**BOAS PRÁTICAS LGPD E COMPLIANCE:**

A sociedade moderna está passando por um processo de digitalização das informações pessoais, uma vez que com o advento da internet cada vez mais pessoas deixam de lado a forma que elas vivenciavam e passam para uma nova fase de globalização e tecnologia.

A partir disso, uma tendência surge, a modernização da vida das pessoas, é muito claro de ser observado como as informações passaram a ter mais importância que os recursos tradicionais, as terras, o petróleo e o ouro. Peter Drucker disserta defendendo esse ponto, sua fala diz: “A difusão da tecnologia confere à informação a mesma importância que os recursos tradicionais, terra, capital e trabalho”

É inegável o valor que as informações possuem na sociedade atual, tendo em vista que a economia se volta para a coleta de informações. Entretanto, as problemáticas que surgem com este advento são inúmeras, tal como a utilização destes dados para manipular as pessoas mais vulneráveis, ou até mesmo serem utilizadas para práticas discriminatórias.

Uma vez atribuído alto valor aos dados, consequentemente ele passa a ser alvo de mentes maliciosas, acontecimentos como vazamento de informações em grandes empresas, ou até mesmo tentativas de hackear a sistemas públicos, bancos, entre outras entidades que possuem em sua base informações importantes das pessoas e dão espaço para que esses dados possam ser utilizados de forma maliciosa por aqueles que os tiverem em mãos.

Deve-se entender o valor que os dados possuem, uma vez que na palma de sua mão, através do celular, as pessoas têm acesso a informações como documentos pessoais, cartões de crédito, entre outros que podem ser utilizados para prejudicar o titular. Além desses, há informações como localização, fotos particulares, histórico de compras, histórico de chamadas, dentre diversos outros.

Deste modo, fez-se necessário uma regulação que descrevesse os padrões para utilização e tratamento destes dados, ressalta-se que não somente é necessário para a proteção dos dados em si, mas principalmente que as empresas, a partir dela mudem sua política interna, e haja uma nova tendência entre as empresas.

Os reflexos da modernidade tecnológica afetam diretamente o Brasil, uma vez que de acordo com pesquisas realizadas pelo Hootsuite We Are Social Report 2019, ele é o segundo país que mais passa tempo conectado, outrossim, uma pesquisa realizada pela Fundação Getúlio Vargas de São Paulo, relatou que o Brasil possui mais de 230 milhões de aparelhos celulares ativos, além de contar com mais de 149 milhões de usuários de internet.

Como resposta a esse contexto mundial, entrou em vigor no Brasil, em agosto de 2020, a Lei Geral de Proteção de Dados, LGPD - Lei 13.708/2018, responsável por estabelecer padrões de tratamento de dados no Brasil. Imprescindível ressaltar que a lei é extraterritorial, ou seja, qualquer empresa que lide com tratamento de dados no Brasil deve estar em conformidade com as diretrizes, implementando políticas internas para utilização dos dados, tal como a capacitação de seus colaboradores.

O não cumprimento das normas estabelecidas é punível com sanções administrativas, que podem ser desde advertência, multa, ou até mesmo o bloqueio ou eliminação dos dados a que se refere a infração. E não somente a empresa se prejudica através destas penalidades mas também, põe em cheque a reputação da empresa com seus usuários, assim como sua imagem.

Entretanto, há que se dizer que não somente basta a criação de uma legislação, haja vista que o mais importante é que ela seja de fato efetiva. Ou seja, apenas sanções nunca foram responsáveis por garantir o cumprimento da legislação, como exemplo, há que se mencionar que se assim fosse, não haveria população carcerária. Portanto, é necessário que além de imposto uma regulação às empresas, que a partir dela a organização mude sua política interna, e haja uma nova cultura entre elas.

A partir desse contexto e da entrada em vigência da norma regulamentadora pela proteção de dados, LGPD, todos aqueles que lidam com tratamento de dados, seja órgão público ou privado, necessitam se adequar, mas não somente com o intuito de evitar sanções, mas sim de se adequar ao mercado corporativo que hoje exige a conformidade com estes regulamentos, uma vez que não se adaptar é seguir em um caminho contrário à modernidade.

Deste modo, surge um ambiente no qual as empresas necessitam reaver suas políticas internas com o fim de se adequarem à norma. As empresas passam então a mudar sua cultura interna através de programas de *compliance* e de uma governança efetiva, visando a criação de regras de boas práticas e estabelecendo procedimentos de instrução, mitigação de riscos e normas de segurança.

Uma vez que a instalação desses é feita dentro da empresa e atinge o fim de refletir como uma cultura interna da corporação, ela passa não somente a observar as diretrizes impostas pelo Poder Público, mas sim, de assumir um papel de protagonista neste âmbito, fazendo com que haja uma auto regulação.

Em suma, uma vez que a sociedade moderna exigiu que o Direito iniciasse seu processo de tutelar as relações no âmbito digital, foi necessário que as empresas se adaptassem a esse feito. Para seguir o mesmo fluxo do mundo, já que diversos países já estão legislando a respeito do tratamento de dados, no Brasil esse acontecimento gerou grande repercussão, e cabem às empresas modernizarem-se conforme o restante do mundo. Todavia, para passarem por essa mudança, há a necessidade de uma governança efetiva e um bom programa de compliance, de forma a manter a empresa sob a legalidade.

**1.1 GOVERNANÇA EFETIVA:**

Conforme citado, convém ressaltar os aspectos mais importantes a respeito da governança corporativa, sendo esta, de acordo com a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) “um sistema segundo o qual as corporações de negócio são dirigidas e controladas”, sua estrutura é distribuída entre os direitos e deveres dos participantes da corporação, ademais, é definido também as bases dos objetivo da empresa, tal como os meios para que se alcance esse objetivo.

**1.2 PROGRAMAS DE *COMPLIANCE:***

Não somente basta a existência de uma governança corporativa, faz-se necessário que haja um mecanismo para que a empresa estejam em conformidade com a lei vigente, por conta disso, surge os programas de *compliance*, fazendo uso das palavras de Marcos Assi (2013), é “um sistema de controle interno que permite esclarecer e proporcionar maior segurança aqueles que utilizam a contabilidade e suas demonstrações financeiras para análise econômico-financeira.”. De modo prático e didático diz-se que compliance são ações colocadas em prática voltadas a garantir relações éticas e transparentes entre empresas.

Apesar de intimamente ligados, *compliance* e governança efetiva não são sinônimos, a compliance, também chamada de programas de conformidade ou de cumprimento, são utilizados para controle da observância de preceitos legais e éticos, enquanto que a governança corporativa possui mais comprometimento com as questões ligadas a reputação e as relações entre *stakeholders* internos e externos.

O compliance tem como principal objetivo proteger as empresas, tanto públicas como privadas, de violar os princípios que norteiam as atividades empresariais, assim como também, preceitos éticos e previsões legais vigentes. Advém ressaltar que ela não atua somente no escopo da prevenção, uma vez que também é responsável por auxiliar na orientação às empresas em que houveram essa violação, conduzindo-as de volta à legalidade e normalidade.

O Conselho Administrativo de Defesa Econômica (CADE) descreve o compliance como “um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores.”. Eles também enfatizam que esses programas não buscam somente ser uma série de procedimentos, mas sim, uma forma de mudança da cultura corporativa, tornando-o efetivo de fato no momento em que esta cultura é impregnada nos colaboradores, de forma a incutir neles a importância de seguir os procedimentos de forma correta.

