INSTITUTO UNIVERSITÁRIO DE LISBOA

Proteção de dados - a questão da privacidade dos cidadãos na internet

LCT- Laboratório de competências transversais

Realizado no âmbito da U.C.- Escrita de textos técnicos e científicos

1º Ano da licenciatura de Ciência de Dados

Docente: Sílvia Cavalinhos

Trabalho realizado por: João Francisco Botas, nº104782, CDA1

12/2021

Índice

Introdução:

Com a evolução exponencial dos utilizadores e do acesso à internet nas últimas décadas, a privacidade dos dados pessoais é um tópico que suscita, cada vez mais interesse a especialistas e escritores, que alertam nos seus textos todos os cidadãos que recorrem às tecnologias constantemente. Por isso, é necessário começar a debater os perigos e a forma de contrariar a crescente falta de proteção de dados que hoje se verifica. Este é um tema polêmico que devia fazer parte das agendas dos vários Estados e das empresas de cibersegurança.

1- A evolução da internet até à internet das coisas

Até chegarmos aos dias de hoje a Internet sofreu diversas alterações quanto à forma como era desenvolvida. Surgiu com a guerra fria, para fins militares, e foi originalmente desenhada por fatores políticos, sociais e económicos. Em seguida, foi apresentada para os espaços académicos e para pesquisas técnicas e científicas. A sua utilização começou por ser restringida a um determinado local, e estendeu-se até à época em que foi trazida para uso público no início da década de 90.

É certo que em 20 anos, aquilo que era um conceito tornou-se numa ferramenta para uso na via pública e isso não estagnou. Hoje, encaminhamo-nos para um conceito revolucionário que permite conjugar várias fontes num caminho linear, "a internet das coisas".

2- A internet das coisas

Após o acesso à Internet tornar-se público para todos os cidadãos, no sentido em que não está restrito a um grupo de pessoas, nasceu um novo conceito denominado de "internet das coisas".

O termo "internet das coisas" é a partilha de dados entre dois ou mais objetos, com ligação à rede, conectados entre si. Desde algum tempo que este tópico se vem transformando, pois é permitida a automatização de quase tudo, usando uma relação dos dados de utilizador por vários dispositivos. Carsten Maple (2017, p.155-184) afirma que este conceito é revolucionário e que pode abranger desde o transporte à educação ou do entretenimento às interações com o governo. Refere ainda que a rapidez e o crescimento no número de aparelhos vão desafiar a nossa segurança e liberdade porque estamos a evoluir numa inovação sufocante.

3- A importância da proteção de dados

A geração de dados é algo que, cada vez mais, adquire maior forma e um valor mais acentuado no tempo atual. Simon Kemp (2021) fez uma pesquisa para o Datareportal no ano anterior, chegando à conclusão que 332 milhões de novas pessoas rumaram neste "mundo online", ou seja, tiveram pela primeira vez contato com um dispositivo eletrónico

ligado à Internet. Refere ainda que os cidadãos ficam, em média, aproximadamente 7 horas "online" por dia, sendo cerca de 93% passado com um dispositivo móvel.

Através de uma análise, podemos verificar que, pelos resultados obtidos, houve quase 632 novos utilizadores por minuto, no intervalo de tempo referido. É óbvio que o aparecimento destes novos utilizadores contribui para o aumento de mais pessoas vulneráveis a diversos tipos de ameaças. Esta chegada ao mundo tecnológico, leva a uma atenção mais pormenorizada devido ao facto de estas pessoas não estarem previamente preparadas e alertadas para onde e como podem fornecer os seus dados.

Já se viu que, com a internet das coisas, a partir de poucos dados de um cidadão consegue-se extrair ainda mais informação de forma instantânea e, assim, obter um rastreio do que a pessoa pesquisa, visita, come ou, simplesmente, faz, no seu dia-a-dia. Por isso, é necessário proteger esses dados a todo o custo, já que traduzem uma parte da identidade de um indivíduo, e deixando a hipótese de saber e controlar o que vai partilhar, de forma acessível e transparente, visto que há uma profusão de utilizadores novos, como referido anteriormente, e vulneráveis.

Porém, por mais severo que seja o sistema de controlo, podem sempre existir brechas, o que demonstra ainda mais a ênfase que os dados têm para uma sociedade. Assim, com o intuito de prevenir, o DHS dos EUA (departamento de segurança interna) prometeu dar a *hackers* "recompensas elevadas por descobrirem os erros mais graves" depois de "oficiais cibernéticos alertarem que *hackers* exploram um novo *software* com vulnerabilidade". (Geneva Sands/CNN, 2021); *traduzido para português.* Estes *hackers* governamentais estão, cada vez mais, a serem procurados pelas grandes empresas para descobrirem fraquezas. Mas será que esta "profissão" do mundo moderno pode tornar a internet mais perigosa por haver uma maior procura?

