REVISTA PAN-AMERICANA DE DIREITO
OPEN ACCESS ABEC BRASIL

A IMPORTÂNCIA DO COMPLIANCE COMO INSTRUMENTO DE COMBATE AOS CRIMES CIBERNÉTICOS

Luís Augusto Antunes Rodrigues[1]

Resumo

Vigora no Brasil a Lei 13.709/2018 – Lei Geral de Proteção de Dados, visando proteger direitos fundamentais de liberdade e personalidade. Nesta visão a proposta está intimamente ligada à análise da implantação de regras do compliance nos setores de tecnologia empresarial a fim de evitar crimes cibernéticos, identificando na prática o que deve ser feito visando eliminar o vazamento de dados dos seus clientes. O artigo informará sobre a importância do *compliance* nos crimes cibernéticos como as empresas devem proporcionar condições para que os criminosos não tenham acesso aos dados dos clientes. O empresário precisa manter seu nível de segurança tecnológico elevadíssimo, incluindo vários cuidados explicitados ao longo deste. As empresas devem ajudar no combate aos ataques cibernéticos visando o cumprimento de leis específicas. Demonstrar-se-á a necessidade da criação de regras específicas, evitando assim invasões à Internet. Esta tornou-se um paraíso para o desenvolvimento de crimes, principalmente por causa do anonimato. Não se pode negar o avanço da tecnologia, todavia deve-se estar consciente que hoje dependemos dela e que atos ilícitos cada vez mais se tornarão realidade. O que se busca é identificar meios concretos de combater os crimes cibernéticos através do correto uso do compliance no setor de tecnologia das empresas.

Palavras-chaves: Compliance. Crimes Cibernéticos. Internet. Tecnologia.

THE IMPORTANCE OF COMPLIANCE AS A TOOL TO COMBAT CYBERCRIME

Abstract

Law 13.709/2018 - General Law of Data Protection - is in force in Brazil, aiming to protect fundamental rights of freedom and personality. In this view, the proposal is closely linked to the analysis of the implementation of compliance rules in the business technology sectors in order to avoid cybercrime, identifying in practice what must be done aiming to eliminate the leakage of their clients' data. The article will inform about the importance of compliance in cybercrime, how companies should provide conditions so that criminals do not have access to customer data. Business owners need to keep their technological security level very high, including several precautions explained throughout this one. The companies must help in the fight against cyber attacks aiming to comply with specific laws. The need for the creation of specific rules will be demonstrated, thus avoiding invasions to the Internet. One cannot deny the advance of technology, but one must be aware that today we depend on it and that illegal acts will increasingly become a reality. What is sought is to identify concrete means of combating cybercrime through the correct use of compliance in the technology sector of companies.

Keywords: Compliance. Cybercrime. Internet. Technology.

Revista Pan-Americana de Direito
ISSN: 2764-2305
Data de aceite: 20/11/2022
https://doi.org/10.37497/RPD.v2i1.60
Organizado pelo Dr. Fabrizio Bon Vecchio Presidente do Instituto Ibero-americano de Compliance - IIAC com o Instituto Superior de Administração e Línguas — ISAL

[1]Universidade Católica Argentina. – UCA, Buenos Aires, (Argentina). Mestrando em Direito Tributário. E-mail:luisaugustoantunes67@gmail.com

1 INTRODUÇÃO

Segundo definição constante da Wikipedia, provavelmente a mais popular referência geral na própria Internet, a definição de "Internet" é a seguinte:

A internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo TCP/IP que permite o acesso a informações e todo tipo de transferência de dados. Ela carrega uma ampla variedade de recursos e serviços, incluindo os documentos interligados por meio de interligações da *World Wide Web* – (www) (Rede de Alcance Mundial), e a infraestrutura para suportar correio eletrônico e serviços como comunicação instantânea e compartilhamento de arquivos (MARQUES, 2012).

Sendo a Internet este paraíso de informações, e pelo fato destas serem verdadeiras riquezas, atiçaram os criminosos, pois "onde há riqueza, há crime" (CORRÊA, 2000).