Através de mecanismos básicos, há como chegar em um efetivo programa de compliance, sendo eles;

1. Avaliação contínua de riscos e atualização do programa;
2. Elaboração de Códigos de Ética e Conduta, que regulam a forma como se deve atuar na pessoa empresa; organização compatível com o risco da atividade;
3. Comprometimento da alta administração; autonomia e independência do setor responsável pela supervisão do programa de compliance;
4. Treinamentos periódicos;
5. Criação de uma cultura corporativa de respeito à ética e às leis;
6. Monitoramento constante dos controles e processos instituídos pelo programa de compliance;
7. Canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes;
8. Detecção, apuração e punição de condutas contrárias ao programa de compliance.

Em vista disso, surge o seguinte questionamento: como tudo isso se relaciona com a LGPD? Simples, *compliance* são programas voltados a realizar o enquadramento das normas e práticas na empresa em conformidade com a legislação, portanto, uma vez que foi necessário que as empresas adequarem-se a nova norma, a compliance facilitou esse processo através de seus mecanismos.

Imprescindível mencionar que ela não trabalha somente ao adequar às normas da empresa em conformidade com o imposto pelo Estado, ou seja introduzindo na cultura da empresa as boas práticas LGPD, mas também é função dela orientar quando erros que podem prejudicar seriamente a empresa acontecem. Ou seja, sua atuação não é exclusiva à prevenção, uma vez que ela estende-se ao cuidado com a imprudência, caso ocorrida.

**1.3 BOAS PRÁTICAS LGPD:**

Considerando que o compliance tem como objetivo adequar a empresa às boas práticas LGPD, questiona-se o que são essas práticas e como elas se alocam dentro da empresa. Portanto, entre todas as práticas, há que se mencionar as principais:

## Realizar um mapeamento de dados: conhecer o ciclo dos dados a que se tem acesso, é uma das principais práticas, haja vista que para proteger algo, a princípio é necessário conhecer exatamente o ele é, como se encontra, onde se inicia e qual é seu fim.

## Investir em Privacy by Design: a principal proposta do Privacity by Design, é justamente juntar a privacidade e a proteção das informações sob todo o desenvolvimento, desde a sua concepção.

## Manter um registro das operações de tratamento: Manter um registro é de suma importância, uma vez que órgão governamentais podem a qualquer momento solicitá-los, no caso do Brasil é cabível ao ANDP (Autoridade Nacional de Proteção de dados), garantindo que a empresa encontra-se comprometida com o correto tratamento de dados de seus clientes.

## Elaborar o Relatório de Impacto à Proteção de Dados Pessoais: Também chamado de RIPD, este documento trata-se de um relatório que deve ser elaborado pelo controlador sempre que o processo de tratamento de dados possa gerar riscos à liberdade dos titulares dos dados.

## Anonimizar dados quando possível: Conforme solicitado pela LGPD “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”.

## Investir em Segurança da Informação: Esta não é somente uma boa prática, mas sim uma exigência, conforme a LGPD.

## Escolher parceiros comprometidos com a proteção de dados: Ao escolher parceiros que sejam compatíveis com as normas exigidas, é possível evitar colocar a empresa em risco, para tanto, é necessário estabelecer critérios de avaliação e exigir que as medidas de tratamento de dados e privacidade sejam devidamente cumpridas.

## Atender os direitos dos titulares de dados: Deve-se estabelecer um processo de resposta às requisições dos titulares, além de também necessitar de um canal de comunicação com estes, inclusive deve ser padronizada as respostas para cada solicitação, assim como critérios para recusar ou aceitar as requisições.

## Criar um protocolo de resposta a incidentes envolvendo dados pessoais: o protocolo baseia-se em um passo a passo de como agir em um hipótese da empresa vivenciar um incidente envolvendo ferimento da LGPD. Este, deve ser baseado nas proprias determinações da LGPD, a qual estabelece o modus operandi dessas situações.

## Treinar e conscientizar a equipe: através de uma equipe com pessoas conscientes da legislação vigente, e que trabalhem de acordo com elas evita que erros ou vazamentos ocorram, desse modo, é perceptível como esse tópico é importante, haja vista que todos dentro da equipe tem que atuar conforme a legislação, outrossim, um erro com o tratamento de dados, ainda que cometido por apenas um funcionário, refletirá sobre toda a empresa.

Imprescindível ressaltar que o governo federal lançou uma cartilha para fins de orientação aqueles a quem desejam seguir as boas práticas LGPD, nesta, ele descreve com detalhes de forma ilustrativa e prática as medidas necessárias que a empresa deve tomar para que esteja em conformidade com a legislação vigente. É possível encontrar no site do Governo Federal, no seguinte link <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd>.

Portanto, uma vez que a sociedade evoluiu ao ponto em que as pessoas mantêm seus dados mais importantes em bancos de dados de empresas, fez-se necessário uma legislação que protegesse o titular, tanto de abusos realizados por empresas, quanto do vazamento desses dados. Exalta-se como a informação passou a ter valor no mercado, e tudo que possui valor, é alvo de desejos maliciosos, em vista disso, não é incomum empresas serem alvo de hackers, na tentativa de furtar esses dados. Por consequência, surge no Brasil a Lei Geral de Proteção de Dados, com o intuito principal de proteger esses titulares. Entretanto, uma vez que não somente basta a criação da norma, e sim que essa de fato seja efetiva, programas de compliance auxiliam as empresas nessa adequação para as boas práticas LGPD, com o intuito de que as empresas possam esta em conformidade com a legislação vigente, além de ir de encontro com as principais corporações , as quais já fazem jus a essas boas práticas.

**LGPD NO MERCADO CORPORATIVO E SEUS IMPACTOS:**

Durante os últimos anos houve uma mudança de chave extremamente importante, uma vez que o valor oferecido aos dados passou a crescer cada vez mais, observa-se que as riquezas em outros séculos advinham principalmente de terras, ouro e até mesmo petróleo, entretanto, nas últimas duas décadas o bem de maior valor passou a ser os dados. Verifica-se que as cinco maiores empresas atualmente são Google, Apple, Microsoft, Facebook e Amazon, e elas possuem exatamente um ponto de convergência, que é o tratamento de dados, ressalta-se que elas desbancaram as empresas de maior riqueza, tal como, as grandes petroleiras.

Convém ressaltar que ao introduzir valor às informações, ela também passa a ser alvo, principalmente de hackers que os buscam para fins maliciosos.

Na Europa, após relatórios de espionagem e violação de dados de clientes envolvendo a Cambridge Analytica e o Facebook, iniciou discussões sobre regulamentos de segurança de dados, que inspiraram a formulação do Regulamento Geral de Proteção de Dados (GPDR), que regulamenta a União Europeia e impunha Medidas para aprovar a legislação sobre segurança de dados pessoais (RAPOSÔ, 2019).

Com o volume de pessoas que possuem acesso a internet e a utilizam com frequência, cada vez mais as empresas passam a possuir dados importantes sobre a vida de seus usuários, desde nome, endereço, até cartões de crédito. Em vista disso, tornou-se necessário que as empresas cuidassem de forma adequada dessas informações, uma vez que podem ser usadas de forma errônea, e desse modo, violar os direitos da personalidade das pessoas.

Uma vez exposto a importância da existência de uma legislação que proteja os dados das pessoas, faz-se de suma importância que as empresas e corporações adequem-se a elas. A Lei 13.709/2018 Lei Geral de Proteção de Dados, disserta em seu 3º artigo a respeito da aplicação da mesma, e aqueles a quem esta deve ser enquadrada.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Uma vez ocorridos diversos escândalos a respeito do vazamento de dados, aquelas corporações em que ao usuário é garantido a proteção de seus dados pessoais, acaba por transparecer confiança, e adquiri vantagem competitiva nesse mercado.

A LGPD afetou diretamente as empresas, visto que a partir dela as empresas e corporações necessitam alterar seus regimentos internos, além das mudanças para adequar-se à norma e entrar em conformidade com as boas práticas da LGPD.

