UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE COMUNICAÇÕES

GRADUAÇÃO EM ENGENHARIA DE TELECOMUNICAÇÕES

Breve Análise Comparativa das Principais Normas Internacionais sobre Proteção de Dados Pessoais.

NATAL
2021

IGOR RAPHAEL GUIMARÃES SOARES

Breve Análise Comparativa das Principais Normas Internacionais sobre Proteção de Dados Pessoais.

Trabalho de Conclusão de Curso, apresentado ao Departamento de Engenharia de Comunicações da Universidade Federal do Rio Grande do Norte, como parte das exigências para a obtenção do título de Bacharel em Engenharia de Telecomunicações.

Natal, 30 de abril de 2021.

BANCA EXAMINADORA

_____
Prof. Dr. Cláudio Rodrigues Muniz da Silva (Orientador)
Professor Titular do Departamento de Engenharia de Comunicações (DCO)

_____
Prof. Dr. Laércio Martins de Mendonça
Professor Titular do Departamento de Engenharia de Comunicações (DCO)

_____
Prof. Dr. Gutembergue Soares da Silva
Professor do Departamento de Engenharia de Comunicações (DCO)

SUMÁRIO

Breve Análise Comparativa das Principais Normas Internacionais sobre Proteção de Dados Pessoais.

Igor Raphael Guimarães Soares*
Curso de Engenharia de Telecomunicações
Centro de Tecnologia
Universidade Federal Rio Grande do Norte

Cláudio R. M. da Silva**
Departamento de Engenharia de Comunicações (DCO)
Centro de Tecnologia
Universidade Federal Rio Grande do Norte

***Resumo* — Nos últimos anos entraram em vigor a Lei Geral de Proteção de Dados (LGPD), o Regulamento Geral de Proteção de Dados (GDPR) e a California Consumer Privacy Act (CCPA). Essas normas foram criadas com base em diversos princípios, pois objetivavam a proteção de dados em diferentes contextos de tratamento. Este artigo apresenta uma breve análise comparativa entre as principais normas de proteção de dados da atualidade, objetivando a utilização de critérios ainda não utilizados pelos trabalhos relacionados disponíveis, tais como os princípios e tratamento dos dados pessoais, fazendo uso da metodologia de levantamento da bibliografia dos principais comparativos disponíveis na literatura, chegando à conclusão de que, as três legislações serviram para ampliar o debate da proteção de dados pessoais em seus respectivos territórios, houve um avanço significativo sobre o tema da proteção de dados pessoais, com leis robustas e fundamentadas, porém com diferenças que são coerentes com a realidade de cada território abrangido sobre o tema.**

***Palavras-chave* — LGPD, CCPA, GDPR, Dados Pessoais, Bases legais.**

Abstract — In the recent years, came into force the the General Data Protection Act (LGPD), the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These legislations are based on several principles, often different from each other, as they aimed at protecting data in different treatment contexts. This article presents a brief comparative analysis between the main data protection norms of today, aiming at the use of criteria not yet used by the available related works, such as the principles and treatment of personal data, using the methodology of surveying the bibliography of main comparisons available in the literature, reaching the conclusion that, as three legislations served to broaden the debate on the protection of personal data in their respective territories, there was a significant advance on the subject of the protection of personal data, with robust and fundamental laws, however with differences that are consistent with the reality of each territory covered on the topic.

***Keywords* — LGPD, CCPA, GDPR, Personal Data, Legal basis.**

1. INTRODUÇÃO

Em 2018, foi lançado o Regulamento 679/2016, o GDPR (General Data Protection Regulation) ou RGPD (Regulamento Geral de Proteção de Dados) que fora aprovado pelo congresso europeu em abril de 2016, porém, executável apenas a partir de 25 de maio de 2018, havendo assim, tempo para que as empresas pudessem se adaptar às novas regulamentações. Pelo fato de se tratar de um regulamento, tem de ser aplicado a todos os países membros da União Europeia. Desta forma, o regulamento vincula toda e qualquer empresa que ofereça bens e serviços que coletam dados pessoais relacionados à residentes da União Europeia. Também em 2018, no Brasil, houve a sanção pelo então Presidente Michel Temer, da Lei Geral de Proteção de Dados, a 13.709/2018, também conhecida como LGPD. A referida lei foi sancionada em 2018, porém, só entrou em vigor em 18/09/2020, pois assim como o GDPR, também houve um período de adaptação para as empresas.

A proteção de dados nos Estados Unidos é regulada por leis dos níveis estadual e federal. Não há uma única legislação de proteção de dados, mas sim, leis fragmentadas que formam o regulamento. Em 2018 surgiu a primeira Lei Norte Americana inspirada no GDPR, a California Consumer Privacy Act (CCPA). Embora tenha inspiração vinda do GDPR Europeu, a CCPA é mais branda e mais específica. Conta com menos regulações e menor alcance. Por exemplo, aplica-se apenas a empresas com sede na Califórnia, ou que trate de indivíduos com residência no Estado. Também é necessário que a empresa tenha uma renda bruta igual ou maior de 25 milhões de dólares, trate de dados de mais de 50 mil cidadãos californianos ou 50% de sua receita anual venha de comercialização de dados pessoais.

O objetivo deste artigo é fazer uma discussão, utilizando os critérios de semelhanças e diferenças entre seus princípios, seus conceitos de dados pessoais, as formas de tratamento e coleta de dados, sanções e alguns aspectos específicos como dados de menores; com o intuito de analisar quais os impactos que essas leis podem trazer, tanto para os usuários, quanto para as empresas e para o nosso cenário moderno.

A importância deste comparativo é de mostrar uma abrangência ampliada aos trabalhos relacionados em que são comparadas, na maior parte, apenas duas legislações.

Nos procedimentos metodológicos aplicados serão explorados os contextos históricos em que a discussão sobre proteção de dados pessoais surgiu com a preocupação da população em relação ao armazenamento e distribuição dos dados pessoais. Iniciando pela Convenção 108, realizada na Europa, que foi o primeiro grande fórum de discussão a respeito de dados pessoais. Em seguida, houve a Diretiva de 1995, também na Europa, em que foram debatidos os mesmos temas. Logo adiante será abordada a definição de dados pessoais, quais as suas características e os seus tipos. bem como as sanções para os crimes cometidos pelas empresas através da malversação dos dados dos clientes. Por

(*) Aluno do 11º período do Curso de Eng. de Telecomunicações
(**) Professor Titular do Departamento de Engenharia de Comunicações

fim, as considerações finais, os impactos e a efetividade das referidas legislações.

O presente artigo está estruturado em seis seções. Após esta introdução, a segunda seção evidencia o referencial teórico que norteia o desenvolvimento desta pesquisa, a terceira seção apresenta os trabalhos relacionados, a quarta expõe a metodologia utilizada na pesquisa, a quinta seção mostra a análise comparativa e discussão dos pontos propostos. Por fim, a sexta seção apresenta as considerações finais do trabalho.

II. Referencial Teórico

Nos dias atuais, é muito comum ver as empresas que oferecem serviços, solicitando dados pessoais, muitas vezes até sem uma justificativa. Para se ter acesso a serviços simples como acessar a wi-fi em um aeroporto, fazer cadastro em um aplicativo, inscrição em um evento online, dentre tantos outros serviços, é necessário que antes se tenha de fazer um cadastro depositando dados pessoais como nome, endereço, telefone e CPF. De posse de um número de CPF, é possível solicitar um cartão de crédito e até mesmo abrir uma empresa. Por isso, existe uma crescente preocupação em relação ao armazenamento dos dados pessoais cedidos a empresas. Mas para onde será que vão esses dados? O que essas empresas fazem com eles? Afinal, os dados pessoais são a parte da identidade de um indivíduo. Um vazamento para mãos erradas pode custar muito caro. Mas onde surgiu a discussão sobre os dados pessoais?

