CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS - CESREI
FACULDADE REINALDO RAMOS - FARR
CURSO DE BACHARELADO EM DIREITO

OSCAR HENRIQUE DE ANDRADE NETO

UMA ANÁLISE DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Campina Grande - PB

2020

OSCAR HENRIQUE DE ANDRADE NETO

UMA ANALISE DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Trabalho monográfico apresentado a coordenação do curso de Direito da Faculdade Reinaldo Ramos – FARR, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador (a): Me. Valdeci Feliciano Gomes.

Campina Grande – PB
2020

A553a Andrade Neto, Oscar Henrique de.
Uma análise da proteção de dados pessoais no Brasil / Oscar Henrique de Andrade Neto. – Campina Grande, 2020.
49 f.

Monografia (Graduação em Direito) – Faculdade Reinaldo Ramos- FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2020.
"Orientação: Prof. Me. Valdeci Feliciano Gomes".

1. Crimes Cibernéticos. 2. Dados Digitais – Privacidade. 3. Internet – Proteção de Dados Pessoais – Brasil. I. Gomes, Valdeci Feliciano. II. Título.

CDU 343.2:004.738.5(043)
FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

OSCAR HENRIQUE DE ANDRADE NETO

UMA ANÁLISE DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Campina Grande, _____ de _____de_____.

BANCA EXAMINADORA:

_____

Prof. Me.Valdeci Feliciano Gomes
Centro de Educação Superior Reinaldo Ramos – CESREI
Orientador

_____

Prof. Me. Rodrigo Silveira Rabello de Azevedo
Centro de Educação Superior Reinaldo Ramos – CESREI
1° Examinador

_____

Prof. Me. Rodrigo Araújo Reul
Centro de Educação Superior Reinaldo Ramos – CESREI
2° Examinador

AGRADECIMENTOS

Agradeço a Deus e nosso Senhor Jesus Cristo pela minha vida, por me ajudar a galgar todos os obstáculos encontrados no decorrer do curso, por permitir que eu conseguisse chegar até este ponto da longa jornada acadêmica, e adquirisse tanto conhecimento nestes longos anos e pelo cumprimento da promessa inicial. Estes cinco anos foram de grandes provações e transformações profundas em minha vida acadêmica e que ficará marcado para mim como um tempo de grandes perdas e ganhos perda do meu Pai e da minha Mãezinha amada e querida em cicatriz aberta jamais curável; de ganho de conhecimentos e verdadeiros amigos onde o mais humilde se faz presente firme.

Aos meus pais, meus maiores exemplos por toda a minha reles vida! Que sem seus exemplos e ensinamentos que me deram e permanecem hoje no meu âmago, absolutamente nada do meu intelecto, dignidade e formação seria possível. Meu Pai LUIZ GONZAGA DA SILVA. Pai por tudo e pelo seu exemplo de vida e retidão de caráter, inteligência e amor, minha Mãezinha ALCIONEAUREA ANDRADE DA SILVA. Mãe por tudo e por todos os dias que esteve e está cuidando de mim, mesmo não estando aqui ao meu lado, nunca deixou de expressar seu amor e incentivar-me todos os dias, todas as horas com seu olhar lindo e sua voz celestial, honrei e cumpri o que mais a senhora me pedia com carinho de nunca desistir! Mesmo assim a sua falta é dor constante!

De modo muito firme e especial ao meu Pai LUIZ GONZAGA DA SILVA e a minha Mãe ALCIONEAUREA ANDRADE DA SILVA, que de tudo fizeram que me incentivaram e apoiaram em tudo para vencer os desafios da vida, e no forjar do meu caráter e dos meus irmãos, e nas minhas formações acadêmicas; sei que estão bem na companhia de Deus e Jesus Cristo onde um dia talvez estarei com o senhor e com a senhora.

Aos meus irmãos únicos amigos eternos, Frederico Andrade da Silva e Luiz Andrade da Silva que, com muito amor, esforços, apoio e perseverança, não mediram esforços para que eu conquistasse mais uma etapa de minha vida.

Aos meus amigos de longa jornada, compartilhando alegrias e tristuras, em especial aos amigos: Elianildo da Silva Nascimento, Alysson Galdino Tertuliano, José Alberto de Macedo, Fábio Cavalcante da Silva, Marek Brükner, Luciano dos Reis Silva, Marivaldo Félix da Silva.

Agradeço aos Professores(as):

Ao digníssimo Professor MS. André Motta de Almeida, pelo convívio, pelo apoio, compreensão, ensino dedicado, confiança e pela preciosa amizade, alem das conversas uma frase marcante que me falas-te foi: "O Direito é como pedalar uma bicicleta, se parar de estudar desatualiza e cai."

Ao caríssimo Professor Thiago Serrano Lewis, por avivar a centelha da temática escolhida, apoiando no processo inicial deste trabalho.

Ao caríssimo Professor MS. José Flôr de Medeiros Junior, pela maestria no ensinar, e por uma frase motivadora proferiste no inicio do curso de Direito, e que acentuaram ainda mais o meu propósito de seguir alem no Direito: "As leis existem, mas quem as aplica?" (Dante Alighieri Monarquia).

A digníssima Professora Ma. Rute Leite Medeiros, por sua impecável dedicação em transmitir ensinamentos acadêmicos que os levo nesta jornada acadêmica e de vida, pela confiança e o apoio em momento difícil.

Ao digníssimo Professor Dr. João da Mata, por ensinar de forma impar as sutis nuances acadêmicas, pela confiança e o apoio em momento difícil.

A digníssima Professora Dra. Mara Karine Lopes Veriato Barros, por seus animados ensinamentos e conselhos impares, gratidão.

A digníssima Professora Dra. Cosma Ribeiro de Almeida, pela nobreza e humildade em aconselhar, ouvir atentamente, em bem ensinar os melindres da ABNT.

Agradecimento especial ao Professor Dr. Cláudio Simão de Lucena Neto, pelo apoio e incentivo e esclarecimentos iniciais e pertinentes à feitura deste trabalho, bem como o incentivo para aproveitar a temática e aprofundar o tema em um mestrado logo em seguida.

Agradecimento especial ao amigo e Professor Marek Brükner por todas as longas conversas e ensinamentos que vem contribuindo indefinidamente na jornada do conhecimento e do autoconhecimento e, por sua humildade e sapiência, como também pela preciosa amizade, dentre os demais amigos aqui listados; Ao amigo Wellison David Silva Pereira não só pela alegre amizade,

mas pela humildade, alegria e pelas oportunidades e ensinamentos a mim proporcionados.

Aos verdadeiros(as) professores(as) não só pelo transmitir o conhecimento e as nuances em áreas distintas, mas pela dedicação em fazê-lo pelo respeito e responsabilidade em ensinar, que contribuíram no processo infinito de aprendizado e formação profissional..

Agradecimento ao meu orientador Professor MS. Valdeci Feliciano Gomes, por ter aceito o desafio em conduzir este trabalho de pesquisa em tão escasso tempo, pelas correções e direcionamentos precisos, e pelo grande incentivo à aprofundar o conhecimento na pós graduação e no futuro mestrado, meu muito obrigado!.

“Não desista dos seus sonhos, é o seu futuro! Eu lhe peço que não desista meu filho! Tenha fé, acredite mais em você! Não desista!”.
(Alcioneaurea Andrade da Silva Mãe)

“Há coisas melhores para você! Você pode e é capaz!”.
(Luiz Gonzaga da Silva Pai)

“Você é um ANDRADE honre seu nome!”.
(Oscar Henrique de Andrade Avô)

Dedico este trabalho aos meus Pais!
In memoriam.

RESUMO

A internet é uma das grandes inovações e fomentadora de novos meios de trabalho, lazer, comunicação e o câmbio de informações inúmeras e de dados.Diante disso, transforma as condutas de comportamento, como também de trabalho, com o surgimento de vários empreendimentos e seguimentos no ambiente virtual e tecnológico. Para a pessoa que é leiga ou experiente a seguridade da privacidade e o trato de dados sigilosos e sensíveis são expostos por esta ferramenta, quer sejam pessoa jurídica ou física e até mesmo na esfera governamental. Esta pesquisa tem como objetivo geral analisar como as relações pertinentes à privacidade e a tratativa de dados e documentos sensíveis de cunho pessoais em face da LEI Nº 13.709/18, que assegura os direitos quanto à proteção de dados das pessoas e empresas. A metodologia utilizada foi à dedutiva e qualitativa, utilizando-se também dados públicos para apresentar o trabalho. A pesquisa foi do tipo exploratório, ao passo que foi feita uma busca no quadro real no âmbito da segurança de dados e documentos sensíveis e privativos digitais; no que tange aos procedimentos técnicos, esta foi do tipo bibliográfico, jurisprudencial, documental e exploratório.

Palavras-chave: Privacidade. Dados Digitais. Crimes Cibernéticos.

RESUMEN

Internet es una de las grandes innovaciones y promotor de nuevos medios de trabajo, ocio, comunicación e intercambio de información y datos variados. Por lo tanto, transforma los comportamientos conductuales, así como el trabajo, con la aparición de varias empresas y segmentos en el entorno virtual y tecnológico. Para los usuarios legos o experimentados, esta herramienta expone la seguridad de la privacidad y el tratamiento de datos secreto y sensibles, ya sean personas jurídicas o personas e incluso en el ámbito gubernamental. Esta investigación tiene el objetivo general de analizar cómo se producen las relaciones con respecto a la privacidad y el tratamiento de datos personales y documentos confidenciales de conformidad con la LEY N ° 13.709 / 18, que garantiza los derechos con respecto a la protección de datos de personas y empresas. La metodología utilizada fue deductiva y cualitativa, utilizando también datos públicos para presentar el trabajo. La investigación fue de tipo exploratorio, mientras que se realizó una búsqueda en el marco real en el ámbito de la seguridad de datos confidenciales y documentos digitales; con respecto a los procedimientos técnicos, esto fue bibliográfico, jurisprudencial, documental y exploratorio.

Palabras Clave: Privacidad. Datos digitales. Crímenes Cibernéticos.

LISTA DE SIGLAS

CF	--	Constituição Federal Brasileira
CC	--	Código Civil
CoE	--	Conselho da Europa
GDPR	--	General Data Protection Regulation
MCI	--	Marco Civil da Internet
STJ	--	Superior Tribunal de Justiça
LGPD	--	Lei Geral de Proteção de Dados (Lei nº 13.709/2018)
EU	--	União Européia
ARPA	--	Advanced Research and Projects Agency Agencia de Projetos e Pesquisas Avançadas
MIT	--	Instituto Tecnológico de Massachusetts
IETF	--	(Internet Engineering Task Force)
PC's	--	Personal Computer Computador(es) Pessoal
CF/88	--	Constituição Federal do Brasil 1988
TI	--	Tecnologia da Informação
LOGS	--	Registro de atividade gerado por programas e serviços de um dispositivo
ANDP	--	Agencia Nacional de Proteção de Dados
GDPR	--	General Data Protection Regulation GDPR

SUMÁRIO

INTRODUÇÃO

A humanidade, em suas mais remotas aglomerações de seres pensantes, une-se motivada por um elo de segurança, que às vezes as põe em mãos do Estado, no imaginário da absoluta segurança e certeza de prover-se da inviolabilidade do seu direito natural, respaldado pela carta magna.

Com a difusão do uso da internet e, a evolução continua desta, como dos recursos computacionais, em que observamos que há um volume exponencial na disseminação de informações na rede[1], nas áreas técnico/tecnológica e em outras áreas do conhecimento e, onde observamos poucos avanços na atualização na área do direito objetivo, em especial a segurança típica, quanto à segurança e manuseio e tratamento de dados.

Tal peculiaridade desta evolução e crescimento vem a corroborar para o surgimento de diversos serviços e aplicações disponíveis na rede para governos e usuários, assim, o volume de tráfego de pacotes[2] de informações na rede tem seu valor agregado tornando-se um verdadeiro tesouro.

Busca-se apresentar os perigos que os usuários estão sujeitos na Era Digital e o nível de insegurança neste meio, especialmente em aplicativos (App's)[3], bem como, expor, sobre o valor que as informações pessoais do cidadão representam para as empresas e Estados, e a frágil política de privacidade quanto aos serviços por estes disponibilizados ao cidadão e por este utilizados.

A expectativa em ralação a este estudo é enaltecer a importância da segurança no tocante a proteção de dados pessoais e a privacidade do usuário, em diversas plataformas de acesso, quer por meio físico, quer virtual, e em especial por aplicativos móveis (App's).

---

[1] É um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados gravados, impressoras, modems, softwares e outros equipamentos (Souza, 1999) (CETAM, ISBN: 478-85-63576-04-0)

[2] Informática - é a estrutura unitária de transmissão de dados ou sequência de dados - comunicação de pacotes em rede de computadores.

[3] App ou App's em português é a abreviação para aplicativo, que é um software para dispositivos móveis, smartphone, tablets ou Smart TV, podendo ser executados on e of line.

