



UNIPAC

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

3º PERÍODO 2021/01

DISCENTES:

ANA LAURA DE OLIVEIRA FERREIRA

BERNARDO RESENDE ANDRÉS

CLAUDIMAR JOSÉ DA CRUZ

PEDRO HENRIQUE PAES NASCIMENTO

RAFAEL DE SOUZA DAMASCENO

PROTEÇÃO DE DADOS PELO MUNDO

Atividade da 1º etapa para a
aprovação da disciplina de Legislação
e Ética em Computação, ministrada
pelo Prof. José Da Silva Filho.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Barbacena – 2021

Resumo

Este trabalho é baseado em mostrar os conceitos de proteção de dados pessoais em alguns dos países que chamam a atenção com o seu uso da internet, além de mostrar as leis que determinam os direitos, segurança e proteção para o bem da população e do país. Uma vez que é apresentado o que são essas leis, como elas contribuem para a sociedade e como elas influenciam na proteção de dados e todos os seus desdobramentos. Explicaremos o como é importante para a formação da sociedade a contribuição de todos em seguir todas as leis propostas. Será abordado também algumas curiosidades, como por exemplo quem possui acesso a internet, os dados utilizados pelo usuário, protocolos de segurança e como cada um funciona.

Abstract

This work is based on showing the concepts of protection of personal data in some of the countries that call attention with their use of the internet, in addition to showing the laws that determine the rights, security and protection for the good of the population and the country. Once it is presented what these laws are, how they contribute to society and how they influence data protection and all its consequences. We will explain how important it is for the formation of society that everyone contributes to following all the proposed laws. Some curiosities will also be addressed, such as who has access to the internet, the data used by the user, security protocols and how each works.

Sumário

1 Introdução.....	5
2 Coreia do Sul	6
2.1 Quem possui acesso à internet?	6
2.2 Código de Proteção de Informações Pessoais (PIPA)	6
2.3 Quem possui acesso aos dados utilizados pelo usuário?	6
2.4 Penalidades Legais	6
2.5 Dados Pessoais e a Pandemia	7
3 Coreia do Norte	8
3.1 Quem possui acesso a internet?	8
3.2 Possui Código de Proteção de Dados?	8
3.3 Rede Doméstica.....	8
3.4 Hackers.....	8
3.5 Ataque à Sony Pictures - Vazamento de Dados	8
4 Estados Unidos	10
4.1 Internet, Acesso e Proteção de dados nos EUA	10
4.2 Quem não possui acesso à internet?	10
4.3 A conexão dos usuários é controlada?	11
4.4 Quem possui acesso aos dados utilizados pelo usuário?	11
4.5 Leis de proteção de dados nos Estados Unidos	11
4.6 Caso Edward Snowden.....	12
5 China	13
5.1 Há previsão que garanta a neutralidade de rede?	13
5.2 MIIT	13
5.3 Lei de Proteção do Consumidor.....	13
5.4 Três leis que regulam o comportamento “online”	14
5.5 Controle da internet.....	14

5.6 Sites bloqueados.....	14
5.7 Conteúdo censurado.....	15
6 Reino Unido	16
6.1 Acesso à Internet	16
6.2 Banda larga.....	16
6.3 Projeto Starlink.....	16
6.4 Regras de Segurança online.....	17
6.5 Regras de acesso das crianças a internet	17
6.6 Regulamentação acerca do uso de internet e os dados da população...	17
6.7 Previsão da neutralidade da rede	17
6.8 Exceções ao princípio da neutralidade	18
6.9 Regulamento Geral da proteção de Dados	18
6.10 Proteção De Dados e devidas penalidades	18
6.11 Entrada e transferência de dados para o Reino Unido	18
7. Suíça.....	19
7.1 Quem possui acesso à Conexão na Internet	19
7.2 Como a Conexão dos usuários é controlada, se é controlada de alguma forma.....	19
7.3 Quem possui aceso aos dados utilizados pelos usuários	20
7.4 Protocolos de Segurança.....	20
7.5 Penalidades Legais.....	21
7.6 Sobre a Suíça Digital, o que se pode falar?	21
8 Conclusão	22
9 Bibliografia.....	23

1 Introdução

A proteção de dados quando entrada em vigor nos países, basicamente estabelece uma série de regras que as empresas e quaisquer organização atuante terão que seguir para assim permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais. É possível concluir que as leis de proteção de dados é uma legislação que irá determinar como os dados dos cidadãos podem ser coletados e tratados, e que se houver conflitos entre as normas, poderá ocorrer punições.

O Brasil junto com países como por exemplo Paraguai, China e Rússia, adotam a Lei Geral de Proteção de dados (lei nº 13.709, de 14 de agosto de 2018 – LGPD) visando suprimir os problemas ao armazenamento, coleta e transmissão dos dados pessoais dos indivíduos. Ela por sua vez, foi inspirado pela regulamentação vigente na Europa (General Data Protection Regulation – GDPR), que a mesma possui um objetivo de buscar a proteção e privacidade dos dados de todos os indivíduos da União Europeia.

