

"NÃO INTERESSA TERMOS LIBERDADE DE EXPRESSÃO SE TUDO O QUE DIZEMOS PODE SER USADO CONTRA NÓS"

Carolina Ormonde



Francisco Core é um jovem estudante e defensor do direito à privacidade. Através da associação sem fins lucrativos PrivacyLx, organiza eventos abertos ao público. Entre outros temas ensina como nos podemos proteger online de perigos como hackers, como podemos ser donos da nossa vida digital e como escolher com quem e quando é que os nossos dados são partilhados.

Em que consiste a PrivacyLx e quais as suas finalidades?

Desde já quero agradecer pelo convite. A PrivacyLx é uma organização sem fins lucrativos cujo principal objetivo é educar as pessoas em relação à privacidade. Organizamos eventos gratuitos destinados ao público em geral e sem a necessidade de qualquer registo antes, durante e após qualquer evento. Nesses eventos, as pessoas podem levar-nos os seus dispositivos e a partir daí orientamos a melhor forma delas se protegerem e avaliamos variadas aplicações fidedignas e seguras que podem instalar. Durante o período de pandemia e o respetivo confinamento, fizemos uma pausa

e cada membro dedicou-se a trabalhar nos seus próprios projetos que, de certa forma, estão relacionados com o tema da privacidade. Atualmente estamos a preparar alguns eventos que em princípio terão lugar em Março.

Porque é que a privacidade é tão importante nas nossas vidas?

Primeiro é preciso desconstruir o mito de que a privacidade não é algo com que as pessoas se devam importar. Pensem por exemplo, que um desconhecido vos tira o telemóvel das mãos e descobre o vosso pin. A partir daí, terá acesso aos mais íntimos detalhes da tua vida. Isto não é algo que desejamos nas nossas vidas. No entanto, as

aplicações que temos instaladas nos nossos telemóveis, nomeadamente, aplicações da Google ou do Facebook, detêm esse mesmo acesso! Têm como principal negócio recolher informação pessoal para nos mostrar anúncios o mais específicos possível de acordo com as nossas preferências. Essas empresas criam um perfil baseado no que vemos, partilhamos ou pesquisamos (mesmo em conversas privadas). Se fizermos uma retrospectiva aos regimes totalitários que passaram pelo mundo, observamos que por exemplo, em Portugal havia sistemas do governo que tentavam obter o máximo de informação sobre as pessoas. Era o caso da PIDE que trabalhava com o intuito de punir quem fosse contra o regime, mas essa

ENTREVISTA

informação não era facilmente alcançada porque exigia um trabalho de recrutamento de informadores ou delatores que estivessem no sítio certo e à hora certa. Hoje em dia, todos nós temos no nosso bolso um telemóvel que faz, essencialmente, o mesmo papel. A privacidade são as “cortinas” da nossa vida e nós é que escolhemos quando é que as abrimos e para quem as abrimos. No mundo moderno isso deveria ser uma obrigação, aliás, o Regulamento Geral de Proteção e Dados (RGPD), supostamente, impede as empresas de recolherem os dados sem consentimento do consumidor, no entanto, o consentimento é quase sempre nulo. Portanto, o que é consentimento se não é informado?

Fomentando o ponto dos regimes autoritários, onde era muito difícil a recolha de dados pessoais, achas que a nossa privacidade encontra-se de tal forma vulnerável, que na realidade já temos um estado hipoteticamente autoritário que não precisa de constituir um grande esforço para adquirir os nossos dados?

Extremamente vulnerável. Esses dados já existem nas gigantes empresas tecnológicas de que todos dependemos. Aliás, os governos já “metem a mão” nesses dados ignorando as constituições dos respetivos países, por exemplo vejamos o caso das revelações de Edward Snowden em 2013. Por exemplo, em Portugal as operadoras são obrigadas a armazenar os últimos dois anos de quem nos

contactou por telemóvel, o lugar e a hora do respetivo contacto para depois as secretas poderem aceder a esses dados. Claro que viola o Estado de Direito ao inverter o princípio da presunção de inocência. Foi declarado inconstitucional em 2019, claro. Mas não impede os políticos de terem estas mesmas ideias. Tal como podemos ler numa notícia do Jornal Público deste ano, “PS admite regressar ao acesso das secretas a metadados”. E por cá não tivemos um whistleblower como Snowden, por isso é bem provável que mais informação seja recolhida em massa, sem que disso tenhamos conhecimento. Mas acontece que informações recolhidas ilegalmente pelo governo e empresas, não podem ser usadas em tribunal. Portanto, o problema do autoritarismo atualmente, é que hoje em dia, temos as ferramentas digitais para ter uma ditadura mais forte do que alguma vez existiu na história, e a China é o maior exemplo disso. Na China, ninguém tem liberdade de expressão, porque não interessa termos liberdade de expressão se tudo o que dizemos pode ser usado contra nós. E não existem espaços privados porque todas as conversas à distância são mediadas através de aplicações cujo governo tem acesso.



