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 12/IN01/DSIC/GSIPR	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 13/IN01/DSIC/GSIPR	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 14/IN01/DSIC/GSIPR	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 15/IN01/DSIC/GSIPR	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1)

Fonte: Departamento de Segurança da Informação e Comunicações – DSI do Gabinete de Segurança Institucional da Presidência da República – GSIPR

O conteúdo dos documentos listados deve ser observado por todos os órgãos da gestão pública federal. Ainda existe todo um conjunto de normas e instruções normativas que não foram listadas neste artigo. A saber, as emitidas pela Receita Federal do Brasil[1] que regulam a segurança da informação nas transações da

1 http://www.receita.fazenda.gov.br/Legislacao/LegisAssunto/certificacaodigital.htm

sociedade com este órgão por meio da utilização de certificados digitais. As publicadas pelo Banco Central[2], normas específicas para gestão segurança da informação que deve ser seguida por todas as instituições financeiras em operação no Brasil. As elaboradas pelo Conselho Nacional de Justiça para entidades do Judiciário. Além de legislações específicas de alguns Estados da Federação.

O Tribunal e Contas da União (TCU) mantém uma comunidade virtual[3] sobre segurança da Informação onde os participantes tem acesso a noticias e documentos que abordam o tema. Outro órgão que disponibiliza material sobre Segurança da Informação é o Ministério do Planejamento, Orçamento e Gestão que além das instruções normativas listadas no quadro 1, o Ministério elaborou o documento e-Ping[4] que trata sobre

> [...] padrões de Interoperabilidade de Governo Eletrônico – define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.(BRASIL, 2012b)

Para os órgãos do poder executivo federal, a adoção dos padrões e políticas contidos na e-Ping é obrigatória, conforme determina a Portaria SLTI/MP nº.5, de 14 de julho de 2005. As recomendações do e-Ping abordam 5 temas: Interconexão; Segurança; Meios de Acesso; Organização e Intercâmbio de Informações; e Áreas de Integração para Governo Eletrônico.

Com documentos e serviços destinados a sociedade em geral, o Comitê Gestor da Internet no Brasil – CGI.br dá uma atenção especial à segurança da informação. Entre os serviços disponibilizados pelo portal CGI.br estão as atividades do Cert.Br que desenvolve projetos de análise de tendências de ataques, com o objetivo de melhor entender suas características no espaço da Internet Brasileira (BRASIL, 2012a).

Entre os conteúdos disponibilizados pelo Cert.br destacam-se a cartilha de segurança[5] e dois portais: o portal da Internet Segura[6] - onde são disponibilizados documentos sobre os riscos de navegar na Internet, como efetuar compras e transações bancárias com segurança, dicas para ensinar filhos e alunos sobre os riscos da Internet e como proteger sua privacidade no mundo virtual - e o portal AntiSpam[7],

> spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE [do inglês *Unsolicited Commercial E-mail*] (BRASIL, 2012c).

Com a promulgação da Lei nº.12.527, parte da documentação indicada deveria ser atualizada.

3 A Lei 12.527 e suas implicações

Conforme exposto, o Governo tenta por meio de seus instrumentos normativos se precaver contra o acesso e uso indevido da informação que está sob sua guarda. É fato que no Brasil as informações dos órgãos governamentais sempre sofreram restrições de acesso, dadas as dificuldades de gestão da informação destes, ou pelo excesso de zelo em manter tais informações em sigilo, ou por razões menos nobres. Contudo, em maio de 2012 entrou em vigor a Lei nº.12.527 que dispõe "sobre os procedimentos a serem

2 http://www.bc.gov.br/?legislacao
3 http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/seguranca_informacao
4 http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade
5 http://cartilha.cert.br/
6 http://internetsegura.br/
7 http://www.antispam.br/

observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações [...]". A Lei

> regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991. (BRASIL, 2011)