Levando como exemplo essas duas leis, é possível determinar que estas são projetos altamente necessários e relevantes. Nem todos os países possuem uma demanda que atuam severamente nessas leis, deixando a mesma com questões vagas. Apesar do grande salto no cenário tecnológico que atualmente o mundo está passando, alguns países ainda precisam olhar mais a fundo as normas e leis e observar que as mesmas precisam andar juntas com todo esse avanço, uma vez que para toda a sociedade, não é certo deixar todos os seus direitos abandonados.

Sendo assim, a maneira de como vai ser abordada sobre os dados pessoais no mundo, vai ser fundamental para dizer como e até onde o cidadão comum poderá se expor sem se preocupar com qualquer problema. Tudo indica que o cenário e a maturidade em se ligar com essa segurança está crescendo e sendo tratado de forma prioritária, porém números de vítimas de ataques cibernéticos crescem a cada dia, porém é possível notar uma postura de aprendizado sobre países exemplos sobre esse assunto, frisando uma garantia de uma legislação pronta para o melhor da sociedade.

2 Coreia do Sul

2.1 Quem possui acesso à internet?

Segundo o Banco Mundial, 96,2% da população sul-coreana possui acesso à Internet, dados de 2019.

2.2 Código de Proteção de Informações Pessoais (PIPA)

No ano de 2011, a Coreia do Sul, por meio da Comissão de Comunicações da Coreia (KCC) aprovou seu Código de Proteção de Informações Pessoais (Personal Information Protection Act - PIPA), considerado um dos mais rígidos do mundo, ele passa a vigorar junto com outros códigos já vigentes desde a década de 90 e 00, como o Código de Promoção da Utilização de Redes de Comunicação e de Informação e da Proteção da Informação.

O PIPA tem por objetivo estabelecer regras para o processamento de informações pessoais, como coleta, armazenamento, utilização, recuperação, divulgação e destruição. Onde todos os interesses e direitos do cidadão serão respeitados.

A aplicabilidade da lei se destina a pessoas, instituições, organizações, sejam jurídicas ou públicas, que manipulem, trabalhem com informações pessoais.

2.3 Quem possui acesso aos dados utilizados pelo usuário?

No PIPA não se tem uma legislação específica de quem é a responsabilidade de coleta e guarda de registros de acesso dos usuários, mas a KCC determinou que a responsabilidade são dos Provedores de Serviços de Telecomunicações, que por sua vez tem a obrigatoriedade de adotar códigos de conduta para padronizar o manuseio de dados pessoais pelo setor.

2.4 Penalidades Legais

Dentro do PIPA encontramos o Comitê de Disputas sobre Informações, este comitê tem por objetivo receber denúncias de usuários relativas a qualquer

uso indevido dos seus dados pessoais pelos chamados “Processadores de Informações Pessoais”. Ele é composto por até vinte integrantes (Especialistas da Área, Advogados, Professores) e pode estabelecer penalizações aos denunciados. Poderão também sofrer processos administrativos pela KCC, e até criminais por órgão competente.

2.5 Dados Pessoais e a Pandemia

No contexto da pandemia o PIPA tem restrições quanto à atuação, ficando a responsabilidade de medidas e de utilização de dados pessoais por conta da Lei de Controle e Prevenção de Doenças Infecciosas (Infections Disease Control and Prevention Act - IDCPA).

Através da IDCPA, Ministério da Saúde e Centro de Controle e Prevenção de Doenças poderão pedir informações pessoais, com o objetivo de rastrear pessoas doentes e também propensas a serem infectadas. Polícia, Empresas de Telecomunicações, Governos Locais, Instituições Médicas, Farmácias, são alguns exemplos de onde se pode buscar essas informações.

Esse rastreamento possibilita ao governo meios precisos para enviar recursos às pessoas infectadas e aos órgãos específicos.

Diante do questionamento com relação à privacidade e o caso da Comissão Nacional de Direitos Humanos da Coreia do Sul (NHRC) ter condenado a divulgação de um histórico de um paciente com Covid 19, o Centro de Controle e Prevenção de Doenças (*Korea Centers for Disease Control and Prevention* – KCDC) publicou novas orientações para captação e divulgação de dados de pacientes, entre eles: Os contatos a serem rastreados devem ser determinados com base nos sintomas e condições de exposição do paciente; Informações de identificação pessoal, incluindo endereços comerciais, não poderão ser mais divulgados.

3 Coreia do Norte

3.1 Quem possui acesso a internet?

Na Coreia do Norte apenas 1% da população tem acesso a Internet, Líderes Políticos e suas famílias em sua maioria. Segundo dados de 2019.

3.2 Possui Código de Proteção de Dados?

Não há uma legislação referente a dados pessoais. O Governo norte-coreano tem grande controle sobre a população.

