Geoprivacidade, pegada digital e vida *online*...

Editor
Associação de Professores de Geografia
Bairro da Liberdade, Rua C2, Lote 9 - Loja 13
1070-023 Lisboa

ISBN - 978-972-99669-9-6
Título - Geoprivacidade, Pegada Digital e Vida Online...
Autor - Pedro Cortesão Casimiro
Suporte - Eletrónico
Formato - PDF / PDF/A

Fonte da imagem de capa:

Teachers Pay Teachers

https://www.teacherspayteachers.com/Product/What-is-my-digital-footprint-poster-3005468

Geoprivacidade, pegada digital e vida *online*…

Pedro Cortesão Casimiro
Geografia e Planeamento Regional - NOVA FCSH
pjcc.casimiro@sapo.pt

"Surveillance and privacy are mutually exclusive: if one increases, the other decreases. […] The two terms can almost be understood as antipodes. The more (or less) surveillance there is, the less (or more) privacy there is. Thus, in an argument about omnipresent surveillance, we commonly speak about the death of privacy".

Paaschel & Klauser (2015)

"In the post-Snowden era, the central question we face is no longer *if* we are being spied on, but *who* gets to decide how our data is used. Who watches the watchers? Will it be a secret court? Or will the public oversee the watchers? As citizens of a democracy, we hold the answer in our hands".

Angwin (2015)

Agradecimento

Agradeço à Direcção da Associação de Professores de Geografia (APROGEO) o desafio, a disponibilidade e o interesse em editarem e partilharem este ensaio como e-Book. Os Professores de Geografia são, quanto a mim, o público ideal para debater o tema-problema da geoprivacidade, fazendo a ponte com os mais jovens, que a par dos menos jovens são, tudo indica, os que têm menos noção dos riscos e questões inerentes à sua pegada digital e privacidade. Estou ao inteiro dispor para os ajudar nessa divulgação e sensibilização.

Resumo

Todos os indivíduos que têm uma vida *online*, deixam atrás de si uma enorme pegada digital, que põe em causa a sua privacidade como pessoas e cidadãos e que a maior parte não conhece. Para se poder diminuir essa pegada e controlar a privacidade, de acordo com os desejos e necessidades de cada um, é essencial entender como essa pegada digital se forma, quais os dados que a constituem, como é recolhida, por que mecanismos, em que actividades e plataformas. Isto é particularmente importante com a banalização e generalização do uso de *smartphones*, que associam capacidade de localização, recolha de informação multimédia e acesso à Internet, a uma total portabilidade.

Um dos aspectos mais importantes dessa pegada, os dados de localização pessoais, podem ser recolhidos de várias formas, conjuntamente ou não, recorrendo a um conjunto de técnicas que é essencial conhecer, por forma a tomar decisões quanto à forma de mitigar ou bloquear a recolha desse tipo de informação. Este tipo particular de dados levanta uma questão específica, da geoprivacidade enquanto direito dos cidadãos, sobretudo quando se tem noção dos perigos subjacentes, caso haja acesso a essa informação.

Apresentando exemplos e casos, concretos, de como a falta de geoprivacidade pode ser perigosa, podendo, no entanto, produzir informação muito interessante, pedagógica e relevante, consegue-se ter melhor noção das situações e circunstâncias em que se deve, ou não, controlar a recolha desse tipo de dados. Um aspecto, também importante e de muitos desconhecido, é a existência de um mercado rentável, obscuro e criminoso, para o roubo e venda de todo o tipo de dados pessoais, que tem levado a grandes fugas de informação, além de ataques, às empresas e organizações a quem muitos dos dados são confiados.

A vida *online* das pessoas depende muito do uso de *smartphones*, que têm impactos a vários níveis na vida dos seus utilizadores, nos seus hábitos, percepção do espaço, sobretudo através das possibilidades de localização, GPS e sistemas associados. Toda a capacidade de recolha de informação, em quantidades enormes, *Big Data*, se centralizada, pode levar a um cenário de vigilância dos cidadãos, autêntico *Big Brother*. Na sequência dessa possibilidade, mas também para a combater, há legislação específica, que deve ser conhecida, pois defende a informação que é recolhida dos cidadãos digitais.

Interiorizando, compreendendo e investigando todos estes aspectos, cada pessoa pode (deve), saber como controlar a sua privacidade, minimizando ou apagando a sua pegada digital, através de várias soluções, depois de procurar e verificar qual é a sua pegada *online*.

Índice

Índice de Tabelas

Índice de Figuras

Todos os *links* nas notas de rodapé, texto e referências bibliográficas, foram verificados entre 23 e 25 de Maio de 2019.

Pegada Digital

Todos aqueles que têm uma vida *online* criam, num Computador Pessoal (*PC*), *Tablet* ou *Smartphone*, voluntariamente ou não, sabendo ou não que o estão a fazer, uma enorme pegada digital que é em grande parte indelével e constitui, actualmente, um dos principais recursos utilizados por algumas das maiores empresas mundiais para gerar lucros prodigiosos. Seja simplesmente navegando *online*, procurando produtos ou fazendo compras, estando presente em redes sociais, partilhando ou não material variado, opiniões e dados, interagindo com entidades oficiais ou procurando informação, em todos os tipos de plataformas, deixamos um enorme rasto de informação. Um dos tipos mais importantes desta informação é, actualmente e cada vez mais, a nossa localização geográfica e sua evolução no tempo. Com a massificação dos *smartphones*, junta-se um telefone a um computador, acesso á Internet e localização precisa graças a *GPS*, continuamente, no espaço e no tempo.

Figura 1 - Bartoon[1]

O objectivo deste ensaio é analisar como se cria esta pegada digital, quais os vários tipos de informação recolhida e como é recolhida. Na sequência dessa análise abordar a questão especifica da geolocalização, aspectos técnicos ligados ao processo e questões de privacidade que essa informação levanta. Serão depois apresentados exemplos de fugas deste tipo de informação, perigos subjacentes à divulgação e disponibilização deste tipo de informação, bem como vantagens práticas quotidianas e das quais dificilmente prescindimos. Serão ainda tratados outros problemas e questões relacionadas com a privacidade dos dados de localização, nomeadamente de ordem legal. Por último, sugestões para resolver este problema, diminuir a exposição e pegada digital ou então, até, tentar desaparecer da Internet.

O que é, então, a pegada digital? Segundo Wikipédia (2019) "A pegada digital ou a sombra digital refere-se ao conjunto pessoal único de actividades, acções, contribuições e comunicações digitais rastreáveis que são expressas na Internet ou em dispositivos digitais. Existem duas classificações

[1] https://www.publico.pt/bartoon/18-05-2019

principais para pegadas digitais: passiva e activa. Uma pegada digital passiva é criada quando os dados são recolhidos sem o proprietário saber (também conhecido como fuga de dados), enquanto pegadas digitais activas são criadas quando os dados pessoais são libertados deliberadamente, por um utilizador, com o objectivo de compartilhar informações sobre si mesmo, de sítios ou redes sociais."

Toda esta informação pode ser armazenada de várias formas, segundo Wikipédia (2019), se for *online*, a pegada passiva pode ficar registada numa base de dados *online* como um "impacto" e pode registar o endereço IP do utilizador[2], quando foi criado e de onde veio, podendo ser analisado posteriormente. Caso seja num ambiente *offline*, a pegada pode ser armazenada em ficheiros, aos quais o administrador pode aceder. Já as pegadas digitais activas podem ser armazenadas de várias formas, dependendo da situação, mas sobretudo quando se coloca informação (*post*) ou se edita algo. Uma grande parte desta informação são metadados, ou seja, informação sobre informação, e.g. hora, data, local e dispositivo utilizados para aceder a determinada página ou serviço, que pode ser analisada posteriormente em grande quantidade (*Big Data* de que se falará, também, mais adiante).

Quando se navega na Internet (*World Wide Web*), utilizando um navegador (*browser*), deixamos um enorme rasto de informação no dispositivo que estamos a utilizar e *online*, pois os sítios visitados guardam dados sob a forma de *cookies*, executam pequenos programas (*scripts*) e registam a actividade do utilizador, mesmo que este não introduza qualquer informação. Embora se explore brevemente e sem aprofundar, mais adiante, os processos pelos quais esta informação é recolhida, o objectivo final é criar perfis dos utilizadores para efeitos comerciais, de marketing e publicidade, tendo, contudo, outras potencialidades e riscos inerentes. No caso das redes sociais, em que se partilha activamente e emite opiniões (de agrado, desagrado), pode-se criar um perfil completo da pessoa e da sua personalidade, gostos, opções políticas, etc.

Toda esta recolha de informação levanta questões, sérias, de privacidade, que vão desde a propriedade dos dados, à existência ou não de autorização para a sua recolha, análise ou posterior utilização. Resumindo, como é referido em Wikipédia (2019): "Embora a pegada digital possa ser usada para deduzir informações pessoais, como traços demográficos, orientação sexual, raça, visões religiosas e políticas, personalidade ou inteligência sem o conhecimento dos indivíduos, também expõe os indivíduos à esfera social". É neste contexto que aparece o Regulamento Geral

[2] "Um Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, *smartphone* etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação. Um endereço IP serve duas funções principais: identificação da interface do hospedeiro ou de rede e endereçamento de localização." Por exemplo: 185.174.156.19, esse endereço é atribuído pelo fornecedor de acesso à Internet e é variável, para saber o seu endereço IP em dado momento: https://whatismyipaddress.com/

sobre a Protecção de Dados (RGPD) Europeu, que pretende garantir a autorização prévia e explicita, do utilizador, para a recolha dos dados. No entanto, como se verá, a maior parte dos utilizadores autoriza sem ler, não tendo plena noção do que está em questão em termos de privacidade, sem se preocupar muito, ou achando que esse é um preço justo a pagar para ter acesso a determinados serviços. Desta forma, aceitamos mecanicamente cookies em páginas, condições para fazer registos, instalação de aplicações, como se isso fizesse quotidianamente parte do "jogo".

A dimensão da pegada digital dos que têm uma vida *online* é enorme e crescente, podendo chegar a um ponto, como refere Oliveira (2019), em que seja "possível criar agentes digitais que se comportem, em muitos aspectos, como as pessoas que deram origem aos registos digitais. Martine Rothblatt, uma conhecida empreendedora, jurista e autora do livro *Virtually Human*, acredita que, num futuro não muito distante, os registos digitais deixados por cada um de nós permitirão recriar seres humanos virtuais, agentes digitais que se comportem como uma espécie de alter-ego para cada um de nós, e que poderão ser usados para preservar digitalmente não só as memórias mas também as personalidades e os interesses dos indivíduos que decidirem usar este mecanismo".