Conforme descrito no inciso XXXIII do artigo 5º. Da Constituição Federal, "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade [...]". Mas alerta que este acesso pode sofrer restrições quando "[...] ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

O inciso II do § 3º do art. 37 trata sobre "o acesso dos usuários a registros administrativos e as informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII". Por fim o § 2º do art. 216 da Constituição Federal indica que cabe "[...] à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem". Para estes artigos da Constituição, a Lei nº.12.527 regula, indica os procedimentos e esclarece qual informação deve ser divulgada e qual deve ser protegida, além de instituir regras para recursos caso haja negação de algum tipo de informação pelos órgãos responsáveis por sua guarda. Em seu capítulo primeiro Art. 4º, são apresentadas algumas definições para termos aplicado na redação da Lei:

> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
>
> II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
>
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
>
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
>
> V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
>
> VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
>
> VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
>
> VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
>
> IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. (BRASIL, 2011)

Observa-se que os itens VI, VII e VIII estão alinhados com as definições de termos sobre segurança da informação contidos na NBR ISO/IEC 27002:2005 e NBR ISO/IEC 27001:2006.

A segurança da informação é caracterizada na NBR ISO/IEC 27002:2005 pela preservação da confidencialidade, integridade e disponibilidade da informação, sendo definidos como:

a) confidencialidade: a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
b) integridade: a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
c) disponibilidade: a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. (ABNT, NBR ISO/IEC 27002, 2005)

Para os órgãos do Governo Federal Brasileiro, a segurança da informação deve ser entendida como:

> A proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000a)

É necessário observar que dar acesso à informação não implica em quebra de sigilo ou de segurança da informação, muito menos que os órgãos de Governo irão divulgar ou publicar informações classificadas como sigilosas na Internet.

A Lei nº.12.527 indica em seu Art. 7º. que a informação, objeto de que trata, compreende, entre outros:

> I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;
>
> II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;
>
> III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;
>
> IV - informação primária, íntegra, autêntica e atualizada;
>
> V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;
>
> VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e
>
> VII - informação relativa:
> a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;
>
> b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.(BRASIL, 2011)

Contudo, neste mesmo artigo, em seu parágrafo primeiro, é feita a seguinte ressalva "[...] o acesso à informação previsto no caput não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado". Em um mundo conectado em rede, onde a informação flui e é tratada como um bem de capital se faz necessário adotar procedimentos para proteger este patrimônio. Organizações, sejam privadas ou públicas, necessitam de pessoal treinado, instrumental tecnológico adequado, processos e controles de segurança para garantir e preservar suas informações de uma gama crescente de ameaças.

Contudo, fica uma questão: o que é "informação sigilosa"? A classificação da informação quanto ao seu sigilo, para os órgãos públicos, foi regulamentada pelo Decreto nº.4.553, de 27 de dezembro de 2002. Este Decreto disciplina a salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam. O artigo 2º. dispõe que:

> Originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. (BRASIL, 2002)

Especifica ainda que, "o acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer" (BRASIL, 2002). Em seu artigo 3º, orienta sobre os processos de gestão da informação, alertando que "a

produção, manuseio, consulta, transmissão, manutenção e guarda de dados ou informações sigilosos observarão medidas especiais de segurança". Em parágrafo único do artigo 3º, atribui responsabilidades, onde "toda autoridade responsável pelo trato de dados ou informações sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento".

No segundo Capítulo, o Decreto nº.4.553 trata do sigilo e da segurança, e apresenta os níveis para classificação da informação, de forma que "os dados ou informações sigilosos serão classificados em ultrassecretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos", determinado que:

> § 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
>
> § 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.
>
> § 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
>
> § 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos. (BRASIL, 2002)

O Decreto nº.4.553 atribui de quem é a competência para classificar os dados e as informações, trata dos prazos de duração da classificação, sobre a reclassificação e desclassificação. No Capítulo III, são apresentados os procedimentos para gestão de dados ou informações sigilosos, aborda tópicos como: a avaliação, preservação e eliminação; expedição e comunicação de documentos sigilosos; registro; tramitação e guarda; reprodução; entre outros.