3.3 Rede Doméstica

A Coreia do Norte possui uma rede doméstica (Intranet), mantida pelo governo, chamada Kwangmyong, de acesso discado e gratuito. Destinada à população, ela possui na maioria dos seus conteúdos páginas com informações sobre política, economia e conhecimentos científicos. Ela não dá acesso à Rede Mundial, o usuário fica limitado a apenas as informações passadas pelo governo.

3.4 Hackers

De acordo com o Serviço de Inteligência da Coreia do Sul e a ONU, a Coreia do Norte possui milhares de hackers altamente treinados que têm por objetivo atacar empresas, instituições, e pesquisadores na Coreia do Sul e em outros países, em busca de informações sigilosas ou mesmo dinheiro para financiar seu programa nuclear.

3.5 Ataque à Sony Pictures - Vazamento de Dados

No dia 24 de Novembro de 2015, a Sony Pictures sofreu um ataque cibernético, onde foram divulgados dados pessoais de artistas e funcionários como, endereços, telefones, número de seguro social. Funcionários e familiares sofreram ameaças, houve divulgação de títulos de jogos e filmes que ainda seriam lançados.

O ataque foi atribuído à Coreia do Norte, o motivo seria o lançamento do filme A Entrevista, uma sátira ao Líder Kim Jong-un.

Após a Sony Pictures adiar o lançamento, ela confirmou o relançamento para 25 de dezembro, entretanto acabou disponibilizando o filme com algumas mudanças por streaming na véspera do natal.

4 Estados Unidos

4.1 Internet, Acesso e Proteção de dados nos EUA

O país mais rico do mundo conta com uma população de cerca de 328 milhões de pessoas e 286 milhões de usuários conectados a redes de internet. Isso representa 87% da população do país, mas quem são as pessoas que não têm acesso a internet? Entre as que usam, a conexão dos usuários é controlada? Quem possui acesso aos dados dos usuários? E quais são as leis de proteção de dados que resguardam os usuários e consumidores que trafegam nas redes? Entenda um caso recente famoso no mundo sobre espionagem de dados: O caso Edward Snowden. Esses são os tópicos abordados acerca da proteção de dados nos Estados Unidos.

4.2 Quem não possui acesso à internet?

Os Estados Unidos possuem cerca de 328,2 milhões de habitantes e 286,9 milhões de usuários correspondendo a cerca de 87% de sua população total. E apesar da percentagem de usuários ser alta, ainda são em torno de 41,3 milhões de pessoas sem acesso a internet. Os Estados Unidos são o 3º país mais conectado do mundo, estando atrás somente da China e Índia. Sendo assim, o mais correto seria esclarecer quem não possui acesso à internet nessa grande potência: Nos EUA, existe um grande grupo religioso cristão anabatista de pessoas denominado Amish, tal grupo é conhecido por seus costumes ultraconservadores, como o uso restrito de equipamentos eletrônicos, automóveis e a internet. Só em 2019, o grupo contava com aproximadamente 270 mil pessoas. Parte da população carente também não possui acesso, em 2016, cerca de 13% da população estadunidense vivia na pobreza. Há também as pessoas mais idosas, que apesar de poderem usar, optam por não saberem ou se considerarem ultrapassadas. No entanto, em termos de números, os Estados Unidos contam com um gigante número de usuários tendendo somente a crescer.

4.3 A conexão dos usuários é controlada?

Quem controla a Internet dos Estados Unidos? Os Estados Unidos. E apesar de parecer engraçado, o governo americano não possui controle só sobre a internet do próprio país como também do mundo. Isso se dá, pois, a ICANN (Internet Corporation for Assigned Names and Numbers), é uma entidade sem fins lucrativos, subordinada ao Governo dos Estados Unidos. Ela é responsável pelo gerenciamento e coordenação do DNS (Sistema de Nomes de Domínio), com a intenção de garantir que cada domínio seja único. Ainda que a ICANN leve o título de controlar a internet, a instituição é limitada. A mesma não controla o conteúdo disponível na Internet, como não pode impedir as atividades de spam e não se responsabiliza pelo acesso à Internet. Nesse caso a conexão dos usuários não é controlada, todavia o país conta com leis de proteção de dados, que guia os usuários no acesso a rede, sujeitos a penalidades caso descumpram alguma lei.

4.4 Quem possui acesso aos dados utilizados pelo usuário?

Além das empresas nas quais o usuário insere seus dados o governo americano também pode obter ter acesso aos dados dos usuários. E não só dos usuários do próprio país, recentemente, foi aprovada uma lei americana chamada Cloud Atc (sigla para sigla para Clarifying Lawful Overseas Use of Data Act), a mesma prevê que a legislação permite abrir o sigilo de servidores de empresas que estejam hospedadas no país e fora dele. Sua intenção é facilitar a obtenção de provas em forma de dados digitais para auxiliar em processos da justiça americana.