Em 1981, houve a Convenção 108 que reuniu os Estados membros do conselho da Europa, como Islândia, Irlanda, Itália, Holanda, Noruega, entre outros. O objetivo da convenção era de ampliar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, juntamente com o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de caráter pessoal susceptíveis para o tratamento automatizado. Já em 1995 houve, novamente na Europa, a diretiva 46 que tratou dos mesmos temas traçando legislações que perduraram por vários anos.

Já em abril de 2016, foi aprovado pelo Conselho Europeu o GDPR que está em vigor desde 25 de maio de 2018 tendo sido concedido o período de dois anos para adequação às mudanças implementadas. Esse regulamento serviu de base para a criação de várias legislações ao redor do mundo, tais como Brasil (Lei 13.709/2018), California/Estados Unidos (CCPA), México (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) entre outras. Atualmente, existem mais de 100 leis de proteção de dados com finalidade de cuidar da privacidade dos usuários [1].

Estima-se que essas leis deverão criar 75.000 empregos ao redor do mundo, dos quais 28.000 se concentrarão apenas na Europa [2].

Embora o GDPR tenha sido considerado o regulamento mais robusto no que tange à proteção de dados, a sua aplicação no território europeu não causou grandes impactos nas tratativas com informações pessoais, pois muitos dos princípios presentes nesta legislação já se encontravam em vigor graças a leis mais velhas pré-1995, de acordo com [3]

Já nos Estados Unidos, as leis referentes a proteção de dados não são tão abrangentes quanto a LGPD e o GDPR. Isso parte de desde a formação do país onde os estados se uniram para formar uma federação e não a federação que se dividiu em estados. Desta forma, legislações sensíveis como pena de morte, legalização de drogas e proteção de dados ficam com a autonomia dos estados. Mesmo assim, em 1998 entrou em vigor a lei federal de Proteção à Privacidade de Crianças Online, a COPPA (Children's Online Privacy Act) [4]. Em 2004, entrou em vigor a California Online Privacy Protection Act (Lei de Proteção a Privacidade Online da California), ou simplesmente, CalOPPA. Esta lei pode ser considerada uma importante precursora do CCPA por tratar de dados online. Essas duas leis são diferentes, a CalOPPA conta com menos complexidade, enquanto a CCPA conta com menor abrangência. A CalOPPA aplica-se a um operador de um site comercial ou serviço online que coleta informações pessoais identificáveis através da Internet, sobre consumidores individuais residentes na Califórnia que usam ou visitam o seu site comercial ou serviço online. Desta forma, não há restrições: A lei aplica-se à todas as empresas que tenham visitas em seus websites de consumidores da California. A CCPA tem um escopo mais reduzido, já que aplica-se apenas a empresas que vendam dados pessoais, tenha uma renda bruta igual ou maior que 25 milhões de dólares, trate de dados de mais de 50 mil cidadãos californianos ou 50% de sua receita anual venha de comercialização de dados pessoais.

Segundo [5], que divulgou uma pesquisa realizada pela Harris Polls, um dos assuntos que mais preocupam os americanos hoje é a privacidade.

> *"Desde a infame violação da Equifax que viu as carteiras de motorista, números de previdência social, datas de nascimento e endereços de 143 milhões de consumidores caírem nas mãos do ator da ameaça, até a recente a violação da Microsoft que expôs 250 milhões de endereços de e-mail de usuários; a atividade do ator da ameaça está aumentando. Ao mesmo tempo, 81% dos americanos dizem que os riscos da coleta de dados superam os benefícios. A pesquisa mostra que as pessoas estão mais preocupadas com sua privacidade quando se trata de anúncios personalizados do que com a capacidade de ver conteúdo relevante. E 60% dos adultos americanos acreditam que não podem passar um dia normal sem que seus dados sejam coletados pelas empresas"* [5].

No Brasil, o direito à privacidade está contido no Art. 5º da Constituição Federal de 1988 [6], referente aos direitos e deveres do cidadão que afirma que 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. Embora o texto não trate de privacidade online, a base do direito já estava pré-estabelecida desde então. Adiante, foi elaborado, na década de 90, o Código de Defesa do Consumidor, conhecido como CDC. Este dispositivo legal serviu como uma espécie de

manual para tratativas entre clientes e empresas. Há, ainda, uma seção que se destina a cadastros e banco de dados, no Artigo 43, que defende o direito do consumidor de ter acesso a suas próprias informações e o não cumprimento da solicitação é considerada uma violação ao CDC [7].

Com estes pilares pré-estabelecidos e com uma crescente preocupação ao redor do mundo acerca da privacidade online, em 2014 foi implementado o Marco Civil da Internet no Brasil. Embora seu foco tenha sido fazer a regulação do uso internet e não cuidar da privacidade online, este marco deu um importante passo para que a justiça pudesse enxergar que o que acontece no mundo virtual tem efeito no mundo real, de acordo com [8].

Porém, apenas em 2018 foi aprovada a Lei 13.709/2018, a LGPD, no Brasil. Inspirada fortemente pelo GDPR, foi sancionada no dia 14/08/2018, contudo, sofreu vários vetos, sendo o mais notável ao dispositivo que instituía a Agência Nacional de Proteção de Dados, a ANPD. Este instituto prevê a fiscalização e aplicação de sanções por descumprimentos à LGPD. Contudo, a agência foi recriada por Medida Provisória em 27/12/2018, no apagar das luzes do seu governo, pelo então Presidente Michel Temer. Já em 08/07/2019 foi sancionada e transformada na Lei 13.853/2019 pelo Presidente Jair Bolsonaro. A LGPD entrou em exercício no dia 18/09/2020, ainda sem a ANPD que atualmente está em fase de definição do seu conselho diretor.

III. Trabalhos Relacionados

Foram escolhidas algumas bibliografias que tratam sobre a comparação das três legislações: CCPA, GDPR e LGPD.

Em [5], há comparações entre trechos das legislações pelos seguintes critérios: escopo territorial, definição de dado pessoal, papel dos dados anônimos, bases legais e penalidades. O artigo conclui comentando que a onda das leis de privacidade e proteção dos dados pessoais só aumenta, com várias leis sendo criadas ao redor do mundo.

No artigo [9], há o objetivo de tratar da aplicação e adaptação das três leis, pela perspectiva das empresas, seguindo critérios de abrangência territorial e legal, competências fiscalizatórias, direito ao consentimento e execução das três leis.

Em [10] há o objetivo de orientar, ainda que de maneira superficial, as empresas que tratam de dados pessoais. Compara os critérios de abrangência territorial, definição de dado pessoal, venda de dados, multas e penalidades. Discorre ainda, brevemente, sobre as semelhanças entre cada legislação.

Artigo [11] aborda abrangência, coleta, tratamento, venda de dados, direito ao esquecimento e autoridades responsáveis. Conclui discorrendo sobre as dificuldades que as empresas terão ao aplicar as legislações.

Por fim, Artigo [12] têm o objetivo de orientar as empresas a como conquistar a confiança dos consumidores. Usa critérios de quais estratégias que as empresas adotarão para conquistar a confiança dos consumidores e conta com uma tabela comparativa que aborda os principais aspectos entre as leis, como entrada em vigor, definição de dado pessoal, autoridades responsáveis, entre outras.