Abordando uma temática atual onde a privacidade a segurança digital de dados e documentos digitais privativos sensíveis, entre o contexto do ato jurídico legal do Estado, e o ato controverso por vezes, obscuro na finalidade, quanto ao uso destes dados privativos, por parte de empresas desenvolvedoras de aplicativos moveis (App's).

Evidencia-se sobre a segurança jurídica do cidadão no tocante ao trato de dados e documentos digitais privativos sensíveis,[4] quer por anuência ou não.

Questiona-se, entretanto, se tal liberdade no trato da privacidade abre convergência para ato libertino de ingerência e manipulação de dados sigilosos lícitos, incorrendo em quebra dos princípios do direito adquirido e do ato jurídico perfeito (art. 5º, XII, da Constituição Federal de 1988) bem como se extrapola o contrato social.

Nesse contexto, o presente estudo teve como objetivo geral apresentar aspectos sobre a privacidade do cidadão e a segurança de dados por estes fornecidos a vários meios tidos e ditos como legais, cogitando as principais escusas e garantias legais acerca do assunto e a importância social, jurídica e política destes dados.

Tendo-se a abordar nos respectivos objetivos específicos:

- Observar a fundamentação da liberdade do Estado no tocante ao trato da segurança digital do cidadão, determinada e alicerçada na Constituição Federal de 1988 e no ordenamento jurídico pátrio.
- Verificar se a nova Lei Geral de Proteção de Dados (Lei nº 13.709 / 2018) que entrará em vigor no ano de 2020, se tem subsídios para coibir a libertinagem de Empresas e Órgãos Públicos no manuseio de dados, e dados sensíveis privativos do usuário.

Este estudo desenvolve-se sob a abordagem metodologia da analise bibliográfica e documental.

> [...] a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e

[4] Dados pessoais sensíveis - DPS: São qualquer tipo de dado que pode ou possa levar a um ou algum tipo de uso ou de discriminação, Ex: filiação a partido, religião, vida sexual, dado genético ou biometria;

> artigos científicos, se utiliza fundamentalmente das contribuições de diversos autores.(GIL, 2002, p.44).

O uso de documentos em pesquisa é a sua natureza de riqueza das informações que eles trazem e que deles podemos extrair e resgatar, e justifica o seu uso e nos dá maior credibilidade.

> [...] o documento escrito constitui uma fonte extremamente preciosa para todo pesquisador nas ciências sociais. Ele é, evidentemente, insubstituível em qualquer reconstituição referente a um passado relativamente distante, pois não é raro que ele represente a quase totalidade dos vestígios da atividade humana em determinadas épocas. Além disso, muito frequentemente, ele permanece como o único testemunho de atividades particulares ocorridas num passado recente (CELLARD, 2008, p.295).

A pesquisa documental tem em si o documento como objeto de investigação principal, porem, esta fonte pode ser escrita ou não, a exemplo de filmes, vídeos, fotografias, slides. Tais documentos são fontes de informações e de esclarecimentos que por sua natureza e conteúdo nos servem para elucidar determinadas questões como suporte para outras informações ou esclarecimentos.

> [...] a pesquisa documental é muito semelhante à pesquisa bibliográfica, a pesquisa documental vale-se de materiais que não receberam, ainda, um tratamento analítico, podendo ser reelaboradas de acordo com os objetos da pesquisa. (GIL, 1999, P. 43).

De modo que no Direito Digital, são aplicados muitos princípios e soluções que estão na base do direito Costumeiro de base documental restrita, mas também de base documental não escrita, pois para o Direito Digital essas aplicações facilitam alcançar o efetivo resultado a que se quer chegar, em razão da tecnologia estar sempre em constante evolução e mudança, conforme afirma Patrícia Peck Pinheiro.

> [...] O Direito Digital estabelece um relacionamento entre o Direito Codificado e o Direito Costumeiro, aplicando os elementos que cada um tem de melhor para a solução das questões da Sociedade Digital. (PINHEIRO, 2013, p.77).

A segurança tem seu papel predominante para o exercício adequado de qualquer tipo de ação dentro de um cenário, quer seja ela geral ou privada, quer seja está um órgão público, uma empresa ou um ser humano natural. Ademais, tem relevante importância devido ao fato de ocorrerem cotidianamente, grandes mudanças tecnológicas que trazem situações de risco, às quais o mundo real encontra-se sujeitado (por exemplo, invasões e manipulações de dados e documentos sensíveis, tanto de pessoas físicas como de pessoa jurídica ou de direito público).

Quanto à abordagem técnica procura-se desenvolver a pesquisa de natureza aplicada, através de análise de documentos e pesquisas de natureza bibliográfica: livros e artigos conceituados. De acordo com GIL “a pesquisa aplicada possui muitos poentos de contato com a pesquisa pura, pois depende de suas descobertas e se enriquece com o seu desenvolvimento”. (GIL 1999, pág. 43)

Através dessa abordagem espera-se que se desenvolva um conhecimento e que este seja aplicado na sociedade, e a partir dessa aplicação gere uma conscientização e sensibilização dos direitos do cidadão no tocante a sua privacidade, em todos os aspectos legais, abordado neste trabalho; desta forma venha contribuir com a liberdade de escolha individual, sem que seja ferido ou tolhido o seu direito privado de usuário em face de abusos no direito de escolha, em especial na utilização de aplicativos móveis, onde que este usuário tenha o direito de habilitar ou permitir o que determinado aplicativo pode ou não utilizar das informações ali contidas.

Quanto aos objetivos essa pesquisa visa desenvolver uma abordagem explicativa, quando temos um confronte no texto Constitucional em seu art.5º, e seus incisos pertinentes ao tema abordado, expressando os Aspectos Jurídicos da Segurança Digital, e o Marco Civil da Internet, sob uma visão paralela da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) que entrará em vigor no ano de 2020, abordando também o aspecto da Proteção de Dados e de privacidade como também direito de personalidade em território pátrio e os riscos de cibercrimes.

Este trabalho não pretendeu apresentar uma solução imediatista, única, e imbuída de dogmatismo comum, a um problema que em si, nos traz múltiplas causas e múltiplas facetas de intervenções a lapidar efetivamente no campo

jurídico e sociopolítico, em diálogo com a sociedade; pois será para esta sociedade atual e as futuras que lança-se o desafio de enfatizar e praticar o ato de segurança nos meios virtuais e físicos, evitando o mal posterior caso desande ao limbo da preguiça política constante e do esquecimento, por conseguinte, abrindo assim veredas aos cibercriminosos em “universidade” de campo profícuo. Porém buscou-se aflorar ao campo jurídico, questão atual de direito natural e objetivo transpondo ao subjetivo.

Este tipo de pesquisa preocupa-se em identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos (GIL,2007). Ou seja, este tipo de pesquisa explica o porquê das coisas através dos resultados oferecidos.

> [...] uma pesquisa explicativa pode ser a continuação de outra descritiva, posto que a identificação de fatores que determinam um fenômeno exige que este esteja suficientemente descrito e detalhado. (Gil, 2007, p.43).

A pesquisa será também de forma descritiva, segundo cita TRIVIÑOS:

> [...] a pesquisa descritiva exige do investigador uma série de informações sobre o que deseja pesquisar. Esse tipo de estudo pretende descrever os fatos e fenômenos de determinada realidade (TRIVIÑOS, 1987).

Neste sentido procura abordar o teor da segurança e da privacidade na Era Digital e o nível de insegurança neste meio virtual, bem como expor sobre o valor que as informações pessoais sensíveis do cidadão representam para as empresas e Estados e, a frágil política de privacidade quanto aos serviços por estes utilizados e, quando não invadida.

Para melhor desenvolvimento será realizada, uma pesquisa de natureza exploratória. "Essas pesquisas podem ser classificadas como: pesquisa bibliográfica e estudo de caso (GIL,2007).

Sendo assim, será abordado um estudo de caso da falta de normatização que venha a prevenir abusos em que os usuários estão sujeitos quanto à privacidade de seus dados e documentos privativos sensíveis em meio virtual e principalmente por aplicativos móveis (App’s), bem como a segurança de dados em base de banco de dados e, a fragilidade funcional e documental na utilização e manipulação destes por parte do Estado e Empresas, frente ao que preconiza à Constituição Federal e, normativos legais

de outros Países, em especial ao bloco da União Européia. Sem sombra de dúvida, a falta de segurança em campo fecundo de redes sociais e principalmente por parte de aplicativos móveis App’s, das mais variadas classes, decorrente da mais grave crise de segurança e, a sobrepujança do Estado e poder judiciário quanto a Lei Geral de Proteção de Dados Pessoais (LGPD), face à Constituição Federal Brasileira.

CAPÍTULO I - RELATO TEXTUAL DE DIREITO POSITIVO

A “Revolução Digital” iniciada na década de 60, em pleno auge da Guerra Fria, foi o marco de um novo período na história da civilização, principalmente no tocante a maneira que a telecomunicação acontece, mudando de forma abrangente a velocidade, volume de informações que rodam o planeta. Assim vemos surgir em 1969 o que entendemos hoje como internet.

A Internet foi criada em 1969 na Agência ARPA (Advanced Research and Projects Agency Agencia de Projetos e Pesquisas Avançadas). Na época, surgiu uma rede chamada de ARPANET que tinha como objetivo conectar os departamentos de pesquisa e as bases militares dos Estados Unidos.(MORIMOTO, 2008b, [não paginado]).

A ARPANET foi financiada pela Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos.(Lievrouw, L. A.; Livingstone, S. M. (2006). Handbook of New Media: Student Edition. EUA: (SAGE. p. 253.)

Em 1962 surgiram rumores e idéias para criação de uma rede[5] de computadores interligada pelo engenheiro do Instituto Tecnológico de Massachusetts (MIT) Joseph Licklider, porém, só sete anos depois houve realmente início ao nascimento da internet.

Nos anos 70-80 se deu início ao termo internet. Foi onde surgirão os protocolos padrões para que a internet finalmente pudesse nascer, são eles: “TCP/IP”[6]*(*Transmission Control Protocol/Internet Protocol*)Ambas as tecnologias se tornaram a base técnica da Internet.* (The accelerator of themodern age. BBC News. August 5, 2008)[7].

---

[5] Estruturas físicas (equipamentos) e lógicas (programas, protocolos) que permitem que dois ou mais computadores possam compartilhar suas informações entre si. Tidas como Redes de Computadores.

[6] TCP/IP grupo de protocolos de comunicação através de computadores em rede. Seu nome advém de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou Protocolo de controle de transmissão).

[7] O acelerador da era moderna Disponível em <http://news.bbc.co.uk/2/hi/technology/7541123.stm>

Tendo como fundadores do protocolo TCP: Net ViltonCerf e Bob Kahn em 1973, mas o termo internet só foi usado em 1974 sendo a primeira publicação do protocolo TCP, que era assinada pela Universidade de Stanford por VintonCerf, YogemDalal e Carl Sunshine.

A Internet é uma “rede de redes” de alcance global. Com base em uma estrutura aberta, é composta por uma coleção de “redes” definida por Sistemas Autônomos que se relacionam de forma estruturada por meio da arquitetura de protocolos TCP/IP. Os protocolos dessa arquitetura são definidos num foro mundial e aberto denominado IETF (Internet Engineering Task Force),[8]em um processo de discussão e consenso.[9]

A internet esta ligada diretamente à atividade de milhões de indivíduos em todo o globo, em que inúmeros benefícios foram surgindo e que são úteis a sociedade através dela, como por exemplo, a facilidade de comunicação, o acesso e compartilhamento de dados, que é até difícil desvencilha-se dela com facilidade uma vez que a internet tem seus encantos, todavia existe também seu lado *nequid luminis.*[10]

Todavia, sem os cuidados necessários devidos, essa tecnologia também pode apresentar sérios riscos à segurança do internauta que a utiliza.

Tendo em vista que atualmente, as pessoas habitualmente fazem uso de aplicativos móveis das mais variadas classes de utilidade, que proliferam em larga escala, como também por meio de alguns destes sistemas capturam e trocam dados/informações entre si através de algoritmos especiais.

Estas novas tecnologias proporcionam diferentes tipos de serviços. Estamos em um momento peculiar e importante de transição onde as relações humanas são cada vez mais interativas por meio dos dispositivos móveis de comunicação (App’s),[11] o que acaba nos tornando cada vez mais vulneráveis e frágeis aos ataques sob a nossa esfera de privacidade.

A privacidade e a segurança são provavelmente as duas maiores questões que os Estados, Governos, Empresas e, Pessoas (não sempre),

[8] IETF (Internet Engineering Task Force) grupo internacional aberto para o desenvolvimento de padrões para a internet em especial o TCP/IP

[9] CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015.

[10] Nequid luminis. Sem luz, obscuro.

