DARK PATTERNS: SERIA MESMO DISTRAÇÃO, OU O DESIGN FOI PENSADO PARA LUDIBRIAR?

Júlia de Moraes Custódio[1]
Henri Alves de Godoy[2]

DOI: 10.47283/244670492023110142

RESUMO

Este artigo tem como objetivo discorrer sobre as *Dark Patterns*, o termo criado por Harry Brignull sobre formas que web designers utilizam para induzir o usuário de um determinado *website* a aceitar, assinar ou adquirir produtos/serviços que ele não deseja, ou então, mascarar a concordância com o compartimento e obtenção de determinadas informações sem que o usuário seja claramente alertado sobre a forma com que as suas informações serão utilizadas. Ao final será feito um levantamento informativo, destacando três práticas que incentivaram as regras que foram incorporadas à Lei Geral de Proteção de Dados da União Europeia (GDPR) e posteriormente foram utilizadas de modelo na criação da Lei Geral de Proteção de Dados Brasileira (LGPD).
PALAVRAS-CHAVE: *Dark Patterns*. Engenharia social. Privacidade

ABSTRACT

This article intends to discourse about Dark Patterns, the term created by Harry Brignull about ways that web designers use to induce the users of a certain site or service to accept, subscribe or purchase undesirable products/services or to hide the agreement of sharing, collecting personal information without clearly informing the user how their information will be used. Finally, informative research will highlight three practices that motivated the rules that were incorporated into the general protection data from the Europe Union and afterward were used as a model for the creation of the Brazilian general data protection law.
***KEYWORDS**: Dark Patterns, social engineering, privacy*

INTRODUÇÃO

A Segurança da Informação baseia-se em três pilares, confidencialidade, integridade e disponibilidade, mas desde a popularização da *Internet* novos métodos têm sido criados para atacar esses pilares e obter ganho financeiro sob o acesso a informações confidenciais. Atualmente um tema que tem sido amplamente discutido é a Engenharia Social e as formas com que o ser humano tem sido usado como uma fraqueza de sistemas *on-line*.

Os usuários de qualquer sistema operacional com acesso a rede estão expostos à inúmeros riscos, e um desses riscos são as *Dark Patterns*, termo criado em 2010 por Brignull (2021) para elencar uma série de doze métodos e práticas que web *designers* tem usado para ludibriar seus usuários a aceitar produtos e serviços indesejados.

Estas doze técnicas e práticas serão exemplificadas seguindo a estrutura de tópicos, onde primeiro é trazido o nome em inglês, uma breve explicação, a situação problema escolhida por

[1] Tecnóloga em segurança da Informação. E-mail: julia.custodio@fatec.sp.gov.br
[2] Docente da Fatec Americana. E-mail: enri.godoy@fatec.sp.gov.br

Brignull (2021) para ilustrar o tópico e uma definição mais aprofundada com o detalhamento dos exemplos. A sessão de levantamento informativo sobre três *Dark Patterns,* que estiveram presentes na mídia internacional nos últimos anos, procura trazer novos exemplos da utilização das *Dark Patterns* e apresentar os impactos dessas práticas para o usuário comum, com situações de grande impacto na sociedade, pois essas técnicas estão presentes por toda a rede e saber identificá-las é um primeiro passo importante para que seja possível uma navegação segura. Ao final, considera-se que apenas um conjunto de leis em constante evolução pode acompanhar as exigências de segurança do ambiente *on-line*.

1 REVISÃO BIBLIOGRÁFICA

Conforme a tecnologia avança e a conectividade chega a todos os aparelhos eletrônicos dentro das casas, como *Smart TV*s, geladeiras, lâmpadas, travas eletrônicas nas portas, carros inteligentes que podem ser controlados pelo celular do dono, assistentes virtuais e afins, as discussões sobre a segurança dos usuários dentro da rede tornam-se cada dia mais necessárias.

Quais os riscos a qual estou exposto ao me conectar na *Internet* diariamente? Com tal exposição diária a *Internet* como que as nossas informações estariam seguras? Como podemos nos proteger de pessoas que viram na *Internet* uma nova ferramenta para cometer crimes? Essas são apenas algumas questões que se pode fazer ao navegar na *Internet* pelo aparelho celular.

Segundo o artigo de Foltýn (2018) sobre a superexposição à *Internet* e as mídias sociais, a incorporação da *Internet* à rotina da população trouxe novas vulnerabilidades, transcendendo as limitações físicas e chegando a uma forma totalmente nova de atacar e invadir a privacidade das pessoas e ter acesso às informações particulares.

A Segurança da Informação possui três conceitos fundamentais, confidencialidade, integridade e disponibilidade, mas como ficam esses três pilares no ambiente familiar e longe dos controles rigorosos adotados pelas empresas para proteger os seus bancos dados?

Machado Júnior (2018) define os três conceitos em sua tese de doutorado como: A confidencialidade diz respeito ao acesso da informação, permitir o acesso apenas para aqueles que possuem permissão para acessar a informação e a tornar inacessível a todos os outros. A forma mais comum de proteção de informação atualmente é a criptografia da informação, seja por métodos clássicos ou modernos. A integridade diz respeito à credibilidade da informação, garantir que os dados não tinham sofrido qualquer tipo de alteração e se mantenham completas e integras, pois, quebras de integridade de informação podem ser catastróficas para empresas e usuários. E por último, a disponibilidade que diz respeito a manter a informação sempre acessível para aquele que tem permissão para acessá-la.