4.5 Leis de proteção de dados nos Estados Unidos

Nos estados Unidos não existe uma lei federal de proteção de dados, embora os estados tenham leis voltadas para o tema. A legislação mais conhecida e mais volumosa é a do estado da Califórnia, a California Consumer Privacy Act (CCPA), seu objetivo são novos direitos para os consumidores, que passam a ter mais controle sobre as próprias informações. Em Nevada, Massachusetts e Minnesota também existem leis com a mesma finalidade. Em

Nova Iorque, existe a New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD), que com o mesmo objetivo da CCPA visa mais transparência e cuidados com os dados. No entanto há um grande movimento que procura aprovar uma lei de proteção de dados federal nos EUA, tal como existe a LGPD no Brasil.

4.6 Caso Edward Snowden

Edward Joseph Snowden é um analista de sistemas e hacker ético, atualmente com 37 anos, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicas diversas informações sobre o sistema de vigilância global da NSA americana. Utilizando servidores de empresas como Google, Apple e Facebook, os Estados Unidos espionavam conversas da população americana e até de presidentes de outros países, entre eles a Ex-Presidente Dilma Rousseff. Após vazar os dados Snowden deixou os USA e pediu asilo a mais de 20 países. Sendo aceito pela Rússia, onde reside atualmente. Acusado nos Estados Unidos por espionagem, roubo e conversão de propriedade do governo. Questionado sobre o motivo do vazamento dos dados Edward disse que “sentiu a obrigação de denunciar ao mundo, mesmo a um custo pessoal alto, os descomunais poderes de vigilância acumulados pelo governo dos EUA. O público precisa decidir se esses programas e políticas são certos ou errados”.

5 China

5.1 Há previsão que garanta a neutralidade de rede?

Na China, não há lei que garanta a neutralidade de rede. O “Regulamento de Proteção de Dados Pessoais de Usuários de Telecomunicações e de Internet” trata o tratamento de dados pessoais, guarda, armazenamento, disciplina coleta. Em vigor desde 1º de Setembro 2013, determina que os operadores de serviços de telecomunicação e os provedores de serviços de informação da internet estabeleçam regras de coleta e uso dos dados pessoais, dando publicidade àquelas atividades em lugares em que os serviços sejam oferecidos ou no “site” (artigo 8º), e requisitando expressa autorização dos usuários para a coleta de dados (artigo 9º). Os operadores ou provedores de serviços de internet devem tomar medidas instantâneas de reparação, caso os dados mantidos por eles sejam danificados, perdidos ou vazados (artigo 14º).

5.2 MIIT

O MIIT (Ministério da Indústria e da Tecnologia da Informação), juntamente com a administração pública local (região autónoma, província ou município) é responsável por supervisionar e inspecionar os operadores e provedores de serviços de Internet (artigo 17º). Em suas inspeções anuais, estes órgãos poderão supervisionar as atividades dos provedores e operadores de serviço ligadas à proteção de dados pessoais de usuários.

5.3 Lei de Proteção do Consumidor

A Lei de Proteção do Consumidor, revisada em 2013 e em vigor desde 15 de Março 2014, prevê que os consumidores têm o direito à proteção de seus dados pessoais no uso de serviços ou produtos “on line” (artigo 14); e que os operadores devem obedecer aos princípios de “Necessidade, legitimidade e justiça”, no uso e coleta de dados pessoais dos consumidores, esclarecendo a maneira, o objetivo e o âmbito de coleta dos referidos dados (artigo 29º).

5.4 Três leis que regulam o comportamento “online”

- A) "Medidas para a Administração do Serviço de Informação via Internet" (2000).
- B) "Decisão de Salvaguarda da Segurança “Online” pelo Comitê Permanente do Congresso Nacional do Povo" (2000).
- C) “Provisões de Administração de Notícias e Serviços de Informações da Internet” (2005).

Apesar de não haver lei que regule o dever de guarda de registros de acesso à Internet, há legislações em que se determina, por exemplo, que os provedores de serviços de divulgação de informação ou de notícias devam manter registro do conteúdo, da conta de Internet, da hora e da identidade do usuário.

5.5 Controle da internet

O Estado chinês controla todo o conteúdo online em circulação no país, barrando o que for considerado impróprio. Outra medida que ocorre com algumas páginas é o direcionamento automático para sites equivalentes. Além disso, todos os provedores de internet precisam passar por aprovação do governo, sendo que tudo que é acessado pelos usuários deve ser canalizado para portas de entradas, as chamadas gateways, onde ocorre uma fiscalização do teor do tráfego. Devido a esses tipos de medidas, criou-se a denominação Great FireWall of China, em referência à Grande Muralha conhecida também como “Escudo Dourado”. Assim como a expressão sugere, firewall é uma barreira de proteção que pode bloquear o acesso a conteúdos considerados indesejados. Monitoram o que as pessoas fazem quando online e aplicam punições que vão de multa a prisões.