A questão que se põe, então, é qual o valor dos nossos dados? Inúmeras empresas recolhem e geram enormes receitas com esta informação que, activa ou passivamente partilhamos, voluntariamente ou não, e pela qual não recebemos qualquer "pagamento", nem participação nos lucros. Como refere Garcia (2019) "A maioria dos modelos de negócio na web têm, também por objectivo, recolher o máximo possível de dados dos utilizadores, persuadindo, premiando ou penalizando o acesso a funcionalidades de aplicações ou sítios webs, para recolherem assim mais dados e utilizarem-nos em benefício próprio ou mesmo vendê-los. E, estes dados têm atualmente um valor cada vez maior. A ciência de dados permitiu que estes tivessem uma importância e uma relevância superior, permitindo às empresas perceberem melhor os seus clientes, os seus hábitos e preferências".

O mesmo autor acrescenta ainda que "Vivemos na era da economia de vigilância, onde todos os nossos dados são vigiados e controlados. […] toda a informação que trocamos e possuímos, é recolhida e controlada na economia, sendo o nosso comportamento enquanto consumidores e cidadãos, controlado por essa análise de vigilância feita por algoritmos de grande volume de dados (*Big Data*). Parte do sucesso desta economia de vigilância, está relacionada com o facto de que existe sempre um benefício na partilha de informações pessoais. É quase sempre oferecido algo em troca dos nossos dados, seja o acesso a um conteúdo, à personalização de uma experiência, ou à utilização completa de um serviço. É este o valor que estamos a atribuir actualmente aos nossos dados pessoais — o valor de um pequeno brinde. […] A curto e a médio prazo, o maior problema da protecção e da privacidade dos dados não está apenas relacionado com o seu valor económico. O grande perigo é o de interiorizarmos e aceitarmos que a vigilância

constante dos dados é o novo normal, e começarmos a autocensurar os nossos comportamentos, hábitos e conversas, perdendo a nossa liberdade individual".

Pode-se abordar a questão da pegada digital, como um modelo de negócio digital com duas faces, a nossa privacidade seria o negócio de outrem (Fish, 2009), ou posto de outra forma: "se um produto é gratuito, nós somos o produto". Efectivamente, quase todos os serviços digitais de busca (e.g. Google, Bing, Yahoo), cartografia (e.g. Google Earth e Maps) e redes sociais (e.g. Facebook, Instagram, Twitter) são gratuitos e estão entre os que maior quantidade de informação recolhem, em todos os dispositivos, mas sobretudo *smartphones*, para produzirem, depois de análise, informação que nos é relevante. Embora muitos não se apercebam, o modelo baseia-se na criação de uma "bolha" com base na nossa pegada digital, que restringe as nossas opções, i.e., o motor de busca Google dá respostas diferentes para cada pessoa, em função do seu histórico de pesquisas e do conjunto de todas as pesquisas. Passa-se o mesmo com o *feed* do Facebook e outros serviços, cujos algoritmos traçam o perfil do utilizador com base na sua pegada.

Para se ter uma noção da importância, dimensão e duração desta pegada, pode-se referir que, segundo Palermo (2013), os motores de busca mantêm registos das buscas: no caso da Google durante 18 meses, tornando o endereço IP anónimo ao fim de nove, mas não o apagando completamente; a Yahoo mantém registos durante 18 meses e anonimiza o endereço IP ao fim de seis, mas não específica se apaga completamente o endereço ou não; a Bing mantém durante 18 meses, anonimiza o endereço IP ao fim de seis, altura em que apaga completamente dos servidores o endereço. No entanto, há ainda os fornecedores de acesso à Internet (*ISP*), muitos utilizadores apagam o histórico de pesquisas e navegação regularmente, mas a empresa mantém informação, registando TUDO o que o utilizador faz, pois, todo o tráfego passa pelos seus servidores.

Naturalmente que as companhias de telecomunicações também o fazem, mantendo registos de chamadas, mensagens de texto e seu conteúdo, localização, etc. Certamente todos concordam que isto é legitimo e importante, pois permite combater actividades criminosas, escutando, localizando e "espiando" as comunicações, mas partimos do princípio, em sociedades desenvolvidas e democráticas, que essa actividade deve ter autorização prévia, no âmbito de processo de investigação, sendo decretada pelo poder judicial. Como, infelizmente, se tem visto nos últimos anos, em Portugal, ficam sérias dúvidas relativamente à legitimidade, metodologia, justificação e práticas neste domínio, mas esse assunto, embora excepcionalmente relevante, está fora do contexto deste texto. Não obstante, colectivamente, consideramos ser um preço a pagar, sobretudo no contexto de um mundo "perigoso", perde-se em liberdade o que se ganha, potencialmente, em segurança, ou tentamos acreditar nisso.

No contexto estritamente comercial a questão é diferente, a nossa pegada digital é importante, pois ajuda a definir cada individuo, todos os dias contribuímos para uma "imagem" de quem somos

online e essa imagem é muito mais pública do que se assume geralmente. Como refere Internet Society (2019), essa imagem "ajuda as companhias a direccionar conteúdos a consumidores e mercados específicos, ajuda empregadores a olhar para o *background* de qualquer um e ajuda os anunciantes a seguir os nossos movimentos através de múltiplos *websites*. […] portanto, independentemente do que se faz *online* é importante saber que tipo de rasto se está a deixar e quais os seus efeitos possíveis". Assim, embora seja virtualmente impossível ter uma pegada digital zero, é essencial compreender o que ela é, como se produz e como geri-la, pois há quem queira torná-la mínima enquanto outros querem tirar partido dela, a nível pessoal, comercial, político entrando-se aí no domínio do Marketing Digital.

Um aspecto pouco ou nada falado e conhecido, relativamente aos dados gerados em redes informáticas, são os *dark data*, "dados que são adquiridos através de várias operações de rede de computadores, mas que não são utilizados de forma alguma para obter *insights* ou para tomada de decisões. A capacidade de uma organização de recolher dados pode exceder a sua capacidade de analisar os dados. Em alguns casos, a organização pode nem estar ciente de que os dados estão a ser recolhidos. A IBM estima que cerca de 90% dos dados gerados por sensores e conversões analógico-digitais nunca são usados […] 60% perdem valor imediatamente" (Wikipédia, 2019). Alguns exemplos deste tipo de dados são: informação relativa a contas, relatórios de análise de dados, registos de chamadas, *emails* e anexos, ficheiros de registo de sistemas informáticos, dados de diagnóstico de equipamento, dados de informação biométrica e, sobretudo, dados de geolocalização (LaMonte, 2018).

Recentemente, o volume de informação recolhido tem aumentado de uma forma assustadora, dados de equipamentos, de utilizadores, consumidores, clientes, de tal forma que se pode falar num "Apocalipse de dados […] segundo a IBM 90% dos dados actuais do mundo foram criados nos últimos dois anos […] hoje, cada humano cria, a cada minuto, 1.7 MB[3] de informação [em média], agora multiplique-se pela dimensão da população mundial" (LaMonte, 2018). Há aspectos neste tipo de dados que são "perturbadores", com o advento da *IoT* (*Internet of Things* [4]), haverá milhares de milhões de sensores a produzir dados, *online*, o que será possível graças à próxima geração de comunicações móveis (5G), estando os *smartphones* incluídos e sendo, potencialmente dos maiores produtores de dados, o que levanta questões ainda maiores quanto à propriedade, uso e tratamento dos dados. O outro aspecto, talvez mais grave e preocupante, prende-se com os dados

[3] MB – *Mega Byte*, um milhão de *bytes*, cada *byte* são oito *bits* que codificam um caracter.
[4] *Internet of Things* – "rede de objectos físicos (veículos, prédios e outros dotados de tecnologia embarcada, sensores e conexão com a rede) capaz de recolher e transmitir dados. É uma extensão da internet actual que possibilita que objectos do dia-a-dia (quaisquer que sejam, mas com capacidade computacional e de comunicação) se liguem à Internet. A ligação com a rede mundial de computadores possibilita, em primeiro lugar, controlar remotamente os objectos e, em segundo lugar, que os próprios objectos sejam acedidos como provedores de serviços. Essas novas capacidades dos objectos comuns geram um grande número de possibilidades, tanto no âmbito académico como industrial". (Wikipédia, 2019).

biométricos recolhidos por equipamentos vários, sobretudo pelos *smartphones*, mas voltaremos a esse assunto um pouco à frente.

A quantidade de informação produzida por cada pessoa é gigantesca, sendo depois analisada, processada e estudada, permitindo casos caricatos e interessante, dos quais referimos dois, num deles o departamento de marketing da Target (grande cadeia de retalho nos EUA), tentou "adivinhar", com base em padrões de consumo dos clientes, se uma cliente poderia estar grávida mesmo que ela não quisesse que se soubesse, para poderem enviar publicidade direccionada: não só conseguiu adivinhar, em grande quantidade, como teve problemas com clientes, por filhas adolescentes terem recebido promoções para roupas de bebés, antes de a família saber que estavam grávidas. (Duhigg, 2012). Noutro caso, a HiQ[5], uma empresa de análise de dados, utiliza informação que encontra na rede para prever quando um trabalhador está prestes a despedir-se, vendendo esta informação aos empregadores (Almeida, 2019).

Para se poder ter uma ideia da quantidade de informação que é recolhida, enquanto se navega na rede, vamos exemplificar sinteticamente: mal se abre um *browser* (navegador como o Edge, Chrome, Internet Explorer, Firefox, Opera, entre outros), começa-se a deixar imediatamente uma pegada digital, pois os sítios visitados vão seguir as actividades e permitir ser-se reconhecido quando se volta, tudo isto é perfeitamente legal. O início da recolha de informação dá-se com o próprio navegador, estando *online* torna-se conhecido o endereço IP (ponto de entrada na Internet), o que pode ser utilizado para saber a localização do utilizador, seguido do Software que se está a utilizar, o equipamento e a ligação. Para se ter ideia da informação recolhida pode-se visitar http://webkay.robinlinus.com/ (What every Browser knows about you) (Figura 2).

Muitos sítios, contudo, "querem" saber o máximo possível acerca do utilizador, seja para personalizar os seus serviços ou para direccionar publicidade, para esse efeito deixam um *cookie*[6] no sistema na primeira visita. São como "migalhas numa floresta" (Nield, 2017b), informam o sítio acerca de onde estivemos antes, sabem a localização (para dar uma previsão meteorológica, por exemplo) e são muito úteis, mas ajudam a acrescentar peças ao puzzle de informação recolhido pelo navegador.

Tentando sistematizar a informação relativamente aos *cookies*, quais são então os principais tipos e funções (Nield 2017a): o principal objectivo, como referido anteriormente, é ajudar o utilizador

[5] https://www.hiqlabs.com/

[6] Um *cookie* HTTP é constituído por um conjunto de dados, enviado pelo sítio visitado, e colocados no computador pelo navegador, tendo sido concebidos como um mecanismo fiável para os sítios se "lembrarem" de informação importante (por exemplo produtos colocados num cesto de compras duma loja *online*), ou para registar a actividade de navegação do utilizador (clicar em determinados botões, *log in*, páginas visitadas). Também podem ajudar a lembrar informação previamente introduzida em campos, para facilitar a navegação, como nomes, moradas, *passwords* ou números de cartão de crédito (Wikipédia, 2019). Para testar o registo continuo de cliques, num tom marcadamente humorístico, mas pedagógico, pode visitar: https://clickclickclick.click/

quando se regressa a um sítio na *web*, mas os *cookies* mais avançados podem registar informação como o tempo que se passou a ver uma página, as ligações em que se clicou, o que se está a pensar comprar (razão pela qual se encontra o produto ainda no cesto quando se volta, passados dias), além e sempre da localização, o que no caso dos *smartphones* abre todo um outro mundo de oportunidades.

