privacidade 404

Filipe Cruz

Introdução

"*Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.*" Artº 12º, Declaração Universal dos Direitos Humanos, 1948.

O direito à privacidade está previsto na declaração dos direitos humanos. A importância da privacidade está documentada cientificamente. A sua inexistência afecta as pessoas ao nível físico, psicológico e emocional. Ter acesso a um espaço que consideramos seguro promove a auto-confiança e capacidade emocional para lidar com a sociedade.

Traçando o paralelo para um mundo cada vez mais conectado: o sigilo e a privacidade digital são essenciais para manter a confiança em serviços críticos para a vida em comunidade: educação, apoio médico, acessos monetários…

No entanto, a tecnologia permite mais do que nunca vigiar e identificar tudo e todos.

A vídeo vigilância tem vindo a ser cada vez mais institucionalizada pelos governos "para nossa protecção". Quase um século após os avisos de Orwell, a sociedade no geral continua a caminhar nessa direcção. Sendo vendido ao público como "Só se importa com isso quem tem algo a esconder." e com vários exemplos de ladrões, terroristas e pedófilos que só poderão ser capturados quando todas as ruas e pessoas estiverem a ser constantemente vigiadas.

Fica sempre por responder quem vigia os vigiantes para evitar os abusos de poder? Quem garante que a informação privada que está a ser recolhida será devidamente encriptada em segurança, ou protegida de acessos indevidos ou apagada quando não for necessária. Haverá sempre acessos indevidos e os dados privados tem grande valor comercial.

Por outro lado temos as redes sociais, que aliciam à partilha pública de informação que deveria em muitos casos ser privada. Há falta de consciência, interesse e cuidado em evitar as partilhas de informação

privada em redes públicas por parte dos utilizadores. Porque é conveniente, porque a partilha cria laços relacionais, porque precisamos da validação pública, porque é publicamente que agora tratamos dos assuntos privados, porque vamos ser “influencers” milionários, porque todos os outros também partilham. Em contrapartida, as empresas vendem os nossos dados privados a terceiros e qualquer pessoa consegue saber facilmente a nossa informação privada, das nossas famílias e amigos. De repente já ninguém quer saber dos ladrões, terroristas e pedófilos que se podem aproveitar dessa informação para causar dano, porque é mais importante os seguidores saberem que eu hoje comi a melhor panqueca de todo o sempre neste local e a estas horas com o Zé e a Mariana e o seu filho pequeno adorou.

Há fortes interesses económicos em vender mais tecnologia de vigilância, inteligência artificial e dados pessoais. Há forte motivação da segurança e poder militar em conseguir monitorizar todas as ruas e todas as pessoas. Há pouco interesse político em fazer cumprir as regras internacionais de protecção de dados e privacidade.

Este é um tema que me incomoda há mais de duas décadas. Fiz/faço parte de alguns grupos que tentam alertar para este tipo de questões. Para os mais interessados deixo aqui as referências de duas associações sem fins lucractivos que trabalham a favor destas causas em nome do interesse público:

EFF – Electronic Frontier Foundation https://www.eff.org/

A trabalhar a partir dos Estados Unidos com alguma projecção internacional.

D3 – Defesa dos Direitos Digitais: https://www.direitosdigitais.pt/

A trabalhar a partir de Portugal e com alguma atenção também às regras europeias.

Tento apoiar dentro do possível estas instituições, com uma vã esperança que o futuro para o meu filho venha a ser melhor do que se vislumbra neste momento. Sendo que já é algo impossível nos dias de hoje viver em sociedade sem termos os nossos dados em vários sistemas públicos sob pena de não termos acesso a cuidados, transportes, emprego. Ou de não utilizar o telemóvel ou o acesso à internet para as comodidades do

dia a dia, sem saber até que ponto a nossa privacidade está a ser respeitada pelas operadoras de telecomunicações, os seus funcionários e até possíveis acessos indevidos.

Tive bastantes insónias a pensar sobre o tópico, a ponderar o que poderia eu fazer para tornar o mundo um bocado melhor para a próxima geração. Não tenho poder para influenciar a política.

Resta-me então tentar influenciar a cultura. Escrevi os meus pensamentos distópicos de como poderá vir a ser o nosso futuro daqui a uns anos. Apresento-os aqui em dois curtos contos, algo relacionados, ambos de ficção cientifica especulativa.

Espero que sejam leituras interessantes de ler do ponto de vista literário mas acima de tudo espero que consigam educar um bocado alguém sobre os reais perigos da falta de privacidade digital na sociedade. Ou dar algumas ideias de como poderão vir a ser combatidos estes problemas no futuro.

Ocorrência na Rua da Lapa

Geo Referenciação Temporal:

2133696921 - Avenida Álvares Cabral, Lisboa

2133697620 - Rua da Lapa, Lisboa

Actores:

Nuno Benite 54636775

João Serzedo 62819311

Reconstrução narrativa contextual (perfil narrador 424):

Era uma vez uma Lisboa no dia 12 de Agosto de 2037. A descer a Avenida Álvares Cabral, pelas 14:35, encontrava-se um veículo branco com duas riscas azuis. Um dos modelos híbridos mais recentes da Polícia de Segurança Pública, com um sistema de comunicação global centralizado incorporado que permite a emissão e recepção de notificações de proximidade a todos os dispositivos activos na área; conta também com um sistema de auto navegação com nível de confiança de 98,9%, que Nuno Benite prefere manter desligado e ser ele a conduzir, para "ter algo para fazer", enquanto está no carro em patrulha. 3 vulnerabilidades de acesso conhecidas.

Nuno, de 34 anos e estatura média, é o tipo de pessoa que vai ao ginásio duas vezes por semana, não porque precisa, até porque tem o mesmo equipamento em casa, e a patroa mantém-lhe a rédea curta, com toda esta nova tecnologia de saber onde andamos a todo momento, nem dá para fazer nada. Só vai ao ginásio mais para socializar com os amigos e ver as vistas às amigas, aproveitar enquanto olhar e pensar ainda não dá multa. Usa a carecada da praxe dos agentes de autoridade, diz que é porque lhe fica bem, mas na verdade é porque dá menos trabalho. E não bebe álcool, porque "isso é para os rotos". Alcunha legitimamente usada por muito boa gente para aquela classe de pessoas que insistem,

obrigadas coitadinhas, em não fazer "parte do sistema", mas que depois também não querem ir viver para a colónia que foi criada para eles no Alentejo, e andam sempre por aí a criar problemas ao trânsito e a chatear as pessoas para deixarem a tecnologia e recuperarem a privacidade. O Nuno diz que se tornou agente da autoridade "porque sim". Índice de possível conversão 0.12

No lugar do pendura, ligado ao sistema imersivo de comunicação com a central, ia João Serzedo, de 25 anos, de estatura média um bocado baixa, mas não muito. Pratica jogging dia sim dia não (quando não está atrasado para o trabalho). Não mantém uma relação “porque nunca calhou” e apesar de ter ficado um bocado desiludido com os seus primeiros seis meses no trabalho de agente de autoridade, ainda acredita que melhora a sociedade em cada dia de trabalho. O João diz que se tornou agente da autoridade porque foi esse o seu sonho desde pequeno, mas nunca revelou em registo o porquê exactamente. Índice de possível conversão 0.67

Transcrição áudio da ocorrência:

- Notificação de ocorrência na Rua da Lapa número 12, somos a unidade mais próxima.