Importante repassar as principais alterações que serão realizadas dentro do mercado corporativo;

1. Aquisição de clientes: É de suma importância que os dados que forem utilizados para a captação de novos clientes tenha sido devidamente autorizados;
2. Manutenção dos clientes: uma vez que haja necessidade de uma manutenção nos dados do usuário, este deve ter prévia autorização do titular;
3. Portabilidade: Dentro do princípio de que os dados não são de posse da empresa e sim do titular, o mesmo pode solicitar a transferência de seus históricos para outras empresas, conforme desejar;
4. Controle: Os tratamentos de dados devem ser devidamente controlados, de forma a que possa ser livremente consultado pelo titular quando assim desejar.
5. Criação de uma política de segurança: As empresas passam a necessitar de uma eficiente política de segurança da informação, com o propósito de evitar possíveis vazamentos ou tratamento incorreto dos dados.

Entretanto, sob uma ótica global, a importância da LGPD não se limita a essas questões, uma vez que não garantir a proteção de dados é o mesmo que ir contra todo o mercado corporativo global. A partir do momento em que o Brasil legisla e protege sob seus cuidados esse tratamento, é seguir de acordo com o mercado internacional, e desse modo, ser atrativo para investidores internacionais.

Outro ponto importante a ser mencionado a respeito do tratamento de dados é como a LGPD também abriu um nicho corporativo extremamente relevante, ora visto que, a quantidade de empresas que realizam tratamento de dados é extremamente significativa, e com o advento da Lei em vigor estas começam a buscar por sistemas operacionais que garantam essa proteção, para estarem de acordo com as boas práticas do código referido. Desse modo há um crescimento nas áreas de sistemas de tratamento de dados, designers que realizem de forma correta a manutenção de suas interfaces, além de juristas que passam a adaptar-se para conseguir dar suporte a essas empresas, auxiliando-os a fim de que estejam de acordo com compliance.

Desse modo, houve a necessidade de as empresas adequarem-se às normas da Lei 13.708/2018, de modo a alterarem políticas internas, criarem protocolos de segurança e políticas de privacidade. Entretanto, não apenas esse foi o impacto, uma vez que, já era esperado que houvesse a necessidade de regular o cuidado com os dados particulares das pessoas, mas sim, o significativo nicho de mercado que abriu-se a partir dele, não somente as empresas tiveram que adaptar-se, mas todos aqueles a quem haviam contato com essa empresa, indo desde os acionistas até mesmo os funcionários.

Portanto, é possível enumerar todos os grandes impactos no mercado corporativo, desde as alterações nas políticas internas das empresa, tal como, o surgimento de grandes empresas com o intuito de auxiliar nas práticas LGPD, em vista disso, apesar das mudanças no cenário corporativo, não deve ser esquecida a importância da regulamentação, uma vez que, não há possibilidade de evoluir sem mudanças estruturais.

**A IMPORTÂNCIA DA IMPLEMENTAÇÃO LGPD EM UMA EMPRESA:**

A revolução tecnológica trouxe diversas mudanças na sociedade, entre elas, o aumento da quantidade de pessoas que passam a ter acesso a internet, a partir desse fato, de forma proporcional, houve o aumento da quantidade de informações que as empresas têm acesso a respeito das pessoas que fazem uso da mesma.

É imprescindível ressaltar que, há uma grande importância quanto ao valor que os dados possuem na sociedade em que as pessoas estão expostas, há que se mencionar a quantidade de informações que as empresas possuem a respeito de cada pessoa, e de como isso pode facilmente ser transformado em abusos, descriminação entre outros.

Escândalos recentes sobre vazamentos de dados de empresas como Facebook, Netshoes e Uber deixaram expostos dados pessoais como nomes, endereços, números de cartões de crédito e colocaram em evidência os efeitos devastadores da falta de rigor com a segurança no tratamento de dados pessoais. Portanto, existe uma grande necessidade de adotar mecanismos eficazes para evitar possíveis vazamentos e garantir a segurança dos dados (FERNANDES, 2019).

Após diversos escândalos envolvendo vazamento de dados, ou uso indevido dos mesmos, tornou-se evidente como esta falta de cuidado com os dados coloca as pessoas mais vulneráveis em risco. Por conta disso, fez-se necessário que, no mundo todo, houvesse a criação de normas que regulam o tratamento dos dados que as empresas têm acesso, de modo a evitar que outros casos aconteçam.

Outra mudança extremamente importante passou a existir após os casos relatados, sendo esta, a reputação que empresa possui quando não existe uma correta cultura a respeito da proteção de dados, uma vez que, dados importantes ficam expostos, como fotos, cartões de crédito e documentos. Desse modo, as pessoas começaram a entender como essas informações são importantes e deixam de colocá-las em risco. Empresas que não se adaptam à norma passam a possuir uma reputação duvidável, e abdicam de passar uma imagem de confiança a seus usuários.

Destaca-se, não somente esses tópicos relatam a importância de estar em conformidade com a LGPD, uma vez que, há o intuito de evitar as sanções administrativas que a legislação impõe, sendo elas: advertências, multas, ou até mesmo bloqueio e exclusão dos dados a que se refere a infração, conforme regulado pelos artigos 52, 53 e 54 da Lei nº 13.709/2018.

Entretanto, não somente basta uma legislação vigente para que a ordem seja restaurada, tendo em vista que, se dessa forma fosse não haveriam criminosos. Portanto, muito além de evitar uma sanção administrativa, as vantagens de se adequar a norma vão desde a credibilidade e confiança adquiridos pelas empresas, que resguardam seus usuários de um possível risco, mas também possuem uma alta vantagem competitiva no mercado corporativo.

Portanto, as vantagens daqueles que encontram-se em conformidade com a LGPD vão desde evitar penalidades, até possuir vantagem em um mercado tão competitivo como é o corporativo.

**i. Segurança da informação e acessos tecnológicos;**

Com o intuito de que haja uma correta regulação das empresas nos parâmetros estabelecidos, há que se ressaltar os principais mecanismos a que esta faz jus, entre eles a Segurança da Informação(SI), a que é definida por Stallings como: “ a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação incluindo hardware, software, firmware, informações, dados e telecomunicações (STALLINGS, 2015).”

Tendo a informação como algo valoroso, o SI tem como função garantir a proteção destes contra qualquer ameaça ou acesso não autorizado, com a finalidade de minimizar possíveis danos e manter a continuidade dos negócios em ambientes corporativos.

Por conta disso, há a necessidade de criação de uma política de segurança da informação, com as medidas que devem ser tomadas quanto ao tratamento dos dados, a fim de garantir a segurança dessa informação.

Algumas práticas são recomendadas, sendo elas:

1. Reveja a forma em que dados pessoais são armazenados, utilizando senhas em planilhas sempre que possível e mantendo os dados físicos em locais seguros, com chave;
2. Registre a identificação de visitantes em áreas reservadas;
3. Use senha nos computadores e usuários diferentes para acessos de pessoas diferentes, mesmo que utilizem o mesmo computador;
4. Defina quais pessoas dentro da instituição necessita acessar informações mais críticas;
5. Programe o bloqueio do computador quando não estiver em utilização;
6. Não deixe senhas acessíveis em post-its, embaixo do computador ou em local de fácil visibilidade;
7. Altere as senhas periodicamente;
8. Evite deixar documentos com dados pessoais expostos a quem não precisa ter acesso a eles, em especial dados sensíveis;
9. Descarte adequadamente os dados que não são mais necessários. CVs devem ser triturados, mídias devem ser destruídas e backups devem ser verificados para eliminar completamente uma informação desnecessária.
10. Dados físicos devem ser rasgados ou triturados. Não reaproveite-os

para fazer rascunho;

1. Faça uso de redes de wi-fi confiáveis;
2. Se possível, invista no uso de um antivírus para rastrear possíveis ameaças aos computadores da entidade;
3. Nos casos em que for possível, anonimize ou criptografe os dados.