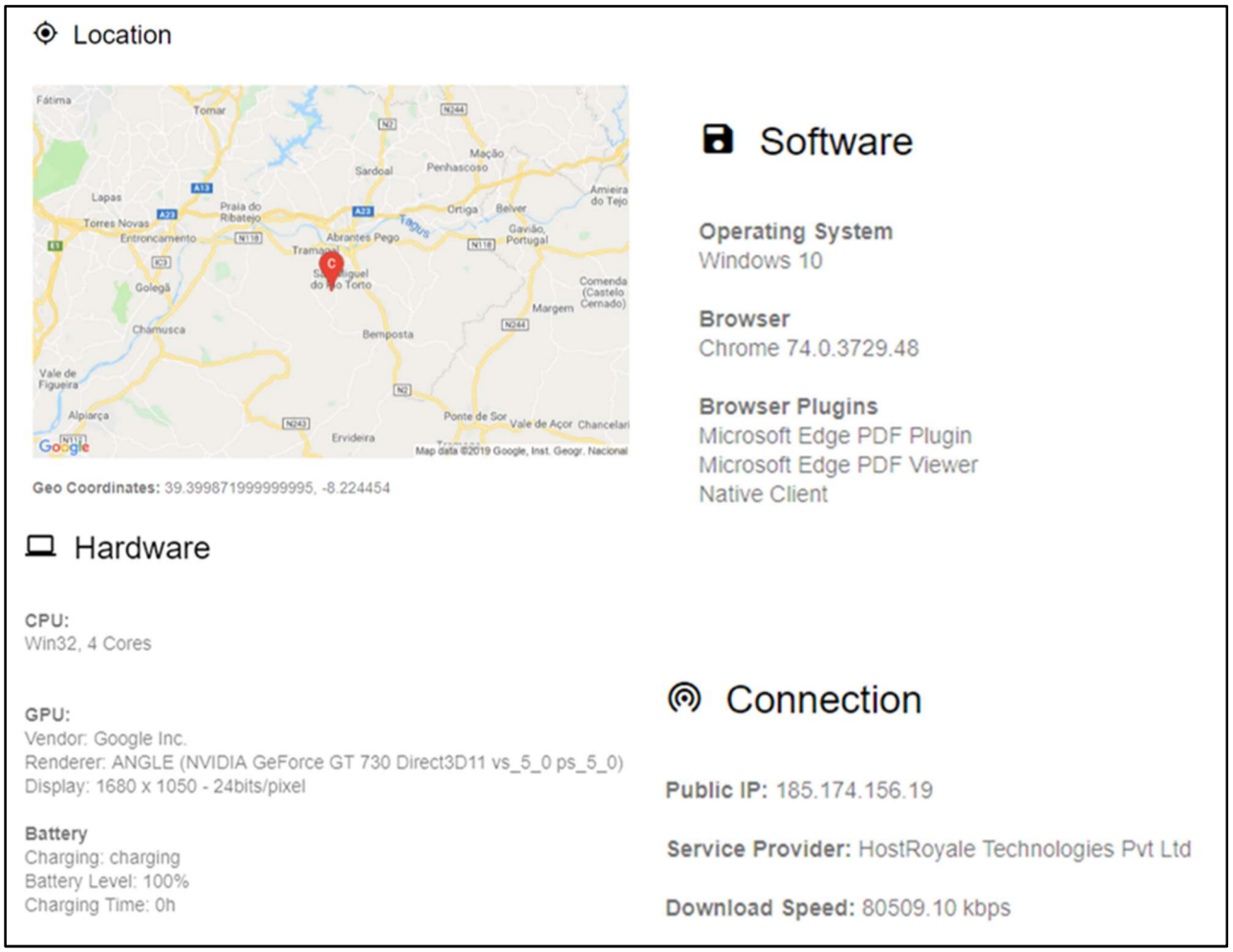


Figura 2 – Informação recolhida pelo navegador, obtida em: http://webkay.robinlinus.com/

No entanto, embora estes *cookies* só devessem ser acedidos pelos sítios que os colocaram, existem outros de "terceiros", que são instalados e registam tudo o que se faz, em todos os sítios, expandindo o conceito através de sítios, motores de busca, redes sociais, geralmente sem a autorização do utilizador[7]. Quantas vezes acontece, porque se procurou por exemplo um guarda-chuva, aparecerem anúncios aos mesmos quando navegamos noutros sítios, durante semanas. Existem, ainda, *super cookies* extremamente invasivos, que são introduzidos a nível do *ISP*, não estando

[7] Quase todos os navegadores têm uma opção de "não aceitar *cookies* de terceiros", mas essa opção está, sempre e por defeito, desligada.

instalados no equipamento do utilizador e sendo, portanto, impossíveis de erradicar quando se limpa o histórico de navegação e *cookies* instalados.

Ou seja, tudo isto é feito para se compreender melhor quem é o utilizador e produzir melhor publicidade, mais direccionada: sítios visitados, pesquisas, *cookies* e o próprio navegador. Segundo um estudo da Universidade de Princeton, nos E.U.A., "[*cookies*] rastreadores embutidos em 482 dos 50.000 sítios de topo na rede estavam a registar virtualmente toda a actividade dos utilizadores dos navegadores para análise posterior" (Nield, 2017b). Se juntarmos a toda esta informação a que é recolhida pelas empresas que fornecem o acesso à Internet (*ISP*), fica-se a saber onde se navega, no que se está interessado, cruzando toda esta informação, talvez por isso os *ISP* vendam, por grosso, dados e navegação a empresas de marketing e publicidade. Nos E.U.A, o Congresso autorizou, inclusive, os *ISP* a venderem o histórico de navegação dos clientes, utilização de aplicações, sem autorização prévia e explicita dos utilizadores que a criam (Watson, 2017)[8].

Embora a ideia subjacente aos *cookies* seja facilitar a navegação aos utilizadores, pode-se tendo acesso a esta informação, alguém com acesso ao equipamento ou um gestor de rede, conhecer os hábitos de navegação do utilizador, o que viu, o que descarregou. Há, contudo, formas relativamente fáceis de controlar os *cookies* nos navegadores, basta ir às definições, procurar em privacidade, avançadas, preferências (consoante o navegador utilizado) e: bloquear as *cookies* de terceiros, deixados por outros que não o sítio visitado(não interfere com as preferências dos sítios, mas dificulta ou impossibilita o rastreio através de várias plataformas); outra forma é navegar de forma privada ou incógnita (quando se sai do navegador toda a história e *cookies* são limpos, bem como os ficheiros temporários e ficheiros descarregados, este modo deve ser SEMPRE utilizado em equipamento de acesso público). O importante é que cada utilizador explore as opções dos navegadores que utiliza, perceba o que está em questão a nível de privacidade e se "defenda" o melhor possível.

No entanto, além dos *cookies*, há outra "ferramenta" que permite extrair informação pessoal dos utilizadores, durante as sessões, quando navegam, são os *scripts*[9]. Estes *scripts* analíticos de terceiros podem registar as páginas visitadas, pesquisas feitas, mas ultimamente cada vez mais sítios utilizam *scripts* de "repetição de sessão", que registam batimentos de tecla, movimentos do rato, *scrolling* de páginas, conteúdo de páginas visitadas, etc. e enviam toda esta informação para servidores de terceiros. "Ao contrário de serviços analíticos típicos, que fornecem estatísticas agregadas, estes *scripts* são concebidos para registar e reproduzir as sessões individuais de navegação, como se alguém estivesse a olhar por cima do ombro" (Engkehardt, 2017).

[8] Há formas de evitar que o *ISP* "veja" o que os clientes fazem, nomeadamente através do uso de uma *VPN* (Virtual Private Network), esse assunto será abordado na parte relativa às soluções.
[9] *Scripts* são código, invisível para o utilizador de uma página *web*, que controla o comportamento da página, facilitam a automação de processos, aumentando a facilidade de utilização e flexibilidade de sítios.

O objectivo é conhecer como o utilizador interage com os sítios e descobrir falhas de concepção, páginas confusas, ou ligações quebradas, contudo, os dados recolhidos excedem em muito as expectativas: "o texto introduzido é recolhido antes do utilizador enviar o formulário, os movimentos precisos do rato são gravados, tudo sem qualquer indicação para o utilizador. Não se pode esperar que estes dados sejam mantidos anónimos. De facto, algumas companhias permitem que os dados gravados sejam, explicitamente, ligados à identidade real dos utilizadores" (Engkehardt, 2017). Esta informação pode recolher dados sensíveis, médicos, cartões de crédito e outra informação pessoal, que sendo interceptados podem ser utilizados fraudulenta e criminosamente. Pode-se evitar isto, parcialmente, escolhendo a opção "Do not track" (não monitorizar) nos navegadores e instalando extensões nos navegadores que bloquem *scripts*, embora a navegação se torne por vezes difícil [10].

Grande parte, ou a quase totalidade da informação até aqui mencionada, faz parte da pegada digital passiva, mas quando se passa para a activa, aquela para a qual o utilizador contribui, a quantidade e qualidade da informação recolhida, ou potencialmente recolhida, para a ser gigantesca e assustadora. Talvez o melhor exemplo seja o Facebook, que também possui a Instagram, WhatsApp e Messenger, com 1.52 mil milhões de utilizadores diários activos e 2.32 mil milhões de utilizadores activos mensalmente[11], o que, só pela escala, permite imaginar o volume possível e susceptível de recolha de pegada digital, activa e passiva. É a quinta maior companhia mundial, em termos de valor de mercado, abaixo da Microsoft (4ª) e Apple (1ª)[12].

Efectivamente, a Facebook sabe muito mais da vida pessoal dos seus utilizadores do que aquilo que eles, provavelmente, podem imaginar, como parte da sua operação crescentemente agressiva de publicidade (o seu negócio principal, no fundo), recolhendo 98 pontos de dados pessoais para permitir maximizar a eficácia do direccionamento de publicidade (Nunez, 2016). Além de toda a informação que recolhe, porque os utilizadores a introduzem (datas, eventos da vida, amigos, contactos, emprego, tudo o que gosta, quem e o que se segue, etc., etc., etc.), o que é assustador é a informação que não comunicamos directamente, como informação bancária, de crédito, ou o equipamento que utilizamos, onde, quando, durante quanto tempo o fazemos, isto porque a empresa rastreia, virtualmente, todos os sítios que visitamos.