[11] App ou App's em português é a abreviação para aplicativo, que é um software para dispositivos móveis, smartphones, tablets ou Smart TV, podendo ser executados on e of line.

defrontam ao pensar em uma estratégia de segurança para seus documentos e dados sensíveis em meio virtual, tidos, pois como sigilosos na maioria das vezes. Como fazer para que o cidadão comum se sinta na plenitude seguro, ao deixar o que ele considera mais relevante ou precioso, seus dados e informações pessoais sensíveis, sob a "tutela" do Estado no o contrato social ou de uma empresa Ex-post-facto?

Ouve-se, algumas vezes, que quando algum bem ou serviço é aparentemente gratuito, provavelmente há uma verdade oculta de que o cidadão esteja pagando por este bem ou serviço fornecendo seus dados. Isto ocorre com frequência, por exemplo, nas redes sociais com mapeamento de IP's[12] e por meio da inserção de cookie(s) "mapeando" as preferências do usuário tais como os cartões de fidelidade de lojas, hipermercados, delivery e transporte, estes propiciam facilidades na aquisição de bens e serviços, principalmente com a utilização de aplicativos (App's) dos mais variados, que oferecem serviços dos mais sortidos fins, em troca de acesso aos dados pessoais do(s) usuário(s) fim, tais como: localização, GPS (Sistema de Posicionamento Global) , fotos, áudios, contatos, agenda, dentre outros documentos digitais e/ou digitalizado, e compartilhado via internet quer por aplicativos móveis, que por sites de relacionamento acessados via estações de trabalho (PCs)[13] ou smartphone[14].

No entanto a utilização inapropriada das técnicas e procedimentos informáticos inclua-se a internet e Aplicativos moveis (App's), onde este último reveste-se de um grave fator criminal de delicado controle. Como decorrência, assiste-se de imediato o relevante impacto das novas tecnologias nas relações jurídicas, em especial o direito digital onde deveria abranger a seara penal nas formas de tipicidade de crimes propriamente cibernéticos (Cybercrime).

As redes sociais, utilizadas por centenas de milhares de pessoas ao redor do mundo detêm dados digitais que o usuário espontaneamente insere porem, também fazem deduções com base nas interações de usuários e informações, compartilha-as indevidamente com terceiros e traça um perfil do

[12] IP (Internet Protocol - Protocolo de Internet, ou Protocolo de controle de transmissão).
[13] PC do inglês: Personal Computer = Computador Pessoal
[14] Smartphone do inglês "telefone inteligente". Aparelho que combina recursos de celular e de computadores pessoais, sobre uma plataforma de software, Sistema Operacional - SO.

usuário que permite determinar ações de prospecção na oferta de produtos e serviços.

1.1. DIREITO DIGITAL

Sendo o direito digital um ramo novo com pouca autonomia, mas que tem dialogo com outras áreas do direito, e traz uma coleção de elementos, no caso as normas, e suas aplicabilidades do conhecimento e de regulações jurídicas em meio digital, onde cria regras e critérios nas interações em ambiente virtual, para que estas ocorram de modo harmônico entre si e as demais, tais como a Lei dos crimes informáticos, Lei de acesso à informação, Marco Civil e a LGDP, para uma proteção de uma sociabilidade no ciberespaço em uma sociedade em evolução.

> As tecnologias digitais surgiram, então, como a infra-estrutura do ciberespaço, novo espaço de comunicação, de sociabilidade, de organização e de transação, mas também novo mercado da informação e do conhecimento (LÉVY, 1999,p.34).

O Direito Digital em especial o aspecto constitucional deste, podemos afirmar que é fundamentado na liberdade de acesso a um meio pelo qual manifesta-se o pensamento, a criação, dentre outros, mais precisamente temos no art. 220 da CF/88 o seguinte:

> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

Uma sociedade "digital" que no cenário atual onde a sociedade, margeada por uma integração mundial global, se percebe que desenvolveu-se uma grande relativização dos conceitos outrora rígidos. Contudo com a evolução dos mecanismos e de inúmeras ferramentas de comunicação vemos que, as tidas barreiras das distâncias parecem não serem mais obstáculos, e as fronteiras tornaram-se menos evidenciada sem um ambiente globalizado.

Na contextualização atual em que vemos os avanços e crescimento exponencial do mundo tecnológico em especial no meio digital, que é incontestável e necessário à inserção digital, quando os computadores antecedentes aos atuais que dispunham de acesso ainda discado “analógico” à internet, e que abriram caminho para os novos modelos de celulares e tablets, e dentre outros meios de navegação web, e que tornaram pontos geográficos equidistantes próximos, mediante um clique de mouse. Um ponto muito e amplamente discutido até o presente momento tem relação com à do anonimato, a propósito, temática sempre atual; onde busca-se saber o que de fato é ser anônimo em ambiente virtual ou em redes de segurança, onde pensa-se que funcionam de modo a não ter a intervenção de um usuário, ademais observa-se cotidianamente que o então usuário sequer tem uma noção plena de que, a cada site acessado, através dos navegadores web em que ha robôs “cookies” e algoritmos muito destes especiais, já capturaram muitos dos dados, localização, rotinas ou do cotidiano do usuário, dentre outras centenas de dados fornecidos pelo utilizador, este no ledo engano de imaginar estar seguro.

As ocorrências deste leque onde se observa à tendência na geração de desavenças em meio a interesses lícitos e ilícitos no tocante a privacidade tão abarcada na atual Carta Magna brasileira, e mitigada frequentemente em processo de rastreabilidade diante das questões de segurança quanto à privacidade, de modo que o campo do direito na área digital vem a tornar-se uma mescla de hibrido embrionário ao concatenar a aplicação do saber jurídico diante da realidade latente de IoT[15] e áreas afins da informação tecnológica a internet e seus ambientes.

A segurança tem seu papel predominante para o exercício correto de qualquer tipo de ação dentro de uma conjuntura geral ou privada, quer seja esta uma empresa ou uma pessoa. Ainda mais, é de relevante importância devido ao fato de ocorrer cotidianamente, grandes mudanças tecnológicas que trazem situações de perigo, a qual o mundo real passou a estar sujeitado a invasões e manipulações de dados sensíveis tanto de pessoas como de empresas diversas.

[15] IoT Internet das coisas

Por conseguinte avistamos despontar o Direito Digital no que diz respeito entre a ciência do Direito e a Informática.

A atuação precípua do Direito Digital que por seu expediente busca a adequação da legislação em voga aos casos virtuais e, vindo empregar / adequar as normas ao mundo da tecnologia. Os avanços e desdobramentos rápidos e rotineiros da tecnologia e dos ambientes digitais nos obrigam a permanecer alerta ao surgimento de novos conceitos relevantes, e desta forma o Direito Digital conforme conceitua Patrícia Peck Pinheiro.

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (PINHEIRO, 2012, p. 75.).

Conforme Paiva, o Direito Digital ou Direito Informático, é o conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador como meio e como fim que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do software; o comércio eletrônico e as relações humanas estabelecidas via Internet. (PAIVA, 2002).

Trata-se, portanto, de um conglomerado de normas jurídicas de aplicações, conhecimentos e relações jurídicas bilaterais, advindas de um universo digital.

Conforme assevera Santos (2018) a consequência desta interação e a comunicação ocorrida em meio virtual, surge à necessidade de se garantir a validade jurídica das informações prestadas bem como das transações de compra e venda, prestação de serviços, moeda virtual[16] "cambio virtual ou moeda virtual" em ambiente da internet, através do uso de certificados digitais.

A tecnologia foi capaz também de facilitar a vida laboral dos profissionais do Direito, com softwares que simplificaram e aperfeiçoaram as tarefas rotineiras no âmbito jurídico.

[16] Moeda Virtual - Estabelecida em 2012 pelo Banco Central Europeu BCE, como "uma forma não regulamentada de dinheiro virtual, comumente distribuída e controlada por seus desenvolvedores, que é usada e aceita apenas entre os membros de uma comunidade virtual específica." Em 2013 o Departamento do Tesouro dos Estados Unidos estabeleceu as moedas digitais como moedas tradicionais sem os trâmites legais.

No entanto, a atual tecnologia introduziu e potenciou o surgimento de crimes cibernéticos e contra a integridade moral e física por exemplo.

Fica claro que o Direito Digital não detém os elementos necessários a ser considerado um ramo autônomo do Direito. Inobstante isto, está presente em todas as áreas jurídicas, podendo utilizar-se de praticamente todos os âmbitos do direito para aplicação de sanções e implementação de direitos.

CAPITULO II - LEGISLAÇÃO

2.1. ASPECTO CONSTITUCIONAL

Trataremos neste item a respeito do que traz o artigo 5º da Constituição Federal de 1988, um dos artigos mais relevantes desta carta magna; para em seguida apresentar as pontuações e apresentar adiante, sobre a privacidade, dentre outras garantias previstas no referido artigo constitucional, em contraponto a LGDP a ser tratada posteriormente no presente trabalho.

É sabido que o artigo 5º da CF/88 possui alta relevância e é tido como cláusula pétrea conforme preconiza o artigo 60,§ 4º, IV, da CF/88 em destaque:

> Art. 60. A Constituição poderá ser emendada mediante proposta:
> [...]
> § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:
> I a forma federativa de Estado;
> II o voto direto, secreto, universal e periódico;
> III a separação dos Poderes;
> IV **os direitos e garantias individuais.** (Grifo nosso)

A Constituição Federal prevê em seu art.5º os direitos e garantias fundamentais aos seres humanos, tais como a vida, a igualdade, o respeito moral, a privacidade e a intimidade, que garantem ao homem a dignidade, possibilitando assim a vida em um ambiente de respeito, liberdade e criando uma sociedade civilizada.

> **Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a **inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade**. (Grifo nosso)

Assim a Constituição destinou aos Direitos e Garantias Fundamentais o “Titulo II”, que inicia no art.5.º e conclui no art. 17.

Lançando assim os Direitos Fundamentais logo no inicio da Constituição, após os “Princípios Fundamentais” (arts. 1º a 4º).

Deve-se então perceber que na Constituição Federal Brasileira, que o artigo 5º o não faz distinção formal de direitos e de garantias. Não raro, um inciso contemplar, simultaneamente duas espécies no mesmo enunciado.

Exemplo: No artigo 5º, inciso X, da CF/88, o qual será dividido para demonstrar o fato:

DIREITO

"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, [...]

GARANTIA

"[...] assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação";

Temos, pois na CF/88; os Direitos de Defesa que são caracterizados por impor ao Estado e a terceiros um dever de abstenção, ou seja, na medida em que todo o homem possui autodeterminação, não pode o Estado interferir nessa esfera individual. Estes direito descortinam-se em:

a) Direito a não impedimentos: em que possibilitam ao titular o direito ao gozo de um bem juridicamente fundamental e, consequentemente, não pode o Estado impor impedimentos ao exercício desse direito. Exemplo: o art.5º, IX, da CF/88, que assegura liberdade de expressão e, ainda, veda a censura ou a licença.

b) Direitos a não afetações: onde estabelecem ao Estado o dever de não afetar propriedades ou situações do titular do direito e, com isso, o Poder Público não pode assumir comportamentos que venha afetar a dignidade e a própria existência da pessoa humana. Exemplo: art. 5º, X, da CF/88, que assegura o direito à privacidade.

c) Direito a não eliminação de posições jurídicas: impõe ao Estado a proibição de eliminar posições jurídicas concretas e, com isso, ficar impedido de revogar determinadas normas, em abstrato. Exemplo: art. 5º XXII, que assegura o direito de propriedade.

Em outras palavras, o Estado não pode extinguir essa garantia.

Ao contrário dos direitos de defesa, que exigem a privação Estatal, um não agir, assim os direitos a prestações positivas sejam assegurar que o Estado atue positivamente, que o Poder Público tenha o dever de manifestar-se de agir fornecendo meios pelos quais se oportunize o exercício dos direitos fundamentais, assim temos:

a) Direito a prestações normativas: Em que o Estado tem o dever de legislar, emitindo normas jurídicas penais, quer de organização quer de procedimento.

Ocorre especialmente no caso dos direitos que dependem de normas infraconstitucionais que definam o significado e o modo de exercício. Ex: art. 5º. XLI, CF/88:

> XLI a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais; (CF/88).

Temos na evolução dos direitos fundamentais as dimensões, em que hoje aponta a evolução dos direitos fundamentais em quatro momentos que vão da primeira até a quinta dimensão e, é nesta ultima Geração que trataremos, tendo em vista que esta dimensão está ligada a realidade virtual.

Os Direitos Fundamentais de Quinta Dimensão representariam os direitos ligados à realidade virtual, ou o seja, estariam relacionados com os enormes avanços da cibernética e da internet, especialmente, levando em consideração que houve uma internacionalização da jurisdição constitucional. (Sylvio Motta, Curso de direito constitucional, 2007, pg.153).