Seus três pilares são, a confidencialidade, uma vez que os dados estarão dispostos somente aqueles com autoridade para isso, integridade, ao garantir que os dados permanecerão íntegros até o fim de sua utilidade, e disponibilidade para que esses estejam disponíveis em qualquer momento, não havendo hiato.

**ii. Como fazer Tratamentos de Dados;**

Havendo na modernidade uma necessidade de as empresas serem responsáveis por tomar medidas que protejam os dados de seus clientes, indaga-se a questão de, como deve ser este tratamento com os dados. No Brasil, a Lei nº 13.709/2018 - LGPD, discorre acerca do tema, estipulando em seus artigos 5º a 15º a respeito do tratamento ideal que deve ser transferido aos dados.

A princípio, faz-se necessário entender o conceito do termo “tratamento”, o qual a referida lei define como:

Art. 5º Para os fins desta Lei, considera-se:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Portanto, uma vez definido “tratamento de dados” como as operações que uma empresa realiza com os dados de uma pessoa, é necessário definir os aspectos mais importantes a serem considerados para que este seja feito de forma correta, baseando-se em boas práticas, seguindo princípios específicos e pré definidos no art 6º da LGPD.

Há princípios como a finalidade, adequação e necessidade que limitam a utilização de dados com base em seu propósito, ou seja, os dados só podem ser coletados quando houver objetivos previamente definidos e devidamente formalizados.

Também é tutelado como princípio, o direito da pessoa a que se refere os dados de terem livre acesso a essas informações, ou seja, a empresa deve conseguir responder como estes dados foram coletados e como são utilizados, havendo também a possibilidade de solicitar a exclusão dos mesmos. Estes a que se referem são chamados de princípios do livre acesso, qualidade dos dados e transparência.

Uma vez definidos princípios que regem o propósito e transparência, há que se mencionar aqueles que asseguram a proteção desses dados, o qual deve garantir que apenas aqueles, que são devidamente autorizados, tenham acesso aos dados, tal como também, que estes não sejam usados com propósito de discriminação.

Há que se mencionar os princípios da responsabilização e da prestação de contas, os quais regem a respeito da comprovação de execução das medidas necessárias, utilizando de artifícios como relatórios e documentos.

Uma vez que definimos os princípios da LGPD, conceitua-se os quatro pilares da LGPD, sendo estes: Proteção à Privacidade, transparência, padronização, e segurança jurídica, é necessário entender a quem essa norma se aplica e de que forma.

Titular: pessoa física, consumidor a quem os dados pertencem;

Operador: Pode ser uma empresa ou pessoa física que seja responsável por realizar o tratamento e processamento dos dados pessoais, estando este, sob as ordens do controlador.

O Controlador: também pode ser uma empresa ou pessoa física, este é encarregado de coletar dados e tomar decisões relativas à forma e finalidade do tratamento dos dados. Ele além de coletar, também controla o uso dos dados e por quanto tempo fica sob domínio da empresa.

O Encarregado: é indicado pelo controlador, responsável pela comunicação entre as partes envolvidas, também fica a seu encargo, orientar os funcionários do controlado a respeito das práticas com o tratamento de dados as quais devem ser seguidas.

Uma vez que definido as partes envolvidas, é necessário conceituar o que a lei entende por dados:

Dado pessoal é toda informação relacionada à pessoa natural identificada ou identificável” (artigo 5º, I, da Lei 13.709/18, já atualizada para 13.853/19), ou tudo o que pode identificar uma pessoa – números, características pessoais, qualificação pessoal, dados genéticos etc.

Dados pessoais: informações ligadas à pessoa física, para a identificação da mesma, como CPF, RG, data de nascimento, número da CNH, entre outros;

Dados sensíveis: informações particulares de cada indivíduo, ou seja, que trazem um entendimento mais profundo e complexo de quem é a pessoa. Nesse caso, estamos falando de informações como orientação sexual, gostos e preferências, opinião política, religião, entre outras informações mais detalhadas.

Visto que, definidos os conceitos e princípios, segue a questão. "Como realizar o correto tratamento de dados?”

O primeiro processo, trata-se da coleta de dados, faz-se necessário que o usuário autorize o uso e tratamento de seus dados para aquela empresa; esta autorização deve ser feita através de uma linguagem o mais clara e objetiva possível. Uma vez autorizados, é necessário mantê-losem posse da empresa, portanto, deve ser realizado um mapeamento dos dados, mapeando-os de forma a identificar: quais dados são esses, qual a origem deles, onde estão armazenados e qual sua finalidade.

Tendo como base a correta captação e armazenamento desses dados, é preciso definir que, após atingido sua finalidade, conforme determinada, é necessário definir como estes dados serão excluídos, uma vez que deve ser feito de forma correta, seguindo a legislação vigente.

Faz-se imprescindível o treinamento da equipe, uma vez que, é essencial que eles possam entender e participar ativamente do processo, mantendo-os incluídos, e não somente deixando que sejam observadores do processo, além de também garantir que não cometam erros que levem a um vazamento de dados ou algo do gênero.

Por fim, é preciso ressaltar que a base de dados deve ser segura, garantindo a proteção da pessoa titular dos dados, portanto, é necessário mantê-lo seguro, e caso haja compartilhamento de informações, esta só deverá ser realizada com a devida autorização do tutelado.

Entretanto, caso haja um vazamento de dados, o controlador deverá avisar à Agência Nacional de Proteção de Dados e ao titular dos dados, a ocorrência de um incidente de segurança.

Em suma, ressalta-se como essas práticas são importantes para manter os dados seguros, uma vez que, sendo tratados de forma correta, a possibilidade de submeter o titular destes em risco torna-se baixa, e ainda quando ocorrido, é imprescindível que aqueles a quem foram exposto ao risco sejam devidamente informados em tempo hábil.

**iii. Interface de Dados / Uso de EDI / Blockchain;**

**Interface de Dados :**

Uma vez que a LGPD começou a vigorar, a partir de Setembro de 2020, as empresas começaram a se adaptar às normas no tocante ao tratamento de dados, principalmente levando em consideração os princípios da norma. Nesse contexto, houveram diversas mudanças que devem ser mencionadas, como a alteração na interface de dados de diversas empresas, a utilização de EDI e também o Blockchain.

Baseando-se nos princípios da transparência, segurança e informações no tocante ao tratamento de dados, convém ressaltar como a interface de diversas empresas passaram por alterações para adequar-se a norma, a exemplo disso, citamos a política de privacidade dos sites, Newsletter, Formulários e Gestão de Cookies.

Para se adequar à norma a empresa deve ser transparente com o titular dos dados, para que este fique plenamente ciente do motivo da empresa precisar dessa informação, em seus formulários passaram a possuir uma tooltip, na qual é detalhada o motivo da exigência daquele dado.

Também se menciona a respeito das Newsletter, a que além do usuário necessitar consentir o recebimento dessa, é exigido um detalhamento do tipo de email que ele irá receber, de forma que aconteça da maneira mais transparente possível, respeitando os direitos do titular dos dados.

E quanto a política de privacidade do usuário? Tendo em consideração o consentimento da pessoa, necessita que além de essa autorização ser realizada, que ela seja feita de forma simples, e que o titular entenda do que se trata de fato. Entretanto, este é um dos desafios quanto a realização deste feito, uma vez que de acordo com a legislação, ao usuário caberia entender sobre a gestão de cookies além de necessitar saber para que cada um deles é utilizado. Entretanto, tal feito ainda é inviável a grande parte dos usuários, uma vez que eles preferem por aceitar a gestão dos cookies, sem ler o regulamento, para que possa dar prosseguimento ao que estava fazendo.