Embora seja um pouco fastidioso, mas elucidativo e preocupante, convém enunciar a informação que a Facebook possui acerca dos utilizadores e que oferece comercialmente, como opções de rastreio a anunciantes, ver Tabela 1.

[10] Dois exemplos de extensões para Chrome, para controlar *scripts* são: https://chrome.google.com/webstore/detail/scriptsafe/ e https://chrome.google.com/webstore/detail/scriptblock/

[11] Dados oficiais no *Newsroom* da empresa: https://newsroom.fb.com/company-info/#statistics

[12] https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/

Tabela 1

Informação que a Facebook possui acerca dos utilizadores (Dewey, 2016).

1 - Localização	50 - Que doaram a caridade (divididos por tipo)
2 - Idade	51 – Sistema operativo do equipamento
3 - Geração	52 – Que jogam jogos de ecrã
4 - Género	53 – Que têm uma consola de jogos
5 – Língua	54 – Que criaram um evento Facebook
6 – Nível de educação	55 – Que utilizaram pagamento Facebook
7 – Área de estudo	56 – Gastaram mais que a média em pagamentos FB
8 – Escola	57 – Qua administram uma página Facebook
9 – Afinidade étnica	58 – Que carregaram recentemente fotos para o FB
10 – Rendimento e valor bruto	59 – Navegador de Internet
11 – Proprietário da casa e tipo de casa	60 – Serviço de correio electrónico
12 – Valor da casa	61 – Adoptaram a tecnologia cedo/tarde
13 – Dimensão da propriedade	62 – Expatriados, divididos por país de origem
14 – Metros quadrados da casa	63 – Pertence u. de crédito, banco nacional/regional
15 – Ano de construção da casa	64 – Que investe, divididos por tipo de investimento
16 – Composição do agregado familiar	65 – Número de linhas de crédito
17 – Aniversário até 30 dias	66 – São utilizadores activos de cartões de crédito
18 – Longe de casa/família	67 – Tipo de cartão de crédito
19 – Amigos aniversário, noivado, casamento, etc.	68 – Que usam cartão de débito
20 – Numa relação à distância	69 – Que têm crédito no cartão
21 – Num novo relacionamento	70 – Que ouvem rádio
22 – Com novo emprego	71 – Preferências de programas TV
23 – Recentemente noivos	72 – Que usam telemóvel, dividido por marca
24 – Recentemente casados	73 – Tipo de ligação à Internet
25 – Que mudaram de casa recentemente	74 – Adquiriram recentemente *tablet/smartphone*
26 – Com aniversário próximo	75 – Que acedem à Internet com *tablet/smartphone*
27 – Pais	76 – Que usam copões de descontos
28 – À espera de criança	77 – Tipos de roupas que compram
29 – Mães, divididas por tipos	78 – Altura do ano em que fazem mais compras
30 – Que é provável envolverem-se em política	79 – Compradores "pesados" de bebidas, tipos
31 – Conservadores e liberais	80 – Compram produtos de mercearia (que tipos)
32 – Estado da relação	81 – Que compram produtos de beleza
33 – Empregador	82 – Que compram medicamentos, tipos
34 – Indústria	83 – Que gastam dinheiro em produtos para a casa
35 – Título no emprego	84 – Compram produtos crianças e animais, quais
36 – Tipo de escritório	85 – Agregado faz mais compras que a média
37 – Interesses	86 – Tendem a compra *online*, ou não
38 – Que possuem motas	87 – Tipo de restaurantes onde comem
39 – Que planeiam comprar um carro	88 – Tipo de lojas a que vão
40 – Que compraram peças auto recentemente	89 – São receptivos a ofertas de companhias, tipos
41 – É provável necessitarem peças/serviços auto	90 – Há quanto tempo vivem na casa
42 – Estilo e marca do carro que guiam	91 – É provável mudarem-se brevemente
43 – Ano de compra do carro	92 – Que viajam frequentemente, trabalho ou lazer
44 – Idade do carro	93 – Interessados Olímpicos, futebol, críquete, etc.
45 – Dinheiro dispostos a gastar no próximo carro	94 – Que se deslocam para o trabalho
46 – Onde é provável comprar próximo carro	95 – Tipos de férias que fazem
47 – Quantos empregados tem a companhia	96 – Que voltaram recentemente de uma viagem
48 – Se possuem um pequeno negócio	97 – Usaram recentemente aplicação de viagens
49 – Se trabalham em gestão ou são executivos	98 – Que participam em timeshare

Ou seja, se juntarmos à utilização dos serviços os próprios terminais, a dimensão é brutal, todo e qualquer *smartphone* Android vê toda a sua actividade rastreada e vigiada pelo universo Google. O que também já valeu uma pesada multa, de 4340 milhões de Euros por parte da União Europeia: "Somando a multa de 2400 milhões aplicada em 2017, Bruxelas pune o gigante tecnológico norte-americano com 6740 milhões de euros num período de 12 meses. […] Desta vez, a investigação – a

mais extensa em oito anos de batalhas legais contra o Google – incide sobre um aspecto central do modelo de negócio prosseguido pela empresa na última década. Bruxelas declarou ilegais as restrições contratuais impostas para a utilização do Android, que favoreceram o domínio do Google nas pesquisas *online* nos telemóveis à medida que largas fatias de consumidores se transferiram dos computadores de secretária para os *smartphone*s. Estes aparelhos são agora responsáveis por mais de 50% do tráfego de buscas na Internet. […] Desde 2011, a Google impôs restrições ilegais aos fabricantes de dispositivos Android e aos operadores de redes móveis com o intuito de cimentar a sua posição dominante nas pesquisas genéricas na Internet" (Ferreira & Siza, 2018), resume a Comissão:

- Exigiu aos fabricantes que pré-instalassem a aplicação de pesquisa Google *Search* e a aplicação de navegação (Chrome) como condição para a concessão de licenças da sua loja de aplicações (*Play Store*);
- Fez pagamentos a alguns fabricantes de grande dimensão e a operadores de redes móveis, na condição de pré-instalarem em exclusividade a aplicação Google *Search* nos seus dispositivos;
- Impediu os fabricantes que pretendiam pré-instalar aplicações da Google de vender um só dispositivo móvel inteligente que fosse, que funcionasse com versões alternativas do Android não aprovadas pela Google (as chamadas «ramificações do Android»).

"A quem pesquisava por roupa, por exemplo, eram-lhe recomendados em primeiro lugar os resultados provenientes da ferramenta do Google. Estes resultados eram, na verdade, anúncios que outros clientes da Google pagam, para estarem nos primeiros resultados da pesquisa. Segundo a Comissão Europeia, mesmo ferramentas concorrentes com mais tráfego surgiam por vezes apenas na quarta página dos resultados de uma pesquisa no motor de busca Google. Apesar de separar o *Shopping* e o motor de busca, a empresa contestou em tribunal a milionária multa que então lhe foi aplicada, após uma longa e complexa investigação da Comissão Europeia" (Ferreira & Siza, 2018).

O alfa e ómega de tudo isto, a recolha, tratamento e utilização dos dados, é o mercado publicitário. Efectivamente, a Google e a Facebook: "sem contar com a China, 86% do mercado de publicidade digital global é investido nas duas multinacionais. Globalmente, 40,9% do mercado de publicidade é canalizado para estas plataformas (há mais números ao lado). As estimativas são feitas pelo Dinheiro Vivo, com a ajuda dos relatórios e contas das duas empresas – a consultora Magna Global fazia previsão semelhante (84%) no início de 2018. E a galinha continua a engordar à conta da publicidade. O ano passado cresceram 22% e 33%, respectivamente, e apresentaram lucros recorde". (Tomé, 2019). A vantagem está nos dados em tempo real sobre os utilizadores, optimizando o direccionamento da publicidade nas suas plataformas, "A Google é quem tem mais volume, daí que tenha recebido 116,3 mil milhões de dólares em receitas publicitárias (contra 55 mil milhões do Facebook, com Instagram e WhatsApp)". (Tomé, 2019)

Também a Microsoft, neste caso o seu software, foi investigado pela União Europeia por recolha indevida de dados (EDPS, 2019): "O organismo que regula a protecção de dados na União Europeia (EDPS) anunciou [...] que está a investigar se os produtos que a Microsoft fornece às instituições europeias respeitam as novas regras de protecção de dados. A União Europeia depende de vários serviços e produtos da gigante tecnológica norte-americana para completar actividades diárias, incluindo o envio de *emails* e a redacção de documentos oficiais. [...] A decisão surge depois de uma investigação na Holanda, feita por uma empresa contratada pelo Governo holandês. Em Novembro, o Governo daquele país manifestou preocupações sobre a forma como os programas da Microsoft oferecidos com o pacote ProPlus – que é utilizado por várias instituições da União e inclui o processador de texto Word, o serviço de videochamadas Skype e o serviço de *email* Outlook – recolhiam dados pessoais e metadados (o "quem, onde, quando e com quem" das comunicações, como a data em que um documento é criado)" (Pequenino, 2019d).

Em determinada época, este nível de preocupação só se punha a nível da utilização de computadores, bem como do acesso à Internet a partir de postos fixos ou computadores portáteis, mas com o aparecimento e difusão dos *smartphones* e *tablets* o acesso tornou-se ubíquo, constante, com elevada largura de banda e barato. Efectivamente, o lançamento do iPhone em 2007 transformou o telefone móvel de uma ferramenta somente de comunicação numa plataforma multifunção, que está constantemente a evoluir. "O *smartphone* é agora um PC em tamanho de bolso, facilita conexões pessoais instantâneas que fazem as conversas telefónicas parecer pinturas rupestres [...] o dispositivo parece ter potencial ilimitado. [...] Segundo o MIT o *smartphone* ultrapassou a TV como tecnologia de consumo com taxa de adopção mais rápida, atingindo 40% de saturação de mercado em somente 2 anos e meio [...] sendo actualmente responsável por mais de 60% do tráfego total da Internet." (Phillips, 2014).

Os *smartphones* tornaram-se uma espécie de fonte de memória externa, sistemas interligados que se lembram, menos por saberem a informação do que por saberem onde essa informação pode ser encontrada, estão próximos de ser uma extensão digital de nós próprios, permitindo-nos ligarmo-nos mutuamente independentemente da localização, segundo um inquérito da Google em 2013, 36% dos utilizadores preferiam desistir da sua TV do que do telefone (Philips, 2014). Realmente, se pensarmos nas funções que os *smartphones* agregam (nativas e aplicações), percebemos porque vários equipamentos foram tornados (quase) obsoletos: além de telefone, leitor de MP3 e vídeo (*streaming* ou não), câmara fotográfica digital, GPS, bússola, despertador, consola de jogos, *e-reader*, afinador de instrumentos, dicionário, controlo remoto, lanterna, gravador de voz, etc.