Vemos, pois, que o princípio da dignidade humana constitui-se como importante direito fundamental de um Estado de Direito e o reconhecimento e a sua aplicação constitui norte para a evolução de uma sociedade e sua história. Não vislumbra-se no presente trabalho exaurir todas as hipóteses no campo dos avanços científicos / tecnológicos, que acabam por vir lesionar a dignidade humana, mas o de descortinar as nuances que se manifestam no tocante a segurança dos dados de usuários diante dos avanços tecnológicos em especial a internet, bem como os aplicativos móveis (App’s) e, os crimes de invasão e omissão a privacidade cerne do presente trabalho.

De modo que passemos para os aspectos normativos, que nos mostra em que a regulação pátria trata no tocante à segurança e a privacidade diante de um visível crescimento exponencial onde a gravidade de ataques cibernéticos, muitos destes com consequências financeiras, tornando-se comum as discussões no tocante aos aspectos da privacidade, da proteção de dados, e da segurança da informação, que são a base principal que constitui as divisas do tema deste trabalho.

É importante observar o artigo 13º do Decreto 8.771/2016, que regulamentou o Marco Civil da Internet (Lei no 12.965/2014), que traz diversas obrigações sobre segurança da informação, das quais precisam ser seguidas pelas empresas e até órgãos governamentais que coletam, usam, compartilham ou armazenam dados pessoais.

Faz-se necessário entender e, compreender o que deve ser considerado como dado(s) pessoal (ais), assim vejamos o disposto no artigo 14º do decreto acima que regulamentou o Marco Civil da Internet no Brasil; O art. 14º definiu dado pessoal como: "à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa", vejamos o dispositivo:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I dado pessoal dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
> II tratamento de dados pessoais toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim sendo, se algo vir a identificar ou a tornar identificável uma pessoa natural, estaremos diante de um dado[17] pessoal. Tem-se, portanto, conceito muito amplo sobre dados pessoais, e que inclui, entre outros os números de CPF, RG, Passaporte, CEP e endereço, como também o número IP,[18] Imei[19] de celular, e de cartão de crédito, placa de veículos, a estes não se limitando.

---

[17]Dados. (Refere-se sob a sua forma eletrônica) Trata-se de uma série de atividades executadas e concatenadas e ordenadamente, em que resultará em uma espécie de disposição de informações, na qual são coletadas informações, ou dados, que passam por uma sequência lógica e organizada, em que será o objetivo de colher informações que o usuário ou sistema pretende utilizar.

[18]Protocolo de Internet (Internet Protocol) é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

[19]International Mobile Equipment Identity (Identificação Internacional de Equipamento Móvel), mais conhecido por IMEI, é um número de identificação global e único para cada telefone celular.

2.2. LEGISLAÇÃO PERTINENTE

No que diz respeito a uma regulamentação brasileira que trate das relações jurídicas em ambiente digital o cenário ainda é tímido como também preocupante, principalmente quando comparada ao grande volume de inserção das pessoas na presente realidade.

No Brasil, além da adaptação das leis do mundo “analógico”, as principais normas criadas pelo Congresso Nacional foram:

A Lei de Acesso à Informação, Lei nº 12.527,/2011. Conceitua a disponibilização das prestações de contas dos entes públicos com o uso da tecnologia.Sendo assim, a legislação pátria ainda necessita de uma maior profundidade no que se refere ao Direito Digital, pois, em muitos casos, as leis antigas não conseguiram proteger o cidadão.

A Lei dos Crimes Informáticos, Lei nº 12.737/2012. Que estabelece os três tipos penais específicos que envolvem os delitos informáticos e condutas que sugiram com a tecnologia são consideradas crimes.

a) Invasão de dispositivo informático artigo 154-A. Código Penal.

b) Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública artigo 266, § 1º e § 2º do C.P.

c) Falsificação de documento particular artigo 298 do C.P.

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

O Decreto nº 7.962/2013, Que regulamenta o Código de Defesa do Consumidor (C.D.C.), para dispor sobre a contratação no comércio eletrônico. E, traz vários esclarecimentos a cerca do atendimento ao consumidor em relação às compras efetuadas pela internet, direito ao arrependimento em comércio eletrônico e, até a temática das compras coletivas.

O Marco Civil da Internet, Lei Nº 12.965/2014. Carta principiológica que estabelece os princípios, as garantias, direitos e deveres para o uso adequado da internet no país, assim como determina esse ambiente seja regulamentado pelas regras do Direito Civil, Direito Empresarial, do Direito do Consumidor, e outros.

Código de Processo Civil de 2015, Lei Nº 13.105/2015. Em proporção menor, cria normas para o desenvolvimento do processo judicial eletrônico que pela Lei nº 11.419/2006. Vem dispor sobre a informatização do processo judicial

O Código Penal, Decreto Lei nº 2.848 / 1940. Que elenca os mecanismos presentes no combate aos crimes cibernéticos perpetrados pela utilização de dispositivo(s) informático(s) como meio capaz para o cometimento das infrações penais.

O Plano Nacional de Internet das Coisas (IoT), Decreto nº 9.854 de 2019,que tem como finalidade dar mais espaço a IoT no Brasil, implementando e desenvolvendo novas tecnologias e considerações sobre a livre concorrência e livre circulação de dados, sem deixar de dar a devida importância à proteção de dados pessoais.

Porém,mesmo com o conjunto legal acima próprios do Estado brasileiro o mesmo carece integrar esforços em âmbito internacional, onde os países estão, aos poucos, buscando novas maneiras de legislar o assunto, mesmo que sofram com a dificuldade de acompanhar a velocidade das mudanças no mundo físico e no ambiente virtual. Neste campo surge o tratado internacional de direito penal e processual penal, que fora firmando na esfera do Conselho da Europa em 23 de novembro de 2001 em Budapeste na Hungria, para definir uma política criminal comum entre os Estados signatários no intuito principal de proteger a sociedade contra a criminalidade no ciberespaço, e as formas de combate proporcional aos delitos e a má utilização da internet. Sendo abordado no tópico a seguir

2.3. CONVENÇÃO SOBRE O CIBERCRIME

Com o surgimento da internet e, da rápida progressão tecnológica que revolucionou e revoluciona os meios das atividades da humanidade, e que muda o mundo do aspecto de sociedade global a uma sociedade da era da informação.

Neste descortinar de contexto onde as novas tecnologias da informação (T.I.)[20] bem como a comunicação e o entretenimento tomaram novos rumos e

[20]Tecnologia da Informação. Área que utiliza a computação como meio para produzir, transmitir, armazenar, e usar diversas informações e facilitar a comunicação e seus processos.

novas aplicações, em que, são presença quase que necessária, na maioria das profissões, como prodiga e indispensável na difusão do saber e do conhecimento humano.

Seguindo este novo horizonte com seus paradigmas onde manifestam-se uma série de ações ilícitas que passaram do ambiente analógico para este novo ambiente, o virtual globalizado, e que na nova dimensão jurídico político desafia o Estado Legal a antever-se aos próximos padrões de comunicação multimodal[21] uma vez que o ciberespaço[22] transformou as fronteiras, antes geográficas, bem como o cidadão off-line para o cibercidadão on-line e da atuação e aplicabilidade dos instrumentos jurídicos de cada Estado frente ao ciberespaço e ao cibercrime, forçando uma abordagem multimodal jurídica.

A necessidade, a tipificação e a regulamentação dos crimes cibernéticos ou ciberespaço. A tipificação dos crimes cometidos no ciberespaço é imperiosa para que os Estados e os seus poderes e entes públicos, possam assim acompanhar "palmo a palmo" o dinamismo atual do mundo globalizado.

Entretanto e de fato notório, o embate com o direito de outros Estados ante o direito brasileiro na questão da má aplicação da Internet e seus derivados produtos, leva a acreditar que para chegar à solução de conflitos nesta esfera se faz necessário recorrer ao Direito Internacional por intermédio de acordos de cooperação e de tratados como o da convenção sobre cibercrimes.

Assim urge a importância do ingresso do Estado Brasileiro à Convenção sobre o cibercrime (Convenção de Budapeste), vez que, ao tornar-se signatário do diploma legal, passará ao patamar de obrigações em um Regime Internacional de natureza cooperativista direcionado ao combate dos crimes virtuais ou cibercrimes, favorecendo a uma cooperação de mão dupla para com outros Estados subscritores do citado diploma, que padecem dos mesmos atos ilícitos, mas que juntos, pelejam contra estas praticas, todavia os Estados da supracitada dispõem de leis distintas entre si.Sendo a convenção sobre cibercrimes, um tratado internacional normativo do bloco Europeu, onde

[21]Coexistência de diversas modalidades comunicativas (fala, gestos, texto, processamento de imagem, etc.) Disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/multimodal>

[22]Conjunto de rede de computadores nas quais todo o tipo de informação é circulada. (William Gibson, Neuromancer 1984)

emprega orientações a respeito dos cibercrimes, e que serve de norte para uma legislação internacional.

Devendo o Brasil observar, e quiçá, repensar a legislação pátria especifica de forma mais benéfica para os cidadãos como um todo para não incorrer um “vício corriqueiro de ter e não servir ou aplicar-se, mais conhecido como (para inglês ver)”.

2.5. LEI DE ACESSO À INFORMAÇÃO

A lei nº 12.527,/2011. Conceitua a disponibilização das prestações de contas dos entes públicos com o uso da tecnologia.

Sendo assim, a legislação pátria ainda necessita de uma maior profundidade no que se diz respeito ao Direito Digital, pois, em muitos casos, as leis antigas não conseguiram proteger o cidadão.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XXXIII 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, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

2.4 MARCO CIVIL DA INTERNET

O Marco Civil da Internet (M.C.I.) desde o seu princípio não seria por si o fim dos problemas com relação à proteção dos direitos dos usuários no país, mas apenas o ponto de partida de uma longínqua jornada neste indiscutível avanço democrático. Ao vir fixar os parâmetros comuns em que se permite a

qualquer usuário cidadão ou empresa bem como na esfera judicial ou parlamentar dialogar com legitimidade a temática ainda turbulenta da banda larga, os direitos autorais, a liberdade de expressão, a privacidade e a segurança prevista no art. 5º da CF/88, bem como a segurança da rede.

Sabe-se que sempre foi notória a necessidade de uma normatização especifica para o espaço virtual, assim como da importância de estabelecer direitos e deveres aos seus usuários e provedores, bem como a atuação do Poder Público. O Marco Civil Internet tem como um dos seus objetivos gerais à regulamentação dos direitos e deveres aos destinatários da legislação. Exemplo disso é o Capítulo II onde se trata especificamente de estabelecer garantias aos usuários, como proteção dos direitos individuais e coletivos no uso da internet, tendo em vista que ainda existia uma grande lacuna no ordenamento jurídico pátrio.

> O MCI foi, aliás, uma reação da sociedade civil contra um movimento legislativo que pretendia regulamentar a Internet no Brasil por meio de leis penais. Nesse sentido, o MCI procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal, que poderia ter efeitos inibitórios para a inovação e a dinamicidade da Internet. (BIONI,2018, p.183)

Tem-se no caso o Marco Civil da Internet Lei 12.965, a lei “regulamentadora” da internet no Brasil, que traz em seu escopo as previsões de direitos, garantias, deveres e de princípios para os que utilizam a rede, quanto concede ao Estado a autorização de diretrizes para a sua atuação.

Esta lei versa sobre os temas da privacidade na rede, o arquivamento de dados, em especial primazia a garantia da neutralidade na rede, e da liberdade de expressão assim como o direito da liberdade e da privacidade dos usuários, a função social da qual se compromete dar cumprimento, a difusão do conhecimento sem omitir-se no tocante às obrigações de responsabilidade civil dos provedores de internet e dos seus usuários. A lei serve como referência para as legislações pátria, e que devem tratar da rede mundial de computadores com a finalidade e que foram estabelecidos para manter o caráter aberto da internet.

A Lei nº 12.965/2014 ressalta o liame quanto à previsão da neutralidade da rede, como o princípio disciplinador da internet, percebe-se, entretanto que há ressalvas expressas para que o Estado possa transformar qualquer conteúdo on-line, obrigando os provedores a tornarem um determinado acesso como indisponível. Outra tônica considerada é a de incumbências quanto a regulamentação das hipóteses de degradação, de gerenciamento e de discriminação e, mitigação do tráfego na rede ao Poder Executivo por meio de decretos, após ser consultado o Comitê Gestor da Internet no Brasil (CGI Br), como se observa na leitura do art. 9.º, § 1.º e seus incisos:

Percebe-se que a lei assegurou os direitos de inviolabilidade da intimidade e da vida privada, conforme está expresso no art. 7º inciso I da Lei nº 12.965/2014:

> Art.7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: Iinviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

Nota-se ainda que a lei procurou regulamentar de maneira mais especifica um direito já era assegurado e amparado pela Constituição Federal vigente, no seu artigo 5º, inciso XII, dando destaque ao propósito da referida lei, isto é, tornando-a aplicável na esfera intima e privada das pessoas.