E fornece alguns exemplos de como esses princípios são ameaçados pelos *cybers* criminosos, como os radares e sensores militares que protegem um país, que só são efetivos se fornecerem informações integras a todo momento. Os ataques de DDoS (*Distributed Denial of Service*), ou seja, negação de serviços médicos, comerciais ou até mesmo militares.

O grande desafio da Segurança da Informação segundo Coelho (2013) é incorporar à cultura das pessoas os riscos que o meio digital trouxe a sua rotina. Grandes empresas e corporações que atuam na *Internet* são sujeitas as legislações de proteção de dados de cada país onde fazem coleta de dados dos seus usuários, e essas empresas trazem nos termos de uso da plataforma uma descrição de quais são as suas obrigações com a segurança dos usuários, e seus deveres para proteger as informações que foram coletadas ou depositadas na plataforma. Leis como GDPR (*General Data Protection Regulation*), da União Europeia que entrou em vigor em

2018 serviu como modelo para a criação da Lei Geral de Proteção de Dados Pessoais (LGPD), são os parâmetros que as empresas internacionais seguem para determinar os seus termos de uso e proteção de dados.

No entanto, isso não quer dizer que utilizar o serviço de tais empresas isenta os usuários dos perigos da *Internet*. Vazamentos de dados com prejuízos milionários ainda acontecem de tempos em tempos e da mesma forma com que as empresas atualizam os seus *firewalls* e as suas camadas de proteção, novas vulnerabilidades surgem todos os dias junto com novas ameaças, vírus e táticas de ataque. Ao se navegar pela rede o usuário está exposto a vários perigos diferentes como sites clonados, *e-mails* de origem duvidosa, mensagens falsas em aplicativos de mensagens, *fake news*, e até a táticas de Engenharia Social, um conjunto de métodos e táticas utilizadas por pessoas mal-intencionadas para se apropriarem de informações confidenciais e sensíveis para obter algum tipo de lucro.

Henriques (2017), comenta que a Engenharia Social pode ser usada por qualquer pessoa e em qualquer lugar, não é algo restrito ao meio digital e explora persuasão, armadilhas psicológicas, padrões de comportamento, entre outros. Ou seja, fraquezas características ao ser humano para atingir os seus objetivos. Os ataques de engenharia social costumam seguir quatro etapas, como demonstrado na tese, que são a coleta de informações sobre um possível alvo, o estabelecimento de algum tipo de relacionamento com a vítima que é uma parte vital para o sucesso do ataque, a exploração deste vínculo com a vítima para levá-la ao estado emocional que o atacante deseja e a execução do ataque propriamente dito onde as informações que o atacante deseja são obtidas.

Alguns métodos utilizados pelos engenheiros sociais são bastante conhecidos e amplamente discutidos no âmbito acadêmico, como apresentado pelo trabalho de Henriques (2017), o *phishing*, método onde o *cyber* criminoso envia um *e-mail* para as suas vítimas se passando por empresas bancárias, serviços públicos, geralmente se utiliza o nome de empresas que vão atrair a atenção da vítima e nesse e-mail se pede que o usuário clique num *link* que vai redirecioná-lo para uma página infectada. Algumas vezes o anexo da mensagem, ou *link*, é um vírus e pode infectar a máquina do usuário, e não é incomum que esses *links* executem downloads de vírus para a máquina do usuário. O recomendado para que não se caia em ataques de *phishing* é sempre prestar atenção no endereço de *e-mail* do remetente do *e-mail* e procurar erros de digitação na mensagem, até mesmo um logo com uma letra na posição errada pode indicar um *phishing*, e caso desconfie, a melhor ação é deletar o *e-mail* imediatamente sem clicar em nenhum *link* ou anexo que possa ter.

Vishing é uma técnica muito similar ao *phishing*, mas é praticado através de ligações, como apresentado por Henriques (2017) no item sobre tipos de ataque de sua dissertação. O atacante liga para as vítimas se passando por alguém de uma empresa de *telemarketing* qualquer e tenta obter as informações da pessoa ao oferecer promoções enganosas, prêmios, ou então, dizendo que o cartão da pessoa foi clonado e ela precisa passar as suas informações para fazer o cancelamento do dito cartão.

O ataque de *Ransonware* esteve na mídia em 2021 com o ataque aos servidores da loja Renner, que ficou alguns dias com o sistema fora do ar. Esse tipo de ataque se caracteriza pelo sequestro do sistema, parte do sistema, ou banco de dados da empresa através de um vírus que faz a cifragem dos dados, depois do ataque o *cyber* criminoso entra em contato solicitando um pagamento para devolver os dados ou tudo será vazado na *Internet* gerando perdas enormes para a empresa.

Um outro método trazido por Henriques (2017) é o *tailgating*, mas essa tática é bem mais antiga do que a *Internet* e passou a ser usada por engenheiros sociais mais ousados para conseguir acesso a áreas que apenas pessoal autorizado tem acesso. O esquema é simples, seguir de perto um determinado funcionário que tem acesso ao local que se quer invadir e quando a pessoa for acessar esse local o engenheiro social aborda a vítima, se passando por um outro funcionário que se atrasou e está sem as credenciais, e pede passagem, conseguindo acesso a área restrita.