Olhando para algumas estatísticas relativas a comunicações móveis (Chaffey, 2018), compreende-se, ainda mais, a importância, penetração no mercado, democratização e banalização do uso dos *smartphones*: em 2008 era feita uma previsão chocante, em 2014 a acesso móvel à Internet ia

ultrapassar o fixo, actualmente, nalguns países, a proporção de acesso telefone para computador é mais de quatro para um, sobretudo países em que o acesso telefónico, por cabo, de banda larga nunca foi fácil (todos os países em vias de desenvolvimento). Para quem vive no mundo "desenvolvido" é difícil perceber que, em grande parte do planeta, o primeiro acesso que muitos tiveram à Internet foi através da rede móvel, com *smartphones*, também por isso a tão grande esperança na geração de comunicações 5G, para tornar melhor, mais rápido e generalizado o acesso (Figura 3).

Um outro aspecto interessante da informação que se pode obter, acerca da relação entre acesso e tempo de acesso à Internet, com dispositivos móveis ou fixos, é como esse acesso varia ao longo do dia, o que constitui um informação essencial para quem quer colocar publicidade, especificamente, em determinado tipo de terminais (através de sítios específicos para acesso móvel ou não[13]). Na Figura 4 pode-se ver como o acesso a partir de *desktop* domina durante o dia nas horas de trabalho, mas é substituído pelos *tablets* à noite e *smartphones* de manhã. As implicações são claras, nestas horas, caso não se atinja a audiência e alvo de publicidade (ou outro tipo de informação) no dispositivo mais utilizado, não se está a optimizar os resultados.

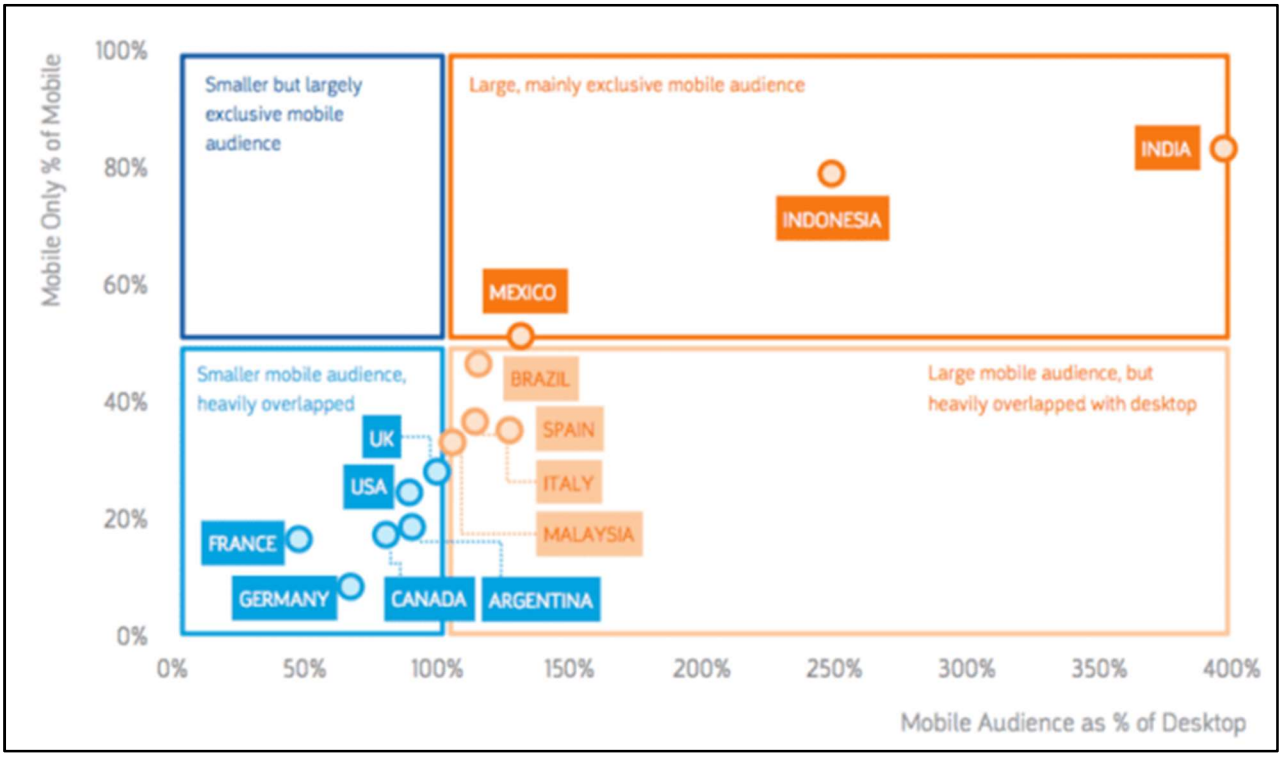


Figura 3 – Relação entre a proporção de acesso à Internet por dispositivos móveis e *desktop* e proporção de acesso exclusivamente móvel (Chaffey, 2018).

[13] Sítios com nomenclatura "m.", concebidos e optimizados para dispositivos móveis e que no Google, por exemplo, aparecem primeiro nas buscas quando estas são feitas a partir de dispositivos do mesmo tipo, nunca parecendo (por razões óbvias), nas buscas feitas em PC's.

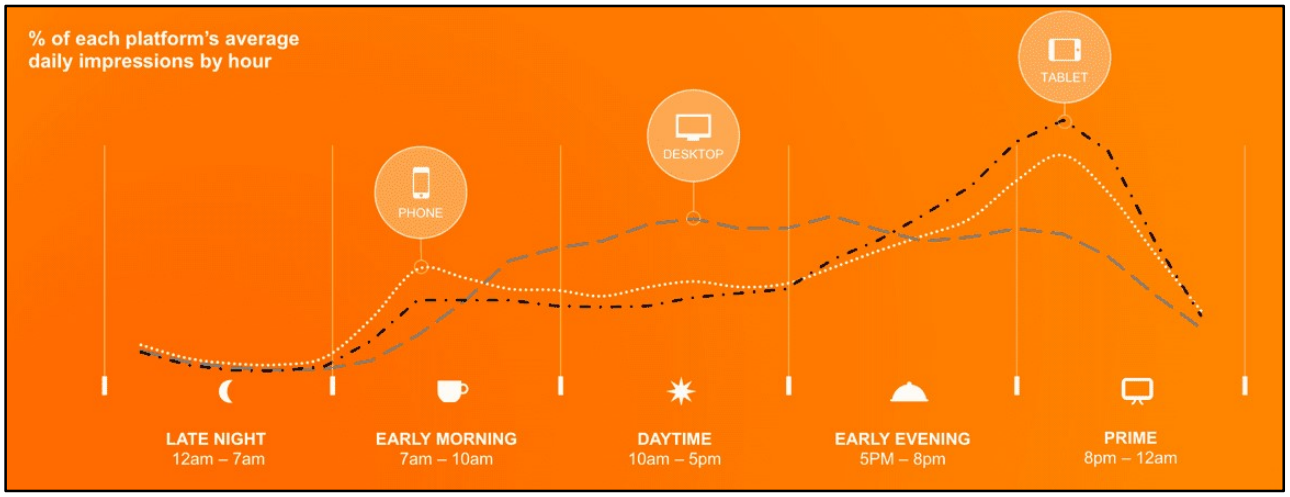


Figura 4 – Percentagem de utilização média diária, por hora, para diversos tipos de plataformas de acesso à Internet (Chaffey, 2018).

A importância, premente, de fornecer acesso à Internet em grandes extensões do planeta onde, por razões técnicas e de ordem económica, não é viável construir redes fixas de apoio, passa pela criação de redes de satélites dedicadas ao fornecimento desse acesso, podendo assim chegar a mais milhares de milhões de utilizadores e, com certeza, recolher ainda mais dados[14]. As principais (dominantes) empresas tecnológicas que já o pensaram fazer, tentaram, estudaram ou estão em processo de implementação (entre outras) são:

- Amazon – Projecto Kuiper – 3236 satélites em órbita baixa (Boyle, 2019);
- Google – 180 satélites, órbita média (Palermo, 2014);
- Facebook – Órbita baixa (Matsakis, 2018);
- Space X – 4425 satélites, órbita baixa, 1 Mbit, 25-35 ms de latência (Palermo, 2014), primeiros 60 lançados em Maio de 2019 (Oberhaus, 2019).

Neste ponto, em que se torna perceptível a quantidade assombrosa de informação que produzimos, activa e passivamente, criando uma enorme e duradoura pegada digital, falta ainda referir dois aspectos mais recentes e emergentes, que exponenciam a preocupação relativa à privacidade dos dados e quantidade de dados produzidos: a recolha de dados biométricos pelos *smartphones* e o advento (eminente) da Internet das Coisas (*IoT*). "A navegação na Internet em *smartphones* é hoje em dia superior (58%) ao computador, o que permite aos fabricantes de telemóveis e empresas associadas, aceder a um conjunto de dados muito mais pessoais de milhões de pessoas, como são as impressões digitais, dados de identificação facial, ou brevemente dados de reconhecimento da íris, e utilizá-los da forma como assim o entenderem" (Garcia, 2019).

[14] Segundo a FAO, em 2018, cerca de 3.8 mil milhões de pessoas não estavam ligadas á internet: http://www.fao.org/e-agriculture/news/un-broadband-commission-aims-bring-online-world%E2%80%99s-38-billion-not-connected-internet

O que são, então os dados biométricos, porque são relevantes neste contexto de pegada digital, privacidade e uso de *smartphones*? Os dados biométricos são quaisquer medidas relacionadas com características humanas, podendo ser utilizadas com vantagem e conveniência na identificação de pessoas. A questão chave que se põe, realmente, é se este tipo de dados estão a salvo do roubo de identidade, pois se é fácil substituir uma palavra-passe que foi comprometida, já "emitir" uma nova iris ou dedo não é possível. Os principais tipos de dados biométricos são os seguintes (Porter, 2019) (Korolov, 2019):

- **Reconhecimento facial** – Medição dos padrões únicos da cara, através de vídeo e imagem, comparando e analisando padrões faciais (utilizado pelas forças da autoridade como forma de autenticação de identidade, mas também para desbloquear *smartphones* e portáteis);
- **Reconhecimento da íris** – Identificação dos padrões únicos da íris, porção colorida em redor da pupila, através de vídeo e imagem, não muito utilizado no mercado de consumo;
- ***Scan* da impressão digital** – Padrões únicos de textura, muitos *smartphones* e portáteis utilizam esta técnica para substituir a palavra-passe ou desbloquear o ecrã;
- **Reconhecimento de voz** – Medição das ondas sonoras únicas de cada voz, quando se fala para o dispositivo, utilizado por telecomandos de TV, assistentes digitais e domésticos;
- **Reconhecimento de assinatura** – *Scan* da assinatura, sobretudo quando o utilizador espera ter de o fazer, como em bancos e comércio;
- **Geometria das mãos** – Medição e registo de medidas várias da mão (comprimentos, espessura, largura, área), utilizada desde os anos 1980 em aplicações de segurança;
- **Características comportamentais** – Análise da forma de interacção com sistemas computorizados, como batimentos de tecla, escrita, forma de andar, de utilizar o rato, entre outras, podem identificar quem é a pessoa.