- OK, que tipo de ocorrência?

- Não consegues ver projectado?

- Já sabes que não gosto de ter essa treta ligada enquanto conduzo. Diz lá que tipo.

- Ocorrência de distúrbios domésticos com PEOP 3.8. - potencial de escalada para ofensas puníveis, calculado em tempo real pelo sistema de autoridade, baseados em modelos de predição aplicados ao histórico local recolhidos em fusão sensorial recolhida dos vários dispositivos com acesso ao local: luzes inteligentes, televisão inteligente, telemóveis, frigorífico, visor de entrada, vibradores, máquinas de lavar, secar e engomar, etc

- Não é um puto a praticar neo punk, a atrofiar o sistema todo outra vez pois não?

- Não, é um casal de homens. Não existem outras pessoas registadas no apartamento. A fusão sensorial entre os sistemas dos apartamentos vizinhos confirma.

- Se os dispositivos da vizinha registaram já estão a pagar multa, porque é que temos de ir nós lá?

- PEOP 3.8, caramba!

- OK, vamos lá visitar os pombinhos chateados antes que se aleijem a sério. Por mim, era deixá-los. A minha avó bem dizia "entre marido e marido, ninguém mete preservativo" hahaha...

- Sim, és um respeitador de privacidade de primeira! Acelera mas é, aqui diz que já está a escalar para as agressões físicas. Vou ligar o acesso directo ao áudio de um dos telemóveis...

- ... de merda! Eu vi no sistema, a Raquel mostrou-me! Quem era a puta que esteve aqui das 11:10 às 11:52!? Meu grandessíssimo cabrão! O meu pai bem me avisou que tu não eras de confiança, que tinhas amigos rotos! Treta toda de ...

- ... não se passou nada, cala-te, estás a activar os sistemas!! Como é que a Raquel te deu acesso sem permissão??

- ... quero lá saber da multa, cabrão de merda, mentiroso! Quero-te fora de ...

- ... fala baixo, cala-te!! Deixa-me explicar! Pára, fodax!! ...

- ... toma, meu cabr ...

- HAHAHA! Ele atirou o telemóvel ao outro!! Estes gajos estão loucos!

- Deve-se ter partido com o impacto, deixou de transmitir. Consigo monitorizar os batimentos cardíacos através dos relógios digitais, mas não consigo escutar através do frigorífico, malditos updates de firmware.

- Então e o outro telemóvel?

- É privacidade falsa, está a transmitir áudio expectável, não real, o rectificador da fusão sensorial detectou essa falha no padrão de sincronismo quando começaram a discutir.

- Ui! É terrorista!

- Não podes assumir que é terrorista por tentar exercer privacidade.

- Só se esconde quem tem algo a esconder! E ouviste o que o outro disse, tem amigos rotos! É terrorista de certeza! Manda lá vir a unidade de tecnofobia.

- Temos de ter provas.

- Já as devemos ter, aquela Raquel que ele mencionou deve ser uma entidade gestora qualquer, ou do apartamento, ou do prédio, ou da rua. Envia-lhe um pedido de acesso aos canais de vídeo vigilância do prédio ou apartamento, temos causa provável para efectuar o pedido.

- Tenho os IDs, mas não sei qual deles é a Raquel.

- Merda da mania do direito à privacidade, sempre a atrapalhar o trabalho, qual era o mal de dizer o nome da entidade nos registos de acesso?

- Sabes bem que ainda há discriminação. Apesar de ser ilegal desligar intencionalmente os servidores, ainda há muita gente que acha que a riqueza dos mortos não devia ficar empatada nas mãos das suas entidades artificiais, mas sim devolvida à sociedade! Vou enviar o pedido aos 3, são obrigados por lei a responder aos agentes de autoridade em tempo útil de 5 mins por largura de banda.

- Essas leis só passaram porque foram pagas por gente rica, isso devia ser ilegal, isso não são pessoas, a herança devia ir para o estado e uma pequena taxa para a família, como sempre foi!

- É a lei que temos, temos de a fazer cumprir. Já recebi duas respostas, a entidade do apartamento está configurada para não manter registos a longo termo...

- Que conveniente! Essa merda é que devia ser ilegal!

- A entidade que gere a rua não se identifica como sendo Raquel mas disponibiliza de acordo com a lei o acesso limitado às câmaras de vigilância da sua responsabilidade com visão para o número 12. As entidades gestoras de ruas são obrigadas a guardar os registos.

- Boa, manda já isso para a unidade de tecnofobia. Olha, número 12, é aqui. Vamos lá separar os pombinhos.

Acaba a transcrição às 14:47.

Conclusões probabilísticas do relatório:

É provável com 74.5% de índice de confiança que o operacional Tomás Farto 737480283 se encontra detido em reabilitação tecnofóbica ou em trânsito para ela, sem acesso inconspícuo aos modos de comunicação sem rastreio exigidos pelo nosso standard de segurança e privacidade de operações em vigor. Todas as ligações a ele estão proibidas até notificação em contrário.

É provável com 12.2% de índice de confiança que a entidade Marques Fino 120937211, habitante da Rua da Lapa 12 tenha relações operacionais com o sistema. Todos os operacionais devem evitar futuros relacionamentos.

É provável com 89.7% de índice de confiança que a operacional Cláudia Mota 232549282 seja considerada suspeita de inter-operação ilegal e esteja a ser monitorizada com acréscimo poder computacional de detecção de anomalias ao padrão comportamental. Todas as ligações a ela estão proibidas até notificação em contrário.

É provável com 12.1% de índice de confiança que o operacional Yassmir Vulkov 832812922CC seja considerado suspeito de inter-operação ilegal e esteja a ser monitorizado com acréscimo poder computacional de detecção de anomalias ao padrão comportamental. Mantém-se as ligações activas segundo o nosso standard de segurança e privacidade de operações em vigor.