Esse é um bom exemplo de como os métodos de engenharia social não estão restritos ao ambiente digital, nem a uma única forma de abordar a sua vítima, seja pelas redes sociais, serviços de *e-mail* ou até mesmo no local de trabalho os riscos estão presentes a todo momento.

1.1 *Dark Patterns*

Com o pano de fundo sobre os riscos aos quais o usuário está exposto na *Internet* é possível aprofundar-se sobre as *Dark Patterns*. Doze métodos amplamente utilizados para a obtenção de vantagens em sites, criando armadilhas voltadas a vitimar todos os usuários e induzi-los a aceitar ou adquirir produtos, ou serviços que ele não deseja.

O termo *Dark Pattern*, foi criado em 2010 por Brignull (2021), PhD em Ciência Cognitiva e desde 2006 trabalha como consultor UX (*user experience design*), com clientes que incluem grandes empresas como *Spotify*, *Pearson* e *The Telegraph*. Ele também é o fundador do *Darkpattern.org*, um site voltado a conscientização do público sobre as *Dark Patterns* utilizadas por empresas de renome.

As *Dark Patterns* funcionam de maneira simples, como exemplificado por Brignull (2021), a forma com que a informação é apresentada ao usuário é levemente diferente do usual, pode ser o botão para fechar um *Add* deslocado para a esquerda com um ícone semelhante no lugar, mas que na verdade vai levá-lo para a página que está sendo destacada na propaganda. Pode ser um botão destacado com título vago que ao invés de sair entra no site indesejado, entre outros.

Um questionamento que pode ser feito é onde que a engenharia social se relaciona as *Dark Patterns* e essa relação está na forma com que ambos se aproveitam da experiência do usuário para tirar vantagem dele.

Conforme Marcondes (2017) exemplifica, um engenheiro social tentaria se aproximar da sua vítima de formas que para ela são familiares para uma comunicação segura com outros usuários da mesma rede, trabalhadores da mesma empresa e afins. E um designer que utiliza as *Dark Patterns,* conforme exemplificado por Brignull (2021), se aproveita da familiaridade do usuário com um determinado padrão de cores, botões, tamanho de fonte, entre outros, para manipular a sua navegação numa determinada página e induzi-lo ao erro.

Essas táticas não estão presentes apenas em sites duvidosos na *Internet*, em sua conta do *Twitter* Brignull (2021) posta diariamente novas táticas e ocorrências de *Dark Patterns* em sites de grande renome. Empresas como *Google*, *McAfee*, *Linkedin,* entre outros.

Em seu site, *Darkpatterns.org,* o autor destaca doze tipos mais comuns de *Dark Pattern*, e os exemplos são fáceis de encontrar navegando na *Internet*, mas não se restringem a apenas esses doze tipos por causa da amplitude da descrição do que são *Dark Patterns*.

O primeiro exemplo são as *Trick Questions*, numa tradução livre seria “Perguntas Enganosas”, e segundo a definição de Brignull são perguntas de formulários que num primeiro momento dão a entender que estão perguntando um tipo de informação, mas numa análise mais cuidadosa percebemos que a pergunta é sobre algo totalmente diferente. No exemplo trazido

pelo site *Darkpatterns.org*, podemos observar um formulário simples que pede algumas informações pessoais, o truque que caracteriza esse tipo de *Dark Pattern* está na parte inferior do formulário onde estão duas caixas de seleção.

A primeira caixa diz que o usuário deve selecioná-la se ele não quiser receber promoções e informações de produtos da empresa. A segunda caixa pergunta se o usuário deseja receber essas informações, só que, ao prestar atenção na mensagem escrita, na realidade o que está sendo oferecido são informações de empresas terceiras recomendadas pela primeira (Brignull, 2021).

O texto da caixa não é claro sobre quais informações estarão sendo enviadas para o usuário ao misturar quase as mesmas palavras da primeira caixa fazendo uma leve alteração no final, ela abre a possibilidade de que o usuário receba mensagens de todas as empresas terceiras que se relacionam a primeira e está é a armadilha representada por este tipo de *Dark Pattern*, onde algo que poderia ser de interesse do usuário que estiver preenchendo aquele formulário vira um pseudo consentimento para receber *spam* de todas as empresas terceiras que tem relacionamento com a primeira.

O segundo exemplo presente no *Darkpatterns.org* é o *Sneak into Baske*t, em português "Deslizar para dentro da cesta", são situações em que o usuário está fazendo uma compra on-line e algum item extra é adicionado ao carrinho de forma automática ou por algum tipo de caixa de seleção que o usuário precisa desativar, mas ela não fica numa posição clara para quem está efetuando a compra, como explicado por Brignull (2021).

Para exemplificar essa situação Brignull (2021) traz uma situação registrada no site do *GoDaddy*, uma empresa que vende domínios para sites. A situação é referente sobre a compra de um desses domínios conforme a promoção que estava sendo oferecida pelo site na época que as capturas de tela foram tiradas. A promoção oferece três domínios por 17 dólares, assim que a opção é selecionada já é adicionado ao carrinho uma opção de proteção de privacidade que custa 7,99 dólares e não tinha sido anunciada na página anterior. Quando o usuário chega a página para efetuar a compra o preço da promoção que estava sendo adquirida inflou até um total de 154,31 dólares, absolutamente diferente do que estava sendo anunciado na primeira captura de tela trazida por Brignull (2021).