Portanto, é perceptível que ainda há diversos caminhos a serem percorridos quanto a questão, mas as empresas estão se adaptando a essa nova realidade a que são todos expostos, que cada vez mais ocorre uma universalização das políticas de privacidade, este papel é refletido principalmente para os designers, que estarão em contato com uma nova realidade para criação de sites e hospedagens.

**Uso de EDI:**

Seguindo o princípio da segurança, nos conformes da LGPD, diversas empresas adotaram o uso do intercâmbio eletrônico de dados, comumente chamado de EDI. Uma vez que se encontram integradas nos conformes dos programas de compliance. Suas funções são diversas, principalmente a de integralização dos dados, havendo assim um intercâmbio eletrônico de dados, o que trata de uma comunicação entre empresas de documentos de negócios de forma padronizada. Desse modo, substitui-se os documentos em formato físico, ou seja em papel, para documentos em bancos de dados compartilhados entre aqueles que necessitam.

Inegável que documentos físicos apresentam uma maior chance de erros causados pelo processamento manual. Por conta disso, hoje diversas empresas se adaptaram à modernização desses processos, garantindo uma maior segurança, agilidade e confidencialidade aos dados.

Em vista disso, há que ressaltar os benefícios ao utilizar o EDI, sendo eles a economia de tempo e dinheiro, uma vez que processos automatizados substituem aqueles anteriormente executados manualmente. Há também melhora na eficiência e produtividade, por meio da economia de tempo e precisão a que tudo ocorre. É possível perceber também uma redução nos erros, uma vez que o EDI cria também padrões a serem seguidos, reduzindo que as informações sejam enviadas de forma errônea.

Ressalta-se que através dele há também uma grande melhora na rastreabilidade e na elaboração de relatórios, tendo em vista que estando os dados de forma eletrônica, abre margem para que ocorra uma integralização a diversos sistemas de TI, com propósitos de coleta, visibilidade e análise de dados.

Entretanto, não é simples de ser implementado nas empresas, uma vez que ocorre a necessidade de a empresa possuir uma governança efetiva, de modo a se manter em conformidade com as atualizações necessárias em regulamentações governamentais, padrões e atualizações. Seja em um ambiente local ou terceirizado, há algumas condições básicas e recursos necessários para a implementação eficaz do EDI. Além de fatores como o entendimento sobre os tipos de documento, os métodos de transmissão seguros e o hardware e software necessários.

**Blockchain:**

Diante de todo o contexto de modernização, não há como deixar de mencionar o blockchain, comumente conhecido como a plataforma do bitcoin. Entretanto, apesar de ter tido seu início com ele, pouco se limita realmente a ele, haja vista que a plataforma tem possibilidades de ascender em diversas áreas.

Convém ressaltar que o bitcoin foi a criptomoeda que houve um crescimento e valorização gigantesca, mas como de fato funciona a plataforma que suporta essa moeda? O sistema garante registros públicos, entretanto não há como saber quem são os titulares do negócio, uma vez que ele garante criptografia. Deve ser lembrado que não há possibilidade de desfazer qualquer operação realizada.

Mas afinal, essa plataforma é realmente segura? Esse é um questionamento extremamente válido, entretanto, ao entender como a plataforma funciona, não há dúvidas que é uma das formas mais seguras. O crescimento do blockchain é visível, uma vez que pela sua confiabilidade ele tem atraído a atenção de corporações e até mesmo instituições governamentais.

Através dessa plataforma que apresenta um mecanismo no qual ao mesmo tempo em que é transparente é seguro, as possibilidades são extremamente expansivas, uma vez que empresas já tem enxergado nela uma maneira de compartilhamento e armazenamento de dados de forma segura e eficaz.

Apesar de ser muito conhecida no mercado financeiro, de forma a estar em crescente crescimento, uma vez que ela passa a se tornar um seguimento válido a fim de evitar as fraudes assim como também as altas tarifas bancárias.

A partir desse contexto, as possibilidades são inúmeras, convém a nós citarmos o armazenamento e compartilhamento de registros de veículos e imóveis, documentos pessoais, prontuários médicos, certificados e históricos dos mais variados tipos.

Entretanto, questiona-se se ele está relacionado com a LGPD, uma vez que ela é o tema principal da nossa pesquisa. Mas a relação entre eles é simples, considerando que uma plataforma justa, que garante segurança aos dados, capacidade de mapeamento e uma disponibilidade mundial, ela se torna um excelente seguimento para investimentos futuros a fim de investimos na criptografia de dados.

Em suma, há que se mencionar que em um contexto de novas possibilidades no Brasil, com o advento de uma legislação a qual cobra transparência e segurança com os dados de seus usuários, o blockchain torna-se cada vez mais atrativo em atividades que vão muito além das criptomoedas, visto que cada informação é possibilitada de capacidade de mapeamento e autenticação. Seus princípios de segurança, acessibilidade e altíssima disponibilidade, tendo em vista que os dados estariam presentes no mundo todo.

**iv. Políticas Internas de Proteção de Dados:**

Tendo em consideração a necessidade de as empresas se adequarem às novas diretrizes impostas pelo Estado, é necessário ressaltar que dentre as mudanças exigidas, e seguindo como princípio as boas práticas LGPD, fez-se necessário a elaboração de uma política de privacidade nas empresas,.

A criação deste,fez-se necessária, posto que se inclui dentro do programa de compliance, a fim de que a empresa fique em conformidade com a lei, e portanto, é aconselhável que essa política de privacidade seja feita com acompanhamento jurídico qualificado, uma vez que esse profissional será capacitado para não somente verificar a legalidade acerca da LGPd, mas também de outros escopos que podem colocar sua empresa em risco.

Nesse contexto, é necessário mapear os dados a que a empresa tem acesso, uma vez que havendo a finalidade e bases legais que legitimam o tratamento de dados, ou seja as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade.

Uma vez definido o mapeamento dos dados, é de suma importância que a política de privacidade cumpra seu efetivo papel, ou seja, as pessoas precisam entender e compreender o que está sendo apresentado, desse modo é recomendado uma linguagem clara e objetiva, evitando o excesso de formalidades, e normas exageradamente cultas, uma vez que se espera que todos entendam, ou seja que repasse o que a empresa quer demonstrar, e uma linguagem apropriada é essencial para que se cumpra objetivo proposto.

Além de elegibilidade, é necessário que haja disponibilidade dessa política, ou seja, que os usuários tenham acesso a ela. Desse modo, o princípio de transparência com os dados das pessoas, cumpre-se de forma a realmente exercer seu papel, uma vez que o usuário deve concordar com a política, mas deve entender o que isso significa.

Portanto, definiu-se como deve ser apresentada, mas não obstante é necessário conceituar o que deve conter nela, em vista disso, faz-se necessário que haja em seu conteúdo os principais tópicos, conforme esclarecido, de maneira clara e precisa;

1. Informar ao usuário a respeito das informações referentes a organização a quem ficou-lhe conferido o tratamento dos dados.
2. Quais os dados pessoais e a finalidade do tratamento deles, inclusiva daqueles que não foram informados pelo titular;
3. Sua base jurídica para o tratamento;
4. Informações de contato do *Data Protection Officer* (DPO) ou encarregado de proteção de dados da organização.

Existem informações que caso sejam aplicáveis, devem estar contidas também, sendo essas:

1. Sobre compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais;
2. Sobre transferência internacional e qual a finalidade;
3. Sobre o tratamento por legítimo interesse;
4. Sobre o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular;
5. Sobre decisões automatizadas;
6. Sobre a proteção de dados de menores de idade;
7. Sobre a proteção dos dados sensíveis.

Ressalta-se que mesmo quando estes não forem o caso de estarem contidos, que o transcreve de forma explícita.

Outro tópico de extrema importância, é a respeito da disponibilidade dessa política, já que pautada no princípio da transparência, é garantido ao titular dos dados que ele possa consultar seus dados, desse modo, dentre os tópicos abordados na política, deve haver um que oriente o usuário como deve ser realizada, quando este assim desejar, alterações, retificações ou exclusão dos dados.