QUADRO I
COMPARAÇÃO DE ALGUMAS BIBLIOGRAFIAS

Artigo	Parâmetros	Ano Publicação
[5]	Abrangência, bases legais, dados anônimos, penalidades.	2020
[9]	Abrangência territorial, competências fiscalizatórias, execução das leis.	2020
[10]	Venda de dados, penalidades, definição de dado pessoal, abrangência territorial.	2020
[11]	Tratamento de dados, autoridades responsáveis, direito ao esquecimento, venda de dados.	2019
[12]	Autoridades responsáveis, definições de dados pessoais.	2020

IV. Metodologia

A metodologia adotada consistiu no levantamento bibliográfico sobre o tema, buscando os seus pontos mais importantes, como a discussão sobre princípios, bases legais, direitos dos titulares, sanções e multas. Especialmente, aqueles que abordaram a comparação entre as três normas, com o objetivo de unificar, melhorar e atualizar as análises com a inclusão de novos critérios e completar essas comparações à luz dos eventos mais recentes relacionados com a proteção de dados. A construção de quadros comparativos fez parte do desenvolvimento deste artigo com objetivo de concentrar informações para melhor entendimento das comparações.

V. Análise Comparativa e Discussão

A. Abrangência Territorial

As diferentes legislações têm como ponto comum a limitação do escopo de quem elas devem proteger e quais os requisitos que devem ser cumpridos para que as leis possam ser aplicadas de forma efetiva. No que tange à abrangência territorial, cada uma tem as suas as suas balizas de acordo com o local da coleta e tratamento. A LGPD aplica-se a qualquer operação feita por pessoa física ou jurídica, independentemente do país onde esteja do país onde estejam os dados desde que o tratamento tenha sido realizado em território nacional e os beneficiários do tratamento e coleta dos dados também estejam localizados em território nacional. A lei não se aplica para tratamento de dados com finalidades não econômicas e fins particulares.

O GDPR conserva uma abrangência similar à LGPD. É aplicado em todos os 28 países membros da União Europeia onde o titular dos dados esteja. Caso o titular esteja fora de algum desses estados, mas seja residente da União Europeia, a empresa a qual coletou seus dados deverá estar de acordo com o GDPR [13].

Já a CCPA, por se tratar de uma lei estadual, tem a sua abrangência bem mais limitada, porém, não tão tanto que possa ser desconsiderada. O estado da Califórnia conta com

quase 40 milhões de habitantes e seu PIB (Produto Interno Bruto) em 2017 chegou a superar o de vários países, inclusive o Brasil [14]. Grande parte disto graças a imensa quantidade de empresas localizadas em seu território. Empresas como Apple, Facebook, Oracle, Visa, dentre várias outras. Por isso a relevância tão grande da CCPA. Estas empresas citadas tratam, diariamente, de dados de milhões de pessoas. Contudo, as condições para que uma empresa se adeque à CCPA são mais restritivas. É necessário que a empresa faça negócios com residentes da California e satisfaça pelo menos uma das seguintes condições [15]:

- Tenha receita bruta acima de U$ 25M;
- Comercialize dados de pelo menos 50 mil residentes da Califórnia;
- Mais de 50% de sua receita anual venha de comercialização de dados de residentes da Califórnia.

Desta forma, ao verificar-se qualquer ameaça, ou violação de dados, há de se saber a nacionalidade da vítima, o país em que foi realizado o tratamento dos dados e, também, a nacionalidade de quem se beneficia das operações envolvendo os dados pessoais.

É importante, porém, que as empresas se atentem às situações em que mais de uma legislação será aplicada, pois os direitos e obrigações devem ser satisfeitos conforme cada lei. A seguir, há alguns exemplos retirados de [5] em que são expostas algumas situações típicas de aplicação das leis.

> *"**Exemplo A:** Big Stuff é uma grande empresa que faz negócios nos Estados Unidos. Como eles são uma grande empresa que fatura US $ 25 milhões ou mais anualmente, eles devem cumprir o CCPA, pois fazem negócios com residentes da Califórnia;*
> ***Exemplo B:** Small Stuff é uma pequena empresa com menos de 50.000 consumidores nos Estados Unidos. Eles ganham cerca de US $ 18 milhões por ano e não lucram com a venda de informações pessoais. A Small Stuff não precisa estar em conformidade com o CCPA.*
> ***Exemplo C:** Tanto a Small Stuff quanto a Big Stuff devem cumprir o GDPR e a LGPD, uma vez que os dois sites recebem visitantes e fazem negócios com pessoas na UE e no Brasil."* [5].

O pleno cumprimento da abrangência territorial expostos em cada legislação é a única maneira de garantir que as empresas não sejam multadas e nem sofram sanções por violações da privacidade dos usuários. A LGPD e o GDPR têm alcance extraterritorial enquanto a CCPA aplica-se apenas para indivíduos que residem no estado da Califórnia.

B. Dado Pessoal

Afinal, o que é um dado pessoal? Esta pergunta é a chave para tudo aquilo que vai se desenvolver neste presente artigo. De acordo com o GDPR:

> *"Dados pessoais são informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa."* [5].

Já segundo a LGPD:

> *"Consideram-se dados pessoais, informações relacionadas a pessoa natural identificada ou identificável."* [5].

O conceito de **titular de dados**, de acordo com a LGPD, em seu Artigo 5 é:

> *"Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento."* [5].

A definição de dado pessoal de acordo com a CCPA é:

> *"São informações que podem identificar, relacionar-se, descrever, estarem associadas ou serem razoavelmente capazes de serem associadas a um determinado consumidor ou residência."* [5].

E qual o conceito de consumidor?

A CCPA define consumidor como uma pessoa física residente na Califórnia. De acordo com os regulamentos estaduais, um residente da Califórnia é qualquer indivíduo que está no estado da Califórnia para fins que não sejam temporários ou transitórios ou domiciliado no estado da Califórnia.

Desta forma, para os três regulamentos, o dado pessoal consiste em uma informação que identifica uma pessoa ou pode identificá-la. Pode-se citar como exemplos:

- Dados pessoais (Endereço, CPF, número de telefone);
- Características físicas (cor dos cabelos, altura);
- Propriedade de bens (Cor do carro, modelo de celular, relógio);
- Características comportamentais (sotaque, maneira de se expressar).

O GDPR identifica uma característica importante, o dado pessoal caracteriza uma informação relativa a uma pessoa **viva.** E o que acontece com os dados pessoais dos mortos? Como se dá a privacidade, já que após a morte, a disseminação de notícias e conteúdos sobre um determinado individuo aumenta consideravelmente, potencializando violação dos direitos? Esta discussão se tornou forte após um caso ocorrido na Alemanha.

Em 2012, após a morte de uma garota de 15 anos, seus pais solicitaram ao Facebook o acesso à sua conta. A finalidade seria para que a sua morte pudesse ser investigada, através de leitura das conversas. O pedido foi aceito pela primeira instância, negado pela segunda e revalidado em última instância.

Antes disto, em 2005, houve um caso nos Estados Unidos em que um pai solicitou ao provedor o endereço de email e senha do seu filho falecido alegando que, por se tratar de uma

propriedade, deveria ser repassada como herança. O pedido foi negado pelo provedor, alegando direito à privacidade [16].

No GDPR, a legislação de cada país membro da UE que deverá tratar da privacidade dos mortos. A Dinamarca, por exemplo, aplica a legislação do GDPR para pessoas mortas até 10 anos após o falecimento. De acordo com o item 27 do regulamento:

> *"O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas."* [16].

A LGPD não traz nenhuma definição em relação aos dados de pessoas falecidas, mesmo que o Código Civil, em seu artigo 12, garanta que o morto não poderá sofrer violação aos direitos relacionados à privacidade, como honra e imagem.

Isto significa que, embora a lei geral de proteção de dados não discorra sobre a proteção de dados de mortos, há dispositivos legais em nossa legislação que suprem esta necessidade.

A CCPA, assim como a LGPD, silencia sobre o tema.