É provável com 6.2% de índice de confiança que o operacional Afonso Polido 7408206931CC seja considerado suspeito de inter-operação ilegal e esteja a ser monitorizado com acréscimo poder

computacional de detecção de anomalias ao padrão comportamental. Mantém-se as ligações activas segundo o nosso standard de segurança e privacidade de operações em vigor.

É provável com 89.1% de índice de confiança que a entidade Raquel Valente 213038263CC, cibercérebro regente do número 12 da Rua da Lapa, tenha relações operacionais com o sistema. Todos os operacionais devem evitar relacionamentos.

Sou hacker, vivo anónimo nas ruas

Sou hacker, vivo anónimo nas ruas. Como são os meus dias? As manhãs são húmidas, as tardes escuras, as noites cheias de luzes a zumbir. As leis de confinamento parcial ajudaram-me a passar despercebido na maioria das metrópoles que visitei nos últimos meses. Durante o dia visto-me de estafeta de entregas. Raramente entrego alguma coisa. Às vezes é preciso entregar mesmo, para conseguir aceder a algum prédio com segurança particularmente alta. Mas normalmente as pessoas deixam-me entrar e não olham duas vezes. A máscara obrigatória ajuda imenso. Desloco-me de bicicleta ou trotinete eléctrica, daquelas que são alugadas à hora electronicamente. Entro no prédio alvo e finjo-me confuso, a olhar para o meu tablet, como todos os estafetas fazem quando procuram a confirmação de uma morada, permaneço a um canto longe das câmaras enquanto procuro a rede alvo, quando a encontro, acedo como conseguir aceder, instalo o que for preciso instalar, escuto o que tiver de escutar, copio o que for necessário copiar. Mais tarde transfiro a confirmação do objectivo atingido para uma dropbox pública na internet através de uma VPN própria e no dia seguinte sou pago o restante do valor acordado.

"*Mais um protesto anti-corrupção que acabou por se tornar violento, aqui mesmo atrás de mim na Praça do Rossio, ontem ao final da tarde a polícia foi chamada a intervir para controlar a multidão que lhes arremessou pedras e cocktails molotov, foram dispersados com canhões de água mas prometem regressar aos protestos na Segunda-feira. Mais uma das já dezenas de manifestações que se tem organizado um pouco por todo o país nos últimos meses. A reivindicação dos manifestantes é clara: aprovem no parlamento a proposta de lei de expedição jurídica imediata para os casos de corrupção activa. Relembro que as eleições legislativas estão agendadas para daqui a 6 meses e as previsões de voto continuam a dar preferência ao novo partido anti-corrupção formado à pouco mais de 2 meses, surgido no rescaldo de mais uma prescrição de processo de investigação de corrupção activa ligada ao 3º resgate do novo banco e as suas ligações aos membros do governo. Se as eleições fossem hoje, as últimas previsões e sondagens indicam que obteriam 35% dos votos.*"

Aos 4 anos desbloqueei o telemóvel do meu pai, queria jogar Angry Birds. Ele bateu-me por mexer nas coisas dele. Aos 7 anos, se calhar por piada, atirou para cima da minha cama dois dos seus telemóveis mais antigos que já não funcionavam e que já ninguém queria comprar para peças. Um deles não ligava (tinha o ecrã partido e a bateria inchada), o outro tinha-se afogado na retrete. Fui à loja do indiano, pedi-lhe emprestado o kit de reparação de ecrãs em troca das peças que sobrassem dos dois telemóveis, estive lá três horas a desmontar e montar, tive de testar umas coisas, demorei mais do que estava à espera demorar, mas no final do dia consegui meter um dos telemoveis a funcionar! Quando regressei a casa o meu pai estava à minha espera, bateu-me por ter chegado tarde ao jantar e ficou com o telemóvel reparado, não o voltei a ver, deve-o ter vendido, não me deu o dinheiro. Aprendi a nunca confiar em ninguém graças ao meu pai. Hoje em dia cumpro rigorosamente as regras da independência interna encriptada e descartável.

À noite tenho um canto reservado anonimamente junto às docas para dormir, é demasiado húmido para o meu gosto mas serve durante uns dias. Entregam-me em mão a comida dos sem abrigo. Não fazem perguntas e cumprem as leis sanitárias da utilização de máscaras e do distanciamento social. O local dá para dormir umas horas, carregar as baterias dos dispositivos e ver as noticias. Vivo numa redoma de prudência sistemática organicamente desenvolvida. Em recantos sem câmaras onde não me fazem perguntas. Desde que tenham acesso à electricidade são muito preciosos! Quem sabe procurar na dark web encontra vários websites onde o rating tem particular cuidado com o respeito à privacidade. Sei que o rating pode ser um engodo para encontrarem as pessoas que não querem ser encontradas. Pelo sim pelo não cumpro rigorosamente as regras da independência interna encriptada e descartável.

"*A associação Transparência e Integridade apresenta os valores, e eles são claros, o dinheiro desviado do orçamento de estado em casos conhecidos publicamente de corrupção activa que prescreveram em julgado durante este ano, pagariam o Rendimento Básico Incondicional 1.67 vezes o salário mínimo nacional actual a todos os 11 milhões de Portugueses! Pense bem no que acabei de dizer, se não houvesse*

corrupção em Portugal podíamos não só eliminar a pobreza e a grande maioria da criminalidade derivada da pobreza que existe em Portugal, para todos nós escolhermos em que área queremos realmente trabalhar independentemente de estar a gerar dinheiro a um patrão ou não, e trabalharíamos ao ritmo que melhor nos desse jeito. Voltaríamos a ter tempo para a família, reduziríamos o stress causado pelo mundo empresarial focado no lucro, eliminaríamos o trabalho precário, a crise de falta de emprego. Com somente 1 ano de desvios de corrupção conhecida, que os nossos tribunais deixaram prescrever."

Disseram-me que a minha mãe morreu de overdose de Metartropina pouco depois de eu dar à luz. Não sabem os efeitos secundários, ainda não há estudos suficientes.

O meu pai também usava Metartropina, todo o seu dinheiro do RBI era gasto em Metartropina, quando já não tinha créditos para comprar mais roubava dos amigos, até que deixou de ter amigos. A minha avó sabia da situação e cuidou de mim durante uns tempos. Lembro-me que ela me deixava brincar com os computadores dela, desde que eu nunca me ligasse à rede. Mas eu ligava-me às escondidas, foi assim que conheci o Victor.