Nesse meio tempo de alguns cliques várias informações deixaram de ser dadas ao usuário, por exemplo, a promoção se referia a uma compra de quatro domínios na realidade e em nenhum momento foi dito ao usuário que seria cobrado a taxa de proteção de privacidade para cada um desses domínios separadamente, ou seja, 7,99 vezes 4 foram adicionados ao carrinho, um total de 31,96 além do que o anunciado, mas como a conta chegou em 154,31 dólares? Outra informação que não foi passada ao usuário explica, ao contrário do que tinha sido anunciado na primeira página, uma taxa de dois anos de registro dos quatro domínios foi adicionada à compra, inicialmente tinha sido anunciado como apenas um ano de registro. Todas essas coisas que foram sendo adicionadas ao carrinho de comprar sem o usuário optar somadas ao valor dos domínios e as taxas chega ao valor de 154,31 dólares mostrado nas imagens, e configura o método de *Sneak Into Basket*. Ao final Brignull (2021) explica que este tipo de prática foi proibido no Reino Unido e nos países da União Europeia pela diretiva de proteção do consumidor [9].

Roach Motel é o terceiro exemplo no *Darkpatterns.org*, "Motel de Barata" em português é sobre uma situação que é muito fácil para se entrar, mas bem mais complicadas para sair. O exemplo que Brignull (2021) traz no site é sobre a compra de ingressos para um *show* que

possuía uma opção que precisava ser selecionada caso a pessoa não quisesse assinar uma revista. Aqui percebemos que temos o método de *Sneak Into Basket* associado a uma página que também irá praticar um outro método de *Dark Pattern*.

Neste exemplo, o *Roach Motel* se caracteriza quando o usuário é forçado a preencher um formulário de próprio punho e enviar por correio para a empresa que vendia os ingressos para desfazer a assinatura, dificultando muito para o usuário se desfazer do serviço que foi adquirido acidentalmente. O autor também pondera que uma situação de demorou alguns segundos para se consolidar precisa de até algumas semanas para ser desfeita, dependendo do serviço postal da região onde a pessoa reside. Esse é o princípio do *Roach Motel*, a dificuldade do cliente em desistir ou cancelar um serviço que ele não desejava obter, ou que ao ser obtido não atendeu as expectativas.

O *Privacy Zuckering*, nomeado por Jones (2010), por causa do *CEO* do *Facebook* Mark Zuckerberg, é uma situação em que a pessoa é enganada a compartilhar muito mais informações pessoais do que era a intenção. Segundo Brignull (2021) esse termo foi cunhado, pois no começo do *Facebook* os termos e condições de uso não informavam sobre a coleta de informações que era feita pelo site. Era muito fácil para algumas permissões de uso de dados passarem batidas, outras ficavam deslocadas em áreas incomuns do site ao invés da página de configuração de privacidade.

No ano em que o termo foi cunhado várias mudanças ocorreram no *Facebook*, como adição de novas funcionalidades que expunham ainda mais as informações dos usuários, o que gerou uma grande reação contrária da comunidade e até mesmo uma investigação criminal como Jones (2010) argumenta em seu artigo *Facebook's "Evil Interfaces"*.

Brignull (2021) explica que atualmente aconteceram várias mudanças nos termos de privacidade do *Facebook*, mas o termo *Privacy Zuckering* continuou e agora é utilizado mais para as empresas que comercializam informações pessoais na *Internet*.

Price Comparison Prevention, numa tradução literal “Evitar a Comparação de Preços” é um método utilizado pelo comerciante para dificultar que o cliente faça a comparação dos preços de dois itens e acabe fazendo uma compra mal-informada. O exemplo trazido neste caso é o de uma página de uma rede de supermercados europeia, e temos o mesmo item, a maçã, apresentada de duas formas, um avulso com o valor relacionado ao peso da fruta e ao lado um pacote com seis maçãs que traz o preço por unidade.

Para poder fazer a comparação neste caso, o cliente precisaria saber o preço médio de uma única maçã para achar o valor desta unidade na oferta por quilo e poder comparar com o valor da unidade reunida no pacote, isso cria uma dificuldade imensa na comparação dos valores da maçã e o cliente pode ser levado a fazer uma escolha pelo produto mais caro mesmo que em ambos os casos ele estaria comprando maçãs.

Segundo Brignull (2021) este método era mais comum no começo dos anos 2000 na Europa, entre operadoras de celular, mas ainda acontece atualmente como no exemplo que ele apresentou no site.

Misdirection, ou em português “Desorientação” é quando o *design* de um site é feito propositalmente para fazer com que o visitante do site preste atenção em um item do site e não no outro. Para exemplificar sobre como esta *Dark Pattern* funciona Brignull (2021) traz o exemplo de um site de venda de passagens aéreas. O site é bem colorido, com propagandas, promoções e a parte para a escolha do voo, com origem e destino e até este momento não temos nada fora do comum.