Um sistema biométrico consiste em três componentes diferentes:

- **Sensor** – Aquilo que regista a informação e a lê, para comparar com o registo, quando a informação necessita de ser reconhecida (muitos *smartphones* têm vários, câmara e sensor de impressões digitais);
- **Computador** – Quando se está a utilizar a informação biométrica para se aceder a algo, tem de existir um equipamento que guarda essa informação para comparação (um *smartphone*, ou na nuvem[15]);
- **Software** – Basicamente aquilo que o *hardware* do equipamento ao sensor (aplicações).

[15] A nuvem, ou *cloud* no original, é aqui utilizada para referir sistemas de processamento e armazenamento de dados, sem gestão directa do utilizador, desmaterializados, localizados em servidores por todo o mundo e aos quais se tem acesso através da Internet.

Actualmente é comum, em várias marcas e tipos de dispositivos (*smartphones*, *tablets*, portáteis), existirem métodos de autenticação baseados em sistemas biométricos. É uma forma extremamente segura de autenticação e identificação, podendo substituir a confusão de recordar palavras-passe, de inúmeras contas, quando se quer ligar dispositivos ou aceder a vários serviços. A vantagem que os fabricantes de *smartphones* apresentam (ver Figura 5), são um maior número de métodos à escolha para proteger equipamentos, contas, acesso a serviços (comerciais e financeiros) e quando se navega ou utiliza aplicações. Supostamente esta informação está guardada a "sete chaves" no próprio equipamento, uma pasta encriptada que só se abre com estes parâmetros biométricos (Samsung, 2017).

No entanto, existem vários aspectos delicados quando à segurança destes sistemas, alguns dos principais riscos são os seguintes (Porter, 2019):

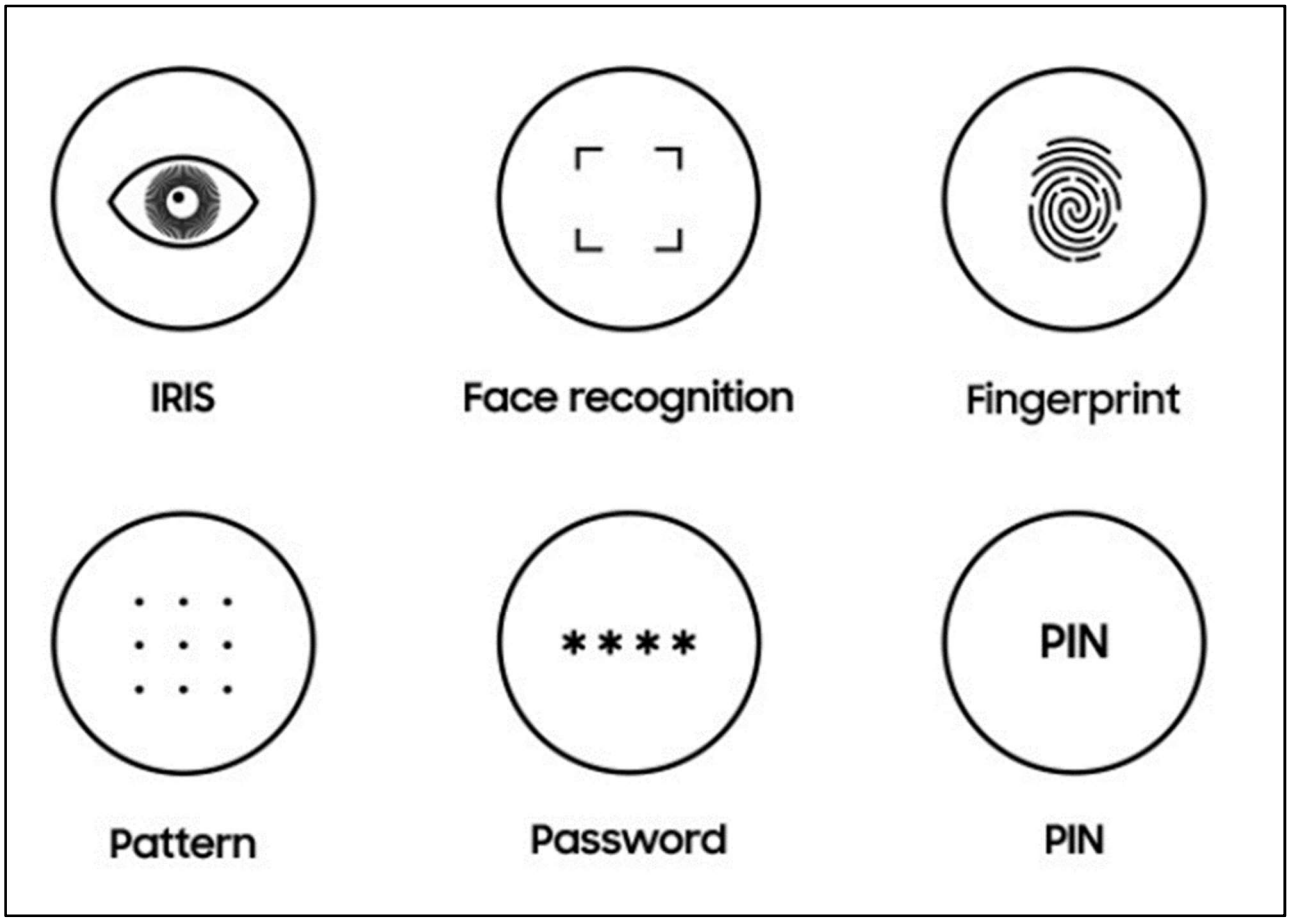


Figura 5 – Métodos de validação e tecnologias biométricas disponíveis nos *smartphones* Samsung S8 e equipamentos posteriores. Samsung (2017).

- Quaisquer dados recolhidos podem ser pirateados, sobretudo dados de alto nível, sendo a boa notícia que este tipo de dados costuma estar bastante mais bem protegido. Contudo, com a generalização do uso destes métodos, sobretudo através dos

smartphones, os dados tenderão a existir em vários locais (i.e. na nuvem) que podem não ter o mesmo nível de segurança;

- A utilização de sistemas biométricos pode banalizar-se de tal forma que os utilizadores se tornam complacentes, não mantendo medidas de segurança que utilizam actualmente e são do senso-comum, por acharem que o próprio tipo de dados resolve todos os problemas de segurança;
- Os dados biométricos guardados numa base de dados podem ser muito mais vulneráveis que outros tipos de dados. Podem-se mudar palavras passe, códigos PIN[16] ou outros, mas não as características físicas de um individuo, a sua impressão digital ou íris[17]. Assim, estando os dados comprometidos, ficam completamente fora de controlo;
- Alguns elementos de identidade física podem ser duplicados, podem-se tirar fotografias sem conhecimento (para utilizar em reconhecimento facial), copiar as impressões digitais de uma superfície, etc. o que pode permitir entrar nos dispositivos ou contas de um utilizador, ou, inclusive, piratear os seus próprios dados biométricos;
- As leis relativas a sistemas biométricos estão ainda em elaboração, podendo variar de país para país, o que também não defende os utilizadores.

Compreende-se, portanto, que estes dados biométricos passam, também, a fazer potencialmente parte da pegada digital de cada individuo, mas com este tipo de dados entra-se numa outra escala de riscos para a privacidade. Há, infelizmente e como é natural, vários casos de utilização problemática ou abusiva destas tecnologias, alguns exemplos:

- Em 2016 foi lançada na Rússia uma aplicação, FindFace, que utiliza uma foto tirada com a câmara do *smartphone* e, utilizando tecnologia de reconhecimento facial, procura a pessoa na rede social Russa Vkontakte, tendo uma precisão de 70% (Olaye, 2017). As implicações são preocupantes, com somente uma fotografia consegue-se, potencialmente, acesso a imensa informação sobre um qualquer estranho, podendo ser utilizada para comportamentos predatórios, de perseguição, criminosos, deixa de haver anonimato em espaços públicos;
- Em 2019 a Microsoft recusou vender tecnologia de reconhecimento facial às forças da ordem nos E.U.A., com receios relativos a questões de direitos humanos, por poder permitir vigilância autoritária, embora a Amazon já o tenha feito, tendo por isso sido muito criticada (Vincent, 2019). O caso da China costuma ser apontado como mau exemplo, pois o reconhecimento facial foi utilizado para ajudar a identificar a minoria muçulmana Uighur (Byler, 2019);

[16] PIN – Personal Identication Number, absolutamente banalizados em todo o tipo de serviços, electrónicos ou não, Multibanco foi dos primeiros que recordo.

[17] Poder pode-se, com operações, mas isso está mais no domínio da ficção, escrita e em filme…

- Já em 2016, nos Michigan, E.U.A., a polícia conseguiu desbloquear o *smartphone* de uma vítima de assassínio, utilizando uma impressora 3D para reproduzir as suas impressões digitais previamente gravadas, criando assim uma impressão digital falsa (Brandon, 2016), (McGoogan, 2016). O problema é que este processo, que também pode ser feito com cabeças de vítimas, além de ser utilizado pelas autoridades para resolver crimes, pode ser também utlizado para hackers piratearem um *smartphone* (Whittaker, 2019).

É importante estar-se atento ao que se passa neste domínio, pois já em Abril de 2019 (dia 15), o Parlamento Europeu aprovou a criação de um Repositório Comum de Identidade (CIR em Inglês), uma gigantesca base de dados biométricos U.E., tanto para residentes como visitantes (Cimpanu, 2019). Consiste na "interligação de uma série de sistemas e bases de dados de controlo fronteiriço, migração e implementação da lei. […] Unificará registos de 350 milhões de pessoas […] incluindo dados de identidade (nomes, data de nascimento, números de passaportes e cartão de identidade) e dados biométricos (dedos e facial)". O objectivo é simplificar a circulação nas fronteiras, o sistema deverá estar em funcionamento pleno em 2023, mas levanta dúvidas quanto à sua possibilidade de vigilância exagerada.

Por último, depois de todos estes elementos que se agregam, com o nosso contributo passivo ou activo, para criar, manter e amplificar a nossa pegada digital, vivemos uma nova etapa no desenvolvimento da Internet, a Internet das coisas (*IoT - Internet of Things*), que pode multiplicar, de facto, a quantidade de informação que produzimos exponencialmente e partir de um número desconcertantemente crescente de dispositivos. Esta revolução está a acontecer e a evoluir actualmente, sendo difícil prever e sintetizar todas as implicações, vantagens, riscos e evolução. Tentemos então um significado de partida, pois embora o termo tenha aparecido em 2005 não há, ainda, uma definição universalmente aceite: a *IoT* é a ligação dos objectos físicos à Internet e entre si, através de pequenos sensores, embutidos e tecnologia sem fios e com fios (FTC, 2015). "Ela representa a próxima evolução da Internet, dando um enorme passo na sua capacidade de ligar, analisar e distribuir dados que podemos transformar em informação, conhecimento e sabedoria" (Evans, 2011).