5.6 Sites bloqueados

Dentre os mais de 18 mil sites bloqueados, 10 deles estão no top 100 de acessos mundial, sendo eles: Gmail, Google, Google Maps, Facebook, Youtube, Twitter, Instagram, SoundCloud, Dropbox e Tumblr.

5.7 Conteúdo censurado

- 1- Sites pertencentes aos grupos "foras da lei" ou suprimidos, tais como o de ativistas pró-democracia e os de Falun Gong.
- 2- Fontes de notícias que frequentemente cobrem tópicos considerados difamatórios contra a China. Exemplos: violência policial, liberdade de expressão, democracia e sites marxistas.
- 3- Sites que contêm qualquer coisa que as autoridades chinesas considerem como obscenidade ou pornográfica.
- 4- Sites relacionados à atividade criminosa.
- 5- Sites ligados ao Dalai Lama, aos seus ensinamentos ou com o Movimento Internacional de independência do Tibet.
- 6- A maioria dos sites de blog sofrem interrupções frequentes ou permanentes como os citados acima.
- 7- Sites considerados subversivos.

6 Reino Unido

6.1 Acesso à Internet

O Reino Unido possui atualmente um grande envolvimento com a internet desde a sua origem, acompanhando sempre todo o desenvolvimento e conseguindo acompanhar toda a evolução da tecnologia, onde que conseguiram um incrível crescimento de mais de 80% do uso da internet em apenas 20 anos. Hoje, o país oferece acesso a internet para as demais empresas e para o público doméstico, seja fibra, cabo, wireless e dados móveis. Além disso, o Reino Unido está bastante focado em pesquisas sobre protocolos de redes de computadores e protocolos de comunicação em escala internacional.

6.2 Banda larga

O acesso à internet de banda larga inicialmente foi fornecido por uma série de televisão a cabo regional e por companhias telefônicas. Com o passar do desenvolvimento a banda larga sem fio ficara sendo cada vez mais utilizada. A velocidade média de conexão atual usando a banda larga a cabo usados por fibra óptica, chega para todos os seus clientes com aproximadamente 1Gb/s (2007 essa mesma velocidade estava na média de 4,5 Mbit/s).

6.3 Projeto Starlink

Pensando sobre o futuro e a grande alta do desenvolvimento tecnológico, o Reino Unido aprovou o serviço de internet dos satélites Starlink, da SpaceX. Tal rede, irá competir diretamente com os provedores de internet já utilizados no país. No momento o Reino Unido aprovou que alguns usuários a comecem a fazer testes de garantia de desempenho da internet. A alta velocidade está sendo bastante satisfatória para a população no geral, chegando em média 50 a 150 Mbps.

6.4 Regras de Segurança online

Assim como cada vez mais cresce o consumo de internet de toda a população, perigos da mesma vem se destacando cada vez mais. O governo Britânico, está sempre propondo novas regras de segurança online para combater quaisquer ataques nocivos a principalmente ao público comum, seja nas redes sociais, sites e aplicativos. O alvo da legislação propõem conceitos de atividades ilegais e inaceitáveis. Para isso, o Reino Unido pretende criar um regulador independente para garantir o comprimento desses mecanismos de defesa.

6.5 Regras de acesso das crianças a internet

No que diz a respeito sobre o acesso de conteúdo na internet das crianças, ficara apenas o uso das redes de computadores educacionais e são assim mantidas pelas organizações como a JANET. Porém, para os pais e responsáveis pela criança, manter o controle do uso da rede é algo extremamente difícil, uma vez são muitos dispositivos conectados e isso pode causar muitas complicações para ambos os lados.

6.6 Regulamentação acerca do uso de internet e os dados da população

O Reino Unido não possui legislação específica sobre o uso da internet. O governo vem optando por fazer alguns tratamentos para tratar este tema de forma satisfatória e segura para todos, uma vez que existe uma complexidade do mesmo, pelo fato dos grandes avanços tecnológicos que são mostrados diariamente.

6.7 Previsão da neutralidade da rede

Uma vez que não existe uma regulamentação sobre o uso de internet, por obsequio não existe nenhuma neutralidade de rede. No momento, este tema é tratado de forma equivocada, por meio da gestão de tráfego de rede.

6.8 Exceções ao princípio da neutralidade

O código de transparência do Reino Unido destaca que a neutralidade de rede poderia ser utilizada para fins de administração operações em geral da rede e assegurar tópicos e cumprimentos das regras dos consumidores.

6.9 Regulamento Geral da proteção de Dados

O RGPD foi aprovado pelo Reino Unido com intuito de proteger os direitos on-line de todos os indivíduos em relação aos seus dados pessoais. Tais medidas e leis se aplicam a qualquer pessoa que coleta informações sobre o indivíduo, seja para fins acadêmicos, lazer, trabalho.