Conheci o Victor724 através de um forum na dark web. Foi ele que me ensinou a mudar a minha identidade digital periodicamente sem rastreios em menos de 10 minutos. Ensinou-me a registar com as credenciais de outros. A aceder às coisas que não devíamos aceder. Passou-me o código fonte do Predator para eu analisar. Nunca conheci o Victor em pessoa, e um dia desapareceu da internet. Se calhar foi apanhado, ou mudou de identidade mais radicalmente. Deixou de me contactar. Eu também tive de mudar, perdemos o contacto. Se calhar ele ainda anda pelos forums da dark web, com outro nome, como eu ando. Tenho saudades de falar com ele, é a única pessoa na internet que sabe o meu nome biológico. Acho que ele não se chamava Victor.

Quando os serviços descobriram que eu vivia com a minha avó cortaram o RBI ao meu pai. Ele não gostou da situação, obrigou-me a voltar para casa com ele. A minha avó ofereceu-me um computador mas o meu pai vendeu-o para comprar Metartropina. Fiquei chateado com a situação, fiz uns cálculos e matei-o. Não foi de animo leve, simulei a minha

previsão de vida com uma rede neuronal num computador da escola, treinei-a para maximizar a minha sobrevivência a curto prazo e os resultados foram evidentes, era melhor que o meu pai não estivesse incluído no meu plano de vida. Estava chateado, decidi matá-lo. E matei. O RBI não estava a funcionar para ele.

Não encontraram o corpo, ninguém veio investigar. A quem perguntava por ele eu respondia que tinha desaparecido, o que não lhes surpreendia. Pediam-me o dinheiro que ele lhes devia, invadiram-me a casa, levaram a pouca mobília que tínhamos, ainda voltaram um par de vezes mas não havia mais nada para levar. Fizeram o mesmo à minha avó, ela queixou-se às autoridades, eles mataram-na.

No dia seguinte as autoridades vieram ter comigo, informaram-me que não podia viver sozinho, perguntaram pelo meu pai e tentaram convencer-me a ir viver com eles mas eu consegui escapar-lhes. Já tinha planeado fugir do sistema há algum tempo, quando tinham começado as investigações na escola às actividades de práticas de acessos ilegais detectados na rede.

Tinha um computador comigo. Deixei de ir a casa, deixei de ir à escola.

"*Rendimento Básico Incondicional proposto não será suficiente para viver em Lisboa! São as conclusões do estudo levado a cabo pela Universidade Católica e divulgado hoje: a especulação imobiliária e falta de objectivos de vida continuam a levar muitas pessoas ao desespero. Os números de desaparecimentos, crimes leves, suicídio e toxicodependência continuam a aumentar apesar dos apoios financeiros à subsistência. A Metartropina em particular tem alastrado em popularidade, com especial foco nas donas de casa reformadas e nos jovens desempregados. Não perca hoje às 10 da noite o painel de discussão na RTP2 com o João Martelo, secretário de estado para a implementação do RBI Português em debate com os comentadores politicos da RTP*."

Não tenho cartão de identidade nem dados no sistema. Se me pedem documentos respondo "perdi-os" ou "sai à pressa e deixei-os no outro casaco". Tenho um saco de roupa suja, um par de hoodies e camisas das diferentes transportadoras e uma toalha para quando precisar de me lavar. Para aceder ao Hacker Trade ligo-me à rede do router do

McDonalds, todos os dias com um mac address falsificado diferente, todos os dias num McDonalds diferente, às vezes noutro estabelecimento, mas há muitos McDonalds espalhados. Estabeleço uma ligação privada segura e fico ligado exactamente 18 minutos e 26 segundos, mais do que suficiente para sincronizar as minhas transferências, aceitar algo local no Hacker Trade e maximizar ilegalmente o tempo de aluguer da bicicleta enquanto almoço e apago os logs de acesso. A dark web diz que aos 20 minutos conseguem rastrear a ligação do Hacker Trade, prefiro não arriscar.

Pago tudo em numerário, tomo banho no pavilhão gimno-desportivo social, têm cacifos de moedas para guardar a electrónica! Mas mesmo assim mantenho sempre tudo encriptado e artilhado para se auto-destruir com a detecção de acesso ilegal. Mantenho um registo ao nível da BIOS de todas as ligações físicas efectuadas e verifico se o padrão de pó talco polvilhado nos parafusos se mantém coerente antes de voltar a usar a electrónica, temos de ter cuidado com o acesso físico directo ao hardware, é um vector de ataque comum.

"*A lei tem de ser idónea e não ter medo de procurar onde é preciso procurar. A privacidade só é relevante para quem tem algo a esconder!*"

Pelo sim pelo não, para as missões mais críticas, alugo equipamento em segunda mão, facilmente revendido no mercado negro. Tenho um método rápido de preparar o equipamento para qualquer novo uso anónimo ilegal descartável. Primeira coisa que faço é desligar fisicamente a câmara, o microfone e o GPS. Factory reset na BIOS e no sistema operativo, instalo uma sandbox encriptada com o toolkit básico que eu próprio revi e compilei com as últimas actualizações de segurança. Tudo pronto a instalar ou apagar e abandonar em menos de 5 minutos. Sem rasto digital. Assumo sempre que todas as redes a que acedo estarão comprometidas e à minha procura. Só executo missões com a minha ligação devidamente camuflada.

Muitas das vezes nem leio o perfil do alvo. Tenho a identificação da rede, sei o padrão de segurança esperado, o mac address e a descrição do objectivo. Se o objectivo não é claro, não aceito. Se não tenho vulnerabilidades conhecidas para o padrão esperado, não aceito. Se o padrão de segurança no terreno é superior ao esperado no contrato,

cancelo. Se demorar mais do que o esperado a encontrar o objectivo, cancelo. Se mais alguém está presente na rede ou com acesso à máquina para além do esperado, cancelo. Não me importo de perder pontos na reputação no Hacker Trade com missões canceladas. Até me ajuda a manter-me abaixo do radar. Só me importa cumprir as regras da independência interna encriptada e descartável para garantir que não serei vinculado ao crime de acesso indevido.