O tipo de equipamentos ligados vai desde produtos de consumo, com sensores vários e que se ligam à Internet (TV, frigoríficos, câmaras, automóveis, *smartphones*, etc.), a máquinas e equipamentos industriais, de comunicação autónoma, robots, identificadores RFID[18] em produtos, todo o tipo de sensores (portas, temperatura, médicos), etc. etc. Em 2008 estimou-se que o número de "coisas" ligadas à Internet ultrapassou o número de pessoas ligadas, que em 2015 havia 25 mil

[18] Identificação por radiofrequência ou RFID (do inglês *Radio-Frequency IDentification*) é um método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos denominados etiquetas RFID, exemplos mais comuns são os chips em produtos nas lojas, os chips de animais domésticos, ou nos cartões de crédito: https://en.wikipedia.org/wiki/Radio-frequency_identification

milhões de "coisas" ligadas e que em 2020 haverá 50 mil milhões (Evans, 2011). Se a "onda" da Internet ligou mil milhões de pessoas, nos anos 1990, enquanto a "onda" móvel ligou outros dois mil milhões, a *IoT* tem o potencial para ligar 10 vezes mais do que isso até 2020, sendo a terceira "onda" da Internet (Banafa, 2015). Num estudo da F-Secure, estimava-se (em 2018) que até 2022 se passaria de nove dispositivos ligados por agregado, para cerca de 500 (Roe, 2018).

Naturalmente que este tipo de crescimento, no número de dispositivos ligados e interligados, tem inúmeras vantagens e certamente mudará a vida quotidiana das pessoas, mas todas estas vantagens têm riscos associados, visto que o aumento explosivo de dispositivos ligados permite a *hackers* e criminosos mais pontos de entrada e acesso a dados. Quais são, então, os principais tipos de riscos de segurança associados à *IoT* (Meola, 2016):

- **Percepção pública** - Se os consumidores têm dúvidas e preocupações de segurança relativamente aos sistemas, é difícil a massificação "descolar". Em 2015, nos E.U.A. um estudo determinou que 44% das pessoas tinham muito receio de investir em "casas inteligentes" e 27% algum receio, porque a informação poderia ser roubada e vários sistemas da casa controlados remotamente (portas, iluminação, segurança, etc.);
- **Vulnerabilidade a *hacking***[19] - Tem sido possível "entrar" em dispositivos já existentes, com alguma facilidade (e.g. na plataforma da Samsung de casa inteligente *Smart Things* (https://www.smartthings.com/);
- **Estarão as companhias preparadas?** – Segundo um relatório da AT&T, depois de um inquérito a 5000 empresas a nível mundial, 85% estavam em vias de disponibilizar dispositivos *IoT*, mas somente 10% se sentiam confiantes que podiam garantir a segurança dos mesmos contra *hackers*;
- **Segurança propriamente dita** – Criar segurança para os dispositivos não é suficiente, tem de se estender esta segurança ao software e aplicações que os controlam e ligações de rede através das quais comunicam.

Apesar de haver um consenso em torno de vários aspectos, "a necessidade de a segurança ter que ser a base fundacional que permite a existência da *IoT*, não haver consensos na forma de implementar segurança da *IoT* nos dispositivos, a expectativa prevalecente (irrealista) de que se pode condensar 25 anos de evolução da segurança nos dispositivos e não haver uma bala de prata que possa, efectivamente mitigar as ameaças" (Hadjarbegovic, 2015), o processo está claramente em marcha. Compreendem-se os riscos, quando a intrusão mais comum, actualmente, já é entrar (*hack*) no sistema de gestão de uma casa (*home-hub*), que permite acesso a todos os dispositivos ligados e que incluem fechaduras das portas, detectores de movimento, sistemas de rega, de controlo de temperatura e, sobretudo, de alarme (Brandon, 2016). Ainda por cima, os

[19] Aqui utilizado como o processo de subverter a segurança de um sistema informático, fazendo-o com objectivos maliciosos.

hackers tendem a congregar e atacar as plataformas mais populares, é ver o caso do Windows em comparação com o Mac, assim qualquer plataforma que se destaque atrairá mais "esforços" de intrusão.

Compreende-se o interesse da indústria, em geral, num mercado que pode valer em 2020, globalmente, 6 biliões (milhões de milhões) de Dólares (Brandon, 2016). Na Figura 6 pode-se ter uma noção mais clara das possibilidades, em inúmeros domínios, para efeitos de medição, como controle, através de vários tipos de sensores/controladores e com vários tipos de protocolos. No contexto deste texto os mais relevantes são os que utilizam a rede celular, Wi-Fi ou *Bluetooth*, pois são os que tornam os *smartphones* em produtores de imensa informação, aumentando o acesso à crescente pegada digital que daqui resultará e alvos potenciais de intrusão, o que acentua as questões de privacidade. Se for possível controlar vários equipamentos com aplicações no *smartphone* (já é actualmente), tendo acesso a ele, podem-se controlar outros equipamentos.

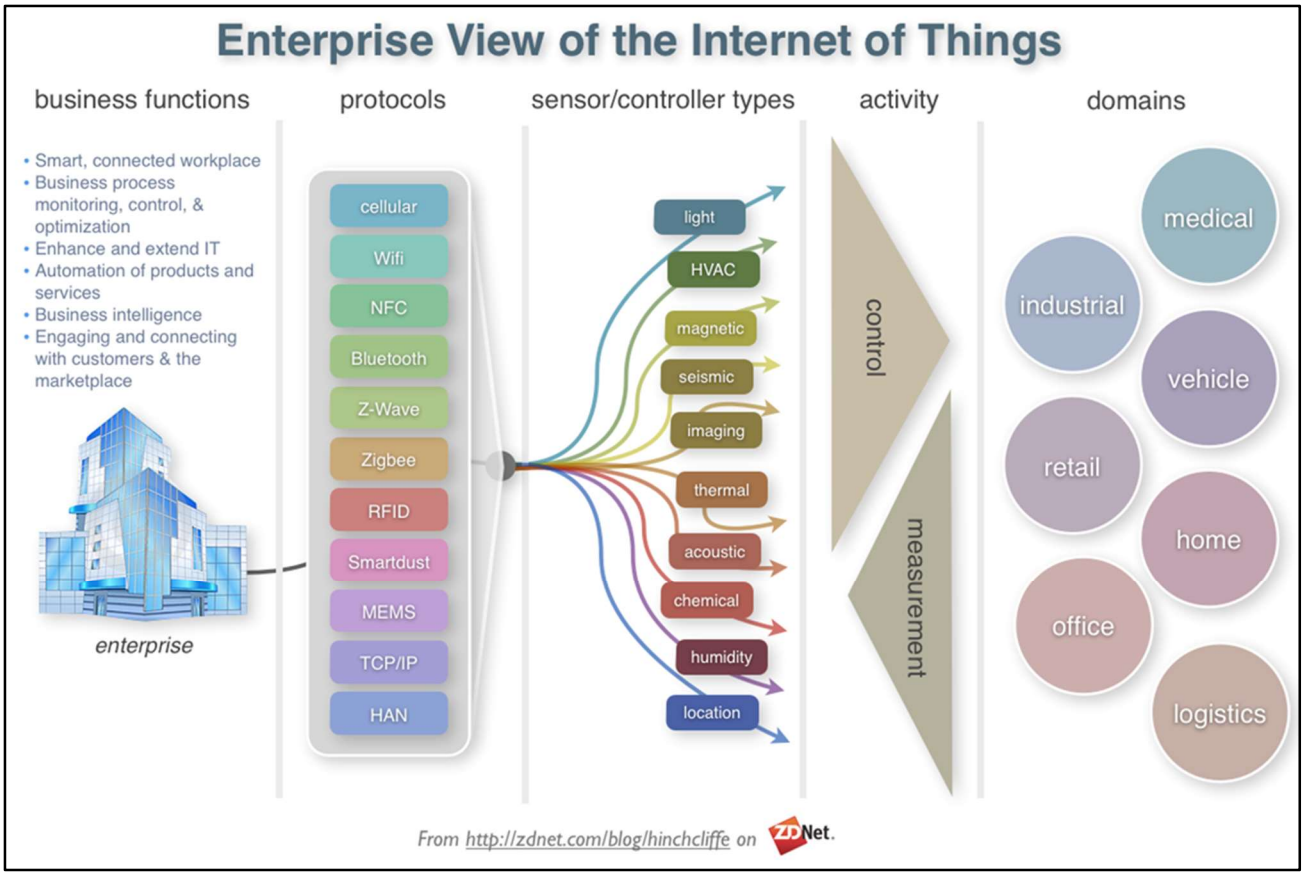


Figura 6 – Perspectiva empresarial da Internet das Coisas (Banafa, 2015).

Há exemplos de ataques a instalações industriais, sistemas de controlo de redes, num contexto de ciberguerra, o que é ainda mais preocupante, grave e assustador, mas está fora do contexto deste texto. Pode-se dar um exemplo, em 2015 um ataque de *hackers* desligou a rede de abastecimento eléctrico da Ucrânia, causando o primeiro *blackout* por ciberataque (Zetter, 2016). Depois de

observar e analisar devidamente a Figura 6, sem ser necessária muita imaginação, é fácil compreender a variedade, gravidade e consequências potenciais de ataques através da *IoT*. A IBM resume os desafios de segurança, para a *IoT*, da seguinte forma: segurança dos dispositivos; autenticação dos dispositivos; gerir as actualizações dos dispositivos; segurança das comunicações; privacidade e integridade dos dados; segurança das aplicações na nuvem, Internet e móveis; assegurar elevada disponibilidade; detectar vulnerabilidades e incidentes; gerir as vulnerabilidades e prever e prevenir questões de segurança (IBM, 2017). Apesar de não haver certezas nem garantias, de uma forma generalizada, a "revolução" está em marcha.

Actualmente, o interesse em dispositivos da *IoT*, por parte dos consumidores, é muito elevado, podendo-se ver na Figura 7, relativa ao fim de 2014, quais eram as buscas globais no Google acerca de aplicações da *IoT*, publicações no Twitter e no LinkedIn. Os dispositivos com mais popularidade são para casas inteligentes (controlo de temperatura, das luzes, frigorifico, fechaduras), seguidos de dispositivos que se podem usar (*smartwatches*, medidores de actividade física, óculos inteligentes), mas há um vasto leque de produtos disponíveis. Em 2019 a lista de dispositivos *IoT* mais populares era: Google Home Voice Controller, Amazon Echo Plus Voice Controller, Amazon Dash Button, August Doorbell Cam, August Smart Lock, Kuri Mobile Robot, Belkin WeMo Smart Light Switch, Footbot Air Quality Monitor, Flow by Plume Labs Air Pollution Monitor, Nest Smoke Alarm, etc. (STH, 2019).

