

Privacidade na internet e uso de dados de usuários

Introdução:

A importância que a informação assumiu após a era industrial, especialmente na época posterior à década de 1980, fez com que o século XX fosse denominado como a era da informação. Em decorrência dessa importância, a discussão em torno de como manter a segurança sobre essa informação que é gerada, se torna recorrente, especialmente com as tecnologias que envolvem a geração e o tratamento dessas informações.

A quantidade de informação gerada nos dias de hoje com as redes sociais, que crescem de maneira exponencial, traz à reflexão as consequências e os desdobramentos acerca da revelação desses dados tão íntimos da pessoa, que por sua vez os disponibiliza muitas vezes de forma espontânea na internet.

A parcela da informação que pertence ao indivíduo pode ser chamada de privacidade, que segundo Jhon Locke, é necessária para a própria liberdade. Os diversos sistemas de informação na internet hoje em dia proporcionam ataques de diversas maneiras à privacidade do ser, esses ataques são considerados, portanto, ataques à liberdade da pessoa.

A liberação de informações sobre a guerra do Iraque por parte do site Wikileaks, a revelação da rede de vigilância mundial estabelecida pelos Estados Unidos da América, denunciada pelo funcionário da CIA (Central Intelligence Agency) Edward Snowden, são exemplos de como nossos dados estão sensivelmente expostos na internet e como a linha entre o que é público e privado têm se tornado cada vez mais tênue.

Este artigo consiste em uma apuração acerca da privacidade e do uso de dados na internet, apresentando situações em que esse direito universal não foi respeitado e, a partir do levantamento desses dados, atingir um maior entendimento sobre o assunto. Utilizaremos como referencial para a análise, alguns dos princípios fundamentais da Doutrina Social da Igreja: Dignidade humana, subsidiariedade, solidariedade e bem comum.

Capítulo 1 - O uso de dados e o princípio da dignidade humana:

O Princípio da Dignidade humana é o princípio base que orienta e dá luz à Doutrina Social da Igreja (DSI), ele é o pilar para o desenvolvimento dos outros cinco princípios. Nele a Igreja postula que o homem é o sujeito e fim de toda vida social e portanto a inviolabilidade e integridade da vida humana são pontos de extrema importância e devem guiar as ações tomadas em sociedade.

Os vazamentos de dados na internet e as violações à privacidade colocam em risco a integridade da dignidade humana, já que expõem a sociedade dados pessoais e sensíveis do

usuário, que podem colocá-lo em posições desconfortáveis e até vexatórias. Temos como exemplo, o maior vazamento de dados nacional, ocorrido no início do presente ano (2021) e que expôs em fóruns da internet o CPF de mais de 220 milhões de brasileiros. Dados como este podem ser usados para diversas finalidades e trazer prejuízos aos seus donos. Exemplificando, caso as informações de um indivíduo forem expostas, o mesmo corre perigo de qualquer tipo de fraude, sendo um alvo fácil para golpes como: abertura de contas em seu nome, retirada de empréstimos sem seu consentimento ou até mesmo seu número duplicado, a fim de pedir dinheiro para familiares e amigos em suas redes sociais.

Com os recorrentes ataques e vazamentos acontecidos, a União Europeia criou uma regulamentação de proteção de dados que busca proteger a privacidade do indivíduo. A GDPR(Regulamentação Geral de Proteção de Dados) é válida para todos os membros do bloco e a toda e qualquer empresa ou organização que ofereça bens ou serviços que colem dados pessoais de residentes da União Europeia. Na prática, a GDPR é um conjunto de regras de controle de processamento de informações/dados pessoais que visa dar ao cidadão da União Europeia maior controle sobre seus dados pessoais.

As empresas adequadas à GDPR têm que garantir que os dados pessoais serão coletados de maneira legal e sob condições estritas e também que irão gerenciá-los de maneira a protegê-los de eventuais ataques ou usos indevidos. Com esse regulamento, as empresas são forçadas a garantir e respeitar os direitos do usuário, já que há uma penalidade para aquelas que não irem de acordo com as normas do documento. Tais medidas representam um conjunto de boas práticas nas atividades orientadas ao tratamento de dados pessoais.

Inspirada na regulamentação Europeia, foi sancionada em 2018 a LGPD (Lei Geral de Proteção de Dados), lei esta que tem o objetivo de regulamentar o uso de dados pessoais pelas empresas, de forma que os cidadãos brasileiros tenham mais segurança e controle sobre as suas informações fazendo uso de práticas transparentes e seguras, garantindo direitos fundamentais. Os principais objetivos da lei são: estabelecer regras claras sobre tratamento de dados pessoais, estabelecer regras únicas a respeito do tratamento de dados pessoais, por todos os agentes que fazem tratamento e coleta de dados, além de fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais.

Sob a ótica empresarial, é preciso considerar que as pessoas têm diferentes preocupações sobre privacidade. Dessa forma, as empresas devem seguir boas práticas de transparência e clareza quanto aos dados que coletam, de modo que o titular possa fazer suas próprias escolhas sobre como eles são utilizados, bem como, no caso de serviços online, oferecer ferramentas e configurações que permitam a implementação prática dessas escolhas feitas pelo titular.

Soluções como a LGPD e a GDPR atuam garantindo a proteção dos direitos da personalidade, assegurando a honra, a integridade física, a imagem pessoal e a intimidade de cada ser humano. Alinhado a isso, o Princípio da Dignidade Humana, discorre acerca da garantia das necessidades vitais de cada indivíduo, sendo sua imagem pessoal, seus dados e

informações, de essencial importância na constituição de um valor intrínseco ao ser humano. A inviolabilidade destas necessidades deve orientar todas as ações tomadas em sociedade. Dessa forma, ambas as regulamentações engajam-se pelo princípio da Dignidade Humana, já que atuam garantindo a dignidade e a integridade do ser humano.