Alerta-se que o Decreto não foi revogado ou teve sua redação atualizada depois que a Lei nº.12.527 entrou em vigor, portanto neste ponto cabem algumas reflexões. A primeira em relação à terminologia *versus* suas definições apresentadas em ambos os documentos, conforme apresentadas no quadro 2.

Quadro 2 – Diferenças entre definições

Termo	Decreto 4.553	Lei 12.527
Disponibilidade	facilidade de recuperação ou acessibilidade de dados e informações.	qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados
Autenticidade	asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino	qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema
Integridade	incolumidade de dados ou informações na origem, no trânsito ou no destino	qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino

Fonte: elaborado pelo autor

A aplicação de termos com definições diferentes indica uma falta de cuidado dos redatores. Apesar de uma Lei se sobrepor a um Decreto, manter textos em documentos normativos oficiais com redações distintas pode gerar confusões ou abrir margem a diferentes interpretações.

Este mesmo problema é observado na indicação dos níveis de sigilo e nos prazos de restrição ao acesso à informação. Em seu artigo 5º, o Decreto indica que "os dados ou informações sigilosos serão classificados em ultrassecretos, secretos, confidenciais e reservados" (BRASIL, 2002) os demais são denominados como ostensivo "sem classificação, cujo acesso pode ser franqueado"(BRASIL, 2002), portanto cinco níveis. Entretanto na Lei são indicados os níveis de sigilo de ultrassecretos, secretos e reservados, não é considerada a classificação para documentos "confidenciais" nem "ostensivos". A diferença nos prazos de classificação do sigilo são indicados no quadro 3.

Quadro 3 – Divergências nos prazos da classificação da informação

Níveis	Lei	Decreto
Ultrassecreto	Máx. de 25 anos	máx. de 30 anos
Secreto	Máx. de 15 anos	máx. de 20 anos
Confidencial	Não indicado	máx. de 10 anos
Reservado	Máx. de 5 anos	máx. de 5 anos

Fonte: elaborado pelo autor.

Tais discrepâncias podem comprometer de forma direta a aplicação das orientações descritas no Decreto nº.4.553 além das orientações da política de segurança da informação instituída pelo Decreto nº.3.505, de 13 de junho de 2000, para os órgãos e entidades da Administração Pública Federal, que tem como pressupostos básicos:

> a) assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
>
> b) proteção de assuntos que mereçam tratamento especial;
>
> c) capacitação dos segmentos das tecnologias sensíveis;
>
> d) uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
>
> e) criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
>
> f) capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado;
>
> g) conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidades. (BRASIL, 2000a)

São objetivos dessa política:

> a) dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
>
> b) eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
>
> c) promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
>
> d) estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
>
> e) promover as ações necessárias à implementação e manutenção da segurança da informação;
>
> f) promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;
>
> g) promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação;
>
> h) assegurar a interoperabilidade entre os sistemas de segurança da informação. (BRASIL, 2000a)

Classificar a informação para determinar seu grau de proteção é uma tarefa necessária nos procedimentos de gestão da segurança da informação. Além de determinar os níveis de sigilo de forma clara, é necessário indicar os responsáveis por esta classificação. No artigo 27 da Lei nº.12.527 são indicados os responsáveis por esta classificação.

> I - no grau de ultrassecreto, das seguintes autoridades:
>
> a) Presidente da República;
>
> b) Vice-Presidente da República;
>
> c) Ministros de Estado e autoridades com as mesmas prerrogativas;
>
> d) Comandantes da Marinha, do Exército e da Aeronáutica; e
>
> e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
>
> II - no grau de secreto, das autoridades referidas no inciso I, dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista; e
>
> III - no grau de reservado, das autoridades referidas nos incisos I e II e das que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade, observado o disposto nesta Lei. (BRASIL, 2011)

Neste ponto os dois documentos são convergentes. Quanto à classificação do grau de confidencial indicado no Decreto nº.4553, são indicados os mesmos responsáveis pela classificação de reservado.