A *Dark Pattern* começa após a seleção do voo, quando o cliente é direcionado para uma página de seleção de assentos. Nesta página o usuário pode escolher o assento onde ele quer viajar, a página tem várias propagandas oferecendo mais espaço para as pernas e outras coisas durante o voo. O que a página não informa claramente ao usuário é que um assento já foi pré-selecionado para ele com a adição (escorregado para dentro do carrinho de compra) de uma taxa de 4,50 dólares, e se o usuário não quiser selecionar o assento, mas não estiver realmente prestando atenção no site ele vai acabar pagando essa taxa extra sem ter feito a escolha, caso o usuário faça a escolha por um assento nesta página, a taxa sobre para 9 dólares.

No final da página de seleção de assento há um grande botão laranja para se continuar para a próxima página, se o usuário estiver prestando bastante atenção ele vai notar que abaixo desse botão existe um link para pular a seleção de assento, essa é a única opção para o cliente não pagar a taxa extra de 4,50 dólares.

Aqui a tática é desviar a atenção do usuário com o grande botão laranja, para que ele não perceba que o link para pular a seleção de assento está ali. Caso o cliente não perceba, e não tenha selecionado um assento ele ainda vai pagar a taxa, pois um assento já foi pré-selecionado para ele.

Brignull (2021) ainda coloca uma conta breve feita com as informações fornecidas pela empresa de vendas de passagens aéreas que mostra que com esse esquema a empresa pode ter até 1 milhão de dólares de lucro extra no ano com a venda das passagens só com essa taxa escondida de 4,50.

Hidden Costs, ou "Valores Escondidos" fala sobre um método onde o cliente faz todo o processo de compra e na última etapa para efetuar o pagamento ele percebe que novos valores foram adicionados a compra, como taxas de entrega ou outros valores do tipo. O exemplo trazido por Brignull (2021) é o de um site de venda de flores e durante todo o longo processo de compra de um dos produtos o valor mostrado é exatamente aquele do item selecionado, na última etapa de confirmar a compra, já tendo colocado as informações pessoais e de cartão de crédito é que aparece a taxa de entrega e de manuseio das flores que não tinha sido mencionado em nenhum outro momento no site.

O autor comenta que depois de todo o processo de compra, o mais provável é que a pessoa acabe finalizando a compra mesmo depois de ter visto que valores inesperados foram adicionados à compra, mais por cansaço de já ter passado por toda a etapa de compra e não desejar recomeçar a busca pelo produto em outro site.

Embora muito similar a tática de escorregar coisas para dentro do carrinho de compras, os valores escondidos não são produtos ou serviços extras para o comprador, eles são taxas que estão embutidos no serviço sem serem declarados ao cliente e elevam o custo do produto que foi escolhido.

Uma outra tática dentro dos websites é o *Bait and Switch*, numa tradução livre Isca e Troca, é quando você acessa um site esperando determinado serviço, mas completamente diferente e indesejado acontece. No *Darkpatterns.org*, Brignull (2021) traz um exemplo de 2016, quando a *Microsoft* quis que os seus usuários trocassem de sistema operacional para o *Windows* 10.

Segundo este autor, tudo começou com um *pop-up* amigável que sugeria a mudança do sistema operacional, mas conforme o ano foi passando a empresa começou a ficar bem mais agressiva com a sua mensagem chegando ao ponto de trocar o significado do botão de fechar do *pop-up* para aceitar a atualização, o que gerou uma grande reação pública dos usuários do sistema Windows.

Confirmshaming, ou numa tradução livre "Envergonhar durante a escolha", é o ato de envergonhar o usuário a ponto de influenciá-lo a aceitar determinado serviço, item ou o que estiver sendo ofertado. Conforme o exemplo apresentado por Brignull (2021), isso acontece fraseando a opção de recusa de forma a fazer o usuário se sentir envergonhado por desistir do que está sendo ofertado e acabar aceitando.

Disguised Ads, ou "Propaganda Disfarçada" é uma tática de disfarçar propaganda no site ou na navegação do site para induzir o usuário a clicar nessas propagandas. O exemplo trazido por Brignull (2021) é do site *Softpedia*, um site para o *download* de *softwares* que traz nas páginas dos *softwares* que ele disponibiliza anúncios que possuem botões chamativos de *download*, mas não são sobre o *software* que o usuário deseja, este está numa aba secundária, o que pode causar confusão e vários cliques acidentais nos anúncios.

Forced Continuity, ou "Continuidade Forçada" é quando algum serviço que possui um período de teste gratuito não avisa o usuário que este período acabou e começa a cobrar o serviço pelo cartão de crédito cadastrado. Para ilustrar essa prática Brignull (2021) traz como exemplo o site de uma empresa internacional de programa de fidelidade, neste caso tudo funciona muito bem até a página de confirmação da compra onde uma propaganda disfarçada com a mesma fonte e o mesmo esquema de cores da página onde se está navegando traz um botão de continuar, caso o usuário clique neste botão ele será levado a uma página que vai tentar convencer o usuário a se cadastrar para receber um *voucher* de vinte euros de desconto.

Se o usuário se inscrever ele acaba fazendo uma assinatura mensal de 15 euros que continua para sempre, que é uma outra tática de *Dark Pattern* que já apresentamos, *Bait and Switch*. Brignull (2021) também afirma que em vários fóruns e artigos as pessoas afirmam apenas perceber a inscrição depois de notarem cobranças estranhas nos cartões de crédito e comenta que nos Estados Unidos essa empresa já foi multada várias vezes e ainda responde a diversos processos civis por causa das suas práticas subversivas.