Tento sempre minimizar o tempo de contacto físico à rede WiFi do alvo. Para missões mais complicadas às vezes tenho de esconder uma máquina dentro do perímetro, para tentar crackar o acesso à rede com mais tempo de acesso, ou à espera que determinado pacote seja transmitido, mas no geral em menos de um minuto o meu software encontra a rede alvo e aplica-lhe a vulnerabilidade para me dar acesso. A partir daí é trivial, acedo ao router e tenho uma lista dos dispositivos por IP, se o router não tiver a password por defeito (ou ter sido configurado para só ser acessível por cabo ethernet) então faço um nmap na rede local que contacta todos os IPs à procura de uma resposta vinda do mac address alvo. Já tenho o metasploit pronto para procurar um protocolo de comunicação vulnerável, é só executar, às vezes demora um bocado, depende do sistema operativo, um Windows Home Edition (5 segundos) é ligeiramente diferente de um Windows Professional (7 segundos) ou de um Windows Server (15 segundos), às vezes também usam Macs (10 segundos) e há sempre um caramelo qualquer com um Linux Ubuntu (15 segundos) que não o sabe configurar devidamente (5 segundos), às vezes também encontro outros brinquedos online, um Raspberry Pi (5 segundos), um ou outro telemóvel Android (20 segundos) ou iPhone (15 segundos), mas o meu preferido são sempre os dispositivos IoT, aquelas luzes, câmaras de vigilância, escovas de dentes, frigoríficos, vibradores e aspiradores com acesso livre à rede instalados sem qualquer segurança na sua configuração (2 segundos). Perfeito para instalar uma backdoor e aceder mais tarde se for caso disso. Se os computadores estiverem seguros devidamente (o que é raro), uso o meu próprio para atacar o router e conseguir snifar o tráfego web. Basta apanhar um pacote não encriptado com um login e password a um website qualquer e já costumo conseguir arranjar qualquer coisa. Em último reduto, se só andarem a usar comunicação encriptada, posso ainda montar um proxy a fingir que sou o website que estão a visitar e explorar as vulnerabilidades

no browser em si: Chrome e Firefox (20 segundos), Opera, Brave (10 segundos), Internet Explorer (5 segundos), Edge (10 segundos). Depois de ter acesso ao browser tenho de escalar os privilégios para ser administrador no sistema operativo, outros 5 segundos. Quando entro na máquina por este método às vezes noto que alguns espertalhões estão a correr uma máquina virtualizada, é uma chatice, obrigam-me a activar o módulo de obter acesso ao sistema anfitrião do VirtualBox (5 segundos) ou Parallels (5 segundos) ou VMWare (10 segundos), depende do que estão a usar e das configurações que activaram, mas todos eles tem vulnerabilidades no kernel conhecidas e o metasploit trata disso facilmente se for configurado para tal. Maior parte das missões estão concluídas em menos de um minuto.

"*Tem sido uma noite histórica, 1 mês após a aprovação da lei, os casos continuam a surgir às dezenas todos os dias, o novo corpo de juízes destacado para fazer cumprir esta lei não tem parado, foram já processados mais de 137 casos, 8 membros do governo foram hoje demitidos. E não é só em Portugal que se celebra, há relatos de dezenas de manifestações de solidariedade à revolução Portuguesa que surgem um pouco por todo o mundo.*"

Às vezes páro uns momentos em frente à instalação interactiva dedicada ao hacker desconhecido, em honra de todos aqueles que possibilitaram a grande limpeza de 2025, a revolução política que obrigou ao abandono de 84% dos deputados da Assembleia da República, grande maioria destes casos foram trazidos a público através do Hacker Trade. Eu fui um desses hackers. Os processos foram investigados e executados imediatamente, ao abrigo da nova lei de expedição jurídica de casos de corrupção.

A prometida reforma jurídica funcionou. Mal a lei foi aprovada houve uma cascata de limpezas de toda a corrupção instalada à décadas no sistema público, de um dia para o outro já não importava se a informação fora obtida legalmente ou ilegalmente, só importava se era verdadeira, e o juiz que não cumprisse a expedição imediata era o próximo a ser investigado. Foi um boom de pedidos de investigação no Hacker Trade, para hackers investigarem mais a fundo certas suspeitas que toda a gente conhecia mas que o ministério público nunca conseguia obter provas definitivas, tornou-se uma batalha de todos contra todos,

toda a gente tinha algum podre, e todos foram escrutinados até só sobreviverem em cargos públicos os nus, aqueles poucos que mantinham idoneidade perante todo o escrutínio à sua privacidade tal como revelado pelo Hacker Trade.

Finalmente tinha sido encontrado o verdadeiro sistema anti-sistema, que conseguiu agregar interesses de todo o espectro político: o populismo, o liberalismo, o socialismo. Todas as tensões sociais que pareciam asfixiar a nossa ténue civilização foram respondidas na auto-destruição canibal da corrupção. Em poucas semanas o panorama político mudou radicalmente. As maiores empresas privadas declararam falência perante a enormidade de casos de aproveitamento ilicito trazido a público. As empresas do estado foram obrigadas a despedir a maioria dos seus gestores e a abrir concursos para posições de admissão de nus. A camada jovem recém formada finalmente encontrou motivação para se formar nas suas áreas de interesse e sair das universidades com uma posição de trabalho garantida. Só tiveram de ceder todo e qualquer direito à sua privacidade.

A falta de capacidade das cadeias para alojar a enorme onda de prisões trouxe o caos e obrigou a uma reforma política também referente ao sistema prisional, instaurou-se definitivamente o modelo de prisão domiciliária sem direito à privacidade e as prisões passaram a só albergar os reincidentes de crimes violentos. O rendimento básico incondicional foi revisto, premiando os nus.

A investigação policial foi rapidamente privatizada para sistemas como o Hacker Trade. Muitos dos culpados de corrupção voltaram aos estudos para conseguirem reencontrar algo que lhes apaixonasse fazer sem participar em esquemas de corrupção. Outros simplesmente entraram em reforma antecipada ou desapareceram do sistema. A onda de interesse neste novo modelo político e social adoptado por Portugal infectou a Europa e rapidamente se espalhou pelo resto do mundo, governos de vários países foram obrigados a adoptar leis similares ou a escalar a censura e repressão activa de quem advocava a adopção destas leis. Muitos países entraram em guerra civil devido a isso, a emigração mundial aumentou.

O Hacker Trade continuou a crescer exponencialmente em oferta e procura... Até que os próprios hackers começaram a ser vítimas das investigações de outros hackers. A oferta de profissionais diminuiu significativamente com o aumento do risco de represálias. Passado 4 anos o mercado de hackers investigadores começou finalmente a nivelar.

Agora a conversa na dark web é outra, como reclamar de volta o direito à privacidade que perdemos para destruir a corrupção? A liberalização da privacidade assume-se agora irreversivel.