ENTREVISTA

Achas que alguma vez vamos presenciar uma sociedade em que a privacidade de cada um é respeitada?

Nos anos 80 era muito raro uma empresa cujo objetivo era extorquir o máximo de dados pessoais porque simplesmente não havia os mesmos incentivos económicos e tecnologia que há hoje. Daqui para o futuro o que é preciso para termos uma sociedade que valoriza a privacidade é fomentar a consciência dos consumidores, de que os seus dados estão a ser utilizar e assim boicotar empresas ou aguardar para que os governos façam leis essenciais, para limitar a venda de dados pessoais sem consentimento. O Regulamento Geral de Proteção de Dados foi um grande passo nessa direção, e aliás, está se agora a ver as primeiras consequências do regulamento geral de proteção de dados e muitas na ordem dos milhares de milhões. No outro dia em França, o Google Analytics, que é uma ferramenta da Google que monitoriza maior parte dos sites a que os visitantes acedem, foi declarado ilegal na União Europeia. Apesar de estarmos a caminhar para o bom sentido, é preciso que hajam pessoas que acreditem nos valores democráticos e que exista um poder judicial sério que proteja

os consumidores.

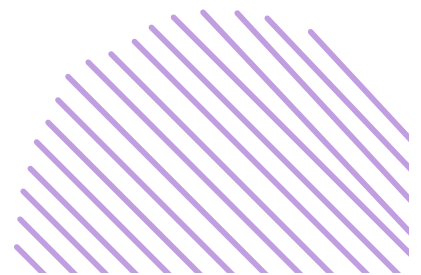
Ao longo da nossa vida somos confrontados com a chamada Dark Web. Em termos genéricos o que é isto da Dark Web?

A Dark web é um mito porque todos os dias acedemos à Dark web. Para aceder a ela basta irmos a um site e registar-nos, portanto é apenas Dark web aquilo que não conseguimos encontrar no google porque é preciso iniciar sessão. Acho que é um mito mediático para tentar colocar medo às pessoas. Depois há um conceito mais falado que é a Deep web que é, mais uma vez, um termo mediático e é uma parte da internet que só temos acesso a partir de ferramentas que protegem a nossa privacidade. Existe uma aplicação designada Tor browser que podemos instalar no nosso telemóvel ou computador. Ao acedermos à internet a partir desta aplicação, conseguimos navegar na internet com razoável anonimato, logo os sites não conseguem perceber quem somos. Esta ferramenta é desenvolvida por uma organização sem fins lucrativas, sediada nos EUA chamada Tor Project e desenvolveram uma maneira de também dar o mesmo nível de privacidade a quem quer ter o seu próprio site. É tal e qual como as facas, que podem ser usadas

tanto para bons fins como para fins cruéis mas não é por isso que as deixamos de usar no nosso dia a dia. O mal não desapareceria se essas ferramentas desaparecessem. Vivemos num mundo que tem os seus próprios perigos e é preciso tomar consciência deles, percebendo as ferramentas que utilizamos, quem as usa e quais as suas vantagens como desvantagens.

Estamos a ser vigiados 24h por dia a partir do momento em que usamos as redes sociais ou há mais fatores que influenciam a possibilidade de não termos a nossa privacidade em segurança?

Atualmente a maior parte dos sites que visitamos contêm pequenos componentes que vigiam a nossa presença. É assim que a Google tem acesso a 68% dos sites que visitamos e o Facebook cerca de 20%, segundo um estudo da universidade de Princeton de 2017. Há que compreender que não vale a pena ficarmos paranóicos com estas coisas, porque apesar de haver muita gente a tentar vigiar as nossas



ENTREVISTA

comunicações também há coisas que podemos fazer e é essencial tomarmos consciência do problema. Eu adoraria que as redes sociais fossem para pessoas, onde eu partilho o que quero e com quem eu quero, o problema é que as redes sociais são administradas por empresas que têm como negócio a recolha e venda dos nossos dados pessoais. Podemos pensar no Meta ou Facebook como um território em que nós não somos soberanos, onde não elegemos quem nos governa, onde não há democracia e onde cada vez há mais pessoas a migrar e a construir lá as suas vidas.

Que conselhos dá aos jovens de hoje para protegerem a sua privacidade caso o desejem?