Embora possa haver esta indefinição quanto ao tema de dados de pessoas mortas, alguns provedores de serviços e redes sociais já têm suas próprias políticas para o que ser feito quando o titular da conta falecer. O Instagram, por meio de sua plataforma de denúncias, permite que usuários denunciem contas de pessoas falecidas para que sejam excluídas. O Facebook possibilita que, em vida, os usuários manifestem o desejo de manter a conta como um memorial ou que a mesma seja excluída após sua morte. O Twitter também atende a exclusão da conta através de solicitações de familiares.

C. Tipos de Dados Pessoais

O GDPR, embora defina que dado seja uma informação relativa a uma pessoa, ele ainda vai mais um pouco além, diz que são dados pessoais o conjunto de informações que podem levar à identificação de uma pessoa. Esta última definição é a de "Dado Cruzado". Para entendermos melhor o que é um dado cruzado e como funciona, vamos relembrar um personagem que ganhou a internet por volta do ano 2008.

O Akinator é um personagem fictício, que se encontra sob o domínio https://pt.akinator.com/, e tem a "capacidade" de adivinhar em que personalidade artística o usuário está pensando. Mas como? O software contém um banco de dados detalhado de várias celebridades e artistas, com o máximo de características possíveis, tais como, cor da pele, cor do cabelo, marcas estéticas e também características pessoais de comportamento.

Basicamente, partindo do pressuposto que o usuário responderia as perguntas de forma sincera e honesta, o software traça um perfil do personagem e adivinha exatamente em quem o usuário estava pensando ao iniciar o questionário. São necessárias, em média, 20 perguntas para adivinhar em quem o usuário estava na mente. É justamente aí que entra o conceito de Dado Cruzado.

> *"Dados Cruzados são o conjunto de informações que, quando combinadas, são capazes de identificar uma pessoa."* [16].

Este conceito está vigente no GDPR.

Para avançar, é necessário discutir quais são os tipos de dados pessoais que são possíveis de encontrar. Existem os "**Dados anônimos**" ou "**Dados anonimizados**" que são dados que não são capazes de identificar algum indivíduo – como dados estatísticos, por exemplo. Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), não permite a identificação de seu titular. Um bom exemplo de dado anônimo é uma planilha com notas escolares.

As notas, por si só, não são capazes de identificar ninguém, pois são apenas dados aleatórios que poderiam ser usados com finalidades estatísticas, para calcular a média de uma turma, desvio padrão entre as notas, porém, ao serem cruzados com algum índice, por exemplo, o índice de ordem crescente da chamada, esse cruzamento conseguiria identificar uma pessoa, já que o cruzamento de dados é identificável.

Sob a óptica da CCPA e do GDPR, os dados anônimos podem ser coletados, retidos e até mesmo vendidos sem o consentimento do titular, pois segundo as suas filosofias, eles não são capazes de identificar o dono. A LGPD não dispõe de nenhum dispositivo que aborde a diferenciação de tratamento dos dados anônimos, sendo então obrigadas as empresas a cumprirem todas as etapas de consentimento a fim de que possam coletar, tratar e vender esse tipo de informação.

Um outro tipo de dado pessoal é o chamado "Dado Pessoal Sensível" que é o dado cujo tratamento pode ensejar a discriminação do seu titular. Por se referir, por exemplo, à opção sexual, convicções religiosas, filosóficas, morais, ou opiniões políticas. Os dados sensíveis, pelo potencial discriminatório que apresentam, de acordo com a proposta em questão, devem ser protegidos de forma mais rígida. Aqui, deve-se debater qual o grau de proteção desses dados e os limites para seu tratamento.

Os dados sensíveis estão previstos no GDPR e na LGPD que instituem que o consentimento deve estar explicito para o usuário, assim como as suas devidas finalidades.

Um bom exemplo que pode acontecer com o mal uso dos dados pessoais sensíveis, é o caso de serem usados aplicativos para entrega de alimentos, como é o caso do "Ifood", que guarda informações dos usuários tais como preferências culinárias e endereço. Caso esses dados sejam vazados e haja um cruzamento destas duas informações, é possível identificar uma pessoa apenas pelo que ela gosta de comer. Se, frequentemente, o indivíduo pede alimentos que não contenham açúcar, pode-se imaginar que tal pessoa tem problemas com glicose. Se for comida árabe, pode-se imaginar religião ou até mesmo proximidade com pessoas árabes, dentre vários outros exemplos. Caso estas informações sejam vazadas para um seguro de saúde, e este seja capaz de identificar o titular destes dados, ele pode, simplesmente, negar a contratação de um seguro de saúde para aquele determinado individuo, já que o seguro de saúde já saberia que ele tem problemas de saúde. Já relacionando com o exemplo da religião, o cruzamento de dados poderia

findar com preconceitos para com o titular dos dados, como a discriminação em uma determinada vaga de emprego.

D. Princípios

As três legislações contam com quantidade de princípios diferentes. A LGPD conta com 10 princípios, o GDPR com 6 e a CCPA não estabelece nenhum princípio fundamental, porém apresenta os direitos dos titulares. Embora haja essa discrepância na quantidade de princípios, a grande maioria dos direitos dos titulares são contemplados na LGPD e no GDPR, a CCPA diverge pois não conta com princípios explícitos, porém com direitos que podem ser associados aos princípios contidos nas outras legislações.

A LGPD abrange 10 princípios que regem a proteção de dados. São estes [17]:

Finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
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;
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;
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;
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;
Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais de perda, alteração, comunicação ou difusão;
Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
Não Discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
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.

O GDPR conta com 6 princípios [16]:

Licitude, Lealdade e Transparência: Dados pessoais devem ser tratados de forma lícita e transparente, garantindo a lealdade do tratamento para com as pessoas cujos dados pessoais estão a ser tratados;
Adequação e Limitação da Finalidade: Devem existir finalidades específicas para o tratamento dos dados e a empresa/organização deve comunicá-las às pessoas quando do recolhimento dos seus dados pessoais;
Necessidade ou Minimização: A empresa/organização deve recolher e tratar apenas os dados pessoais necessários para cumprir essa finalidade;
Qualidade dos Dados ou Exatidão: A empresa/organização deve garantir que os dados pessoais são exatos e estão atualizados;
Limitação da Conservação:
A empresa/organização deve garantir que os dados pessoais são conservados apenas durante o tempo necessário às finalidades para as quais foram recolhidos;
Segurança, Integridade e Confidencialidade: Assegurar que a informação é acessível somente por pessoas devidamente autorizadas.

A CCPA, como já dito, não conta com princípios claros e explícitos como as suas similares. Porém, estabelece direitos aos consumidores que podem facilmente serem associados aos princípios do GDPR e LGPD [18]. São eles:

Acesso: Os consumidores californianos têm o direito de acessar as categorias e informações pessoais que uma empresa coletou sobre eles a qualquer momento que desejarem.
Notificação: A empresa não tem permissão para coletar, processar e armazenar qualquer tipo de informação pessoal identificável sem enviar um aviso de tal ação para seus clientes.
Consentimento: Para qualquer tipo de dados pessoais valiosos, a empresa deve ter o consentimento do consumidor para obter a oportunidade de coletá-los e processá-los posteriormente.
Opt-out: Em qualquer fase e por qualquer motivo, um consumidor tem o direito de optar por não participar dos processos de compartilhamento de dados e desabilitar suas vendas.
Igualdade: Significa que você deve prometer a seus clientes que não os discriminará, ou seja, fornecerá um serviço de qualidade inferior se eles decidirem não fornecer seus dados para fins não essenciais.
Exclusão: Todo cliente tem o direito de ser esquecido. Assim, eles podem solicitar a exclusão de seus dados completamente se desejarem.