Importante enfatizar o fato de que este direito tem que ser mais preservado e defendido, como assevera Pereira:

> “[...] o direito das pessoas de defender e preservar um âmbito íntimo, variável segundo o momento histórico imperante, no qual estas possam desenvolver sua personalidade, bem como o poder de controlar suas informações pessoais [...]” (PEREIRA, 2006, p.140).

Ainda no art. 7º nota-se a preocupação em estabelecer garantias de segurança, como o sigilo de comunicações, que podem ser tanto armazenadas pelo servidor, quanto aquelas transmitidas pela internet:

> [...]
> II inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Assim, é notório que este direito foi de grande valia na regulamentação dos direitos e garantias dos principalmente em relação aos usuários:

> Além disso, o usuário passa a ter direito reconhecido em lei de não ter seus dados, incluindo hábitos de navegação e "logs"[23] repassados a outras pessoas sem o seu consentimento expresso e livre. (VANCIM et al, 2015, p.69).

Houve também a regulamentação sobre registros de navegação, assunto esse não era tratado na legislação pátria, assim como a monitoração ilegal de dados que também se encontrava sem norma:

> À medida que a pessoa se dispõe a “navegar” pela internet sua privacidade fica extremamente comprometida. É que com cada clique do mouse a pessoa vai deixando seu caminho marcado pela rede e, consequentemente os seus hábitos, seus vícios, suas necessidades e suas preferências. (GUERRA, 2004, p.78).

Tendo em vista que ao regulamentar ainda sobre a previsão legal de procedimento judicial, estabeleceu-se requerimentos para a parte interessada, como também como o usuário que foi prejudicado deve proceder. Com isso, tem-se norma legal dos direitos fundamentais do usuário nhoque diz respeito ao direito de informação.

> O armazenamento de informações sobre uma determinada pessoa é, assim, algo inquietante em razão da ameaça de que estes dados possam ser acessados indevidamente, dado que os cookies são responsáveis pelo armazenamento das informações pessoais dos usuários da internet, pois abrem caminho até o disco rígido do internauta e armazenam ali um arquivo de texto que identifica o computador com um numero único. (GUERRA, 2004, p.81).

Um único e simples acesso à internet, já traz uma quantidade enorme de registros, com isso é perceptível à vontade do legislador de exigir sanções quanto a isso.Observa-se ainda a intenção de sobrepor a norma em âmbito nacional às empresas que forem estrangeiras e que prestam serviço no Brasil, como dispõe o art. 11:

> Art. 11.Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em

[23] Log - É um registro de atividade gerado por programas e serviços de um dispositivo. Ele pode ser de diversos tipos como, por exemplo, de conexão (informações sobre número IP, incluída a data e hora de seu uso, atribuído a um dispositivo que utiliza a Internet) e de acesso a aplicações de Internet. Disponível em: <https://cgi.br/publicacao/diretrizes-recomendacoes-e-especificacoes-tecnicas-para-a-aplicacao-da-lei-sobre-internet-no-Brasil/>

> território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, (Lei 12.965/14)

A Lei 12.965/14 prevê sanções para caso haja o descumprimento dos artigos, conforme descrito a seguir:

> Art.12.Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I advertência, com indicação de prazo para adoção de medidas corretivas;
> II multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III suspensão temporária das atividades que envolvam os atos previstos no art. 11;
> IV proibição de exercício das atividades que envolvam os atos previstos no art. 11 (Lei 12.965/14)

Mesmo com este vasto rol de direitos e deveres, as sanções previstas nos art. 12 não causam prejuízos para as demais sanções decorrentes destes atos, onde se pode incorrer também nos âmbitos cíveis, penal e administrativo.

Dessa forma, é de suma importância, destacar aqui os pontos fundamentais a respeito do Marco Civil da Internet para uma melhor compreensão:

Em relação aos direitos, o Marco Civil considera a internet uma ferramenta fundamental para o exercício da liberdade de expressão e apregoa que ela deve ajudar o brasileiro a se comunicar e manifestar-se como bem entender, nos termos da CF/88.

A neutralidade é um dos pontos essenciais no que tange o estabelecimento neutro da rede. Em linhas gerais, significa que as operadoras estão proibidas de comercializar pacotes de internet espécie ou categoria de uso. O governo pode até fazer essa discriminação, mas só em duas situações: se ela for imprescindível para a prestação dos serviços; ou se os serviços de emergência precisarem serem priorizados.

No tocante a guarda de registros e informações, os provedores de internet e de serviços se obrigarão a fornecer as informações dos usuários, através de ordem judicial. Na provisão de conexão à internet, o administrador

do sistema autônomo tem o dever de manter os registros de conexão, sob sigilo e pelo menos por um ano, no entanto os registros de acesso a aplicações têm o prazo menor: seis meses.

É sabido que qualquer empresa que tenha base operacional no Brasil, mesmo sendo estrangeira, precisa respeitar e seguir a legislação do país e entregar informações solicitadas pela Justiça. Sob pena de sanções, tais como: advertência, multa de até 10% de seu faturamento, suspensão das atividades ou até da proibição de exercício da atividade. No tocante a responsabilização pelo conteúdo, a empresa que fornece conexão nunca poderá ser responsabilizada pelo conteúdo postado por seus clientes. Já quem oferece serviços como redes sociais, blogs, vídeos etc. corre o risco de ser culpado, caso não tire o material do ar depois de avisado judicialmente. Haverá um prazo para que o conteúdo considerado ofensivo saia de circulação, mas o juiz que cuidar do caso pode antecipar isso se houver “prova inequívoca”, levando em conta a repercussão e os danos que o material estiver causando à pessoa prejudicada.

Quanto as obrigações por parte do governo; administrações federal,estaduais e municipais terão uma série de determinações a cumprir. Entre eles estabelecer “mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do ramo empresarial, e da sociedade civil bem como da comunidade acadêmica”.

Os governos serão obrigados a estimular a expansão e o uso da rede, ensinando as pessoas a utilizar a tecnologia para “reduzir as desigualdades” e “fomentar a produção e circulação de conteúdo nacional”.

Os serviços de governo eletrônico precisarão ser integrados para agilizar processos, inclusive com setores da sociedade, e a internet ainda será usada para publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada, conforme o inciso VI do art.24 da Lei nº 12.965/2014.

Finalmente, há ainda a predileção por tecnologias, e padrões de formatos abertos e livres, e ha de se estimular a implantação de centros de armazenamento, gerenciamento e de disseminação dos dados no Brasil, “promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa”.

O Marco Civil da Internet que define regras claras com respeito dos: Direitos, Deveres e Princípios para o uso da rede no Brasil. Em que reconhece no âmbito virtual os princípios constitucionais como a liberdade de expressão, a privacidade e os direitos humanos, além de definir responsabilidades dos provedores de serviços bem como orientar a atuação do Estado no desenvolvimento e utilização da rede.

A lei está alicerçada em três princípios:

Neutralidade, que garante o tratamento de forma isonômica para qualquer pacote de dados, sem que este acesso ao conteúdo dependa de valor pago.

> O princípio da neutralidade de rede previsto na Lei 12.965/2014 consiste na garantia de tratamento isonômico dos pacotes de dados pelas redes dos sistemas autônomos sem degradação nem discriminação por conteúdo, origem e destino, serviço, terminal ou aplicação (cf. MCI, Art. 9º). (CGI.br, pg.02)

Privacidade, o usuário terá a garantia do direito à inviolabilidade e ao sigilo das comunicações. As empresas terão que desenvolver mecanismos para garantir que os e-mails só sejam lidos pelos emissores e pelos destinatários

A garantia de proteção a dados pessoais e registros de conexão. A cooperação das empresas de internet com órgãos de informação estrangeira se tona ilegal.

Liberdade de Expressão, onde a decisão sobre retirada de conteúdo fica limitada à justiça.

O Marco Civil da Internet no Brasil, veio para assegurar a liberdade e a segurança do usuário e do provedor de acesso à internet, estando, a lei, diretamente relacionada a diversas outras, como o Estatuto da Criança e do Adolescente, o Código de Defesa do Consumidor, dentre outros. O aspecto colaborativo da elaboração do Marco Civil, no qual o processo participativo foi inédito na criação de uma lei brasileira com participação popular, dando direito a participação ativa. Foi a primeira vez que os cidadãos puderam ter voz ativa na criação de uma lei, tendo em vista que é uma norma que os beneficia diretamente. Com isso, pode se constatar que o conteúdo abordado pela lei seja um tanto quanto superficial, e com isso possa vir a mudar com o passar dos anos.

Todavia vemos no art. 13 do MCI estabelece o dever legal de prazo de guarda de logs.

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Afora a discussão se tal dever legal de retenção de dados é uma interferência excessiva ao direito à privacidade a atrair a sua inconstitucionalidade, fato é que o MCI adotou tal política legislativa. Nesse contexto, importa verificar como tal escolha foi arquitetada, levando-se em conta os limites impostos pelo MCI ao fluxo informacional dos registros de conexão e navegação dos usuários.(BIONI, 2018, pg. 304)

Propagar as informações ao usuário respeitando a lei do Marco Civil da Internet tende a impulsionar as questões ligadas à localização, liberdade, segurança, acesso, uso, criação e disponibilização da informação na Internet.

Um dos maiores avanços tidos com a promulgação da referida lei foi na questão da privacidade e a segurança do usuário, que foi diretamente assegurada com mecanismos de defesa que protegem tanto na esfera civil, penal ou administrativa com as sanções que devem se impostas pelo Estado caso esses direitos sejam violados.

2.6. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A partir do pressuposto necessário de se ter uma norma pátria que fosse eficiente e eficaz no intuito primordial de vir a proteger os usuários nacionais como também os usuários em passagem pelo território nacional tanto no ambiente físico e principalmente no âmbito de ambiente virtual, edita-se a Lei Geral de Proteção de Dados Pessoais (LGPD) Lei 13.709/2018; com base na norma da União Européia a: General Data Protection Regulation (GDPR Regulamento Geral de Proteção de Dados).

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi aprovada em 14 de agosto de 2018, onde contou com um veto presidencial, ao que se refere à criação de uma agencia reguladora a Agencia Nacional de Proteção de Dados

(ANDP), posto que se esta autarquia de fato fosse instituída e sob o “manto” do Ministério da Justiça, poderia ser realmente considerada inconstitucional; de modo que a MP. 869 de 2018 institui a criação da citada autarquia sob a presidência da republica.

A LGPD (Lei nº 13.709/18) que entrará em vigor no ano de 2020. Trata-se de um conjunto de regras jurídicas para coleta, armazenamento e processamento de dados determinados ou determináveis, feitos por pessoas físicas, empresas e organizações do Estado.

A Lei visa regulamentar a política de proteção de dados pessoais e privacidade no Brasil e que, modifica alguns dos artigos presentes no Marco Civil da Internet (Lei 12.965/2014), e impactará de forma significativa o modo outras normas do ordenamento brasileiro, como também modificando fortemente a forma como os órgãos públicos e as empresas tratam a privacidade e a segurança das informações e dados dos usuários e clientes.

A referida lei teve como fonte direta o então Regulamento Geral de Proteção de Dados (General Data Protection Regulation GDPR) regulamento da União Européia em vigor desde 25 de maio de 2018, fazendo com que entidades e empresas no bloco da União Européia tivessem de se adaptar antes da sua vigência.

Definições relevantes contidas no art.5º da Lei nº 13.709/18:

> I dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

> VI controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (Lei nº 13.709/18)

Destacamos o art.6º da lei no tocante aos princípios do tratamento da LGPD

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

> I Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V Qualidade Dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X Responsabilização E Prestação De Contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Lei nº 13.709/18).

Mediante o tratamento de dados, junto com a tecnologia utilizada atualmente, Bioni (2018) assevera que são geradas classificações e segmentações das preferências, das tendências ideológicas e até mesmo do histórico de compras dos usuários, num processo conhecido como “profiling”, em que:

> Os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. [...]. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes [...]. (BIONI, 2018, p.122).

Nota-se que a privacidade e a liberdade estão diretamente conectadas, chegando a serem, muitas vezes, confundidas nas relações do mundo digital:

> A liberdade de informação tem sido definida como a mãe de dois direitos: de informar e de ser informado. A informação deve ser observada sob o aspecto ativo e passivo. No primeiro caso, aborda-se a possibilidade de acesso aos meios de informação em igualdade de condições, possibilitando o direito de expressar o pensamento e informar; o aspecto passivo salvaguarda o direito de assimilar e receber as notícias e as opiniões expressas por alguém. Neste último caso, tem-se a liberdade de se informar, que Casavola define como atividade de indagação ou inspectio. É do equilíbrio entre esses dois perfis ativo e passivo da liberdade de informação que se garante a comunicação no interior de uma sociedade pluralista. (PAESANI, 2014 apud CASAVOLA,1996)

Assim, observa-se que a coleta de dados, quando ilícita, gera invasão de privacidade, o tratamento destes dados com a formação de um profiling[24] do titular, que toma diversas decisões, acaba violando o direito de liberdade de informação, pois acarreta a possibilidade de exposição aos conteúdos que não estejam de acordo com o perfil gerado para o titular, em outras palavras, cria uma bolha.