Percebe-se isto quando sinais digitais, que venham a representar enormes quantias de dinheiro, podem ser interceptados e "furtados". Os criminosos digitais não precisam mais usar seus revólveres, pistolas ou fuzis para assaltar um banco e trocar tiros com policiais, expondo muitas vezes sua própria vida. Estes agora usam a Internet e sofisticados programas para cometer os mesmos crimes. Sacam o dinheiro dos correntistas dos bancos sem disparar nenhum tiro e evitando colocar suas vidas em risco. Mas este se trata apenas de um dos delitos possíveis de operar pela Internet. Ao longo deste artigo observaremos outros, principalmente na esfera empresarial, e como as empresas devem se precaver destes golpes. Justamente nesta prevenção que se faz muito importante a implementação do Compliance.

2 CRIMES DIGITAIS

Para Neil Barret os "crimes digitais" seriam: (…) a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a Internet ou redes bancárias de maneira ilícita" (BARRET, 2015).

Sabemos que toda sociedade depende da informação e por isto acaba sendo vítima de simples ameaças até o terrorismo exercido na maior rede mundial de computadores.

Já dizia Neil Barret: "(…) a era da informação não afeta apenas as nossas empresas ou correio eletrônico, mas também toda a infraestrutura nacional como a economia. Se os "hackers" podem penetrar em sistemas de computadores existentes em universidades e empresas, por que não em sistemas bancários, de tráfego aéreo, ferrovias, televisão e rádio?" (BARRET, 2015).

Precisamos entender esta nova realidade apresentada com o advento da Internet, baseada na tecnologia de ponta. Como conciliar esta evolução com a evolução das relações humanas? Não resta alternativa, senão buscarmos incansavelmente a prevenção das futuras implicações resultantes deste relacionamento entre humanidade e máquinas, onde a estrutura e a capacidade oferecida pelas máquinas e pelas novas tecnologias igualmente serão utilizadas por criminosos e ciberterroristas. Estes utilizarão estas novas tecnologias para lavar dinheiro, esconder arquivos sobre material ilegal, ou até em uma situação extrema, armar uma conspiração contra determinada ordem, de um Chefe de Estado por exemplo, o que acarretaria até uma guerra mundial.

A Internet com certeza hoje se trata de um lugar propenso ao desenvolvimento de fraudes, devido, sobretudo, a impossibilidade de identificar os seus usuários e à imperfeição dos programas de computadores utilizados para o acesso a ela e seu desenvolvimento. E na esteira de quem busca coibir estas fraudes e crimes, igualmente surgem dificuldades inerentes às novas formas utilizadas para a prática corrente de delitos, vindo à tona a dificuldade em se punir os praticantes destes delitos e de se fazer valer o direito da vítima de tais crimes, porque tal efetividade esbarra no direito de sigilo dos dados de quem está na Internet.

A própria proteção conferida pelos provedores fornece aos criminosos uma falsa sensação de anonimato e, com esta dificuldade de identificá-los, até mesmo uma sensação de ficaram impunes em razão do ordenamento jurídico ainda carecer de normas legais que abriguem todo o arcabouço de crimes praticados pela Internet.

E no campo empresarial, como as empresas vêm sofrendo com estas novas opções de fraude no que diz respeito aos seus controles financeiros e/ou contábeis? Quais as seguranças que as mesmas podem oferecer a seus colaboradores e clientes que não tenham seus dados furtados por “Crackers” ou até mesmo retirados valores de suas contas correntes?

3 A SEGURANÇA CIBERNÉTICA

A informação nos dias atuais trata-se de um ativo organizacional essencial, e consequentemente, deve ser protegida da melhor forma possível. A segurança cibernética tem como objetivo primordial proteger a integridade, a disponibilidade e a confidencialidade de toda e qualquer informação, sendo desenvolvida nas empresas para reduzir a ocorrência dos crimes cibernéticos. Com a implantação de um programa de Compliance eficaz, as empresas atingirão estes objetivos, seguindo alguns procedimentos básicos, tais como: (a) Montar um plano de ação

adequado; (b) Criar um código de conduta; (c) Estabelecer canais de comunicação, internos e externos; (d) Capacitar todos os colaboradores; (e) Monitorar o funcionamento de todo o programa e (f) Avaliar e corrigir os problemas durante a implantação do programa.