Expostos os princípios, é possível notar semelhanças entre os mesmos. A GDPR dispõe de apenas seis princípios, porém quase todos estão englobados nos dez princípios da LGPD, exceto o princípio da "Responsabilização e Prestação de Contas" que se encontra apenas na LGPD, o que não significa que o GDPR não conte com este dispositivo, já que será visto neste artigo os institutos da fiscalização e das penalidades para o não cumprimento adequado das normas. Está abaixo um quadro com as equivalências entre os princípios das três legislações.

QUADRO II
EQUIVALÊNCIA DOS PRINCÍPIOS DE CADA LEGISLAÇÃO

GDPR	LGPD	CCPA
Licitude, Lealdade e Transparência	Livre acesso; Não Discriminação; Transparência	Consentimento; Igualdade; Acesso
Adequação e Limitação da Finalidade	Finalidade; Adequação;	Notificação
Necessidade ou Minimização	Necessidade	-
Qualidade dos Dados ou Exatidão	Qualidade dos Dados	-
Limitação da Conservação	Finalidade	-
Segurança, Integridade e Confidencialidade	Segurança; Prevenção	-
-	Responsabilização e Prestação de Contas	-
-	-	Exclusão
-	-	Opt-out

Embora as equivalências entre a LGPD e o GDPR sejam triviais, visto a própria nomenclatura de cada princípio, os direitos da CCPA não são facilmente encaixados nestas equivalências. Porém, é possível aferir que o direito da "Notificação" contido na CCPA é equivalente ao da "Adequação e Limitação da Finalidade" do GDPR e "Finalidade" da LGPD, pois garante que só poderão ser utilizados os dados previamente consentidos pelo titular. O direito à "Igualdade" pode ser comparado com o da "Licitude, Lealdade e Transparência" e da "Não discriminação" da LGPD, já que garante ao titular que seus dados serão tratados de forma igualitária perante os demais. O direito ao "Acesso" pode ser associado ao da "Licitude, Lealdade e Transparência" do GDPR e da "Transparência" da LGPD com a garantia de acesso transparente, a qualquer momento, pelos titulares.

E. Consentimento

O consentimento, também chamado de "Opt-In" pelo GDPR, para utilização dos dados é o direito que todos os usuários têm de só terem os seus dados recolhidos e tratados, quando solicitados e aprovados pelo titular. A solicitação, por parte da empresa, deve ser feita com uma linguagem direta e de fácil entendimento para que os usuários não tenham dúvidas a respeito das finalidades e das maneiras que as empresas utilizarão as informações.

O consentimento deve estar, não em letras minúsculas, mas de maneira explícita com todas as condições de uso e tratamento dos dados afim de evitar as famosas "pegadinhas" nos termos de aceitação.

Na CCPA, não é exigido o consentimento antes da coleta e tratamento de dados a não ser que a finalidade da coleta seja para venda de informações.

Há, por outro lado, o direito inverso, em que os titulares podem solicitar a retirada dos seus dados pessoais do banco de dados das empresas. Chamado de "Opt out" pelo GDPR, este conceito também se estende para as outras legislações. O usuário deve informar a empresa que não deseja mais que ela utilize os seus dados para qualquer fim, tendo a empresa a obrigação de cumprir o requerimento, sob pena de sofrer sanções e multas.

F. Direito ao Esquecimento

O direito ao esquecimento é o direito que garante ao titular dos dados a revogação do consentimento dado para que as empresas possam utilizar as suas informações e também a exclusão das mesmas de seus bancos de dados.

Este direito foi introduzido no GDPR, porém já estava presente na Diretiva de 1995 que diz que o titular dos dados pode solicitar a remoção de resultados de pesquisa em que seu nome esteja incluído.

Existiu um caso na justiça espanhola que ilustra bem o conceito do esquecimento: O caso Google Espanha vs Mário Costeja González. Ao buscar o nome de Mário Costeja González, havia duas matérias de um jornal que mostrava que González tinha imóvel que seria hipotecado para pagamento de uma dívida pública com a seguridade social espanhola. Acontece que o titular já havia pago esta dívida e, mesmo assim, os resultados da pesquisa continuaram sendo expostos por mais de 10 anos. González solicitou ao jornal "La Vanguardia" a retirada da matéria, o que foi negado pelo mesmo sob alegação de que a matéria era legítima. Até que González solicitou à justiça para que o buscador, no caso, o Google, retirasse às matérias do resultado das pesquisas. A justiça negou, González recorreu até que o Tribunal de Justiça da União Europeia (TJUE) decidiu que o titular tem o direito de solicitar a veículos de busca e pesquisa que retirem suas informações dos resultados obtidos [20].

Na LGPD, o direito ao esquecimento já era previsto no Marco Civil da Internet, Código de Defesa do Consumidor, Lei de Acesso à Informação e a Lei do Habeas Data, porém, de forma tímida.

O procedimento para que o titular tenha seus dados excluídos, de acordo com a LGPD, é mediante solicitação encaminhada ao Controlador dos dados, a qualquer tempo. A solicitação deve conter a identificação do titular, juntamente com a relação dos dados que deseja que sejam excluídos.

De acordo com [21], os residentes da California têm o direito de pedir que seus dados sejam excluídos, porém, apenas em algumas situações que são:

- As informações pessoais foram coletadas pela empresa junto ao consumidor;
- Não seja mais necessária para a empresa ou provedor de serviços manter as informações pessoais para cumprir uma das finalidades.

Ao responder a solicitação de exclusão, a empresa pode apresentar ao consumidor a opção de excluir partes selecionadas de suas informações pessoais apenas se uma opção global para excluir todas também for oferecida e

apresentada de forma mais destacada do que as outras opções. Ou seja, a empresa terá de dar, obrigatoriamente primeiro, uma opção para que todas as informações sejam excluídas para, em seguida, dar uma a opção de excluir dados de forma fragmentada [21].

G. Bases Legais

O tratamento de dados nas legislações se dará obedecendo os princípios previstos em cada legislação, porém existe o conceito de Bases Legais. Este conceito define situações hipotéticas em que o tratamento de dados será realizado. Os princípios são regras que balizam a maneira com que as empresas coletarão, tratarão e descartarão as informações. As bases legais funcionam como a justificativa que as empresas têm de ter para que possam utilizar os dados. A coleta de dados que não estiver prevista em alguma base legal será passível de penalidades.

A LGPD conta com 10 bases legais. São elas: [22]

1 – Consentimento:
Esta base legal define que o tratamento e a coleta dos dados se darão por via consentida do titular.
2 - Legítimo Interesse:
Considerada a base legais mais controversa e confusa, abre portas para que os dados pessoais do titular sejam utilizados sem o devido consentimento.
2.1 - Quando o consentimento do usuário for muito difícil de ser obtido. Exemplo: Titular não encontrado via telefone, email ou endereço postal.
2.2 – Quando o consentimento do usuário for considerado desnecessário.
2.3 – Quando houver um impacto mínimo na vida do titular.
3 – Contratos:
Para realização de contratos pré-estabelecidos ou que venham a se estabelecer com o titular. Para contratar um funcionário, uma empresa precisa que sejam fornecidas uma série de informações pessoais necessárias para formalizar o contrato (dados do contratante, dados bancários) que farão parte do futuro contrato de emprego do titular dos dados.
4 - Obrigação Legal:
Casos em que há exigência de armazenamento de dados do cliente para fins judiciais.
5 - Execução de Políticas Públicas:
Casos em que há interesse público nos dados.
6 - Estudos por órgãos de pesquisa:
Permissão de uso dos dados para fins de pesquisa.
7 - Processo Judicial:
Casos para cumprimento de ações judiciais.
8 - Proteção da Vida:
Quando o seu uso é de interesse vital seja do titular do dado.
9 - Tutela da Saúde:
Quando é necessário que profissionais de saúde tratem os dados de determinado paciente. Exemplo: Informações como tipo sanguíneo, histórico de doenças e dados de identificação.
10 - Proteção de Crédito:
Casos em que são compartilhados dados para criar score de um cliente. Muito utilizado pelo SERASA e SPC.