Porém, é notório que mesmo estando em um tratamento realizado licitamente, não apenas o titular será afetado por tais informações, interferindo

[24] Inglês = Criação de perfil. Técnica auxiliar de investigação criminal; a atividade de coletar detalhes importantes e úteis sobre alguém ou algo.

em sua liberdade de acesso à informação, de forma que acarreta em um processo totalmente contrário à proposta inicial da internet, causando diversos problemas, como por exemplo, isolamento social e uma ignorância daquilo que não está definido dentro dos parâmetros estabelecidos pelo algoritmo que decide o conteúdo ao qual o titular será exposto.

Salienta-se ainda sobre o conceito de “consentimento”, que conforme (Bioni 2018) é a definição central da LGPD, estando contido no artigo 5º, inciso XII, da LGPD, assim dispõe, sobre o instituto do consentimento, que:

> [...] grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio do quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais “modernos”, como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (minimização de dados). (BIONI, 2018, p.186)

Observa-se que termo “consentimento” foi inserido 35 vezes na LGPD, o que mostra o quanto é necessário para que se tenha uma efetiva proteção de dados e consequentemente da privacidade, uma vez que, em muitos casos, o fato de ser verificado o devido consentimento transforma uma prática ilícita em lícita.

Já o artigo 15 da Lei em questão elenca seis hipóteses para que se efetue o término do tratamento de dados, sendo de grande importância estudá-los pois qualquer tratamento que continue acontecendo após a verificação de um desses cenários será tido como violação do direito à privacidade, fazendo incidir responsabilidade dos agentes.

> I verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II findo período de tratamento;
> III comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

> IV determinação da autoridade nacional, quando houver violação ao disposto nesta Lei nº 13.709/18. (BRASIL, 2018)

Quando o tratamento acabar, de acordo com o artigo 16 da LGPD, devem ser excluídos os dados pessoais, para que assim se garanta maior segurança ao titular, sendo possível a conservação apenas para:

> I cumprimento de obrigação legal ou regulatória pelo controlador;
> II estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Lei nº 13.709/18.(BRASIL, 2018).

Dessa forma, em conformidade com o inciso IV, o término do tratamento não se dará em todos os seus termos de uso exclusivo do controlador, de forma que a utilização de dados é espécie de tratamento. Assim, ainda que se tenha o término do tratamento levando em consideração alguma das circunstâncias previstas no texto do artigo 15, o inciso IV do artigo 16 abre espaço para uma interpretação de forma que o tratamento não irá alcançar o seu término, desde que preenchidos tais requisitos.

> Juntamente com o direito à privacidade, invoca-se o princípio constitucional da presunção de inocência. Na medida em que se retêm dados de forma indiscriminada para posterior persecução criminal, presume-se que todos são, a priori, potenciais criminosos, violando-se, assim, tais preceitos constitucionais. Veja-se, ainda, a discussão travada no direito europeu em que a Corte de Justiça da União Europeia declarou a invalidade da diretiva da retenção de dados por ser uma "serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary".[25] ("Séria interferência nos direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais, sem que essa interferência seja limitada ao estritamente necessário") "tradução nossa" (Court of Justice of the European Union, Nº 54/14, 2014)

No tocante dos direitos que são conferidos ao titular por intermédio da Lei Geral de Proteção de Dados que estão elencados entre os artigos 17 e 22.

[25] Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>.

Onde é garantido ao titular o acesso a correção, a portabilidade de seus dados, assim como a anonimização[26] e a eliminação dos dados nas hipóteses cabíveis, desde que haja o requerimento para tal.

Entende-se que qualquer ato humano, sendo de natureza tecnológica ou não, é de extrema importância se ter como prioridade o respeito aos princípios constitucionais pátrios vigentes. Um dos Princípios da Constituição Federal está evidente no artigo 5.º, XII e que fala expressamente a respeito da inviolabilidade da correspondência ou dos dados:

> Art.5.º, XII é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.
> X são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988).

Quanto à constitucionalidade, observa-se que o Controle de Constitucionalidade está fincado na Base da Supremacia Constitucional, no que se refere e se fraciona em Supremacia Material, pertinente ao conteúdo constitucional (direitos fundamentais, organização do estado, organização dos poderes) e Supremacia Formal, que sucede da rigidez e do processo de elaboração das normas constitucionais.

Nessa perspectiva, considera-se que a rigidez constitucional desdobra-se exatamente da previsão de um processo especial e agravado, em que está reservado para a/as alteração(ões) da(s) norma(s) constitucionais, consideravelmente distinto do processo comum e, simples, previsto, para a produção e modificação das leis complementares e ordinárias.

Dessa forma percebe-se que, o controle de constitucionalidade está nitidamente presente nos ordenamentos jurídicos em que há rigidez

[26]Dado pessoal e/ ou sensível que foi tratado para que suas informações não possam ser vinculadas ao seu titular original. Que é uma técnica de processamento(s) de dados que remove ou modifica informações que possam vir a identificar uma pessoa / usuário. Pela própria definição da lei, dado anonimizado “perde a possibilidade de associação, direta ou indireta, a um indivíduo”.

constitucional onde temos na constituição federal de 1988 de forma tácita em seu artigo 60 §4º.

> Art. 60, §4º, IV os direitos e garantias individuais.

Com isso, para uma melhor adequação e segurança dos indivíduos que são usuários de internet houve a necessidade de criação de uma Lei que tratasse especificadamente dos pontos acima expostos, referente à garantia de segurança e liberdade dos direitos e deveres dos usuários e provedores de internet.

Neste sentido destaca Luiz Edson Fachin expõe que:

> Os direitos fundamentais, que o artigo 5° da Constituição Federal de 1988 considera invioláveis, são inerentes à dignidade humana, neles se traduzem e concretizam as faculdades que são exigidas pela dignidade, assim como circunscrevem o âmbito que se deve garantir à pessoa para que aquela se torne possível. (FACHIN, p.181).

A titulo de apresentação trazemos o art. 8º da então Carta dos Direitos Fundamentais da União Européia, em que versa sobre a Proteção de Dados Pessoais (*ipsis litteris*) .

> ARTIGO 8.º Protecção de dados pessoais
> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por
> lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Antes de embrenhar nas características ora CRITICAS da LGDP 13.709/2018. é necessário observar que o artigo 5º da CF/88 expõe e cumpre taxativamente como alicerce o arcabouço legal protetor de todos os cidadãos, inexistindo dúvidas no tocante a preservação das informações prestadas em diversos meios de cadastros e de banco de dados, estes que podem vir a abalar a privacidade do cidadão.

2.6.1 As implicações sociais da LGPD

Quiçá o leitor esteja indagando, em que aspecto à LGPD é importante? Resumidamente em uma única frase que é PRIVACIDADE ! Tão simples mas ao mesmo tempo complexa em si, tendo em vista que há normas que tratam disto em especial o art. 5º da CF/88 e outras normas espaças no ordenamento brasileiro !

Esta lei surge para proteger o cidadão(ã) de possíveis violações contra a nossa privacidade, em verdade, quanto mais uma entidade pública ou empresa sabe sobre nós mais ela poderá urdir as estratégias e ações que possam vir a "perturbar" a sua tomada de decisão natural, ou seja moldar sua decisão e/ou comportamento direcionado.

Também é possível que os dados pessoais de alguém influenciem o modo como outras pessoas nos vêem e observam, pois querendo ou não fazemos parte de um corpo chamado sociedade, e esta sociedade tem "N" olhos e cada qual sofre influências do meio, no olhar e no nosso proceder.

Não causa espanto o fato pelo qual, a cada geração e/ou surgimento de novas tecnologias modifiquem consideravelmente o prisma do olhar, bem como o modo de vida das pessoas diante do acesso e utilização de tais tecnologias digitais.

Algumas destas tecnologias são destrutivas, em que uma inovação tende a transformar um nicho ou setor já existente ou criando um novo por meio da introdução da conveniência, acessibilidade e simplicidade, que ao seu uso tendem muitas vezes a reformulam conceitos e trazendo algo totalmente novo a exemplo do não tão novo como o Facebook, WhatsApp, Instagram, YouTube, Telegram, Uber; e as mais recentes que irão certamente impactar de modo positivo quando bem empregadas, são: O Blockchain um serviço de exportação de criptomoedas os famosos Bitcoins (moeda virtual), Bitcoin e carteiras de Bitcoin Cash que viabilizará sistemas sem um órgão de regulação. De modo que blocos inalteráveis de informações e dados compartilhados poderão mudar as dinâmicas na gestão de negócios e empresas, fomentado o surgimento de novos nichos de mercado como a segurança digital e o sistema jurídico, onde já temos algoritmos especializados para a busca e implementação no feitio de petições, quando não ao todo. Outras consistem em adaptações ao que já se tem. Em todo caso, esses avanços não incidem

somente na esfera econômica, com o maior lucro auferido pelas empresas, mas repercutem no âmbito social e, consequentemente, no jurídico.

Aparecem novos negócios, que nos deixam perplexos com a relação entre os valores de bens concertos e o valor da informação. chega-se a um estágio do desenfreado capitalismo e a volatilidade das ações de empreendedores sobre a rapidez com surgem e se concretizam e se valorizam de modo impressionante. Nesta conjuntura há o lado benéfico, porem pode gerar também vários danos à uma sociedade.

Diante de novidades dentro e fora do mundo tecnológico surgem as Startups que buscam inovar em qualquer área ou segmentos de atividades no intuído de desenvolver um modo de negócio viável e de solução a um determinado produto e/ou nicho para atender a sociedade.

Muitas destas encontram-se em ambiente de produção e desenvolvimento de aplicativos móveis os App's comuns em smartphones, para executar tarefas das mais variadas, bem como de entretenimento no campo de jogos e comunicação por som, vídeo, e transmissão de dados e documentos.

Neste ponto encontra-se a Internet das Coisas (IoT)

Já experimentamos diariamente a Cloud computing e o Edge e cloud computing (Computação nas nuvens e Computação em borda nas nuvens) "tradução nossa", no uso de soluções na nuvem, onde a computação de "extremidade" ou borda, que é o processamento que acontece em local físico ou perto de um usuário ou da fonte de dados. Com essa proximidade o usuário se beneficia de serviços bem mais céleres e confiáveis. Tem-se também

Diante do apresentado acima, e neste ponto em especial, abordaremos a segurança em atenção ao MIC e a LGPD, como também os crimes em ambiente virtual os cibercrimes. De modo tal em que veremos adiante os aspectos críticos, no tocante a segurança; bem como a forma pela qual os aplicativos móveis (App's) atuam, em especial quanto a proteção e a inviolabilidade dos dados, como também a tratativa da violação da privacidade, de dados e dados gerais, estes utilizados de forma desmedida sem a devida precaução de atenção e de segurança por parte do usuário.

A maioria dos aplicativos móveis, no momento em que um usuário escolhe instalar um App (aplicação móvel) em seu smartphone, abre-se uma tela inicial informando que "precisa de acesso a: ", e segue um lista com

conteúdo resumido de cada item que o App terá acesso; em nenhum menu ou sub-menu desta operação, há uma opção de bloqueio ou não permissão por parte do usuário em não instalar ou dar acesso a um determinado item ou subitem da lista apresentada, a única opção é a de não instalar o aplicativo, com isto, fica indefeso e refém do próprio aplicativo.

A titulo de ilustração do apresentado, segue as telas capturadas de um aplicativo móvel, no caso o Telegram, aplicativo de comunicação entre usuários.

APLICATIVO	FUNÇÃO	DESENVOLVEDOR
TELEGRAM	Troca de mensagens	Telegram Messenger LLP

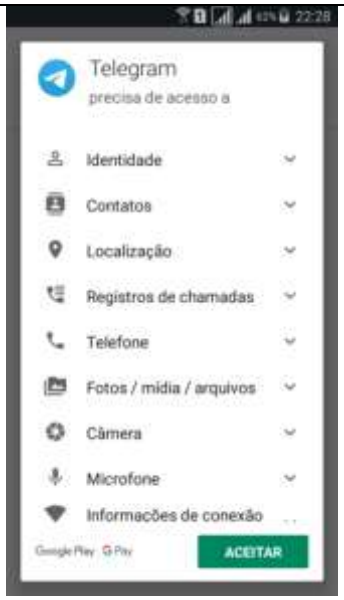

Imagem 01

Imagem 02

Imagem 03

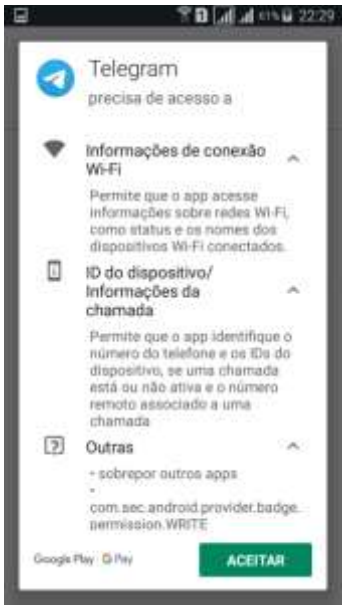

Imagem 04

Imagem 05

Imagem 06

Como podemos notar nas imagens acima, que em todo o processo de instalação, não há, opção de suprimir ou desabilitar algum dos itens que o aplicativo terá acesso ao aparelho do usuário. isto ocorre na grande maioria de aplicativos desenvolvidos para a plataforma base do sistema operacional ANDROID, baseado em núcleo Linux[27]

Ao observar todo o processo de instalação passo a passo, e, durante a utilização e usabilidade do aplicativo, que não há nenhuma opção nas configurações antes e pós instalação, em que o usuário possa desabilitar um determinado item ou função do aplicativo e, isto ocorre na grande maioria dos app's.