6.10 Proteção De Dados e devidas penalidades

Mesmo com a saída do Reino Unido saindo da União Europeia, o parlamento Europeu aprovou oficialmente que as leis da RGPD Seguiria em vigor. Tal legislação irá dar poder ao governo para assim conseguir atribuir as penalizações financeiras necessárias entre as empresas que não contribuírem com os seus requisitos. As empresas ou companhias devem pagar até 4% da sua receita global. Inicialmente eram poucas que se asseguravam em estar cumprindo as leis das regulamentações de dados.

6.11 Entrada e transferência de dados para o Reino Unido

Qualquer transferência de dados para o Reino Unido, a organização responsável deverá acompanhar de perto, como um plano de recurso uma vez que o país está vindo de um período transitório, e isso pode se considerar que o país não oferece um nível tão adequado de segurança para a transferência de dados de forma legítima. Mesmo com a país esteja trabalhado forte para conseguir êxito nesse processo, essa medida de acompanhar a trajetória dos dados é bastante útil, deixando a qualquer modo de ser contestada devido a algum problema.

7. Suíça

7.1 Quem possui acesso à Conexão na Internet

Tendo em vista que o país é um dos melhores classificados economicamente na Europa, com apenas 6.6% da população estando abaixo da linha da pobreza, difícil imaginar em quais situações faltaria o contato digital dentre sua população. Todavia, sendo uma nação onde mais de 32.45% da população possui idade superior a 55 anos, é plausível afirmar que quase um terço de seus moradores não utiliza veementemente a Internet, quando comparado aos mais jovens. Sendo um paraíso fiscal conhecido no mundo inteiro, a internet de lá não foge esta mesma regra.

7.2 Como a Conexão dos usuários é controlada, se é controlada de alguma forma

De acordo com a definição de Paraíso Fiscal, Paraíso fiscal consiste numa determinada região (país ou território) com condições fiscais atrativas para investidores estrangeiros, principalmente por ter baixos impostos e total sigilo bancário. Legalmente, os paraísos fiscais são considerados offshores com regimes tributários especiais, onde a legislação local admite que capitais de outros países possam ser gerenciados de modo mais “fácil”, sem a necessidade de identificar os envolvidos com as contas bancárias. Um país onde a sua principal ideologia oferece essa “abertura” para movimentações financeiras sem revisões do Estado, a internet segue a mesma ideologia, onde a mesma é amplamente utilizada em todo o planeta para se vender e comprar informações, eventos que considerados em outros lugares como criminosos, são de certa forma brandificados na Suíça, com sua política de não-deportação, diversos fugitivos digitais de outros países se mudam para a Suíça com o intuito de se proteger das penalidades de sua nação natal. O site mundialmente conhecido, WikiLeaks, por como seu próprio nome sugere, “vazar” informações é sediado na Suíça, o site, especializado em revelações de segredos oficiais, começou a distribuir no domingo centenas de telegramas confidenciais do departamento de Estado americano. Para garantir sua distribuição, o WikiLeaks garantiu abrigo em pelo menos dois servidores, o sueco Bahnhof e o americano Amazon e o seu principal servidor se encontra na Suíça em local não informado. Fica fácil de se

imaginar quanto um país controla o acesso à informação quando o mesmo mantém em seu solo um dos principais sites que ferem informações sensíveis governamentais em todo a Terra.

7.3 Quem possui aceso aos dados utilizados pelos usuários

Diferentemente da LGPD brasileira, a Suíça conta com uma equivalente a este conjunto de leis sendo conhecido por Escudo de Proteção da Privacidade, onde a mesma foi projetada pelo Departamento de Comércio dos EUA e pela Comissão Europeia e Administração da Suíça, respectivamente, para oferecer às empresas dos dois lados do Atlântico um mecanismo para atender aos requisitos de proteção de dados ao transferir dados pessoais da União Europeia e da Suíça para os Estados Unidos. Onde a transferência de dados pessoais é proibida para países fora do EEE (Espaço Econômico Europeu), a menos que sejam confirmados níveis elevadíssimos de proteção. Os 23 Princípios do Escudo de Proteção da Privacidade definem um conjunto de requisitos que governam o uso e o manuseio de dados pessoais transferidos da UE, bem como mecanismos de resolução de conflitos e acesso que as empresas envolvidas devem oferecer aos cidadãos da UE. As empresas devem informar às pessoas como seus dados são processados, limitar as finalidades para as quais eles são usados, proteger os dados pelo tempo em que forem mantidos e garantir a responsabilidade pelos dados transferidos para terceiros. Os requisitos também incluem o fornecimento gratuito de uma resolução de conflitos acessível e transparência com relação a solicitações governamentais de dados pessoais.