4- Perigos da falta de proteção de dados

Vejamos agora os perigos que a excessiva quantidade de informação que circula por segundo pode tomar, enumerando os mais recorrentes e impactantes no nosso quotidiano.

4.1- Gestão de passwords

Hoje em dia, em qualquer *website* onde dados pessoais estejam armazenados no sistema é necessário apresentar uma palavra-passe como forma de autenticar a pessoa que está a aceder. Contudo, isto poderá ter diversos riscos acentuados à sua utilização, sendo o maior destes o acesso de um desconhecido a dados de uma determinada pessoa.

Quando se vai definir uma *password* há uma tendência para escolher uma cadeia de caracteres fácil de memorizar e, normalmente, associar a conta a criar a uma plataforma já criada, seja ela correio eletrónico ou outra semelhante. Desse modo, no caso de um possível esquecimento, é possível redefinir a palavra-passe usando um simples código que consegue ser facilmente rastreado por um *hacker*, pois, "desde que os *hackers* entrem com a palavra secreta, eles ganham controlo sobre o alvo. Podem fazer mudanças à configuração do produto de segurança (…)" (Buchanan, 2020, p. 80); *traduzido para português*. Assim, com estas ligações a bases de dados pequenas (correio eletrónico) anónimos conseguem alterar os dados pessoais.

Para além da redefinição de senha, que é perigosa por estabelecer ligação entre contas, o histórico e armazenamento de palavras-passe pode também impactar num acesso facilitado por terceiros pelo mesmo motivo. Isto porque, deixa-se no sistema entradas a múltiplas contas que, como referido anteriormente, pode contribuir para chegar a um indivíduo em específico e tirar todo o proveito disso.

4.2- Plágio de identidades reais e *phishing*

Se pararmos para analisar a evolução e o lucro que as empresas tecnológicas têm tido ao longo das últimas duas décadas, vê-se que existe uma maior possibilidade de haver pessoas ou grupos de pessoas que se fazem passar por elas e colocar armadilhas para ninguém as identificar.

Nos últimos tempos, vemos novas maneiras de se efetuarem pagamentos, nomeadamente com aplicações nos aparelhos móveis. Com o passar do tempo, acontece com maior frequência a receção de mensagens de pessoas de sites de comércio eletrónico, que querem obter os nossos dados e, até, encontrarem-se connosco para fins maliciosos. O OLX (2021), plataforma de comércio eletrónico, adverte, e tem no seu *website* medidas

de identificação de burlas, sendo as principais a certificação que o enderenço de e-mail e o *url* dos *links* é o correto ou se as mensagens não apresentam erros de ortografia.

De facto, é surpreendente que através de uma manipulação que possa vir a acontecer com alguma pessoa desinformada, pessoas anónimas consigam descobrir a pessoa em questão.

4.3- *Clickbait* nos *websites*

À semelhança do plágio de identidades reais, o *phishing* é uma forma de atrair um alvo, fazê-lo adotar uma atitude e suscitar uma vontade de querer clicar em ligações chamativas, que aparecem em sites pouco protegidos (*clickbait*). Neste caso, o *clickbait* desperta o interesse para coisas que a pessoa pesquisa na internet, de forma a levá-la a ligações falsas que contenham algum artifício ou vírus que acesse os dados da pessoa no dispositivo.

O *clickbait* é um dos tipos de *phishing* mais antigos e que aparecem em maior número, mais concretamente em anúncios e janelas a referir que, por exemplo, o utilizador ganhou ou pode ganhar alguma recompensa se clicar nos botões indicados e desejados, que aparecem com frequência em *websites* pouco fidedignos. Apesar de estes *clickbaits* já serem usados há muito e havendo outros métodos mais eficazes para os *hackers*, há pessoas que continuam a serem enganadas, seja por ingenuidade do próprio ao acreditar no que é transmitido ou, seja por a pessoa não estar totalmente familiarizada com estes ataques indiretos.

As maneiras de prevenir estes golpes são as mesmas indicadas pelo OLX para prevenir o *phishing* e a criação de identidades falsas, mas o fundamental deveria ser a maior informação dos utilizadores sobre estas formas de ataque.