É evidente que um aplicativo por mais "inocente" ou que tenha em sua pós instalação, informes da "política de privacidade" por parte do desenvolvedor, o usuário leigo ou o experiente não estarão 100% seguros, vez que os estes não tem ou terá acesso ao código fonte ou diretivas operacionais de leitura ou não permissão de determinada linha de código fonte, excerto se o usuário realizar engenharia reversa, obtendo assim o código fonte original e, permitindo em alguns casos até mesmo modificá-lo e/ou recompilá-lo, tal pratica neste caso é maliciosa, e nesta esfera encontram-se os crackers, que fazem uso desta pra burlar assim os arquivos executáves.

Um aplicativo pode solicitar permissão de acesso a dados do dispositivo, como contatos do usuário, mensagens SMS, armazenamento montável (cartão SD), câmera, Bluetooth etc. O usuário precisa conceder essas permissões de forma explícita.[28]

Notamos que fica evidente a não atenção ao disposto no art.5º da CF/88, bem como nas demais normas jurídicas vigentes no Brasil e a viger, no caso a LGPD Lei 13.709/2018, devendo esta ultima de atualizações que abranja a coibição de tal pratica danosa ao usuário, considerando que este está completamente exposto e desmuniciado de proteção ao utilizar um App em seu aparelho. Embora possa contar com as normas espaças já listadas em capitulo anterior. Fatos mais alarmantes encontam-se o aspecto tecnológico das casas inteligentes que serão o lado "domestico" da Internet das Coisas

[27] Sistema Operacional baseado em Unix inicialmente criado para desktops, também é utilizado em outros equipamentos como tablets, smatTV, servidores, smartphones e outros.
[28] Disponível em: https://developer.android.com/guide/components/fundamentals

(IoT), onde robôs, utensílios e aparelhos autônomos, um verdadeiro "Big Broder Invasivo". O leitor poderá assistir o filme: Invasão de Privacidade (2017). Um filme de John Moore com elenco de Pierce Brosnane outros. Onde mostra um homem "analógico inserido em um mundo digital e, sofrendo as consequências de por a "segurança" em aparelhos e aplicativos. Um filme que não é um "dejá vu" de Psicose, vale salientar.

Deste modo. listado anteriormente passamos para uma abordagem de cibercrimes, que não impede sua concretização por meio dos aplicativos móveis (App’s).

CAPÍTULO III - CRIMES CIBERNÉTICOS

3.1 A CONDUTA HUMANA EM AMBIENTE CIBERNETICO

A conduta humana em ambiente virtual pode determinar um ato delituoso ao caracterizar ações que vão contra o que está previsto em leis e/ou instrumentos regulatórios. Sob este prima, a internet devido as avanços alcançados até hoje, tornou-se um oceano de águas revoltas e turvas em que antes um simples navegante deleitava-se, hoje deve ter cuidados redobrados

> Na Internet, vige o regime da livre iniciativa e inovação: não é necessária autorização prévia para se criar um novo serviço ou aplicação, desde que seguidas às recomendações técnicas do IETF. As redes de telecomunicações existentes em cada país servem como alternativas de suporte para o funcionamento da "rede de redes" que é a Internet. Apesar de estarem intimamente relacionadas, Internet e telecomunicações são atividades distintas.[29]

O comércio eletrônico, a instalação de aplicativos móveis (App's) torna-se um vasto campo fecundo para a atuação das categorias de práticas criminosas descritas abaixo.

Os hábitos dos usuários, tais como o compras online, pagamento por maquinetas sem fio, localização geográfica (GPS), fotos, compartilhamento de informações em rede não segura, são fontes preciosas para a atuação de empresas no direcionamento de consumo, bem como um leque de oportunidades para a atuação de cibercriminosos.

Os usuários no uso constante da internet através de tecnologias móveis e virtuais, notebooks, smartphones, tablets, relógios smartwatchs, cloud computing (computação em nuvem) e outros, permitiu avanços significativos na otimização do tempo e execução de tarefas, desta forma as pessoas a cada dia estão, cada vez mais, conectadas à internet, e as funcionalidades de aparelhos, e também de aplicativos móveis os (App's), que oferecem uma infinidade de recursos úteis e recreativos.

---

[29] CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015. (pg. 01 e 02).

Porém, diante de tanta facilidade para uns e dificuldades para outros na utilização destas tecnologias e recursos, encontram-se perigos não tão visíveis

Assim, a começar pela forma de comportamento dos usuários em uma "simples corrida de Uber" ou o compartilhamento em tempo real da geo localização, bem como dos hábitos de consumo de cada um; desta forma os "experts" cibercriminosos de plantão podem colher estas preciosas informações e dela traçar estratégias que vão dos golpes até algo mais relevante e sério, a exemplo de roubo de dados, perfis da agenda de contato, projetos hospedados em nuvem não tão seguras etc.

> Essa onipresença da Internet permitiu, de forma acoplada com a possibilidade do monitoramento da localização geográfica (global positioning system/GPS) dos smartphones, que as publicidades também sejam direcionadas com base em tal informação. Leva-se, assim, em conta, a proximidade física do potencial consumidor ao bem de consumo ofertado, como, por exemplo, seria o caso de um restaurante. (BIONI,2018, p.45)

3.2 CIBERCRIME

Cibercrimes ou crimes informáticos são em si os crimes praticados por meio da internet em sua grande rede w.w.w.,[30] onde se alastram após o advento da mesma em diversos *modus operandi* da interação entre os usuários ao logo do tempo, de modo que novas modalidades e meios de interação entre os usuários surgem em proporção semelhantes a novos meios de se praticar crimesdiversos.

> Segundo Chaves (apud SILVA, 2003, p.19), Cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação”. Assim, por meio do conceito analítico de crime, pode-se chegar à conclusão de que “crimes cibernéticos” são todas as condutas “típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática” (SCHMIDT, 2014, [n.p.]).

[30]World Wide Web ou W.W.W. Em português significa: Rede Mundial de Computadores, que é o sistema de documentação interligada em hipermídia,que funciona em parâmetros URL (endereço), HTTP (protocolo) e HTML (método da codificação das informações a serem exibidas), executado em ambiente virtual, ou seja, internet.

A conceituação dada pela INTERPOL é a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita no âmbito da internet. Tal ato lesivo consiste em enganar a seguridade de computadores e dispositivos móveis portáteis, sistemas de comunicação e redes corporativas. Assim,ocibercrime, nada mais é do que uma conduta ilegal realizada por meio do uso do computador da internet (ROSA, 2002, p. 53-57).

Quanto ao delito que é definido no meio jurídico, como: “Quaisquer açõese/ou comportamentos que infrinjam uma lei já estabelecida; ação punível pela lei penal; crime; todo ato caracterizado por uma transgressão de uma moralpreestabelecida; falta; flagrante delito. O delito no momento exato em que é praticado; Corpo de delito. Elemento material (indícios) dainfração, provadocrime; e,etimologicamente(origem dapalavra delito):do latim *delictum*”.

Ouve-se algumas vezes, que quando algum bem ou serviço é aparentemente gratuito, provavelmente há uma verdade oculta de que o cidadão esteja pagando por este bem ou serviço fornecendo seus dados. Isso ocorre com frequência, por exemplo, nas redes sociais com os cartões de credito, cartões fidelidade de lojas e hiper e supermercados que propiciam facilidade e, principalmente com inúmeros aplicativos (App’s) que oferecem serviços dos mais variados e relevantes, emtroca não mais que, dos dados pessoais deusuários.

As redes sociais utilizadas por milhares de pessoas e,detêm dados digitais,que o usuário espontaneamente os coloca em ambiente virtual, e que são capturados por robôs, porém, também faz deduções com base nas interações on-line[31] e off-line[32] entre usuários, e estas informações são muitas vezes compartilha-as com terceiros onde algoritmos programados de formas especiais traçam um perfil do usuário e que permite determinar as ações de prospecção na oferta de produtos e serviços com basenas informações capturadas.

[31] Conectado direta ou remotamente a um computador, sistema, equipamento ou dispositivo (pronto para o uso).

[32] O Contrário de on-line (conectado) aquele que não está conectado a um computador ou que não pode ser us. em um dado momento (quer seja de sistema, equipamento ou dispositivo).

Faz-se necessário abrir um parenteses e, apresentar ao leitor o que sejam os algoritmos e a atuação,a usabilidade e o empregodestes no ambiente virtual.

A conceituação simples de algoritmo já existe há séculos e o uso do conceito pode ser atribuído a matemácicos gregos, a exemplo da Peneira de Eratóstenes e o algoritmo de Euclides. Ilustra-se o conceito como uma receita culinária, embora os algorítimo sejam demasiado complexos que uma receita de bolo.

Segundo Dasgupta, Papadimitriou e Vazirani, "algoritmos são procedimentos precisos, não ambíguos, mecânicos, eficientes e corretos". (Algoritmos. Porto Alegre: AMGH, 2010).

De maneira que os algoritmos são utilizados na internet de modo a capturar as ações do usuário e interpream o comportamento e qualquer ação, que este faça, seja visualizando uma foto, assistindo a um filme online ou realizando buscas de produto de consumo, ou até mesmo acessando as redes sociais, neste instante os algoritmos conseguem capturar uma grande parte do comportamento do usuário, e assim aprendem e reaprendem, são estes algoritmos parte importante na IoT.

Assim uma pessoa pode ser influenciada por um determinado algoritmo que de acordo com o que aprendeu do "costume" do usuário, possa a vir orienta-la em suas tomadas de decisões e/ou escolhas. Porem, não é tão fácil identificar como tudo isso possa estar acontecendo ao redor.

Os algoritmos que são utilizados em redes sociais os famosos cookies (robôs) atuam para apresentar e até sugestionar o melhor caminho ou conteúdo para uma experiência online e que possa até ser concretizada no campo real, como por exemplo a escolha de um notebook, smartpnhone, um carro ou qualquer outro bem. Embora tal fato seja pareça esquisito, boa parte dos algoritmos ajudam, mas nem tantos tem em si a beneze de "santo", muitos são como "santos do pau oco".[33]

[33] No imaginário popular era uma imagem de um santo esculpida em madeira e oca por dentro, onde escondia-se ouro e gemas preciosas para contrabandear ou esconder do fisco na época Brasil Colonial.

Os algoritmos são muito utilizados na publicidade, em sites, estão envolvidos no sobe e desca das bolsas de valores ao redor do mundo, em programas complexos de computacionais e em mutias outras aplicabilidades e funções. No entanto há uma preocupação no tocante a falta de clareza, de transparencia na utilização destes sistemas de inteligência artificial, em que tomadas de decisões podem acarretar algum dano; todavia com a popularização destes algoritmos surge uma gama de questões no tocante a segurança, uma vez que um algoritmo pode até decidir pela pessoa e, até mesmo realizar a dozimetria da pena "merecida" por um determinado agente criminoso, ou até que pondo um robô autonomo pode ir e interferir na privacidade e segurança de uma família, empresa e governos.

A privacidade e a segurança são as duas maiores questões relevantes na atualidade onde governos, empresas e pessoas se defrontam ao pensar em como proteger seus dados e como assim o fazer sem que se sintam lesados.

Um dos problemas em relação aos crimes praticados na internet é a sensação de impunidade, uma vez que a criminalidade cresceu mais rápido que a legislação foicapaz de acompanhar em paços largos, no intuito de parartaisdelitos,assimcomo também às técnicas para identificar os autores dos crimes.

Como efeito disso os crimes virtuais se tornaram corriqueiros tanto no Brasil quanto no mundo de forma geral e, a dificuldade do poder legislativo em tipificar essas modalidades de delitos onde se fez surgir um clima de “terra sem lei” naInternet, já que os criminosos sabem a real dificuldade na identificação dosautoresde crimes. Importante salientar inclusive que, no Direito Penal brasileiro ou a conduta é considerada típica ou não existe delito.

Um dos maiores problemas enfrentados hoje em dia, na questão do combate aos crimes virtuais ou cibercrimes, tem sido buscar a correta tipificação dentro da legislação brasileira vigente, uma vez que a utilização indevida dos meioscomputacionais, em condutas delituosas, extrapola em muito os limites dos delitos existentes a um enquadramento penal propriamente dito.