Friend Spam, é quando um site ou serviço pede o *e-mail* ou rede social do usuário sobre o pretexto de encontrar amigos, mas na realidade ele começa a enviar mensagens de *spam* para os contatos utilizando o nome do usuário. Para ilustrar esta *Dark Pattern,* Brignull (2021) traz um exemplo do *LinkedIn* que no ano de 2015 foi condenado a pagar 15 milhões de dólares por causa desta prática.

Como parte do processo de se inscrever no *LinkedIn* era perguntado se o usuário gostaria de compartilhar os seus contatos do *e-mail*, sob o pretexto de fortalecer o "*networking*" profissional do usuário, só que ao conseguir essa permissão de acesso o *LinkedIn* começava a disparar e-mails para todos os contatos do usuário como se ele estivesse convidando essas pessoas a participarem do *LinkedIn* e não como mensagem da própria empresa.

3 LEVANTAMENTO INFORMATIVO

3.1 *Privacy Zuckering* e o escândalo de privacidade do *Facebook*

Quando Jones (2010) escreveu seu artigo comentando as interfaces malignas do *Facebook*, a regulamentação das mídias sociais ou até mesmo da *Internet* de forma geral ainda estavam no processo de elaboração. Naquela época, a venda de informações pessoais era um mercado que gerava algo em torno de 200 bilhões de dólares, como demonstrado por um infográfico disponível no site *Darkpatterns.org*.

Neste mesmo ano Van Buskirk (2010) trouxe em sua reportagem para o site WIRED, um *tweet* publicado por Nick Bilton, na época o líder do *The New York Times Bits Blog*, dizia que numa conversa informal um funcionário do *Facebook* tinha lhe dito que Zuckeberg não acreditava em privacidade.

A reportagem trás que quatro meses antes da declaração de Bilton, uma alteração nos termos do *Facebook* deixava toda a lista de amigos e os conteúdos que os usuários se marcassem como '*fans*' como sendo informação pública e no mesmo mês de publicação da reportagem, apenas uma semana antes numa conferência o *Facebook* tinha anunciado que enviava pacotes de informações dos seus usuários para empresas como *Yelp*, *Pandora* e *Microsoft*. Causando uma reação de alguns senadores americanos que exigiram que a empresa mudasse a sua política de privacidade para que as informações só fossem enviadas a outras empresas caso os usuários desejassem e optassem por ter suas informações compartilhadas. O artigo também traz que Bilton tentou retratar suas afirmações, mas utilizou alguns termos de forma errónea para se defender.

As consequências dessa repercussão são apontadas por Jones (2010) como parte da definição do nome da *Dark Pattern*, já que para atender a exigência dos senadores a plataforma criou uma caixa de permissão de visibilidade da lista de amigos, mas não dava mais informações sobre os direitos do *Facebook* de usar aquela informação e nem onde, outro ponto é que a caixa ficava numa área inusitada do site e não junto as outras configurações de privacidade.

Como o *Privacy Zuckering* se refere a uma prática de dificultar o acesso do usuário as configurações de compartilhamento de informações e a descrição do que está sendo coletado e com qual finalidade, o fato da caixa de permissão de compartilhamento de informações ficar deslocada das outras configurações de privacidade com um texto que não especifica do que aquela permissão se trata configura bem a descrição que Harry Bignull traz para a *Dark Pattern*: *Privacy Zuckering*.

Em 2018 o *Facebook* retornou à mídia com um novo escândalo de privacidade, oito anos depois da decisão judicial que determinava a necessidade de o *Facebook* melhorar suas políticas de privacidade surge o caso da empresa *Cambridge Analytica*, reacendendo o debate sobre proteção de dados e do uso indevido dos dados dos clientes por empresas do setor tecnológico.

Segundo as informações publicadas pela BBC News Brasil (2018) essa venda de dados teria supostamente influenciado as eleições americanas, ao desviar as informações dos eleitores para que as propagandas eleitorais pudessem ser manipuladas de acordo com as informações que eram publicadas no *Facebook*. A coleta dessas informações aconteceu através de um quiz que coletava as informações daqueles que participavam voluntariamente e de todos os contatos dessa pessoa livremente.

A reportagem da BBC (2018) explica que o quiz tinha sido montado sob um algoritmo que fazia a análise da inclinação política da pessoa através de páginas curtidas e publicações na plataforma do *Facebook*. No entanto, em nenhum momento os usuários eram informados do alcance da coleta de dados que seria feita quando os usuários aceitavam participar do questionário. Essas informações que foram coletadas entre os anos de 2014 e 2016, posteriormente foram vendidas à empresa *Cambridge Analytica* e utilizados para direcionar a campanha de Donald Trump para pessoas que tinham sido identificadas pelo algoritmo como indecisas em relação ao seu voto, efetivamente influenciando as eleições nos Estados Unidos.

Pouco tempo depois, como publicado por Santino (2018), o *Facebook* anunciou que 87 milhões de pessoas teriam sido afetadas pelo vazamento de dados provocado pelo quiz,

mudando a estimativa inicial de 50 milhões de pessoas afetadas. Embora a venda dos dados coletados pelo criador do quiz à *Cambridge Analytica* tenha infringido os termos de uso do próprio *Facebook*, isso só serviu para deixar claro que a plataforma não tinha qualquer controle sobre as informações que eram coletadas dos seus usuários.