Capítulo 2 - Privacidade na Internet: uma análise sob a ótica da subsidiariedade:

O princípio da subsidiariedade é considerado o terceiro pilar da Doutrina Social da Igreja (DSI) e tem por objetivo garantir o respeito à justa atribuição de cada uma das camadas da sociedade, de forma que, as camadas mais altas garantam o auxílio necessário e complementam as atividades realizadas pelas camadas mais baixas, sem interferir ou prejudicar o desenvolvimento de sua autonomia. De forma resumida, o termo subsidiariedade significa *ajuda* ou *socorro* e sugere que tudo aquilo que pode ser realizado pela sociedade deve ser incentivado e complementado pelos poderes públicos cabíveis.

Dessa forma, este importante princípio tem a função de equilibrar a liberdade em sociedade, reduzindo a intervenção do estado em certas instâncias sociais e instigando os poderes públicos a ajudar, coordenar e controlar as atividades destes grupos. Através de um estado com princípios subsidiários a valorização da pessoa torna-se algo mais recorrente, aguçando sua criatividade e sua consequente capacidade de gerar engajamento social e obras em sua comunidade, melhorando a realidade vivida no dia a dia das pessoas envolvidas.

A privacidade é um direito fundamental e inerente ao ser humano que serve de base para a personalidade e a liberdade de pensamento da pessoa. Garantir a privacidade nos meios digitais é, antes de tudo, garantir a integridade do usuário que tem seus dados coletados. Tal conceito vai de encontro com o Princípio da Dignidade, apresentado anteriormente. Em contrapartida, o Princípio de Subsidiariedade não se alinha às questões referentes à privacidade e coleta de dados na internet, já que não há uma colaboração por parte das empresas em tornar tais dados públicos e disponíveis a qualquer cidadão que deseje consultá-los, o que acaba prejudicando em alguns pontos a autonomia e a eficiência das ações das camadas mais baixas.

Um exemplo da não colaboração das empresas em tornar os dados coletados disponíveis ao público pode ser observado na nova política de envio de dados do aplicativo de mensagens *WhatsApp*. Neste caso, os usuários do *WhatsApp* que não aceitarem os novos termos que permitem o compartilhamento de dados com o *Facebook* e seus patrocinadores terão sua conta suspensa até concordarem com o contrato. A péssima novidade alcançou os usuários do aplicativo de forma gradativa, até interromper a navegação no aplicativo, impondo a leitura dos novos termos e notificando a data limite. Embora os dados compartilhados não incluam as mensagens em si, toda a agenda de contatos do celular, bem como foto de perfil e outras informações serão obrigatoriamente enviadas ao *Facebook*. Isso

chamou a atenção dos usuários, principalmente pela falta de opções fornecidas pelo aplicativo, o que distancia ainda mais as premissas do princípio de subsidiariedade.

Uma maneira efetiva para um melhor alinhamento com os princípios da subsidiariedade seria a implementação de legislações de proteção de dados, que forçariam as empresas a tornarem seus procedimentos mais transparentes e garantiriam o acesso aos dados dos usuários. Ao implementar um conjunto de leis deste tipo, a empresa torna-se mais confiável frente à sociedade, além de promover a conscientização quanto à proteção de dados em toda a internet. A GDPR e a LGPD são exemplos de legislações que trazem um grande benefício à população e evitam diversos vazamentos e incidentes cibernéticos.

A implantação efetiva da LGPD, por exemplo, pode trazer diversos benefícios à empresa, como maior segurança da base de dados, maior transparência, maior precisão, entre muitos outros, além de fazer com que a empresa coopere e auxilie durante o desenvolvimento de atividades pelas camadas inferiores da sociedade, o que corrobora com o princípio da subsidiariedade, tornando os cidadãos antes desinformados, em cidadãos cientes de seus direitos e mais conscientes quanto ao uso dos dados e a privacidade na internet.

Grande parte da população não tem noção alguma do quão perigoso é colocar seus dados em qualquer formulário na internet, essa falta de cuidado parte da falta de informação relacionada ao assunto, já que desde pequenos não somos instruídos e informados sobre. Muitos depositam total confiança de seus dados pessoais em sites e aplicativos que não fazem ideia de quem são os donos, aceitando termos de contrato sem mesmo ler com cuidado, se colocando em risco e compartilhando seus dados pessoais de forma indiscriminada. Uma outra solução idealizada pelo grupo é a de que para que isso deixe de ocorrer é necessário a conscientização da população acerca dos perigos da internet, assim como do seu uso de forma segura, instruindo desde cedo todos os cidadãos. Uma boa maneira para realizar essa instrução, seria por meio da implantação de cursos básicos de informática em todas as escolas, atentando sempre desde a base o quão importante é tomar cuidado com seus dados e sempre pensar duas vezes antes de informá-los.

4.1

João Pedro Rosa Cezarino - R.A: 22.120.021-5

Lucca Bonsi Guarreschi - R.A: 22.120.016-5

Vítor Martins Oliveira - R.A: 22.120.067-8

Murilo Gomes Munhoz - R.A: 22.120.035-5

4.2

Índice de comentários

- 4.1 Para finalizar, poderiam colocar como papel do Estado aqui favorecer e facilitar que esses cursos atinjam mais gente e essas instituições consigam fazer ainda melhor o trabalho que já fazem.
- 4.2 Bom capítulo, cumpriu o que foi pedido.