"*Esta foi a terceira manifestação agendada contra a chamada destruição da privacidade, seguida de perto, mesmo aqui ao lado, por uma contra manifestação que conta com protestantes a favor do endurecimento das medidas anti-corrupção. Os ânimos exaltaram-se um pouco durante a tarde, a polícia de segurança pública foi chamada a intervir para evitar desacatos. De um lado exige-se o regresso ao direito à privacidade tal como originalmente previsto na constituição. Do outro lado gritos de ordem para se continuar a avançar com a nova república, travar agora a revolução seria voltar à podridão que tínhamos, dizem os protestantes.*"

Enquanto esta vulnerabilidade de acesso aos routers locais da Exces se mantiver activa vou ficando mais uma semana por Paris, a França ainda está em estado de bruma na sua própria revolução de transparência legislativa. A situação ainda não chegou politicamente ao que aconteceu em Portugal mas é considerado inevitável pelos peritos. Entretanto os números de missões acessíveis no Hacker Trade vão-se multiplicando como cogumelos. Algumas vulnerabilidades são mais caras ou difíceis de arranjar do que outras, e os routers são ligeiramente diferentes. Ir para outra cidade implica quase voltar à estaca zero mas de vez em quando convém mudar de ares. Cumpro rigorosamente as regras da independência interna encriptada e descartável. Não posso usar vulnerabilidades que mais ninguém esteja a explorar, seria unicamente identificativo. Quando encontro algumas dessas, vendo-as no mercado negro! Só quando outros tantos já as usam é que as passo a usar também.

"*Mais um grupo de anarquistas foram hoje identificados e sujeitos a termo de identidade e residência. Uma célula de 12 operacionais que dinamizavam anonimamente na internet a organização de novas*

manifestações a apelar à restauração da privacidade em Portugal. Foram apontados à policia através do conhecido portal Hacker Trade."

Não gosto das missões em que tenho de apagar os meus passos. Pode-me sempre escapar qualquer coisa e é algo impossível de automatizar em segurança, ouvi rumores de que algumas equipas, se calhar a cargo de projectos nacionais ou privatizados tem acesso a esse tipo de software, mas nunca o vi a funcionar ao vivo e duvido da sua eficácia. Podem sempre estar a snifar tráfego ou monitorizar alterações aos logs. É bastante mais fácil fingir ser tráfego normal do que andar a tentar apagar entradas em logs aqui e ali e acoli que ainda podem estar a deixar mais logs suspeitos no sistema. Por estes motivos não gosto desse tipo de missões, evito-as. Quando são missões de fingir que não estive lá, não aceito. Quem as foi aceitando acabou a ser apanhado. Mesmo assim há quem as rotule como o sendo o real desafio que determina quem é o verdadeiro hacker. A mim parece-me engodo para tentar estabelecer contacto com os melhores hackers que existem e apanhá-los para acabar com a sua actividade ou os forçarem a trabalhar para eles. Cumpro rigorosamente as regras da independência interna encriptada e descartável. Não gosto dessas missões.

"*Em discussão hoje na assembleia esteve o pedido de alteração ao modelo de divisão e taxamento de serviços privatizados, o bloco liberalista referencia números do recente estudo da Universidade Católica sobre o impacto nos últimos 5 anos do RBI em Portugal: Ainda há muito caminho a percorrer, temos de dar mais apoios às empresas privadas para conseguirem contratar.*"

Às vezes o maior problema é mesmo conseguir pagar sem deixar rasto. Algumas cidades só aceitam electrónica para pagamento, o que implica acessos rotativos a contas previamente comprometidas por outros, pode ser perigoso, os algoritmos desenvolvidos para detectar transacções suspeitas estão sempre em mutação, é incerto se o nosso acesso foi detectado ou não, assumo sempre que foi. As transacções tornam-se ainda mais perigosas se houver câmaras presentes, e hoje em dia há câmaras em todo o lado! Se pagar electronicamente deixo rasto digital para as câmaras irem investigar. Por outro lado obter dinheiro real para pagar em numerário também apresenta os seus desafios, a única vantagem é a menor frequência de o ter de fazer, se se levantar uma

grande quantidade. Mas obviamente que levantar grandes quantidades irá activar com mais probabilidade os algoritmos de detecção de comportamentos suspeitos. Acabamos por ter de confiar nos contactos locais do mercado negro. O que é muito arriscado, não recomendo. Tive de mudar de cidade várias vezes na minha vida devido a isso. Na europa do leste é que é lindo, torna-se tudo mais fácil quando há máquinas de moedas de criptocurrência com anonimato assegurado em vários pontos da cidade. A volatilidade do valor é significativa mas ao menos não tenho de andar a hackar torres de comunicações para obter códigos telemóvel necessários para confirmar o 2FA, que nunca sei quanto tempo vai continuar a funcionar, e tenho sempre medo que me estejam a triangular a posição. Pena que não haja tantos contratos disponíveis no Hacker Trade para a europa do leste senão ficava por lá a tempo inteiro. Quando tenho de levantar dinheiro fisicamente tento fazê-lo com uma regularidade disruptiva, nunca no mesmo multibanco, excepto quando repito um multibanco para confundir a detecção do padrão. E mesmo assim só vou à noite, com o meu hoodie bem posto e uma máscara dinâmica de geração aleatória de identidades falsa. São ilegais nos países de privacidade apertada mas vale a pena o risco de se ser filmado. Se o código do cartão não for processado em 23 segundos ponho-me a andar. Já perdi alguns cartões à conta disso mas é melhor jogar pelo seguro e cumprir rigorosamente as regras da independência interna encriptada e descartável.

"*Números históricos apontados hoje pelo porta-voz do governo do PAC (Partido Anti Corrupção), o famoso portal de pedidos de denúncias Hacker Trade atingiu os números mais baixos de missões transaccionadas em território Português da última década, cito o porta-voz: Sinais claros que a revolução anti corrupção cumpriu o seu objectivo em pleno, vivemos hoje num país transparente, já não precisamos de alguém para nos apontar o dedo, não há nada a apontar que já não se saiba.*"

Cheguei a ter uma identidade falsa com algum histórico comprovável, mas não era profundo suficiente, foi comprometida por um hacker quando a usei para aceder ao sistema de saúde para tratar de um dente que me andava a chatear. Tive de abandonar a identidade e agora o

sistema tem a minha aparência (e registo dentário) nos registos suspeitos. Foi aí que decidi ir para Paris à boleia.

Desde a revolução que os preços se tornaram bastante mais.. competitivos.. para obter uma nova identidade falsa, especialmente das credíveis, que são verificáveis pelo governo sem activar alarmes. Mesmo quando encontro um desses negócios em oferta fico sempre na dúvida se não será um engodo…

Agora o meu sonho é conseguir viver anonimamente com um número de segurança social, história de estudos resistente ao escrutínio, impostos, histórico de renda da casa e registo dentário privado. Quanto mais velho fico mais difícil se torna arranjar uma identidade falsa real. E há sempre um hacker como eu a tentar encontrar falhas nas histórias dos outros para ganhar créditos no Hacker Trade. Tenho andado à procura de vulnerabilidades nos diversos sistemas, a ver se um dia consigo eu mesmo criar a minha própria identidade sem ser detectado. Mas houve muita gente a pensar o mesmo, criaram sistemas com redundâncias e controlos de acesso mais restritos, são outro campeonato de hacking, só posso avançar quando tiver acesso em todos os sistemas ao mesmo tempo. Enquanto tento encontrar uma maneira de aceder à segurança social, a segurança do sistema de saúde foi actualizada e tenho de voltar a começar a busca de vulnerabilidades desde o inicio... Começo a perder a esperança de me poder reformar anonimamente.