Quanto ao GDPR, existem 6 bases legais [23]:

1 – Consentimento:
Deliberação do titular para que haja o tratamento dos dados.
2 – Contrato:
Para cumprimento de contratos firmados entre a empresa e o titular dos dados.
3 - Obrigação Legal:
Para execução de algum tipo de solicitação judicial.
4 - Interesses Vitais:
Proteção de indivíduos contra riscos que podem comprometer vidas.
5 - Tarefas Públicas:
Quando há interesse público nos dados, em casos de pesquisas, ou censo de governo.
6 - Interesses Legítimos:
Razão legítima para que os dados sejam coletados mesmo sem o consentimento do titular.

A CCPA não conta com nenhuma base legal em seu texto, na qual as empresas podem coletar ou vender informações pessoais. Ela apenas dispõe que as empresas devem obter o consentimento dos consumidores quando eles entram em um negócio de comercialização com base nas informações pessoais fornecidas. Abaixo segue mais um quadro comparativo com as equivalências entre as bases legais de cada legislação.

QUADRO III
EQUIVALÊNCIA DAS BASES LEGAIS DE CADA LEGISLAÇÃO

GDPR	LGPD	CCPA
Consentimento	Consentimento	Consentimento
Interesses Legítimos	Legítimo Interesse	-
Contratos	Contratos	-
Obrigação Legal	Obrigação Legal; Processo Judicial	-
Tarefas Públicas	Execução de Políticas Públicas	-
Interesses Vitais	Proteção da Vida	-
-	Tutela da Saúde	-
-	Proteção de Crédito	-
-	Estudos por órgãos de pesquisa	-

H. Autoridades Fiscalizatórias

A LGPD instituiu a Autoridade Nacional de Proteção de Dados (ANPD), porém ela foi vetada no ato da sanção pelo então Presidente Michel Temer, recriada posteriormente via Medida Provisória e sancionada pelo Presidente Jair Bolsonaro [24]. Esse instituto prevê a fiscalização e a regulação da LGPD. Será vinculada à Presidência da República e terá sua própria autonomia, assim como deverá servir como orientadora do tratamento de dados pessoais para órgãos governamentais. A autoridade contará com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. O colegiado será composto por 23 titulares, não remunerados.

O GDPR conta com autoridades responsáveis em todos os países integrantes. São eles quem tem a autonomia para criar e manter estes órgãos. São funções dessas autoridades, a supervisão e aplicação das sanções para empresas que violem as regras descritas no regulamento. Alguns países, inclusive, contam com agências regulatórias, responsáveis por garantir a aplicação das diretivas de privacidade e comunicações eletrônicas, chamadas de ePrivacy Directive (Privacy and Electronic Communications Directive 2002/58/EC) [19].

Na Irlanda, a Autoridade Nacional é chamada de Data Proteccion Comission (DPC) e foi estabelecida pela Data Proteccion Act. A autoridade nacional de Portugal é a Comissão Nacional de Proteção de Dados. O Reino Unido conta com Information Comissioner's Office que tem as funções de investigação, fiscalização e aplicação de sanções, também gerencia inscrições dos Data Protection Officers, (DPO's) indicados pelas organizações.

Já a CCPA conta como autoridade o Attorney General da California, algo próximo com Procurador Geral da Califórnia, autoridade eleita pelos residentes do estado, que tem o poder de emitir multas de não conformidade e fiscalizar ações de empresas [9].

As atribuições das autoridades responsáveis pelas fiscalizações são semelhantes no GDPR e LGPD, garantindo uma autonomia de formação das comissões pelos países. No caso da CCPA, trata-se de uma diferença nos fundamentos da formação da autoridade, já que o Attorney General não é alguém eleito especificamente para tratar da fiscalização de uma lei singular, como a CCPA, mas sim, um operador do direito que tem como dever tratar de todas as questões jurídicas envolvendo o estado.

I. Dados de Menores

As três legislações têm abordagens diferentes quanto ao tratamento relativo aos dados pessoais de menores de idade, porém, sempre pedindo consentimento dos responsáveis pelo uso, tratamento e venda de dados.

A CCPA determina que haja consentimento dos responsáveis consistente com o regulamento do COPPA (Política de Proteção da Privacidade Infantil estabelecida em 2000 para tratamento de dados de crianças na Internet) para crianças menores de 13 anos. Para crianças entre 13 e 16 anos, ainda é necessário o consentimento do titular dos dados. Todos os direitos para os dados pessoais de menores de idade são previstos da mesma forma que para outros cidadãos [4].

A LGPD regimenta que o uso dos dados pessoais de menores de 16 anos deve seguir as normativas previstas no ECA (Estatuto da Criança e do Adolescente) e só podem ser coletados e tratados via autorização expressa de um dos pais, ou responsáveis, por aquele menor. Além da confirmação, será necessário que a empresa realize todos os esforços razoáveis para verificar a identidade do fornecedor do consentimento [26].

O GDPR vai de encontro com as legislações brasileiras e Californianas e prevê que dados de menores de 16 anos devem ter expressa autorização dos responsáveis e conforme regimento já instalado

J. Penalidades

A autoridade responsável pela fiscalização da LGPD é a ANPD, como visto anteriormente neste artigo. Porém, enquanto a mesma não estiver em pleno funcionamento, os órgãos responsáveis pela atribuição de fiscalização é o Ministério Público e os órgãos de proteção e defesa do consumidor.

A legislação prevê algumas das seguintes sanções administrativas aplicáveis pela Autoridade Nacional, dispostas no artigo 52 de [17]:

- Advertência, com a indicação de prazo para adotar medidas corretivas - artigo 52, I, da LGPD;
- A multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, com a exclusão dos tributos, limitada, no total, a R$ 50.000.000,00 por infração - artigo 52, II, da LGPD;

Todas as sanções e multas serão aplicadas após instaurado o devido processo legal, garantindo o amplo direito de defesa e notificação das empresas. Também deve ser respeitado o princípio da proporcionalidade às infrações aplicadas.

O valor arrecadado com as multas, serão destinados ao Fundo de Defesa de Direitos Difusos de que tratam o artigo 13, da Lei nº 7.347 de 1985 e Lei nº 9.008 de 1995. A aplicação das sanções deve respeitar o princípio da proporcionalidade das infrações realizadas.

O GDPR tem como multas para descumprimento dos seus princípios e dos direitos do consumidor as seguintes penalidades:

- Multas de até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, para casos em que são violados os princípios da Licitude, Lealdade e Transparência.
- Multas de até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, para casos em que haja violação dos dados e menores [27].

A CCPA cobra U$ 2500 por infração ao regulamenta, e caso haja dolo, esse valor pode chegar até U$ 7500. Isso tudo por cada violação e por cada titular prejudicado. A ação civil será instaurada em nome da população do estado da Califórnia pelo Attorney General [28].

K. Aplicações das Leis.

As três legislações já estão em vigor e vamos analisar alguns cases de aplicação de sanções contra empresas que descumpriram princípios e direitos dos usuários.