Os objetivos da segurança cibernética nas empresas serão alcançados por meio da implantação de um conjunto de regras e controles, tais como políticas internas, processos gerenciais eficazes, procedimentos internos bem-adaptados às reais necessidades da empresa, estruturas organizacionais enxutas, softwares e hardwares capazes de identificar quaisquer anomalias em seus sistemas operacionais, gerenciais, contábeis e financeiros. Estes controles devem ser continuamente monitorados e atualizados para garantir um perfeito alinhamento com os objetivos do negócio em questão.

Sabemos que estes criminosos virtuais já realizaram invasões em organizações tradicionais da área da segurança, tais como Interpol, CIA, NASA, Pentágono, OTAN, e muitas outras, incluindo também os principais bancos mundiais e operadoras de cartões de crédito. Os cibercriminosos atuam no mundo todo e de forma organizada, desafiando todas as medidas de segurança, por mais fortes e eficazes que sejam, e os principais órgãos de investigação no mundo inteiro. Eles têm como propósito principal a violação da confidencialidade, integridade e disponibilidade de dados e informações. Adulteram, indiretamente, a legalidade, a propriedade e a rastreabilidade do conteúdo produzido e armazenado na Internet.

Em determinadas situações, aspectos internos nas empresas podem estimular o rompimento das regras estabelecidas. Frustração, indignação, trabalhos forçados, pressão interna de chefia, raiva ou um simples descontentamento que envolva elementos psicológicos, financeiros e/ou sociais, podem motivar pessoas a tomar o caminho da criminalidade, tanto no meio físico como no digital. Neste último, vindo a utilizar habilidades e conhecimentos em prejuízo de terceiros. Trata-se de uma realidade em empresas, principalmente de grande porte, que indivíduos que detinham status de confiança tenham se envolvido com violações de segurança. Em virtude de fatores pessoais e profissionais, aproveitando oportunidades específicas, falhas nos controles das empresas e do conhecimento adquirido internamente, essas pessoas praticam o crime digital.

4 COMPLIANCE INTERNO NAS ORGANIZAÇÕES

E na prática como um Programa de Compliance instituído dentro de uma organização pode contribuir para diminuir os riscos de ocorrência destes crimes em seus quadros? Como já

identificado anteriormente, algumas ações podem e devem ser realizadas pelas organizações com este intuito, são elas:

a) Fazer uma análise dos riscos – Nessa primeira etapa se faz necessário avaliar todos os problemas de conduta que a empresa possa vir a ser submetida de acordo com a área que atua. Importante destacar que o decreto que regulamenta a Lei Anticorrupção prevê a diferenciação entre as empresas relativas às suas relações com o mercado internacional e/ou com a administração pública.

b) Montar um plano de ação adequado – Nesta segunda etapa se faz necessário o planejamento de uma estratégia interna com o propósito de implantar o programa de Compliance. Neste, para alcançar o resultado almejado, deve ser descrita cada etapa, como serão realizadas, além de pontos nevrálgicos, como a divulgação, a capacitação dos colaboradores e o monitoramento das ações.

c) Criar um código de conduta – Nesta terceira etapa precisa-se que o documento (planejamento elaborado na etapa anterior) seja claro, objetivo e pertinente à realidade da empresa. Não interessa a estética do documento e sim o real significado alinhado aos valores e às necessidades da organização.

d) Estabelecer canais de comunicação, internos e externos – Na quarta etapa, o código criado tem que ser colocado em prática. Para isso, devem ser criados e divulgados canais de denúncia (ouvidoria) e análise de situações. Esses canais obrigatoriamente devem ser abertos tanto para o público interno (os colaboradores da empresa) bem como para o externo (clientes e fornecedores), com o único propósito de identificar ações fraudulentas, procedimentos errôneos e suspeitos, bem como propor soluções internas a fim de evitar prejuízos futuros, consequentes indenizações e/ou ações no judiciário.

e) Capacitar todos os colaboradores – Nesta nova etapa se faz necessário que todos os funcionários estejam conscientes de suas responsabilidades e de seus atos. Todavia, mais importante ainda que essa consciência é o fato deles aderirem ao programa de Compliance. Para proporcionar um engajamento maior por parte dos mesmos devem ser feitos treinamentos periódicos aliados a campanhas de conscientização e de comunicação interna.