7.4 Protocolos de Segurança

As maiores vantagens da Suíça estão pontuadas em neutralidade, segurança jurídica e estabilidade também se aplicam na segurança digital. Nível gigantesco de proteção e baixa densidade de regulamentações. Seguindo à risca sua tradição de segurança de informação, diversos bancos de dados de companhias gigantescas se encontram em solo suíço, onde os mesmos acabam gerando Centros de informações mundiais, onde possuem diversas regulamentações que garantem a segurança dos dados ali mantidos.

7.5 Penalidades Legais

Tendo em vista que a própria Suíça lida com seus problemas internacionais, as leis voltadas para crimes digitais também são puramente aplicadas dentro da legislação desses países. Sabendo que a informação digital é feita para ter uma certa anonimidade, a Suíça acaba por criar um ambiente muito confortável para aqueles que querem utilizar de certa má fé nas respostas legais existentes no país facilita e muito as mentes mais más intencionadas.

7.6 Sobre a Suíça Digital, o que se pode falar?

Um paraíso fiscal acaba gerando em sua existência, várias brechas para a anonimidade da informação, dados sensíveis ficam fisicamente protegidos dentro de suas fronteiras e sem risco de sofrerem sanções Federais e multinacionais. Tendo em vista que aquilo que é feito dentro de um Estado é represado de acordo com as suas leis, as informações armazenadas no mesmo, seguem o mesmo rumo legal: neutralidade.

8 Conclusão

Concluimos por fim que, diante do processo de proteção de dados, onde que existe uma quantidade brusca de coleta e tratamentos de dados, uma lei para a proteção de dados pessoais é uma forma de garantir que todos que manipulem dados pessoais passam a tratar com seriedade todos os dados da população do país. A LGPD, por exemplo, é a lei que se aplica no Brasil, porém não é a única, existem várias regras em todo o mundo, mas todas com o mesmo objetivo de manter todos os dados pessoais na maior privacidade. Atualmente, com o grande avanço da tecnologia, é possível perceber que em um futuro próximo, essas leis irão passar por um processo de sofrer ainda mais pressões com o único intuito da segurança de informações para o bem da sociedade.

As empresas em geral, sejam elas grandes ou de pequeno porte, precisam entrar com os seguimentos das leis, uma vez que qualquer vazamento das informações podem acarretar em multas milionárias, e a base de uma empresa confiável irá estar no suporte e na infraestrutura para a segurança da informação. A relevância e o precedente estabelecido por este tema demonstram uma construção adequada e feita com toda a cautela para a implementação dos dados pessoais, uma vez que qualquer mudança gera efeitos práticos em curto espaço de tempo.

9 Bibliografia

Lista de países por número de usuários de Internet. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Lista_de_pa%C3%ADses_por_n%C3%BAmero_de_usu%C3%A1rios_de_Internet. Acesso em: 26 de abril de 2021.

SHAMBAUGH, Jay. Quem são os 41 milhões de pobres dos Estados Unidos, o país mais rico do mundo. BBC News Brasil. Disponível em: <https://www.bbc.com/portuguese/internacional-42323066>. Acesso em: 26 de abril de 2021.

Amish. Wikipédia. Disponível em: <https://pt.wikipedia.org/wiki/Amish>. Acesso em: 26 de abril de 2021.

Corporação da Internet para Atribuição de Nomes e Números. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Corpora%C3%A7%C3%A3o_da_Internet_para_Atribui%C3%A7%C3%A3o_de_Nomes_e_N%C3%BAmeros. Acesso em: 26 de abril de 2021.

Sobre a ICANN. ICANN. Disponível em: <https://icannlac.org/PO/sobre-ICANN#:~:text=A%20ICANN%20n%C3%A3o%20controla%20o,mais%20sobre%20a%20ICANN%20aqui>. Acesso em: 26 de abril de 2021.

SIMÕES GOMES, Helton. Futuro da internet sem o controle dos EUA passa pelas mãos de brasileiros. TECNOLOGIA E GAMES G1. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/06/futuro-da-internet-sem-o-controle-dos-eua-passa-pelas-maos-de-brasileiros.html>. Acesso em: 26 de abril de 2021.

PADRÃO, Márcio. Nova lei permite que EUA acessem dados de usuários que estejam fora do país. tilt Uol. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/04/25/nova-lei-americana-de-obtencao-de-dados-traz-perigos-a-soberania-de-paises.htm>. Acesso em: 26 de abril de 2021.

O que é o Cloud Act – e como a lei americana pode refletir no Brasil?. Jusbrasil. Disponível em: <https://jotainfo.jusbrasil.com.br/noticias/580261760/o-que-e-o-cloud-act-e-como-a-lei-americana-pode-refletir-no-brasil>. Acesso em: 26 de abril de 2021.

Veja como são as leis de proteção de dados nos Estados Unidos. ConectaJá. Disponível em: <https://conectaja.proteste.org.br/veja-como-sao-as-leis-de-protecao-de-dados-nos-estados-unidos/>. Acesso em: 26 de abril de 2021.

Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. MUNDO G1. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 26 de abril de 2021.