Se calhar devia deixar de ser hacker, de viver anónimo nas ruas. Ir até à segurança social, dar o meu nome verdadeiro e pedir para me regularizarem a situação. Comprometo as regras da independência interna encriptada e descartável, provavelmente seria identificado por alguém contratado no Hacker Trade. Se calhar colocam-me numa casa de vidro sem qualquer acesso à internet e uma cama sem humidade o resto da minha vida… não seria muito mau para uma reforma, poderia voltar à escola e completar os estudos. Se calhar o Victor até está a monitorizar essas bases de dados e eu voltaria a entrar em contacto com ele! Mas o mais provável seria recrutarem-me para trabalhos forçados de cibersegurança mercenária. Por enquanto prezo mais a minha privacidade mas gostaria de ter opções.

Boas práticas reais

Estes contos são ficção especulativa mas muita da tecnologia referida é real. Fica aqui um guia de boas práticas para ajudar a reflectir e melhorar a privacidade digital do ponto de vista do utilizador:

Acesso físico à máquina do utilizador

A maneira mais simples de espiar alguém digitalmente é ter acesso físico à máquina ou à rede em que a máquina está ligada.

Com o acesso físico conseguimos roubar a máquina (para aceder mais tarde com tempo e vagar) ou instalar dispositivos que escutam a máquina (com baixa probabilidade de serem detectados), torna-se mais simples aceder aos dados do disco rígido do computador (se não estiverem devidamente encriptados), e até poderá ser possível instalar software que permite ver e ouvir tudo o que acontece na máquina.

É aconselhável que máquinas com dados privados importantes se encontrem num local de difícil acesso físico que impeçam a manipulação indevida. Portas com fechaduras, câmaras de vigilância, instaladas em locais que não seja trivial alguém aceder ou manipular sem ser identificado.

É igualmente aconselhável encriptar os dados do disco (usando o Veracrypt por exemplo), mantendo cópias de segurança encriptadas regulares da informação mais crítica e guardá-las em duplicado em locais separados mas igualmente seguros.

E o mais óbvio, ter uma senha de acesso ao computador segura.

Os telemóveis também são máquinas, também podem ser acedidos e manipulados. Trate-os com igual cuidado. Cada vez mais os telemóveis são alvo preferencial de vulnerabilidades e ataques.

Sistema operativo

Tudo o que fazemos na máquina pode ser observado pelo sistema operativo instalado. Foram recorrentes as notícias de abuso de acessos a dados privados por parte da Microsoft, Apple e Google e outros

operadores. Por serem os sistemas mais usados são também alvos constantes de novas aplicações de software maligno.

Novas aplicações de anti-virus ou assistentes de Inteligência Artificial querem aceder a todos os dados do sistema operativo “para nos poderem ajudar”, tenha a certeza que estes sistemas de vigilância não estão instalados quando não precisa deles. Não há garantias de respeitarem e protegerem os seus dados privados.

O sistema operativo menos intrusivo à privacidade e menos alvo de spyware continua a ser o Linux, há várias distribuições à escolha com maior ou menor foco na privacidade e encriptação de dados.

Igualmente importante é usar contas diferentes para tipos de acessos diferentes. Todas devidamente protegidas com senha de acesso segura e distinta. Não abandone a máquina com as suas sessões abertas para outros usarem. Eles não precisam de acesso aos seus bookmarks, ficheiros de passwords, logins automáticos, e-mails, documentos privados, etc.

Browser

Maior parte da actividade online hoje em dia passa por usar um browser de internet para navegar por diferentes páginas. Maioria dos browsers guarda cookies de navegação que podem ser usados em conjunto com a informação da máquina e do browser para identificar unicamente a pessoa que está a utilizar o computador.

Fazer login no browser na cloud para partilhar atalhos e acessos de outras sessões suas de outro computador é útil mas está sujeito a acessos indevidos de terceiros. Toda essa informação está guardada algures. A cloud consiste em servidores num centro de dados desconhecido que podem estar a ser acedidos por terceiros se não estiverem devidamente protegidos.

A maioria das páginas web também usa anúncios como maneira de monetizar o seu conteúdo, estes anúncios são usados como camada adicional de identificação da pessoa e a informação sobre a pessoa e os seus hábitos de navegação são vendidos a terceiros.

Para maior segurança e privacidade online recomenda-se usar browsers sem cookies (modo incógnito), utilizar bloqueadores de anúncios (como

o adblock), ou browsers com maior foco na privacidade (há vários gratuitos em constante desenvolvimento, encontre um que mais se adeque à sua utilização).

Email

Por conveniência a maioria das pessoas costuma usar contas de email gratuitos de grandes operadoras. Muitas delas não usam tráfego encriptado na transmissão dos emails.

O tráfego não encriptado pode ser lido por operadores do serviço de internet ou outros agentes maliciosos presentes na rede. Também é conhecido como prática comum as grandes operadoras lerem o conteúdo dos emails para melhorar o algoritmo de venda de anúncios, sem garantias de quem tem acesso a essa informação e com acordos conhecidos com agências do governo para dar acessos às contas (o projecto PRISM exposto por Snowden por exemplo).

Para quem não tem nada a esconder não importa muito quem está a escutar, mas imagine que vive num país onde o jornalismo e activismo democrático são activamente reprimidos, o perigo é real em se enviar um email com conteúdo que não agrade a alguém no poder.

A alternativa mais privada é usar servidores de email próprios (que vem com os seus próprios desafios e custos) ou serviços de e-mail como o protonmail que tem a privacidade em primeiro lugar de importância.

Outra prática recomendável é usar telemóveis e contas de e-mail distintas para utilizações distintas. O exemplo mais óbvio é separar a vida pessoal do ambiente de trabalho, aplique a mesma lógica a outros pontos de interesse que não necessitam da sua informação pessoal. Múltiplas contas de e-mail são mais chatas de gerir e configurar, mas garantem que não há cruzamento de informação.

Evite nomes óbvios para as contas de e-mail dissociadas. Se usar primeiro e ultimo nome ou sempre o mesmo nome de acesso em todas as contas torna-se trivial terceiros associarem a pessoa ao e-mail ou adivinharem o seu nome de acesso em outros websites.