Importa-se mencionar quanto ao uso de cookies, mas geralmente ele pode ser encontrado em um arquivo separado, a política de cookies.

Por fim, uma vez conferido legitimidade a esta política, é importantíssimo que ela seja apresentada ao usuário, antes que seja realizada a coleta ou tratamento dos dados, pois ele deve concordar e autorizar que assim seja realizado. Além de constituir,essa política deve estar localizada de um modo que esteja com fácil acesso para que quando o titular assim desejar, possa consultá-lo, o último tópico a ser observado, é a importância de manter disponíveis as versões anteriores de controle de políticas.

Em suma, através do desenvolvimento acerca do tema, é imprescindível não mencionar a importância da política de privacidade para uma empresa que deseja adequar-se a LGPD, tal como os programas de compliance. Ressaltando que esta deve ser feita com o acompanhamento jurídico, haja vista que há a necessidade de que especificidades sejam devidamente cumpridas. Quando feita de forma correta, havendo todos os tópicos necessários, ela assegura ao titular dos dados de que suas informações serão devidamente tratadas.

Através dela é garantido o princípio da transparência ao usuário, lhe sendo assegurado que seus dados serão utilizados conforme sua autorização. Muito além dese adequar à legislação vigente, à política de privacidade que garante confiabilidade à empresa, estabelecendo uma relação de confiança com seus usuários.

**SANÇÕES DA LGPD:**

Através da fiscalização, responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD), as empresas poderão sofrer auditorias com a finalidade de garantir que a empresa está de acordo com a LGPD, e que os dados estão sendo tratados com seriedade, conforme legislação vigente.

A Lei nº 13.709 - LGPD traz consigo em seus artigos 52, 53 e 54 os aspectos referentes às sanções quando feridas suas normas. Há que se mencionar que as sanções são administrativas sendo o autor penalizado de acordo com a gravidade do fato, podendo ser advertências, multas pelo faturamento, ou até mesmo o bloqueio dos dados a que se refere o descumprimento, conforme disposto no art 52:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

VIII- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

IX- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Ressalta-se ainda que, em seu §1º, ela discorre quanto a intensidade da penalidade que poderá variar sob diversos fatores tais como, a gravidade, a boa-fé do infrator, a vantagem a que obteve o infrator, condição econômica, reincidência, grau do dano, adoção de procedimentos internos, políticas de boas práticas e governança, pronta adoção de medidas corretivas e por fim a proporcionalidade entre a gravidade e intensidade da sanção.

Salienta-se que as penalidades não se restringem em um âmbito administrativo,sendo a empresa exposta por sua falha nos cuidados com as informações das pessoas, sua reputação é posta em cheque com seus usuários, passando a perder a confiança deste.

As sanções realmente ferem a empresa tanto de forma econômica quanto sua reputação, a exemplo disso, cita-se o ocorrido pelo Grupo Raia Drogasil, a qual refere-se a uma rede de farmácias espalhadas pelo Brasil. Entretanto, ocorre que ao coletar a biometria dos clientes e também a autorização dos clientes quando aos termos de politica e privacidade, contudo, nada disso foi informado aos usuários, disseram a eles que eram para o benefício do desconto. Ao analisar a íntegra do ‘Termo de Consentimento de Uso de Dados Pessoais’, o Procon verificou que a autorização permitia ao grupo Raia Drogasil coletar e utilizar os dados pessoais e de comportamento de compra de produtos obtidos em seus canais de atendimento como sites, aplicativos, televendas, SAC e lojas. Diante das denúncias, o PROCON Mato Grosso, multou em R$ 572.680,71 o Grupo Raia Drogasil.

É imprescindível não dizer da importância de estar de acordo com a LGPD nos dias de hoje, principalmente com o abrangente conhecimento e acesso às informações que as pessoas possuem.

Em suma, confirmado pela auditorias que houve uma falha no tratamento de dados, o órgão responsável poderá abrir um processo administrativo para que a empresa sofra as penalidades aplicadas na LGPD, estas serão sempre proporcionais ao dano causado, entretanto, sabe-se que há fatores que podem ser intensificadores, como a reincidência, mas também há aqueles em que permite uma sanção mais branda, como a aplicação de medidas para evitar que algo do gênero ocorra novamente.

**CONCEPÇÃO DE NOVOS PRODUTOS E SERVIÇOS COM O PRINCÍPIO DE PROTEÇÃO DE DADOS:**

A partir da última década houve uma mudança muito significativa no mercado, pois o bem de maior valor passou a ser os dados, considerando que a modernidade levou as pessoas a se adequarem ao modelo de consumo imposto, ou seja, dados pessoais passam a cada vez mais serem guardados em bancos de dados.

Houve diversos exemplos que podemos basear nossa pesquisa, mas iniciaremos com a CNH, que passou de um documento impresso a um documento digital, o qual é disponibilizado através de um aplicativo de celular. Outro exemplo muito relevante para maior parte das pessoas, é o documento do veiculo, deixando de emiti-lo de forma manual, e passando a ser feito de forma digital, da mesma maneira que a CNH.

Menciona-se um advento em que nem todos possuem acesso, mas é extremamente relevante, que é NFC, através dele você deixa de precisar do seu cartão de crédito físico por meio do celular, é possível realizar os pagamentos na maquininha de cartão.

Inegável a existência da importância de proteger esses dados, sendo que em mãos maliciosas, o titular dos dados estaria sujeito a um risco indescritível. Para assegura-lo, a LGPD - Lei 13.708/2018 através de princípios e estabelecendo boas práticas LGPD, para que entes públicos ou privados, estejam em conformidade com o correto tratamento de dados.

Através de todos esses acontecimentos, um novo contexto surge, um mercado que oferece produtos para que as empresas possam estar em conformidade com a legislação vigente.

Um exemplo muito explícito desse feito é o chamado “privacy by Design”, ele é um framework com uma proposta de incorporar a proteção de dados pessoas em todos os escopos desenvolvidos pela empresa, desde o início e seguindo-o até o fim. Ele tem um objetivo claro de garantir a privacidade do usuário, e ainda podem ser aplicados sob qualquer ecossistema de informação, o que o torna extremamente versátil.

Ainda sobre ela, menciona-se seus 7 princípios, sendo eles:

1. Proativo, e não reativo; Preventivo, e não corretivo: ou seja, possui atuação na prevenção, evitando multas ou mesmo gastos excessivos quando acontece um erro;
2. Privacidade como padrão, Privacy by Design é que a privacidade deve ser sempre a configuração padrão em qualquer sistema ou mesmo prática de negócio, não exigindo qualquer interação ou configuração por parte do usuário. Ou seja, o indivíduo não precisa agir para adotar configurações de privacidade mais restritas: elas já vêm embutidas de forma padrão no produto, tecnologia ou serviço.
3. Privacidade incorporada ao design; Este princípio coloca a privacidade como incorporada ao design e à arquitetura de sistemas de TI e práticas de negócio. Ou seja, a privacidade é um componente essencial do sistema, sem diminuir sua funcionalidade.
4. Funcionalidade total; A metodologia do Privacy by Design também procura evitar a existência de falsos dilemas, como privacidade versus otimização. A ideia é acomodar todos os interesses e objetivos legítimos da organização, e não apenas os relacionados à privacidade. O objetivo principal é somar e permitir a funcionalidade total do sistema ou projeto, trazendo benefícios e resultados para todos.
5. Segurança de ponta a ponta; Outro princípio essencial do Privacy by Design prevê a adoção de medidas robustas de segurança, protegendo os dados coletados durante todo seu ciclo de vida. Ou seja, da coleta, uso, acesso e armazenamento até o seu descarte.
6. Visibilidade e transparência; Um dos objetivos da metodologia Privacy by Design é garantir que a organização, tecnologia ou negócio de fato opera segundo o que promete. A transparência é, portanto, um ponto fundamental do PbD, e permite estabelecer responsabilidades e confiança.
7. Respeito pela privacidade do usuário: o último princípio do Privacy by Design foca no respeito pela privacidade do usuário. É preciso sempre manter os interesses do usuário acima de tudo, oferecendo configurações fortes de privacidade, informações claras e opções user-friendly.