f) Monitorar o funcionamento de todo o programa – Na sexta etapa imprescindível que se monitore o funcionamento de cada uma das ações do programa de Compliance. Não basta colocá-las em prática, é necessário acompanhar o desenvolvimento e testar cada um dos componentes do programa, incessantemente, para ter certeza sobre sua efetividade.

g) Avaliar e corrigir os problemas durante a implantação do programa – Por fim, mas não menos importante, as soluções não devem considerar apenas casos isolados, mas sim todo o ambiente que proporcionou tais ocorrências. Ou seja, um programa de Compliance não se trata de um simples adiamento de soluções (quando a chefia identifica os problemas e guarda-os em uma "gaveta" para resolver mais além). O principal objetivo do programa é propor mudanças permanentes na conduta dos membros da empresa, evitando assim inúmeros dissabores no futuro (quem sabe bem próximo!).

5 LEIS DE COMBATE AOS CRIMES CIBERNÉTICOS

E qual a forma legal (leis) que alguns países estão usando para combater estes crimes cibernéticos?

Nos Estados Unidos da América as leis relacionadas ao tema são divididas em duas categorias, quais sejam: as leis estaduais, responsáveis por coibir os casos relevantes de cada Estado, e as leis federais que abrangem crimes com impacto superior, como por exemplo, o movimento de fundos e materiais ilícitos entre os Estados. Atualmente quase todos os Estados norte-americanos possuem leis regulamentando o acesso ilícito a sistemas de computação (software) e a manipulação de dados. O mais interessante é que estas regulamentações classificam ações como a simples posse de informações protegidas por computadores, como por exemplo, palavras-chaves.

O *Wire Fraud Act,* antes ainda do advento da Internet, estatuto federal que regulamenta a matéria, se preocupou em registrar atos ilegais envolvendo a comunicação via telefone, telégrafo, televisão, entre outros meios, entre Estados. Nos dias atuais podemos inserir a Internet nesta modalidade, pois as informações trocadas no seu ambiente virtual (tráfego de dados) estão diretamente relacionadas a comunicação entre os Estados, deslocando a competência para a Justiça Federal.

Sem dúvida alguma, a lei mais importante relacionada aos "crimes" cibernéticos nos Estados Unidos foi promulgada em 1986, denominada *Computer Fraud and Abuse Act* – Lei de Fraudes e Abusos por Computador. Referida lei tipificou atividades divididas em várias categorias, tendo o objetivo de esclarecer ao violador de determinado sistema que sua atividade era ilegal, e, por isso, seria suscetível de penalização, quais sejam:

a) acessar sistemas sem autorização, com o objetivo de obter informação governamental restrita;
b) acessar sistemas sem autorização, com o objetivo de obter informação financeira restrita;

c) ter a intenção de acessar, sem autorização, qualquer computador do governo, ou qualquer computador utilizado pelo governo;

d) transmissão de dados através de computador objetivando fins ilícitos;

Neste contexto é fácil perceber o maior interesse do Estado sobre o particular, pois referidas categorias, fazem menção, quase que de forma exclusiva, com os computadores do governo.

Diferentemente dos Estados Unidos, no Reino Unido não há diferenças entre lei estadual e federal. Todas são igualmente aplicáveis sobre a totalidade do território. O *Computer Misuse Act* – Lei de Abuso por Computadores baseou-se no modelo das leis Norte-americanas. Todavia extrapolou o nível de autorização que lhe havia sido outorgado. Existem na Lei três tipos de crimes em termos genéricos, sendo o segundo e terceiro suscetíveis de privação de liberdade, quais sejam:

Seção 1 – ofensa envolvendo ganhos não autorizados de acesso ao computador que não tenha autoridade. Trata-se da mais geral das especificações, enquadrando desde “hackers” até tentativas de localização de informações específicas dentro de algum sistema.

Seção 2 – ofensa envolvendo o acesso não autorizado a quaisquer computadores, com o propósito de violar a lei, como por exemplo, a publicação de informações obtidas, utilização de informações obtidas, ou para uso de dados com o propósito de violar a segurança de outros sistemas.