Se está a criar uma conta num website que não irá voltar a usar, utilize um gerador de contas de e-mail temporárias descartáveis, há vários disponíveis online.

Outro dos problemas mais comuns com a utilização de e-mail são os e-mails de phishing, onde alguém através de uma mensagem enviada pede ao utilizador para clicar num link ou executar uma aplicação ou script. Este tipo de e-mails são desenhados para enganar as pessoas e os perigos são reais, esses links tipicamente contém vulnerabilidades que permitem a terceiros obter acesso remoto à nossa máquina e informação. É importante ter o cuidado de reconhecer a legitimidade de quem nos está a enviar o e-mail, e sempre que possível ter contas de e-mail com filtros de spam que filtram este tipo de conteúdos malignos.

Rede de acesso à internet

A rede de acesso à internet é das camadas mais exploradas para violar a privacidade. Quer ao nível da rede local, quer ao nível do serviço de internet.

Se o tráfego que sai do computador não está encriptado, qualquer máquina com acesso à rede local consegue-o ler. O serviço de internet em si consegue igualmente ler todo e qualquer tráfego que passa pelo seu serviço. E mesmo quando os dados estão encriptados na transmissão e temos garantias que o serviço de internet não espia nos seus utilizadores, nem está comprometida por terceiros que o possam estar a fazer, nem mantém acordos com o governo para facilitar acesso a esse tipo de informação, os pontos de entrada e saída da encriptação podem mesmo assim estar comprometidos, à escuta, ou a servir de identificador de acesso (se sabemos que esta pessoa acede ao seu computador 3 vezes num dia usando um serviço de anonimização e 3 vezes no mesmo dia à mesma hora aparece actividade num dado website, conseguimos inferir que a actividade vem provavelmente dessa pessoa). Avanços na tecnologia de sistemas de detecção de padrões torna estas tarefas triviais.

Há várias protecções que podem ser usadas para minimizar o problema mas todas elas envolvem contrapartidas e nenhuma é 100% segura. Usar uma VPN de confiança ou encaminhar o seu tráfego pelo Tor ajuda imenso a anonimizar o tráfego mas não são soluções invulneráveis e a sua utilização torna toda a navegação mais lenta devido aos passos extra necessários.

Outros projectos recentemente anunciados como o Veilid prometem melhor segurança no futuro mas ainda se encontram em desenvolvimento.

Redes sociais

As redes sociais são dos websites mais usados pela população. Tem vulnerabilidades a vários níveis. A mais óbvia é a partilha pública voluntária de informação que deveria ser considerada privada.

Outra das vulnerabilidades é o múltiplo acesso em diferentes máquinas e diferentes redes públicas (quando usadas no telemóvel), que aumenta as probabilidades de uma delas ser comprometida.

A terceira vulnerabilidade é o uso de senhas de acesso fracas, para serem mais facilmente introduzidas, e muitas vezes até são reutilizadas para contas do mesmo utilizador em vários websites, outra falha de segurança grave.

Alguns websites tem como perguntas de recuperação de password informações que podem em alguns casos serem obtidas por alguém que conheça a pessoa. E muito raramente estes sistemas usam 2FA (two factor authentication) para confirmar o acesso.

Se tudo isto não bastasse, os sistemas de mensagens destes websites são tipicamente não encriptados (qualquer máquina na rede consegue ler a mensagem), são alvos recorrentes de ataques malignos devido à sua popularidade (o que significa uma maior probabilidade dos nossos dados privados serem acedidos ilegitimamente) e a maioria deles tem acordos com o governo para facilitar o acesso a quaisquer contas suspeitas de crimes.

Este tipo de páginas também tende a requerer fotocópia de um elemento identificativo e um número de telefone para confirmar que a conta não é de uma identidade falsa. Ficando com mais informação identificativa do utilizador.

Recomendo não utilizarem este tipo de websites. Há alternativas de frontend de websites como youtube e instagram, que garantem melhor anonimidade / privacidade, por exemplo o Invidious ou o Piped.

Telemóveis

Os telemóveis tem sido cada vez mais alvo de ataques de segurança. São computadores e tem as mesmas vulnerabilidades que os computadores de secretária. Em alguns casos talvez até mais, por terem mais serviços que transmitem informações privadas activados por defeito. O GPS sendo o mais óbvio, a operadora sabe a todo o momento onde o telemóvel se encontra.

O número de telefone estar sempre associado oficialmente a uma identidade real com nome e comprovativo de morada associados em sistema torna o telemóvel um identificador único notório. Isto torna os telemóveis de números descartáveis a única maneira de ter alguma privacidade.

Mas há outros usos do telemóvel que também deixam rasto:

- o serviço de bluetooth ou WiFi hotspot activo pode ser usado para georeferenciar com mais detalhe do que o GPS o histórico de viagem da pessoa (há aeroportos e centros comerciais a usar essa informação)

- a memória das redes WiFi visitadas pode indicar associações georefenciadas a terceiros em análise forense

- os dados de contactos telefónicos guardados “na nuvem” em servidores desconhecidos podem ser obtidos por terceiros

- as conversas de mensagens privadas através de serviços que não são encriptados por defeito deixam toda a conversa à escuta de terceiros

- o 2FA obrigatório por SMS em certas páginas web obrigam a ter o telemóvel ligado e presente consigo naquele momento

O telemóvel acaba por ser um dos pontos mais vulneráveis da privacidade digital dos indivíduos na sociedade actual. É fascinante como toda a gente anda com um na mão ou no bolso pronto a ser perdido ou roubado sempre que sai à rua.

Conclusão

É bastante inconveniente garantir a nossa privacidade digital e anonimidade online.

A privacidade completa, verdadeiramente anónima implicaria a completa separação de acessos às máquinas, redes e contas que possam identificar

a pessoa, não basta usar a internet do vizinho e achar que se é invisível, temos de usar outro computador, outro número de telefone, outras contas de e-mail e redes sociais. Ser efectivamente outra pessoa.

Na prática não é preciso ser tão radical para evitar problemas, podemos facilmente reduzir os riscos com pequenas acções e hábitos:

- Evitar publicar dados privados em websites públicos

- Usar passwords complexas seguras, não reutilizar passwords em vários websites

- Não dar acesso das nossas contas ou máquinas a terceiros

- Usar sistemas operativos, browsers e aplicações mais conscientes da importância da privacidade

O mais importante, acima de tudo, é estar ciente dos problemas e perigos, para conseguir ter o mínimo de cuidado para se proteger de possíveis ataques e abusos sempre que achar relevante ter de o fazer para proteger o seu direito à privacidade.