Ainda segundo a BBC News Brasil (2018) as consequências do escândalo foram imediatas, no mesmo dia da divulgação do vazamento o *Facebook* perdeu 35 bilhões de dólares de valor na bolsa de tecnologia americana. A repercussão também pressionou a aprovação da lei brasileira de proteção de dados (LGPD) que entrou em vigor em setembro de 2020. A lei determinou até onde vai a responsabilidade das empresas pelos dados coletados dos seus clientes, e as sanções cabíveis em situação de vazamento. Agora com a LGPD as empresas são obrigadas a detalhar quais informações serão coletadas, com qual intuito e a definição das medidas de segurança para a preservação dessas informações enquanto estiverem sob o poder da empresa, ela também permite ao usuário revogar as permissões cedidas a empresa que fez a coleta e permite a solicitação de exclusão dessas informações.

3.2 Os preços inflados durante ou na finalização de compras *on-line*.

O segundo tipo de *Dark Pattern* trazido pelo autor Harry Brignull, o *Sneak into Basket* foi uma prática que causou grande comoção no Reino Unido. Esta *Dark Pattern* trata de situações em que serviços e produtos são inseridos nos carrinhos de compra dos usuários sem terem sido solicitados.

O exemplo trazido pelo autor ilustra que esses serviços e produtos ficam em sua maioria camuflados ou embutidos em enunciados confusos e que servem para redirecionar a atenção do consumidor para longe do que está sendo adquirido, mas não se limita a isso, podendo também estar associados a caixas de seleção escondidas na página onde o usuário poderia desmarcar para indicar que não deseja os serviços ou produtos extras.

No exemplo do autor sobre os *Sneak into Basket* uma assinatura que está sendo oferecida sobre um pacote de 4 domínios por 17 dólares, pelo processo de empurrar serviços indesejados ao carrinho do cliente, ao final da compra a assinatura terá um preço inflado de 154,31 dólares com tudo o que foi adicionado ao seu carrinho e o preço enganoso mostrado pela propaganda na página inicial da *GoDaddy* de onde o exemplo foi retirado.

Em 2019, o governo do Reino Unido criminalizou essa prática com um pacote de Revisão dos Direitos do Consumidor da União Europeia, modernizando o conjunto de leis existentes para as práticas online. O que também trouxe impacto num terceiro tipo de *Dark Pattern*, o *Hidden Costs*.

Numa tradução livre como Custos Escondidos, esta *Dark Pattern* possui muitas similaridades com o *Sneak into Basket*, no entanto, os custos que serão adicionados a compra estão mais relacionados a serviços como o frete do envio do produto adquirido, taxas de manutenção como trazido pelo exemplo do autor e outros serviços relacionados ao produto que foi adquirido.

No exemplo do *Sneak Into Basket* trazido por Brignull (2021), os valores extras foram sendo adicionados ao produto por todo o processo de compra através de indicadores enganosos a cada etapa. No exemplo dos *Hidden Costs* eles aparecem apenas na etapa final, depois do cliente já ter cadastrado o cartão de crédito, fazendo uma adição de algo em torno de 18 dólares ao preço final a ser cobrado com custos de transporte e manutenção do arranjo floral que estava sendo adquirido.

Brignull (2021) considera que o fato de o valor escondido aparecer apenas na última etapa do processo de compra é proposital, já que o cliente investiu certo esforço e tempo na compra e por ser a última etapa, não estaria tão inclinado a desistir e recomeçar a compra em outro site acabando por aceitar o acréscimo ao valor final do produto ao invés de investir mais tempo e mais esforço em outro site.

Ambas as práticas buscavam atingir clientes desatentos, mas com a Revisão dos Direitos do Consumidor as empresas passaram a precisar declarar todos os seus custos de forma clara em seus sites. No entanto, ainda é vital que o comprador se mantenha atento a todas as etapas de uma compra on-line para não incorrer em erros ou acabar caindo em outras práticas similares.

CONSIDERAÇÕES FINAIS

O trabalho de Brignull (2021) traz ao conhecimento público as práticas dúbias do mercado *online*, embora não tenha muito alcance no Brasil, é importante para mostrar a necessidade de uma legislação bem estruturada e abrangente.

Seu site, embora traga mais exemplos dos Estados Unidos e da antiga União Europeia é uma ferramenta chave para entender o termo *Dark Patterns* e ter o entendimento de como essas práticas afetam o consumidor. O autor também utiliza suas redes sociais, como o *Twitter*, para denunciar marcas de alcance global que se utilizam de práticas dúbias diariamente.

Empresas como a Meta, dona do *Facebook*, já protagonizou uma série de escândalos relacionados a vazamento de dados, como também o próprio Google já apareceram nas redes sociais do autor com práticas enganosas de *Dark Patterns*, e muitas outras que o autor se esforça para denunciar até o presente momento da edição deste artigo.

A criminalização de algumas dessas práticas é um começo, mas muitas ainda acontecem livremente pela *Internet* e o usuário está suscetível a essas práticas a todo momento.