Dos crimes no ambiente virtual que já são tipificados pelo CP, previstos nos outros diplomas:Lei nº 12.737/2012, Decreto nº 7.962/2013, e Lei nº 12.965/2014, listados acima; como, por exemplo: os crimes contra a honra, racismo, estelionato, uso indevido de dados pessoais, propaganda enganosa, pedofilia, etc.

Em que se buscam soluções legais em que deverão objetivar a circulação licita de dados na rede, dando a privacidade devida ao usuário sem cercear ou por controle ditatoriais ou escusos e obscuros ao acesso as informações.

Assim faz-se necessário atualizar as leis vigentes bem como regulamentar a captura, destino e uso dos dados dos cidadãos usuários.

3.3 SUJEITOS DO CIBERCRIME

Faz-se necessário distinguir alguns dos sujeitos do cibercrime, pois muito se fala em hackers, ocorre que "tecnicamente" o termo tem sido empregado de forma genérica pelos veículos de notícia e grande mídia, quando na verdade não deveria ser. Há uma diferença tanto conceitual quanto técnica entre os termos Hacker e Craker.

O Hacker é um usuário experiente e excelente programador que invade sistemas computacionais para provar as falhas e provar a sua capacidade e habilidade no ambiente computacional, porem este, opera sem o intuito de obter lucro, dados ou destruir os sistemas computacionais ou softwares,vindo a atuar em empresas e em algumas esferas do Estado.

O Craker é o sujeito com as mesmas capacidades do primeiro, no entanto este invade os sistemas para praticar o delito, ou seja, roubar as informações e dados, estes estão muitas vezes ligados a outros indivíduos que decifram os códigos e algoritmos, destruindo assim todo o código e as proteções dos softwares e, vindo assim acarretar danos às vítimas, bem por suborno ou ameaças obter ganhos financeiros como também apratica ilícita da venda de produtos ilegais.

3.4 CIBERCRIMES E ALGUMAS DAS MODALIDADES

Algumas das modalidades do cibercrime encontram-se o roubo de dados. Um fato/ato que ocorre de modo corriqueiro na internet, e em

especial nas redes sociais, com maior abundância no whatsapp, este tipo de crime é enquadrado e definido no Código Penal Brasileiro como Estelionato, Art.171:

> Art.171- Obter,para si ou para outrem, vantagem ilícita,em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento[...]

Este ocorre por divulgação de links que levam o usuário incauto a sites ou redes sociais onde precisam realizar um cadastro quer no próprio site criminoso ou após a instalação de alguns App's, devendo fornecer seus dados como: nome, cpf, data de aniversário etc.

Também por meio da utilização de softwares falsos e verdadeiros onde alguns destes após a instalação têm acesso aos dados do usuário gravados na máquina. Dispondo do acesso a tais dados há a possiblidade de falsificar cartões bancários, realizando transações dentre outros danos.

Embora de forma muito abrangente e indefinida em alguns pontos o Art.154-A do Código Penal Brasileiro (conhecida como "Lei Carolina Dieckmann") diz:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Severas críticas agudas afetando a então norma ligada aos crimes informáticos em especifico a este artigo 154-A tendo-se em vista, por exemplo, a uma parte deste no que diz respeito à Dificuldade probatória.

> [...] A dificuldade em atribuir a autoria do fato vem em grande medida determinada pela dificuldade probatória que rodeia a ilicitude informática. Isso se deve à própria dinâmica do processamento informático, que impede detectar uma determinada atividade ou processo posteriormente à sua realização, e em outras ocasiões, devido à facilidade para fazer desaparecer, de forma fraudulenta,por meio da manipulação de programa e dados, as atividades, operações, cálculos ou processos que foram realizados anteriormente.(GRECO, p. 764)

3.5 CIBERESPIONAGEM

Outro dado preocupante com respeito às ameaças cibernéticas é a espionagem econômica onde empresas que tiveram seus dados roubados bem como suas inovações e descobertas, tendo a concorrência antecipando ações causando prejuízos financeiros e materiais.

Segundo André Luís Wolosyn, “a espionagem tem como objetivo transmitir informações sobre o inimigo para proporcionar uma ampla visão da situação, e assim, apontar tendências e elaborar estimativas” (WOLOSYN, 2013, p. 136-7).

Outro dado que chama a atenção foi o ocorrido em 08/04/2009, onde os Ciberespiões da China, Rússia e outros países invadiram o sistema elétrico dos Estados Unidos e instalaram programas que podem vir a ser usados para interromper o funcionamento da rede.[34] Os hackers lançaram o ataque para "navegar pelo sistema elétrico americano e seus controles".

Os chineses tentaram traçar a planta das infraestruturas dos EUA, como a rede elétrica, e os russos também disse uma fonte do serviço de informação, segundo quem cada vez mais espiões tentam obter informações sobre as infraestruturas do país.

A reportagem do Wall Street Journal[35] diz ainda que quem descobriu os piratas foi o serviço secreto, e não as empresas, o que fez aumentar o temor de que ciberespiões consigam tomar o controle de instalações elétricas, de uma usina nuclear ou das redes financeiras via internet.

3.6 MANIPULAÇÃO DE INFORMAÇÕES

Manipulação de informações "Guerra de Palavras", que consiste em manipular as informações com objetivos politicos, com o proposito de interferir e/ou intervir em processos de cunho eleitoral, até mesmo de outros países.

Também obter informações privilegiadas de cunho privado, sendo estas sob aspecto comprometedor de qualquer tipo de governo e suas instituições, privada, comercial ou de um outro tipo, e usá-la com um finalidade determinada, é uma das armas mais poderosas da batalha cibernética no século 21.

"Não é possível intervir nos sistemas eletrônicos de uma eleição para mudar seus resultados", (Brian Lord, ex-diretor encarregado de Inteligência e Ciberoperações do Centro de Comunicações do Governo (GCHQ, órgão de inteligência britânico.)

---

[34] FONTE: AGÊNCIA EFE Disponível em:<http://www.clicrbs.com.br/especial/rs/tecnologia/19,0,2469226,Crackers-invadem-sistema-eletrico-norte-americano-diz-jornal.html>

[35] FONTE: Wall Street Journal Disponível em : https://www.wsj.com/articles/SB123914805204099085

CONSIDERAÇÕES FINAIS

De todo o exposto, conclui-se que, apesar de o Marco Civil da Internet abordar a temática, é necessária uma lei específica que abranja também a questão da segurança dos dados pessoais dos usuários. Com isso, faz-se necessário e extremamente importante a discussão e estudo revisional da Lei Geral de Proteção dos Dados Pessoais. Para que dessa forma se possa conseguir salvaguardar efetivamente os direitos dos titulares dos dados, onde se possa abordar as lacunas existentes em relação aos agentes e as autoridades envolvidas, instituindo mecanismos fiscalizadores imparciais e autônomos bem como em viabilizar meios eficazes para a proteção dos dados pessoais.

Assim, a utilização comercial dos dados pessoais é um dos temas que deve maior proteção pelo Estado. E, nesse aspecto a lei ,ao nosso ver, não é tão clara, como também é obscura quando em si não trata a respeito dos aplicativos móveis os App's fonte estes de maior afronta a legislação Brasileira, alcançando os aspectos comerciais e estabelecendo os princípios e direitos devidos, além de determinar mecanismos e procedimentos efetivos para a proteção dos dados pessoais e de seus titulares.

Em suma o modelo que o Brasil apresenta revela-se genérico, quando não omisso em algumas partes, insatisfatório e com várias lacunas a serem preenchidas, e partes outras melhor trabalhadas, todas devendo observar e alicerçar-se da constituição em especial o artigo 5º da Carta Magna.

O presente trabalho não se esgota neste tempo, visto que será aprofundado na pós graduação em curso e no mestrado em vista, que certamente renderão bons frutos no desenvolvimento de matéria específica ao tema aqui abordado.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas** A Função e os Limites do Consentimento. São Paulo: Editora Forense, 2018.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988.

BRASIL. **Lei de Introdução às normas do Direito Brasileiro** (LINDB). Disponível em: <(http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm)> Acessado em: 10 out. 2019.

BRASIL. **Lei de Proteção Geral de Dados Pessoais**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 19 fev. 2020.

BRASIL. **Marco civil da internet.** Lei 12.965, de 23 abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 19 fev. 2019.

BRASIL. **Código de Processo Civil** de 2015 (Lei nº 13.105/2015).

BRASIL. **Lei de Acesso à Informação** (Lei nº 12.527/2011).

BRASIL. **Lei dos Crimes Informáticos**: (Lei nº 12.737/2012).

BRASIL. **Plano Nacional de Internet das Coisas** Decreto nº 9.854 de 2019

BRASIL. **Lei Brasileira de Inclusão da Pessoa com Deficiência** (Estatuto da Pessoa com Deficiência).Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm>Acesso em: 19 jan. 2020.

BRASÍLIA, Câmara dos Deputados **Definição de Dados Pessoais, Sensíveis e Anonimizado** Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-e-eventos/paulo-rena-representante-do-instituto-beta-para-a-internet-e-democracia-ibidem> Acessado em: 16 mar. 2020.

CGI.BR **O Livro do IETF** Disponível em: <https://cgi.br/publicacao/o-livro-do-ietf/> Acessado em 20 mai. 2020.

CGI.BR **Diretrizes, recomendações e especificações técnicas para a aplicação da lei sobre Internet no Brasil** Disponível em <https://cgi.br/publicacao/diretrizes-recomendacoes-e-especificacoes-tecnicas-para-a-aplicacao-da-lei-sobre-internet-no-Brasil/ > Acessado em: 25. mai. 2020.

SITES

Convention on Cybercrime ETS Nº.185 Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> Acessado em:17 mai.2020.

Dasgupta, Sanjoy; Papadimitriou, Christos; Vazirani, Umesh. **Algoritmos.** Porto Alegre: AMGH, 2010.

DENNY, Danielle M. T. **Internet Legal.**São Paulo, Editora Imagens DD , 2018. ISBNCDU17:340

Dicionário Jurídico Acqua Viva 7ª Ed. editora Rideel 2015.

Estudo "**Internet das Coisas**: um plano de ação para o Brasil" Disponível em: <https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil> Acessado em: 15 mai. 2020.

GUERRA, Sidney. **O Direito à Privacidade na Internet.** 1ª edição, editora América Jurídica, 2004.

LÉVY, Pierre.**Cibercultura** Ed. 34, São Paulo: 1999.

MARTINS, Helena. **Entenda o Marco Civil da Internet.** 2014. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2014-04/entenda-o-marco-civil-da-internet. Acesso em: 22 mar. 2020.

O acelerador da era moderna Disponível em: <http://news.bbc.co.uk/2/hi/technology/7541123.stm> Acessado em: 05 mar. 2020.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**. 4ª edição, editora Juruá, 2006.

PAESANI, Liliana Minardi. **Direito e Internet**: Liberdade de Informação, Privacidade e Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2014

PAIVA, Mário Antônio Lobato de. **Primeiras linhas em direito eletrônico***.* Elaborado em 11/2002. Disponível em: <http://jus.com.br/artigos/3575>. Acesso em: 09 de mar. 2020.

PEREIRA, Leonardo. **5 Pontos essenciais para entender o Marco Civil da Internet.** 2014. Disponível em: <https://olhardigital.com.br/noticia/5-pontos-essenciais-para-entender-o-marco-civil-da-internet/41053> Acesso em: 08. mar. 2020.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**. 4ª edição, editora Juruá, 2006.

PINHEIRO, Patricia Peck. **Direito Digital**. 5. Ed. São Paulo. Saraiva, 2012.

SANTOS. Edméa Oliveira. **Ambientes Virtuais de Aprendizagem**: por autorias livre, plurais e gratuitas. In: Revista FAEBA, v.12, no. 18.2003. Disponível em: <http://www.comunidadesvirtuais.pro.br/hipertexto/home/ava.pdf.> Acesso em 10 abr. 2020

SILVA, José Afonso da. Curso de direito constitucional positivo, 41ª edição, São Paulo: Malheiros, 2018.

VANCIM, Adriano Roberto.NEVES, Fernando Frachone. **Marco Civil da Internet.** 2ª edição digital, editora Mundo Jurídico.

GLOSSÁRIO

ANDROID Um sistema operacional de dispositivo móvel criado pelo Google, maior parte do qual é liberado sob as licenças de software livre Apache 2.0 e GPLv2.

APLICATIVOS MÓVEIS (App's)

BITCOIN Criptomoedas ou dinheiro eletrônico para transações (em inglês: peer-to- peer electronic cash system).

CRACKER(s) Termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança.

HACKER(s) Indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas.

REDE De computadores ou Rede de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores ou nós da rede) interligados por um sistema de comunicação digital (ou link de dados), guiados por um conjunto de regras (protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos

IoT Internet das coisas (em inglês: Internet of Things).