1. Em setembro de 2020, a construtora Cyrela foi condenada a pagar R$ 10 mil de multa a um cliente que teve seus dados de telefone compartilhados com

empresas parceiras da construtora em questão. O cliente passou a receber diversas ligações oferecendo produtos correlacionados a compra de um apartamento novo, tais como mobília planejada e produtos de decoração para casa nova. A juíza da 13º Vara Cível de São Paulo, Tonia Yuka Koroku, descreveu em seu despacho "Resta devidamente comprovado que o autor foi assediado por diversas empresas pelo fato de ter firmado instrumento contratual com a ré para a aquisição de unidade autônoma em empreendimento imobiliário." A Juíza também afirmou que fora descumprido o princípio da finalidade, já que ao fornecer os dados à empresa, o cliente não fora informado que teria seus dados compartilhados com empresas parceiras [29];

2. A rede de supermercados Carrefour, foi multada em €3 milhões pela Comissão Nacional de Computação e Liberdade (CNIL) sob alegação de violações a princípios e direitos contidos no GDPR De acordo com a matéria do site The Hack: "A justificativa da CNIL para as multas é que as informações sobre proteção e uso de dados de clientes eram muito complicadas, imprecisas e em alguns casos estavam até escondidas em longos documentos, misturadas com outras informações. Além disso, a empresa utilizava cookies de forma ilegal e quando um cliente perguntava sobre como seus dados estão sendo utilizados pela empresa, o Carrefour não era transparente, operava com uma política restritiva e não respondia às solicitações dentro do prazo legal. A CNIL considerou também que havia poucas informações sobre as transferências de dados para fora da União Europeia." A empresa foi condenada por ter violado o princípio da transparência, o primeiro contido no GDPR [30].
3. Ainda não há conhecimento de empresas que tenham sido punidas ou multadas com base nos dispositivos da CCPA.

VI. CONSIDERAÇÕES FINAIS

Foi feita neste artigo comparações à luz dos principais critérios entre as três legislações apresentadas. Foi possível identificar que o tratamento dos dados pode ser diferenciado caso o titular venha a falecer ou seja menor de idade. Também foi possível notar que há extraterritorialidade na LGPD e no GDPR, fazendo com que as empresas devam adequar-se às duas legislações. Embora os princípios balizem a maneira com que os dados sejam tratados, as bases legais podem ser consideradas, pelas empresas, mais comprometedores, visto que elas ensejam as hipóteses em que, efetivamente, as empresas podem coletar as informações. Caso uma empresa faça o tratamento dos dados de maneira correta, seguindo os princípios de cada legislação, e não tenha uma base legal que justifique a coleta destes dados, a mesma estará infringindo a legislação e terá de ser punida. Foi importante destacar a importância do consentimento e quais as condições em que este dispositivo é posto. Ainda hoje, é possível verificar que tem de se aceitar termos de uso para cada aplicativo que é utilizado, cada website que é acessado e cada serviço que é contratado. São nestes termos de uso que se encontram o pedido de coleta dos dados, muitas vezes ainda de forma minúscula, o que induz os titulares a não ler de maneira adequada e aceitar os termos de uso. Esta prática é uma das que as legislações mais tentam coibir, pois afirmando que receberam o consentimento dos titulares, as empresas podem coletar e tratar os dados da maneira que bem entendem.

Embora em níveis diferentes, as três leis abordadas neste artigo estão muito bem fundamentadas quanto aos direitos dos titulares e em relação às fiscalizações e sanções, tornando as legislações bastante robustas. A CCPA, embora mais branda e com menor escopo, traz importantes avanços no tema da privacidade, como regulamentação da venda e tratamento de dados que antes só foram tratados via legislação de 1998, a COPPA, já abordada anteriormente. O GDPR, embora tenha servido de base para, não apenas, as leis em questão, mas a grande maioria das legislações atuais acerca de proteção de dados pessoais ao redor do mundo, não trouxe grandes novidades sobre o tema, já que muitos dos seus princípios já estavam vigentes desde a Diretiva 46. A LGPD, por sua vez, trouxe muitos desafios para as empresas brasileiras e as que atuam no território brasileiro, já que nunca houve uma legislação tão ampla e com tamanha abrangência no Brasil. O escopo de abrangência de pessoas, somadas as 3 leis, chega a quase 700 milhões de pessoas.

A troca de informações entre empresas está na casa dos milhões, diariamente. Porém, há uma preocupação iminente, por parte das organizações, em relação ao cumprimento integral das exigências previstas em cada uma dessas legislações. No Brasil, por exemplo, os desafios encontrados são maiores, já que a proteção de dados online era muito tímida, com poucas menções no Código de Defesa do Consumidor até antes de 2018, para uma regulamentação robusta e complexa que entrou em vigor em 2020. Há de se considerar, também, que o tempo para adequação é, relativamente curto. Multas e sanções como visto, quando acumuladas, podem levar empresas a fecharem as portas devido ao não cumprimento integral dos princípios de proteção de dados. Acontece que que devido as complexidades de cada lei, aliadas ao fato de terem que se adequar a lei de cada território pode fazer com que as empresas recebam "Chuvas" de sanções e multas, extraterritoriais, o que pode inviabilizar o tratamento de dados pessoais.

Sob a óptica dos usuários, as legislações vêm em boa hora. A cada dia, os seus dados estão mais expostos, graças a grande quantidade de serviços online que são contratados. Com isso, as trocas de informações entre empresas fazem com que o risco da malversação dos dados seja maior. Como visto no início deste artigo, o simples uso do CPF pode realizar diversas operações. Houve um aumento na importância do consentimento no que se refere ao tratamento dos dados, por outro lado, as empresas têm usado diversas promoções como artimanhas, em que se dá por necessário o compartilhamento de dados para fazer com que os usuários compartilhem suas informações em busca do uso de um determinado serviço. A garantia de que existem legislações fortes, com intensas fiscalizações e princípios justos, pode ser um ativo que faça os usuários adentrar ainda mais em serviços oferecidos pela internet.

REFERÊNCIAS

[1] VALENTE, Jonas. Entenda o que muda com a Lei Geral de Proteção de Dados. Agência Brasil, 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/entenda-o-que-muda-com-a-lei-geral-de-protecao-de-dados>. Acesso em: 13 de out. de 2020.

[2] Nova lei de proteção de dados abre vagas para profissional que valerá ouro no mercado. Panorama Farmacêutico, 2019. Disponível em: <https://panoramafarmaceutico.com.br/2019/10/18/nova-lei-de-protecao-de-dados-abre-vagas-para-profissional-que-valera-ouro-no-mercado/>. Acesso em: 13 de out. de 2020.

[3] CAPEZ, Fernando. Lei Geral de Proteção de Dados: origem histórica. IG Economia, 01 de jun. de 2020. Disponível em: <https://economia.ig.com.br/colunas/defesa-do-consumidor/2020-06-01/lei-geral-de-protecao-de-dados-origem-historica.html>. Acesso em: 14 de out. de 2020.

[4] DINI, Aline. Lei que protege os dados pessoais de crianças entra em vigor. Crescer, 16 de agosto. de 2018. Disponível em: <https://revistacrescer.globo.com/Criancas/Seguranca/noticia/2018/08/lei-que-protege-os-dados-pessoais-de-criancas-entra-em-vigor.html>. Acesso em: 14 de out. de 2020.

[5] ONETRUST, What Are the Differences Between CCPA and GDPR and LGPD?. OneTrust, 28 de agosto. de 2020. Disponível em: <https://www.onetrust.com/blog/what-are-the-differences-between-ccpa-and-gdpr-and-lgpd/>. Acesso em: 10 de out. de 2020.

[6] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Centro Gráfico, 1988.

[7] BRASIL. Código de defesa do consumidor. Lei 8.078 de 11/09/90. , Diário Oficial da União, 1990.

[8] HISTÓRICO das leis de proteção de dados e da privacidade na internet. Assis e Mendes. Disponível em: < https://assisemendes.com.br/historico-protecao-de-dados/>. Acesso em: 29 de set. de 2020.