Seção 3 – ofensa envolvendo o acesso não autorizado a computadores, com o propósito de alterar os seus dados, obstando assim o funcionamento ou acesso de usuário autorizado.

Já neste contexto, do Reino Unido, nota-se que as três seções da lei conseguem proibir uma gama maior de “crimes” cibernéticos, como a publicação de material particular, confidencial e protegido por direitos autorais, assim como a criação e disseminação de vírus e outros ataques, atingindo assim, seu objetivo principal, qual seja, de tipificar os atos maléficos ao desenvolvimento tecnológico.

No Brasil as principais leis que versam sobre o tema são: a) A lei de Crimes Cibernéticos (Lei 12.737/2012); b) A lei que regulamenta o E-commerce (Lei 7.962/2013); c) o Marco Civil da Internet (Lei 12.965/2014); d) Cadastro Base do Cidadão (Lei 10.046/2019) e a mais importante delas a e) Lei Geral de proteção de Dados (Lei 13.709/2018).

Lei de Crimes Cibernéticos (Lei 12.737/2012)

Até o ano de 2012, o Brasil não possuía nenhuma sanção para crimes de violação ou invasão de sistemas ou outros dispositivos digitais (celulares, tablets e outros), somente existindo algumas

vagas determinações na Lei de Interceptações ou hipóteses de alguns crimes cometidos por funcionários públicos contra a administração pública (leis específicas).

Todavia, em decorrência de fatos envolvendo o vazamento de fotos íntimas de uma atriz global muito conhecida, o Brasil, através de seus legisladores, percebendo a lacuna existente sobre o assunto, criou a Lei nº 12.737/2012, acrescentando os artigos 154-A e 154-B do Código Penal Brasileiro, não recebendo alterações até maio do ano de 2021.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:(Redação dada pela Lei nº 14.155, de 2021)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.(Redação dada pela Lei nº 14.155, de 2021)
>
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012)
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> § 4 Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (Incluído pela Lei nº 12.737, de 2012)
>
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012)
>
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012)
>
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012)

> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012)
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012)
>
> Ação penal(Incluído pela Lei nº 12.737, de 2012)
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012)

A recente criação da Lei nº 14.155/21 agrava as punições previstas no Código Penal acerca de crimes conhecidos como crimes cibernéticos. De acordo com o texto da lei, os crimes de violação de dispositivo de informática, furto e estelionato cometidos de forma eletrônica ou pela internet, ficaram ainda mais graves. Com a nova legislação, a punição que anteriormente era detenção de três meses a um ano e multa passou a ser de um a quatro anos de reclusão e multa visando inibir um pouco mais as ações destes cibercriminosos.

A lei sancionada prevê que a pena de reclusão seja aplicada em condenações mais severas e que o regime de cumprimento possa ser fechado. Já a detenção é aplicada para condenações mais leves e não admite que o início do cumprimento seja em regime fechado.

6 LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018)

A Lei 13.109/18 entrou em vigor em agosto de 2020, tendo como principal objetivo regulamentar a proteção dos dados pessoais, bem como a privacidade desses dados. É uma forma de impor que as empresas e organizações lidem de forma mais responsável com as informações das pessoas.

Com isso, ficam assegurados os direitos fundamentais, que são a liberdade, a privacidade e também o desenvolvimento da personalidade da pessoa natural.

Com a Lei Geral de Proteção de Dados (LGPD) em vigor, as empresas e organizações precisaram mudar o seu comportamento rapidamente. As mesmas têm a obrigação de desenvolver um sistema que assegure a proteção total dos dados de todas as pessoas que nasceram, vivem e/ou estão em território nacional, ou ainda de dados que foram coletados no país.

Através da LGPD tanto os consumidores quanto as empresas em si passaram a observar a importância dessa proteção, que vale tanto para o mundo digital quanto para as empresas físicas. A lei também versa sobre o consentimento e a permissão em compartilhar seus dados, visto que os dados de uma pessoa titular necessitam de autorização expressa para serem compartilhados, bem como o consumidor tem o direito de solicitar o cancelamento ou a exclusão de suas informações de qualquer sistema onde estejam inseridas.