Novamente, no âmbito online a melhor forma de se proteger dessas práticas é o conhecimento e a navegação cuidadosa, atenciosa aos elementos que são apresentados nos sites em que navegamos. Da mesma forma que os golpes online estão sempre se desenvolvendo e se tornando cada vez mais convincentes as *Dark Patterns* também estão em constante evolução e não se limitam as que já foram nomeadas pelo autor, pois, elas também interagem entre si, em muitos casos tendo mais de um tipo de *Dark Pattern* sendo aplicado na mesma página. E dessa interação novas práticas surgem, sempre com o intuito de manipular o usuário durante a sua navegação nas redes para trazer lucro indevido aos donos do site.

Com um cenário de constante mudança como o das redes, as leis precisam se manter atualizadas, tendo revisões constantes para identificar e criminalizar essas práticas, trazendo um padrão de excelência e proteção a todos os usuários da *Internet*, independentemente de qualquer fator de identificação, mitigando a ação dos *cybers* criminosos.

REFERÊNCIAS

BBC NEWS BRASIL. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751 Acesso em: 31/03/2022.

BRANCO, D. C. **Canaltech**. **O que é engenharia social? Veja como evitar problemas de segurança.** 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-e-engenharia-social-195773/ Acesso em: 24/10/2021.

BRIGNULL, H. **What are Dark Patterns?** 2021. Disponível em: https://www.darkpatterns.org/ Acesso em: 24/10/2021.

BUSKIRK, E. V. Report: Facebook CEO Mark Zuckerberg Doesn't Believe In Privacy. **WIRED**, 2010. Disponível em: https://www.wired.com/2010/04/report-facebook-ceo-mark-zuckerberg-doesnt-believe-in-privacy/ Acesso em: 05/11/2021.

CANDIDO, J. P. S.; ARAÚJO, T. F.; RIBEIRO, W. A. C. Histórico da Lei Geral de Proteção de Dados (LGPD). **Advocatta**, 2018. Disponível em: https://advocatta.org/historico-da-lei-geral-de-protecao-de-dados-lgpd/ Acesso em: 19/04/2022.

COELHO, C. F.; RASMA, E. T. e MORALES, G. ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO. **Exatas & Engenharias**, no. 3, v. 05, 2013. Disponível em: https://doi.org/10.25242/885X305201387 Acesso em: 24/10/2021.

CUNHA, D. A segurança da informação e a sua importância para a auditoria de sistemas. **Revista Científica Semana Acadêmica**. Fortaleza, ano n. 29, 2013. Disponível em: https://semanaacademica.org.br/artigo/seguranca-da-informacao-e-sua-importancia-para-auditoria-de-sistemas Acesso em: 26/10/2021.

KASPERSKY. **Engenharia social: definição.** 2021. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering Acesso em: 24/10/2021.

EUROPEAN COMMISSION WEBSITE. C**onsumer Rights Directive.** Disponível em: https://ec.europa.eu/info/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en Acesso em: 19/04/2022.

EUROPEAN COMMISSION WEBSITE. **Consumer protection policy**. Disponível em: https://ec.europa.eu/info/policies/consumers/consumer-protection-policy_en

Acesso em: 19/04/2022.

FOLTÝN, T. Entenda como a superexposição em redes sociais pode trazer problemas. **Welivesecurity,** 2018. Disponível em: https://www.welivesecurity.com/br/2018/06/29/entenda-como-superexposicao-em-redes-sociais-pode-trazer-problemas/ Acesso em: 26/10/2021.

FOLTÝN, T. Biografia. **Welivesecurity,** 2021. Disponível em: https://www.welivesecurity.com/br/author/tfoltyn/ Acesso em: 26/10/2021.

INTERSOFT CONSULTING. General data protection regulation (GDPR), 2021. Disponível em: https://gdpr-info.eu/ Acesso em: 03/11/2021.

HENRIQUES, F. A. F. **A influência da Engenharia Social no fator humano das organizações.** Dissertações de Mestrado - Ciência da Computação. Universidade Federal de Pernambuco, 2017. Disponível em: https://repositorio.ufpe.br/handle/123456789/25353 Acesso em: 04/11/2021.

JONES, T. **Electronic Frontier Fondation,** 2010. Disponível em: https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces Acesso em: 05/11/2021.

LORD, N.Social engineering attacks: common techniques & how to prevent an attack. **DIGITAL GUARDIAN**, 2020, Disponível em: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack Acesso em: 24/10/2021.

MARCONDES, J. S.. Engenharia Social: o que é? conceitos e como se proteger. **Blog Gestão de Segurança Privada**, 2017. Disponível em: https://gestaodesegurancaprivada.com.br/engenharia-social-o-que-e-conceitos/ Acesso em: 24/10/2021.

MACHADO JUNIOR, D. M. **Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas.** Tese (Doutorado em Tecnologia da Inteligência e Design Digital) - Programa de Estudos Pós-Graduados em Tecnologia da Inteligência e Design Digital, Pontifícia Universidade Católica de São Paulo, São Paulo, 2018. Disponível em: https://tede2.pucsp.br/handle/handle/21366 Acesso em: 03/11/2021.

SANTINO, R. Escândalo de privacidade do Facebook pode ter afetado 440 mil brasileiros. **Olhar Digital**, 2018. Disponível em: https://olhardigital.com.br/2018/04/04/noticias/escandalo-de-privacidade-do-facebook-pode-ter-afetado-440-mil-brasileiros/ Acesso em: 31/03/2022.

Testimonium sobre Harry Brignull, 2021. Disponível em: https://testimonium.co/ Acesso em: 24/10/2021.