[9] WEISS, Fernando L. Paralelo entre a Lei Geral de Proteção de Dados, o CCPA e o GDPR europeu. Conjur, 28 de out. de 2020. Disponível em: < https://www.conjur.com.br/2020-out-28/weiss-paralelo-entre-lgpd-ccpa-gdpr-europeu>. Acesso em: 02 de nov. de 2020.

[10] FONTANA, Leo. GDPR, LGPD e CCPA: o que são essas leis, semelhanças e diferenças. 27 de fev. de 2020. AdOpt. Disponível em: <https://goadopt.io/blog/gdpr-lgpd-e-ccpa-o-que-sao-essas-leis-semelhancas-e-diferencas/>. Acesso em: 04 de nov. de 2020.

[11] ARAÚJO, Antonio. Entenda a diferença entre LGPD, CCPA e GDPR e porque essa sopa de letras irá mudar o mundo ?. 01 de dez. de 2019. Tá Justo Business & Law. Disponível em: <https://antonioaraujojr.com/2019/12/01/entenda-a-diferenca-entre-lgpd-ccpa-e-gdpr-e-porque-essa-sopa-de-letras-ira-mudar-o-mundo/>. Acesso em: 03 de nov. de 2020.

[12] SHAH, Ratul. GDPR, CCPA, and LGPD: Time for a global consumer data privacy strategy. 21 de out. de 2019. The Future of Customer Engagement and Experience. Disponível em: <https://www.the-future-of-commerce.com/2019/10/21/gdpr-ccpa-and-lgpd-global-data-privacy/>. Acesso em: 03 de nov. de 2020.

[13] Principais Diferenças entre a LGPD e a GDPR. Click Compliance, 2018 Disponível em: <https://clickcompliance.com/principais-diferencas-lgpd-gdpr/>. Acesso em: 07 de out. de 2020.

[14] DIEZ, Beatriz. Como a Califórnia foi da beira da falência a 5ª economia do mundo. BBC, 03 de jun de 2018. Disponível em: < https://www.bbc.com/portuguese/internacional-44293330>. Acesso em: 16 de out. de 2020.

[15] BRANDAO, Graziela. CCPA: Lei de Privacidade do Consumidor da Califórnia. BL Consultoria digital, 11 de fev. de 2020. Disponível em: < https://blconsultoriadigital.com.br/ccpa-lei-de-privacidade-do-consumidor-da-california/>. Acesso em: 17 de out. de 2020.

[16] UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679, de 27 de abril. de 2016. Regulamento Geral de Proteção de Dados Pessoais (RGPD), UE, abril 2016.

[17] BRASIL. Lei n. 13.709, de 14 de ago. de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília,DF, ago 2018.

[18] LAZZAROTTI, Joseph J. California Consumer Privacy Act FAQs for Covered Businesses. Jackson Lewis, 10 de out. de 2019. Disponível em: <https://www.jacksonlewis.com/publication/california-consumer-privacy-act-faqs-covered-businesses>. Acesso em: 25 de out. de 2020.

[19] LEAL, Lívia. Proteção post mortem dos dados pessoais?. AB2L. 26 de jan. de 2019. Disponível em: <https://ab2l.org.br/protecao-post-mortem-dos-dados-pessoais/>. Acesso em: 01 de dez. de 2020.

[20] MENEZES, Victor H. O Caso Google Spain vs. Mário Costeja González. JUSBRASIL. 23 de mar. de 2017. Disponível em: <https://victorhugotmenezes.jusbrasil.com.br/artigos/441755309/1-o-caso-google-spain-vs-mario-costeja-gonzalez>. Acesso em: 09 de dez. de 2020.

[21] TORRE, Lydia F. Right to delete under CCPA. 5 de jan. de 2020. Disponível em: <https://medium.com/golden-data/right-to-delete-under-ccpa-55338a324944>. Acesso em: 09 de dez. de 2020.

[22] NONES, Fernanda. Princípios da LGPD: a importância na adequação de bases legais. Blog de Marketing Digital de Resultados, 30 de jul. de 2020. Disponível em: <https://resultadosdigitais.com.br/blog/principios-da-lgpd/>. Acesso em: 30 de nov. de 2020.

[23] ZOHO. Gerenciamento de bases legais para processamento de dados. ZOHO. Disponível em: <https://www.zoho.com/pt-br/crm/help/gdpr/lawful-bases-data-processing.html/>. Acesso em: 30 de nov. de 2020.

[24] A nova lei de privacidade e proteção de dados na Califórnia (CCPA). Jota Info, 6 de mai. de 2019. Disponível em: <https://jotainfo.jusbrasil.com.br/artigos/704577523/a-nova-lei-de-privacidade-e-protecao-de-dados-na-california-ccpa>. Acesso em: 28 de out. de 2020.

[25] Quem vai regular a LGPD?. SERPRO. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd/>. Acesso em: 30 de nov. de 2020.

[26] CÉ, Lucas L. O que crianças e adolescentes ganham com a nova lei?. SERPRO, 18 de jul. de 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/criancas-adolescentes-lgpd-lei-geral-protecao-de-dados-pessoais>. Acesso em: 20 de nov. de 2020.

[27] FAILLA, Daniel A. Data Breach: a violação de dados no GDPR. Migalhas. 23 de mai. de 2018. Disponível em: < https://migalhas.uol.com.br/depeso/280551/data-breach--a-violacao-de-dados-no-gdpr>. Acesso em: 20 de nov. de 2020.

[28] TERMSFEED. CCPA Penalties: What We Know So Far. Termsfeed. 06 de jul. de 2020. Disponível em: <https://www.termsfeed.com/blog/ccpa-penalties/>. Acesso em: 28 de nov. de 2020.

[29] Empresa descumpre LGPD e é condenada a pagar R$ 10 mil de multa. Tecmundo 30 de set de 2020. Disponível em: <https://www.tecmundo.com.br/mercado/204559-empresa-descumpre-lgpd-condenada-pagar-r-10-mil-multa.htm/>. Acesso em: 30 de nov. de 2020.

[30] PETRY, Guilherme M.. Carrefour é multado em 3.8 milhões de euros por descumprimento da GDPR. The Hack, 02 de dez. de 2020. Disponível em: <https://thehack.com.br/carrefour-e-multado-em-3-8-milhoes-de-euros-por-discumprimento-da-gdpr/>. Acesso em: 03 de dez. de 2020.

ANEXO

RESUMO	LGPD	GDPR	CCPA
APROVAÇÃO	14/08/2018	15/04/2016	28/06/2018
ENTRADA EM VIGOR	18/09/2020	25/05/2018	01/01/2020
PRECURSORES	CDC, MARCO CIVIL	CONV 108, DIR 46	COPPA
TERRITÓRIO DE ABRANGÊNCIA	BRASIL	UNIÃO EUROPEIA	CALIFORNIA/EUA
PRINCÍPIOS	10	6	6
BASES LEGAIS	10	6	0
PRAZO RESPOSTA A SOLICITAÇÕES	15 DIAS	30 DIAS	45 DIAS
AGENTES DE TRATAMENTO	CONTROLADOR, OPERADOR, ENCARREGADO	CONTROLADOR, PROCESSADOR, DPO	PRESTADOR DE SERVIÇOS
AUTORIDADES RESPONSÁVEIS	ANPD	INDICADO PELOS ESTADOS MEMBROS	ATTORNEY GENERAL
CONSENTIMENTO DADOS MENORES	> 16 ANOS	>16 ANOS	>13 ANOS
MULTAS	ATÉ R$ 50 MILHÕES, 2% FATURAMENTO ANUAL	ATÉ 20 MILHÕES EUR, 4% FATURAMENTO ANUAL	ATÉ U$ 7500/INFRAÇÃO