Proteção de Dados Pessoais pelo Mundo. Pensando o DIREITO. Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/27-hina.pdf>. Acesso em: 25 de abril de 2021.

MEYER, Maximiliano. Como funciona a censura e o acesso à internet da China. OFICINA DA NET. Disponível em: <https://www.oficinadanet.com.br/tecnologia/19933-como-funciona-o-acesso-a-censura-na-internet-da-china>. Acesso em: 25 de abril de 2021.

Saiba como funciona o controle da internet na China. Terra. Disponível em: <https://www.terra.com.br/noticias/tecnologia/saiba-como-funciona-o-controle-da-internet-na-china,57182d8e6545b310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 25 de abril de 2021.

Internet na China. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Internet_na_China#Jogo_on_line. Acesso em: 25 de abril de 2021.

Projeto Escudo Dourado. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Projeto_Escudo_Dourado. Acesso em 25 de abril de 2021.

KANG, Margareth. O uso dos dados pessoais na Coreia do Sul no combate ao coronavírus, o que podemos aprender?. CRYPTO ID. Disponível em: <https://cryptoid.com.br/banco-de-noticias/o-uso-dos-dados-pessoais-na-coreia-do-sul-no-combate-ao-coronavirus-o-que-podemos-aprender/>. Acesso em: 27 de abril de 2021.

Entenda cancelamento da estreia de 'A entrevista', após ataque hacker. CINEMA G1. Disponível em: <http://g1.globo.com/pop-arte/cinema/noticia/2014/12/entenda-cancelamento-da-estreia-de-entrevista-apos-ataque-hacker.html>. Acesso em: 27 de abril de 2021.

9 Fatos curiosos sobre a economia da Coreia do Norte. ÉPOCA NEGÓCIOS. Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2019/04/9-fatos-curiosos-sobre-economia-da-coreia-do-norte.html>. Acesso em: 27 de abril de 2021.

Proteção de Dados Pessoais pelo Mundo. Pensando o DIREITO. Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/14-C3%A9ia-do-Sul.pdf>. Acesso em: 27 de abril de 2021.

ONU diz que Coreia do Norte usa cyber ataques para pagar programa nuclear. DW Brasil. Disponível em: <https://www.dw.com/pt-br/onu-diz-que-coreia-do-norte-usa-ciberataques-para-pagar-programa-nuclear/a-56528132>. Acesso em: 27 de abril de 2021.

Internet na Coreia do Norte. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Internet_na_Coreia_do_Norte. Acesso em: 27 de abril de 2021.

Estrutura de Escudo de proteção da Privacidade UE-EUA e Suíça-EUA. Microsoft Build. Disponível em: <https://docs.microsoft.com/pt-br/compliance/regulatory/offering-eu-us-privacy-shield#:~:text=A%20transfer%C3%AAncia%20de%20dados%20pessoais,n%C3%ADveis%20%22adequados%22%20de%20prote%C3%A7%C3%A3o>. Acesso em: 26 de abril de 2021.

Como abrir conta offshore na Suíça: um guia definitivo. Remessa Online. Disponível em: <https://www.remessaonline.com.br/blog/como-abrir-conta-offshore-na-suica-um-guia-definitivo/>. Acesso em: 26 de abril de 2021.

CARMELLO CORRÊA DE MORAES, Reginaldo. Paraísos fiscais (2) – Bem mais do que uma Suíça. JORNAL DA UNICAMP. Disponível em: <https://www.unicamp.br/unicamp/ju/artigos/reginaldo-correa-de-moraes/paraisos-fiscais-2-bem-mais-do-que-uma-suica>. Acesso em: 26 de abril de 2021.

Contas na Suíça? Saiba mais sobre os paraísos fiscais. politize!. Disponível em: <https://www.politize.com.br/contas-na-suica-saiba-mais-sobre-paraisos-fiscais/>. Acesso em: 26 de abril de 2021.

Cláusulas Modelo da União Europeia. Microsoft Build. Disponível em: <https://docs.microsoft.com/pt-br/compliance/regulatory/offering-eu-model-clauses>. Acesso em: 26 de abril de 2021.

Espaço Económico Europeu (EEE), Suíça e região setentrional. Europarl. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/home>. Acesso em: 26 de abril de 2021.

ALECRIM, Emerson. O que você deve saber sobre a lei de proteção de dados pessoais do Brasil. tecnoblog. Disponível em: <https://tecnoblog.net/250718/lei-geral-protecao-dados-brasil/>. Acesso em: 25 de abril de 2021.

PINTÃO, Ricardo. Brexit & RGPD: sinais de um mundo interdependente. SAPO. Disponível em: <https://jornaleconomico.sapo.pt/noticias/brexit-rgpd-sinais-de-um-mundo-interdependente-687005>. Acesso em 25 de abril de 2021.

Categoria: Internet no Reino Unido. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Categoria:Internet_no_Reino_Unido. Acesso em 25 de abril de 2021.