Portanto, é muito perceptível como o produto se adequam as boas práticas LGPD, e eles parte desse exato seguimento de que com a necessidade das empresas estarem adequadas, um novo mercado emerge.

Entretanto, o mercado de softwares não foi o único que se expandiu, o mesmo também ocorreu com designers gráficos, que se especializaram no assunto, a fim de evitar que a empresa cometa erros durante uma coleta de dados pela internet por exemplo,portantoele deve colocar as informações a vista e de forma clara para o usuário.

Iniciou-se também, um mercado jurídico a respeito da norma, sendo advogados especialistas em direito empresarial que passam a orientar empresas como trabalhar estando em conformidade com a lei. Orientam a respeito das mudanças necessárias, como proceder, que medidas cabíveis tomar quando por ventura houver um vazamento de informações.

Portanto, proporcional ao quanto havia necessidade da norma, para que os direitos fundamentais da pessoa fossem devidamente resguardados, houve também um crescente mercado, com a criação de novos produtos e especialistas auxiliando nessa mudança, podendo ser claro mencionar a concepção de novos produtos nesse nicho de mercado.

**O DIREITO DIGITAL E A LGPD**

Durante as duas últimas décadas, a internet mudou a vida das pessoas, uma vez que passa a vigorar a modernização da vida desses indivíduos, através desse advento, processos foram automatizados, e tornaram-se mais simples, documentos passam a ser digitalizados, não mais necessitando carregá-los e até mesmo cartões abrem espaço para o NFC.

As mudanças ocorridas com o advento da expansão da tecnologia não afetam somente os usuário e aqueles que trabalham diretamente com ela, pois houve diversas consequências com esse crescimento, principalmente na última década, quese encontra em constante evolução, e é necessário que as pessoas se adaptem a ela, contudo, ressalta-se, não somente elas devem moldar-se para estarem introduzidos na sociedade, e sim, tudo o que a engloba.

Todas essas mudanças tiveram consequências no âmbito legal, sendo necessário uma legislação que protegesse as pessoas de terem seu direito da personalidade ferido, tendo em vista que a exposição de modo a entregar seus dados para essas empresas, o titular dos dados necessita que seja garantido o devido cuidado com eles, evitando que aconteçam situações como vazamento, furtos ou até mesmo que façam mal uso deles.

No mundo todo foi iniciado o processo de legislar quanto ao tratamento de dados, inclusive, no Brasil, a chamada Lei Geral de Proteção de Dados, a vista disso, empresas necessitam atualizar diversos aspectos para estarem de acordo com a legislação e evitar sanções advindas do descumprimento.

Muitas profissões sofreram mudanças ao se adaptarem ao novo mercado, o qual exige cada vez mais conhecimento a respeito de assuntos relacionados à internet. Na mesma proporcionalidade em que certas profissões se extinguiram, novas profissões surgiram e outras tiveram severas mudanças.

Nesse contexto, dentro das diversas profissões, cita-se o ramo do Direito, o qual está sempre em processo de adaptação para se adequarem às necessidades a que lhe são conferidas. Os códigos sempre visam proteger algo”, seja a pessoa, a personalidade dela, empresas, entre outros. Ressalta-se que desde que o Direito surgiu, ele passou por mudanças, de tal modo que revogações acontecem com muita frequência, sempre se adaptando.

A fim de se incluir nesta adaptação, surge uma nova área do Direito, chamada, Direito Digital, que se responsabiliza por tratar dos assuntos relacionados à internet pelo mau tratamento dos dados das pessoa que pode haver abusose resultar no ferimento dos direitos das pessoas. Em vista disso, percebe-se a importância de legislar a respeito, uma vez que crimes podem ser cometidos e devem sofrer as devidas sanções.

Através do Direito Digital, e dos profissionais qualificados, as empresas iniciaram o correto protocolo para tratamento de dados, considerando-se que as maiores empresas do mundo se encontram classificadas no tocante a tratamento de dados. É um mercado em expansão e está em processo de constantes mudanças, juntamente com a sociedade moderna, sempre visando a se adaptarem.

Em suma, entende-se que com as atualizações que acontecem no mundo, principalmente no tocante a tecnologia, o Estado necessitou intervir, de modo a legislar com o fim de proteger o titular dos dados, contra as corporações que fizeram mau uso desses. A LGPD deu espaço para o crescimento de diversas áreas, o qual profissionais escolheram se especializar sobre o do tema, ressaltando ainda o crescente crescimento desses profissionais, uma vez que existe uma alta demanda de empresas que buscam por esses serviços.

1. O Direito Digital:

Diante das mudanças apresentadas pela sociedade, o direito estabeleceu novas diretrizes, uma vez que é imprescindível que ele esteja em conformidade com o presente momento a que as pessoas estão expostas. Desse modo, iniciou-se uma discussão acerca da atualização da legislação, para que esta continue refletindo de forma a proteger sob seu escopo as pessoas.

No Brasil, já era de conhecimento que as leis precisavam de atualizações, entretanto, um caso ocorreu e para a época foi tema de grande repercussão. Ocorre que uma atriz deixou seu computador sob os cuidados de uma empresa de manutenção, entretanto, ao ter acesso aos dados particulares, o técnico tomou posse de fotos íntimas e a chantageou, ameaçando expor os conteúdos sob posse dele. A atriz chama-se Carolina Dieckmann, o caso foi entregue às autoridades e a partir desse acontecimento observaram a necessidade de proteção dessas pessoas, em vista disso, entrou em vigor a lei n º12.737/2012, a qual possui como apelido Lei Carolina Dieckmann.

O caso relatado, é apenas um dos diversos que acontecem, por conta disso, o Direito têm atualizadas as diretrizes em sincronia com as mudanças que ocorrem na sociedade, regulando a fim de evitar que casos como esse ocorram. Abordando sobre o tema, é perceptível como além da internet abrir caminhos antes não imagináveis, como encontrar e ver alguém do outro lado do mundo na tela do celular, ou comprar diversos produtos em país estrangeiros e chegar na porta da casa, ela abriu portas para um novo caminho da ilegalidade, os crimes cibernéticos, como o que aconteceu a Carolina Dieckmann.

Desse modo, surge uma necessidade para que haja uma base jurídica que proteja as pessoas, o poder Legislativo brasileiro a passos curtos vem realizando as mudanças, tais como, o Marco Civil da Internet, a Lei do E-commerce e a que ficou mais conhecida, a Lei Geral de Proteção de Dados - LGPD. Ressalta-se que não é exclusivo do Direito Brasileiro, uma vez que todos os países estão adaptando suas leis para esse novo mercado.

No Brasil, a Lei nº 13.708/2018, Lei Geral de Proteção de Dados, foi um marco muito relevante, uma vez que ela afetou diretamente todas as empresas, desse modo, elas precisaram se adequar para que estivessem dentro da legalidade.

Em vista das diversas mudanças na legislação, surgiu uma demanda por uma área jurídica denominada de Direito Digital. Uma nova vertente do Direito especializou no assunto, de maneira a estudar como as empresas devem agir para que não colocassem em risco a personalidade das pessoas, através de um acompanhamento jurídico.