Mesmo sendo um ativo importante para qualquer organização, é necessário observar que nem toda informação deve ser protegida, pois os custos e os esforços demandados tornariam os processos inviáveis de serem implementados. Portanto, conforme indicado na NBR ISO/IEC 27002:2005, a informação deve ser classificada com foco na gestão da segurança da informação, seguindo orientações específicas.

Este processo visa definir quais ativos de informação devem ser protegidos, e os níveis de proteção que devem ser aplicados, portanto as instruções do Decreto 4.553 são fundamentais para a implementação dos procedimentos de gestão da segurança da informação. É necessário observar uma unicidade na terminologia que indique os níveis de classificação e a definição dos procedimentos de classificação da informação. Como foi demonstrado, esta unicidade não pode ser observada na redação da Lei e no Decreto.

No Brasil, a implementação e as interpretações das Leis sempre passam por um processo de amadurecimento em seu entendimento. Este processo pode ser observado na Lei nº.12.527, em seu Art. 6º é indicado que "cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar[...]" a "proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso".

Contudo, o Portal da Transparência[8] passou a divulgar informações sobre os vencimentos dos funcionários concursados de alguns órgãos públicos do executivo federal. O que levanta as indagações: as informações sobre os salários apresentadas de forma individualizada como está no Portal, não pode ser considerada informação pessoal? Por que os salários dos Ministros, diretores das empresas estatais, não foram disponibilizados? A divulgação deste tipo de informação não coloca esta parte da população vulnerável a ações de engenharia social?

Muitas outras questões podem ser levantadas, cabe à sociedade e aos juristas a busca por repostas.

8 http://www.portaldatransparencia.gov.br/. Consulta em 08 de Ago, 2012.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 27002**: Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 27001**: Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT/CB-21 projeto 21:027.00-017:** Tecnologia da informação, técnicas de segurança, gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000a. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 20 mar. 2012.

BRASIL. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 28 dez. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/ D4553.htm>. Acesso em 20 de mar. 2012.

BRASIL. Lei 9.983, de 14 de julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 17 de jul. 2000b. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9983.htm>. Acesso em 08 de ago. 2012.

BRASIL. Lei 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 de Nov. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 08 de ago. 2012.

BRASIL. CERT.BR. **Incidentes Reportados ao CERT.br - Abril a Junho de 2012**. Brasília: Comitê Gestor da Internet no Brasil, 2012a. Disponível em: < http://www.cert.br/stats/>. Acesso em 08 de ago. 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Padrões de Interoperabilidade de Governo Eletrônico**. Brasília, 2012b. Disponível em: < http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em 14 de ago. 2012.

BRASIL. ANTISPAM.BR. **O que é spam?.** Brasília: Comitê Gestor da Internet no Brasil, 2012c. Disponível em: < http://www.antispam.br/conceito/>. Acesso em 14 de ago. 2012.

O GLOBO. CPI investiga vazamento de informações sigilosas. **O Globo**, Rio de Janeiro, 26 de jun. de 2012. Disponível em < http://glo.bo/LLkl1D>. Acesso em 08 de ago. 2012.

RIBEIRO, S. Polícia prende quadrilha que vendia dados sigilosos da Receita Federal em SP. **G1**, São Paulo, 24 de abr. 2007. Disponível em <g1.globo.com/Noticias/SaoPaulo/0,,MRP26487-5605,00.html>. Consulta dem 08 de ago. 2012

SINGH, S. **O livro dos códigos**: a ciência do sigilo o do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

VIEIRA,T. M. **Quadro da legislação relacionada à segurança da informação**. Departamento de segurança da informação e comunicação. 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#_ftn2>. Acesso em 08 de ago, 2012.