5- Soluções possíveis para proteger mais os cidadãos

Não há soluções possíveis para mitigar drasticamente os principais problemas da falta de proteção de dados, mas sim formas de controlar e deixar os cidadãos um pouco mais protegidos. É verdade que atualmente, desde 2018, está implementado o RGPD (Regulamento Geral sobre a Proteção de Dados), todavia, começamos a ter um grau de problemas mais expansivo, que englobam mais dados. Por isso, se quiséssemos extinguir

o problema em questão, isso não bastava. A única solução seria retroceder nos avanços tecnológicos para desenvolver a partir de um ponto de partida semelhante ao atual (com mais tecnologia). Tal não sendo possível temos de encontrar soluções "menos" complexas.

A primeira solução possível é-nos proposta por Miguel de Bruycker, diretor do centro de cibersegurança belga, que diz ser preciso "implementar mais camadas de segurança baseadas na identidade digital" e dá um exemplo bastante pertinente, "se eu quiser visitar um website de receitas para churrasco não me interessa se o proprietário é desconhecido. Mas se tiver de deixar o meu cartão de crédito, eu prefiro que o proprietário tenha um certificado de validação". É evidente que esta medida tornaria a internet um pouco mais segura e não requereria tanta atenção para navegar na mesma, porém isto faria com que os cidadãos fossem menos livres e levaria a uma grande diminuição e limitação de sites.

De outro ponto de vista, Maxime Sbaihi fomenta a ideia de dar mais destaque ao utilizador para decidir o grau de profundidade que quer atribuir aos sites quando fornece os seus dados.

> "Se quiser dar os seus dados pessoais de geolocalização, de preferências, dos seus amigos, as suas preferências culinárias, viagens, etc… deve ter a hipótese de o fazer, deve estar numa posição de negociação com essas plataformas. Hoje, isso não acontece. Hoje é binário, ou tudo ou nada e a nossa ideia é implementar um sistema que volte a dar o poder ao utilizador". (Sbaihi, 2018)

A solução apresentada contém um bom pensamento, mas poderia trazer algumas discordâncias com os criadores de *websites*, por não se sentirem seguros com uma pessoa que não deseja fornecer praticamente nada e tenta aceder ao sistema como benefício pessoal.

Assim, percebe-se que este tópico é fundamental e merece uma discussão assertiva, mas que pode trazer alguma divisão de ideias. Contudo, deve-se arranjar uma solução funcional pois, estamos a "entrar numa corrida ao armamento onde os países começam a armazenar armas, apenas não são aviões ou reatores nucleares, mas sim armas cibernéticas". (Mykko Hyponnen citado por Singer & Friedman, 2014, p.118). Ou seja, devemos também agir mais rapidamente, para que não se dê "início a uma guerra onde todos percamos" (Leslie Harris citado por Singer & Friedman, 2014, p.118).

Conclusão

Foi abordada a questão da privacidade dos cidadãos na internet e formas de solucionar a falta de proteção a que os utilizadores estão sujeitos atualmente. Começou-se por ver a evolução da internet e o crescimento que esta vai tomando nos dias de hoje, e vemos que é mais e mais relevante a preocupação com os perigos da utilização incrementalmente alargada e intensiva.

A solução encontrada é que é impossível extinguir as ameaças completamente, pelo que se devem ir dando pequenos passos, de forma gradual, para que se consiga correr a maratona. As soluções indicadas, e pertinentes, que contribuem para o desenvolvimento deste tópico foram propostas por Miguel de Bruycker e por Maxime Sbaihi.

Referências Bibliográficas:

Euronews, 2021. Web users must accept less anonymity for more security, says expert. https://www.euronews.com/2021/06/08/web-users-must-accept-less-anonymity-for-more-security-says-expert

Singer, P., W., & Friedman, A., (2014). Cybersecurity: What Everyone Needs to Know. Oxford

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. 1st edition. Harvard University Press

Datareportal. 2021. 6 in 10 people around the world now use the internet.https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet

Salgueiro, R., RTP. 2018. O valor dos dados pessoais.https://ensina.rtp.pt/artigo/o-valor-dos-dados-pessoais/

OLX. 2021. Dicas de segurança na venda de artigos pelo serviço de entregas OLX. https://help.olx.pt/hc/pt/articles/360015826697-Dicas-de-seguran%C3%A7a-na-venda-de-artigos-pelo-servi%C3%A7o-de-Entregas-OLX

Maple, C., (2017,08/24). Security and privacy in the internet of things. Journal of cyberpolicy, Volume 2, 155-184.https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536

Sands, G., CNN politics.2021. US government to offer up to $5,000 'bounty' to hackers to identify cyber vulnerabilities.https://edition.cnn.com/2021/12/14/politics/dhs-bug-bounty-hackers-cyber-vulnerabilities/index.html