Entretanto, há uma grande demanda quando mencionada à área, visto que ainda há muita insegurança jurídica acerca do tema, considerando que ainda há escassez de normas a respeito, outros tópicos também são relevantes, como por exemplo o fato de a tecnologia estar em constante evolução e ser inserida de forma tão rápida pela sociedade, o que dificulta o Direito de acompanhar a evolução. Nesse caso, o mais recomendável é que as normas não sejam específicas, e sim que possuam uma abrangência maior, de maneira a tentar tutelar a maior parte das condutas ilícitas.

Uma vez que possui uma norma vigente, e pessoas, físicas ou jurídicas, que precisam estar em conformidade com elas, emerge uma nova área de trabalho para aqueles que desejam. Dos diversos modos que esse auxílio poderá vir, ressalta-se os principais, uma vez que ele pode agir de modo consultivo, contencioso, criminal, contratos ou até compliance.

Agir de modo consultivo, diz respeito à demanda acerca de empresas que precisam de consultas periódicas a respeito do tema, de modo que o profissional deve orientá-los a respeito das condutas no ambiente virtual, eles também auxiliam a zelar pela segurança digital da empresa.

Os profissionais contenciosos são aqueles que diante da necessidade, contestam acerca dos crimes cometidos, como desrespeito a direitos autorais, fake news, violação de privacidade, dentre outros. Entretanto, os crimes relacionados a área criminal como calúnia, difamação e roubo de dados são acometidos pelos profissionais da área criminal. Há também aqueles que trabalham de forma a realizar contratos seguindo as normas do direito digital e principalmente nas questões relacionadas a isso.

Por fim, o advogado de compliance, que são notadamente uma área muito crescente, devido a introdução da LGPD na legislação brasileira. Diversas empresas buscaram esses profissionais, a fim de se manterem incluídos na legalidade e evitar sanções a que estão sujeitas.

Em suma, diante de todo o contexto apresentado, o Direito Digital tem se expandido e conquistando espaço. Notadamente é uma área em desenvolvimento e que ainda precisa de estudos, entretanto, com grande potencial de crescimento,tendo em vista a expansão desenfreada da tecnologia. Com o passar do tempo, e com as pessoas dependendo cada vez mais das redes para sua vida, estar sujeito a ter sua personalidade violada não deve ser uma possibilidade, e para isso, deve-se o direito tutelá-la da melhor forma.

**A PEC 17/2019**

Desde o momento em que o Direito passou a existir, regulando o comportamento das pessoas que vivem em sociedade, ele sofreu diversas alterações, conforme entendido que ele deve estar em conformidade com as demandas do mundo e das pessoas, de forma a tutela-las da melhor maneira possível. Uma vez que a sociedade evolui para o ponto em que, pessoas são prejudicadas ou colocadas em risco por conta do mau uso, pelas empresas, dos dados privados das pessoas, surge a necessidade de a lei adaptar-se a essa nova realidade.

Nesse contexto, entrou em vigor no Brasil, no ano de 2020, a Lei Geral de Proteção de Dados, com o intuito de legislar a respeito do correto tratamento que as empresas devem oferecer aos dados de seus clientes. Alterando em diversos âmbitos a política de diversas empresas.

Entretanto, é entendido que somente a LGPD não garante proteção suficiente as pessoas, em vista disso, faz-se necessário, entender brevemente como funciona o ordenamento jurídico, tendo em vista que, há uma hierarquia de normas, estando a Constituição federal no topo da pirâmide, e o restante das leis abaixo dela, de forma que devem estar em conformidade e subordinadas a ela. Por conta desse ordenamento, entendeu-se a necessidade de constitucionalizar o direito à proteção dos dados das pessoas.

Para tanto, foi apresentado ao senado e aprovado por ele, a Proposta de emenda à constituição (PEC) nº 17/2019, a qual acrescenta ao rol dos Direitos Fundamentais, o direito de proteção de dados, tanto nos meios físicos quanto nos meios digitais, desse modo, deixando sob responsabilidade da União a função de legislar acerca do assunto, impedindo que novas leis que ferem esse direito vigorem.

A constitucionalização da proteção de dados garantiu a todos os brasileiros a proteção com o tratamento de seus dados como uma garantia fundamental, no mesmo patamar que a liberdade, o trabalho, a educação, entre outros direitos garantidos pelo art 5º da CF/88.

É questionável se uma vez com o advento da vigência da LGPD, a real necessidade de constitucionalizar esse direito. Nesse aspecto, o professor e advogado Antonio Carlos Freitas Júnior disserta: “"O rito da proteção já estava na LGPD. Tudo o que a sociedade poderia fazer caso tivesse seus dados violados, já estava nela. Porém, a PEC veio mais como um reforço e eleva esse status da proteção de dados para a mesma importância de outros direitos fundamentais".

A partir da constitucionalização da norma, há o impedimento de que novas leis contrárias a ela surjam, desse modo, se porventura ocorrer de criar-se uma lei contrária, o Supremo Tribunal Federal terá amparo e base legal para solicitar o anulamento."Com a previsão na Constituição, definitivamente se abrem as portas para o STF analisar eventualmente alguma violação a esse direito fundamental. Isso não é pouca coisa", destaca Bruno Bioni, consultor na área de regulação e tecnologia e diretor da Data Privacy Brasil.

Em suma, esse acontecimento é de extrema importância, ora visto que ao constitucionalizar esse direito, aplica-se real importância a ele, a partir desse feito, não apenas há uma lei a respeito dessa garantia, mas um embasamento constitucional sobre ela, deixando sob tutela do Estado a proteção dos dados e dos titulares dos mesmos.

**CONCLUSÃO:**

Diante dos diversos aspectos apresentados, notou-se que em vista da modernização crescente e desenfreada da tecnologia, a legislação não conseguiu acompanhar, de forma que, somente em 2020 houve a vigência de uma lei que protegesse realmente as pessoas de terem seus dados violados.

Entende-se que a urgência da Legislação, uma vez que o Brasil é um dos países que mais possui usuário de internet no mundo, além dos milhares de usuários de redes sociais.

A Lei Geral de Proteção de Dados, foi um marco muito grande, para todos aqueles envolvidos, isso desde os acionistas das empresas, quanto aos consumidores. Em vista disso, as empresas adaptaram-se de forma a tentar estar em adequação com as boas práticas da LGPD.

Para que isso ocorra, há diversos modos de estarem em conformidade com a Legislação, uma recomendação são os programas de compliance, os quais através de protocolos e treinamentos orientam as empresas que desejam regular-se de forma correta.

Diversos são os protocolos para o correto tratamento com os dados, incluindo mecanismos e programas que assegurem a privacidade dos titulares dos dados. Menciona-se que através da disposição das empresas, surgiram diversas novas carreiras, especializadas na internet, desde através da criação de softwares e até mesmo na área jurídica, a qual especialistas estudam e prestam consultoria.

As empresas adaptaram-se da melhor forma possível, através de consultorias e auditorias internas, a fim de evitar as possíveis sanções administrativas a que a LGPD impõe, mas também, com o intuito de evitar possíveis escândalos a respeito, uma vez que os usuários passaram a valorizar os seus direitos de privacidade e empresas com uma imagem duvidável passam a perder cada vez mais consumidores.

O tratamento correto dos dados, possui um peso tão importante na sociedade atual, ao ponto de que ele passou a ser um direito protegido pela constituição federal, no rol dos direitos fundamentais, haja vista que destacou-se sua importância e como a violação do mesmo deveria ser evitada e protegida sob escopo da União.

Em suma, a importância que os dados possuem na sociedade moderna é indescritível, por esse motivo, as empresas passaram por diversas mudanças a fim de adequar-se à norma vigente. Ressalta-se que não há evolução sem mudanças significativas, e que a proteção dos titulares dos dados é de suma importância, e a partir da PEC 17/2018 tornou-se um direito fundamental, devendo ser garantido e mantido sob proteção da União.