A primeira fase é perceberem exatamente o que está a acontecer, e para isto uma das formas mais fáceis é acederem a um site qualquer num portátil e verem enquanto carrega a página, no canto inferior esquerdo, verem todos os sites que o vosso computador contacta enquanto estão a abrir esse site. Quando sentirem que isto vos incomoda podem instalar uma aplicação ou extensão para o browser chamada uBlock Origin. Isto vai bloquear os anúncios e também pequenas

partes que nos controlam quando estamos a visitar sites. Se tiverem preocupados com o roubo de identidade, podem utilizar uma aplicação de gestão de palavras-passe. Portanto em invés de confiarmos em nós mesmos para fazer palavras-passe fortes, o melhor compromisso é termos uma aplicação em que temos uma só palavra-passe forte a proteger todas as outras. Essa aplicação permite-nos fazer login em qualquer site com um só clique (depois de escrevermos a nossa palavra-passe principal) e quando nos registamos, ela gera as passes por nós e armazena-as. A minha recomendação para isto é uma aplicação chamada Bitwarden.

Quais são algumas das mudanças que implementou na sua vida e

que ajudam a proteger os seus dados?

Eu já faço isto há pelo menos 7 anos e algumas das coisas que eu faço são as que referi anteriormente. Para além disso, há coisas que tenho implementado na minha vida e que não podem ser feitas de um dia para o outro, mas que a meu ver são benéficas a longo prazo. Uma delas é sair das redes sociais todas, isto é uma escolha que as pessoas têm de fazer por elas próprias porque podem ter razões pessoais para utilizar uma determinada aplicação. Por isso uso hoje só aplicações de mensagens, onde escolho diretamente com quem quero falar. Recomendo a aplicação Signal. A vigilância que encontramos na internet está também a acontecer no nosso dia a dia, com por exemplo cartões de fidelização. As cadeias



ENTREVISTA

de supermercado registam todas as compras que fazemos com a simples pergunta “Tem cartão cliente?”, a verdade é que nunca nos informam o que está por detrás disso. Eu faço o sacrifício de não ter as vantagens que a empresa proporciona porque não quero que ninguém saiba aquilo que eu consumo. Isto tem algumas consequências, tal como, se no cartão de fidelização estiver presente alimentos não saudáveis, caso eu queira iniciar um seguro de saúde e a seguradora tenha acesso aos meus dados, eu vou ter de pagar mais porque sou apresentada como uma pessoa que tem maus hábitos alimentares. Por outro lado, procuro sempre pagar em dinheiro as minhas compras e preferencialmente de forma presencial, por razões semelhantes às de não usar cartões-cliente.

Ultimamente algumas empresas em Portugal foram vítimas de ciberataques, qual é a sua opinião em relação a este tema?

Temos de ter consciência que já há muito tempo que estamos numa permanente ciber-guerra. As empresas são constantemente atacadas e qualquer empresa que tenha computadores ligados à internet, se prestar atenção, vai concluir que sofre tentativas de

ataques de 5 em 5 minutos. Uma ciber-guerra é muito mais barata do que uma guerra convencional, logo o que agora nós temos vindo a deparar é com uma maior intensificação de ciber ataques e começámos a perceber que isso também nos afeta. No caso da Vodafone, uma das empresas atacadas em Portugal onde parece haver uma razão e interesse geopolítico e não tanto económico, mas é sempre difícil perceber a razão e quem é que fez este tipo de ataques. No caso particular da Vodafone há uma coisa bastante integrante: no dia 7 de fevereiro à noite foi quando a Vodafone descobriu que estavam a ser atacados e quando começaram a haver alguns problemas na sua rede. No dia seguinte, por volta do meio dia, já estava a haver uma conferência de imprensa em que afirmavam que não havia indícios dos dados pessoais dos clientes terem sido roubados. A pergunta que coloco é, como é que a empresa pode ter tanta certeza disso? É interessante ver a estratégia imediata da Vodafone de automaticamente negar qualquer tipo de roubo de dados pessoais, na tentativa de afastar os holofotes. De acordo com Regulamento Geral de Proteção de Dados, de que tanto falei hoje, as empresas são

obrigadas a notificar todas as pessoas afetadas sempre que haja um acesso ilegítimo aos seus dados pessoais. O problema é que isso não acontece pois não há fiscalização adequada, já para nem falar que, muitas vezes, as empresas nem precisam da maior parte dos dados pessoais que exigem ao consumidor. Em conclusão é essencial reduzirmos o fornecimento dos nossos dados pessoais, ter consciência sobre a importância da privacidade e tem de haver uma maior regulamentação, porque não são as medidas tecnológicas que vão proteger as pessoas para sempre. As empresas vão sempre arranjar novas maneiras de explorar os nossos dados pessoais e de os usarem contra nós. Se um dia destes vier uma ditadura, podemos ter a certeza que vai ser cem vezes pior do que qualquer uma que alguma vez experienciamos. Por isso, o melhor é protegermo-nos enquanto podemos e fortalecer a democracia, para que isso nunca aconteça.