A Lei Geral de Proteção de Dados é um marco deveras importante no Brasil. Com o avanço da internet, o aumento significativo do E-commerce, bem como de bancos digitais, o acesso e a propagação de dados importantes e privativos aumentou de forma exponencial. Por conta disso, aumentou-se também o vazamento de dados.

Assim sendo, uma lei que regulamenta e fiscaliza empresas para que existam dentro delas normas e softwares para proteger os dados dos seus clientes é, sem dúvida alguma, uma decisão essencial.

O rigor da lei 13.709/18 garante uma fiscalização severa às empresas, para constatar se de fato estas estão seguindo as normas estipuladas pela Lei Geral de Proteção de Dados. O órgão responsável por fiscalizar e apresentar penalidades para quem descumpre as determinações da lei é a Autoridade Nacional de Proteção de Dados Pessoais (ANPD); sendo a autoridade máxima para determinar as multas a serem aplicadas pelo descumprimento da lei, bem como orientar essas empresas sobre a importância de proteger os dados de seus colaboradores, consumidores, fornecedores e clientes.

A Lei vem para autorizar a punição caso exista um ataque cibernético em algum sistema, evitando o uso destes dados para algo ilícito, sobretudo os dados sensíveis. Afinal, nenhum dado pessoal pode ser cedido sem prévio consentimento. A liberdade de escolher entre ceder ou não deve ser exclusivamente do indivíduo.

Concluindo, entendemos que as empresas no seu ambiente de trabalho devem proporcionar condições para que os criminosos virtuais não tenham acesso aos seus dados. Para obter êxito nesta demanda o empresário precisa manter seu nível de segurança empresarial elevadíssimo, incluindo alguns cuidados fundamentais, tais como:

a) Monitoramento contínuo da rede na detecção de ameaças – necessário verificar constantemente, através de softwares específicos e confiáveis o comportamento e possíveis alterações dos seus dados na rede;

b) Manter sempre atualizado a infraestrutura de sua TI – assim a empresa evita riscos de invasão aos seus dados;
c) Implantar, sempre que possível, uma rede virtual privada – deste modo, o empresário proporcionará uma conexão mais segura com a rede de sua empresa e com a Internet;
d) Desenvolvimento de planos alternativos em casos de recuperação de perda de dados – assim, a empresa poderá criar opções em casos de emergência na eventual perda de dados.

7 CONCLUSÃO

Por fim, não se pode negar o avanço da tecnologia no dia a dia, todavia também devemos estar conscientes que hoje em dia há uma dependência quase que absoluta da Internet e que atos ilícitos cada vez mais se tornarão realidade. O que precisamos buscar a todo instante é identificar meios concretos de combater os crimes cibernéticos através do correto uso do Compliance no setor de tecnologia das empresas.

REFERÊNCIAS

Azevedo e Souza, B. (2016). Direito*, Tecnologia e Práticas Punitivas*. Editora Canal Ciências Criminais.

Barret, N. (1997) *Digital crime*. London: Kogan Page.

Chandler, Y & Neal-Schuman, J. (1997). Guide *to finding legal and regulatory information on the Internet (serial).* Estados Unidos, dez.

Corrêa, T. G. (2010). *Aspectos Jurídicos da Internet*. Editora Saraiva.

Goodman, M. (2015). *Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isto*. São Paulo: HSM Editora.

Huber, P. (1997). *Law and disorder in cyberspace*. New York: Oxford University Press,

Inellas, G. C. Z. (2009). *Crimes na Internet. 2ª ed*. São Paulo: Juarez de Oliveira

Lucca, N., & Simão F., A. (2000). *Direito e Internet – Aspectos Jurídicos Relevantes* – Edipro.

Marques, J. & Faria, S., M. (2012). O *Direito na Era Digital*. Livraria do Advogado.

Olivo, L. C. C. (1998). *Direito e Internet: a regulamentação do ciberespaço*. Florianópolis: UFSC, CIASC.

Fisher, D. (1999) *Calúnias via Internet desafiam a Justiça. Gazeta Mercantil*, São Paulo, 11 março.

Lima, N. B. M. H. (1997). A *lei alcança o ciberespaço*. Diário Catarinense, Florianópolis, Caderno Informática.

Moron, A. P. F. (1996). A *Internet e o direito*. Travelnet jurídica, São Paulo, fev.