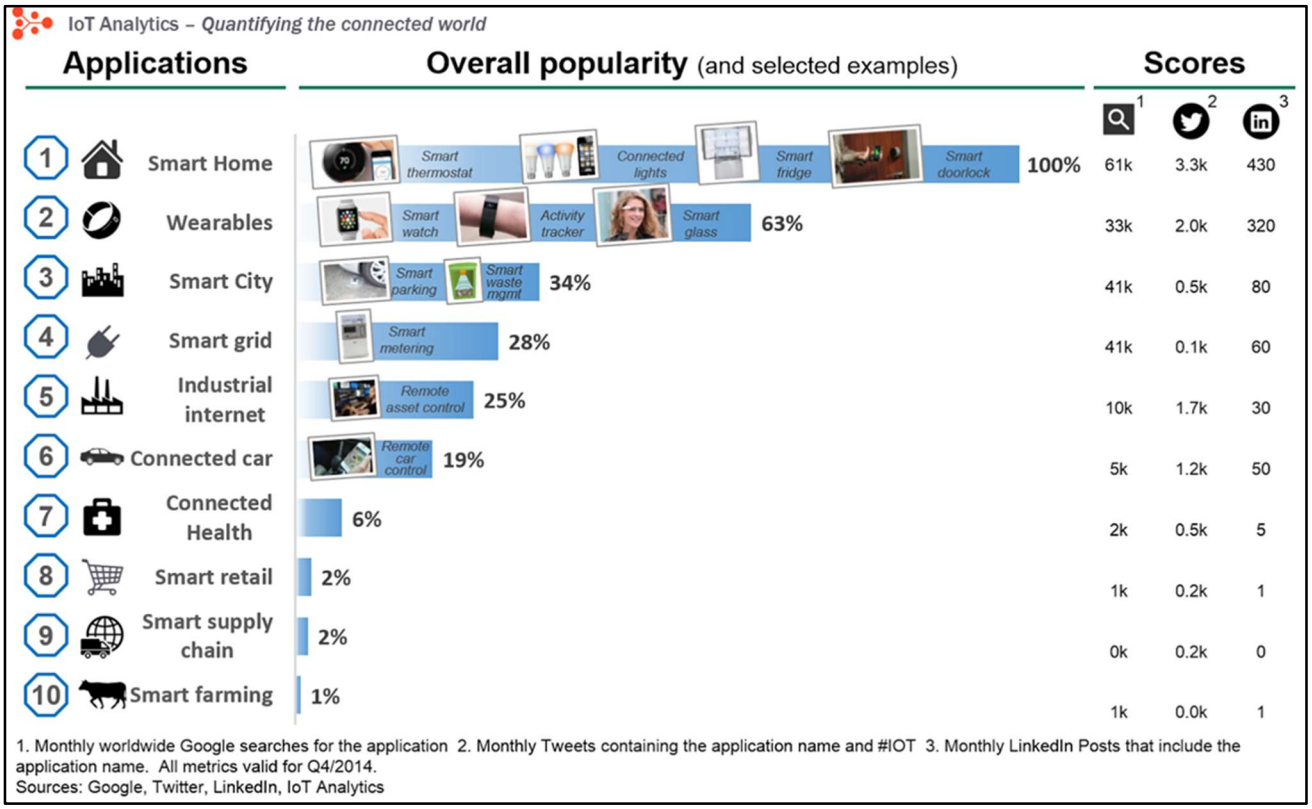


Figura 7 – Popularidade e exemplos seleccionados de aplicações da *IoT*, (Banafa, 2015).

Uma das principais ameaças à *IoT* é, como se percebe, a segurança, mas outra é visivelmente a privacidade, o que se enquadra nas questões da pegada digital e vida *online* que este texto pretende, sinteticamente abordar. Os consumidores acabam por abdicar da sua privacidade, passo-a-passo, sem se aperceberem, pois não sabem como os dados estão a ser recolhidos e utilizados. Quanto mais aplicações móveis, *wearables* e outros produtos "burros" são substituídos por equipamento inteligente ligado via *Wi-Fi*, deixando de ser possível comprar produtos "burros" que não os rastreiem (Bannan, 2016).

As principais questões de segurança podem ser agrupadas da seguinte forma (Meola, 2016)

- **Demasiados dados** – O volume brutal de informação que os dispositivos *IoT* podem gerar é desconcertante. Segundo um estudo da FTC, 10.000 casas podem gerar 150 milhões de pontos de dados discretos todos os dias, isto pode criar mais pontos de entrada para os *hackers* e deixa a informação vulnerável;
- **Perfil público indesejado** – Já alguém leu, efectivamente e até ao fim, os termos de prestação de um serviço? Sobretudo relativamente à recolha, uso e tratamento dos dados recolhidos? Uma companhia pode recolher dados dos hábitos de condução de um carro e vendê-los às companhias de seguros, ou os dados dos monitores de treino para efeitos de seguros de vida e saúde;
- **Escutas** – Os fabricantes, ou *hackers*, podem usar um dispositivo ligado para invadirem a privacidade da casa de uma pessoa. A Samsung avisou os clientes que as pessoas podiam estar a ser escutadas através do microfone das suas Smart TV's[20], a Amazon através do Echo[21], ou a Google através da Alexa[22];
- **Confiança dos consumidores** – Cada um destes problemas faz uma "mossa" no desejo que os consumidores têm de adquirir produtos ligados, o que limita o verdadeiro potencial da *IoT*.

As ameaças são reais, os dispositivos podem recolher e transmitir dados pessoais sensíveis, a geolocalização, dados de saúde e financeiros. Estes dispositivos tanto podem estar ligados directamente à pessoa, na sua casa e em equipamentos na casa, no carro, em barcos, etc. Há

[20] https://www.dailymail.co.uk/sciencetech/article-2945766/Is-TV-eavesdropping-PRIVATE-conversations-Samsung-warns-users-smart-sets-capture-word.html, ou https://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html

[21] https://www.telegraph.co.uk/technology/2017/08/01/amazon-echo-can-used-eavesdrop-conversations-hackers-reveal/ ou https://www.slashgear.com/how-private-is-amazon-echo-07354486/

[22] https://www.bloomberg.com/news/articles/2017-12-11/is-alexa-really-eavesdropping-on-you-jb25c6vc ou https://www.tomsguide.com/us/alexa-google-home-privacy,news-27038.html

casos de *hacking* a TV's [23], carros[24], GPS[25], sistemas de controlo de casas (*Home Control Hubs*)[26], câmaras de vigilância[27] etc. Potencialmente, todos os dispositivos da *IoT* podem ser atacados, as comunicações interceptadas, os dados roubados, ou seja, uma perspectiva de pesadelo para uma pegada digital ainda maior e mais vulnerável, a partir de cada vez mais pontos de acesso.

A ameaça também pode ser dupla, utilizando um dispositivo para atacar outro, como no caso de um *hacker* que conseguiu aceder a contas de utilizadores GPS (ProTrack e iTrack), sistema de gestão de frotas e localização de viaturas, o que lhe permitiu, em países de todo o mundo, "atacar" os carros em que estão instalados, desligando o motor, abrandando, etc. (Franceschi-Bicchierai, 2019).

[23] https://lifehacker.com/how-to-protect-your-smart-tv-from-getting-hacked-1822805501 ou https://mashable.com/2013/08/02/samsung-smart-tv-hack/?europe=true

[24] https://mashable.com/2013/08/02/samsung-smart-tv-hack/?europe=true ou https://www.caranddriver.com/features/a15124906/can-your-car-be-hacked-feature/

[25] https://nationalinterest.org/feature/the-pentagon-worried-about-hacked-gps-14898 ou https://www.hackread.com/hacking-*smartphones*-gps-in-car-navigation-system/

[26] https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/ ou https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes

[27] https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/ ou https://www.bankinfosecurity.com/2-million-iot-devices-have-to-p2p-software-flaw-researcher-a-12428

Geolocalização, questões técnicas

Aqui chegados, deverá ter ficado definido o que é a pegada digital, a sua tipologia (activa e passiva), o tipo de informação recolhida, os métodos e mecanismos de recolha, bem como os riscos e questões subjacentes de privacidade, pode-se então passar a um tipo específico de dados, os da geolocalização.

Para se poder compreender a importância da geolocalização, enquanto parte da pegada digital, é necessário começar por definir o que são Serviços Baseados em Localização S.B.L. (*Location Based Services LBS*). Estes S.B.L. são políticas, em serviços a nível de software, que permitem acesso a dados, ficheiros, objectos de memória ou outros serviços *online*, são serviços de informação utilizados em redes sociais, entretenimento, comércio e serviços, segurança e que são acessíveis com dispositivos móveis, através da rede móvel, utilizando informação da posição geográfica do equipamento (Wikipédia, 2019). No fundo, trata-se de dar acesso (ou não) a "serviços" em função da localização em que se está, o que acontece com computadores pessoais, portáteis ou não, *tablets* e *smartphones*, ou objectos.

Para os S.B.L. funcionarem o equipamento tem de permitir geolocalização, definida como o processo de encontrar e determinar a localização exacta de um computador, dispositivo em rede ou equipamento, baseada em coordenadas geográficas, utilizando GPS (sistema de posicionamento global) ou outras técnicas e métodos (Techopedia, 2019). No caso dos *smartphones* e *tablets* a determinação é sobretudo feita através de GPS (mas não exclusivamente), pode ser feita em função do endereço IP[28] do terminal (seja ele qual for), endereço MAC[29], sistemas RFID[30], dados EXIF[31] de ficheiros, ou outros sistemas de posicionamento sem fios (*WiFi*). Quando se está *online*, como já foi explicado (Figura 2) pode saber-se qual o endereço IP e qual a sua localização, seja num PC, *tablet* ou *smartphones*, mas estes últimos – os que são actualmente mais utilizados para navegar na Internet e criar vastas pegadas digitais – têm várias formas de determinar onde está o seu utilizador.

[28] Ver nota de rodapé Nº 2.

[29] *MAC address* (*Media Access Control*) – é um endereço físico associado à interface de comunicação, que liga um dispositivo à rede. O MAC é um endereço "único", não havendo duas portas com a mesma numeração, é usado para controle de acesso em redes de computadores. A sua identificação é gravada em hardware, isto é, na memória ROM da placa de rede de equipamentos como desktops, notebooks, rooters, *smartphones*, tablets ou impressoras de rede (Wikipédia, 2019).

[30] Ver nota de rodapé Nº 18.

[31] *EXIF – Exchangeable Image File Format* – é uma especificação seguida por fabricantes de câmaras digitais que gravam informações sobre as condições técnicas de captura da imagem, som e vídeo, junto ao arquivo propriamente dito na forma de metadados etiquetados, um desses dados são as coordenadas geográficas (Wikipédia, 2019).

Realmente, uma das mais importantes capacidades de um *smartphone*, quer se queira ou não, é saber-se onde se está; são os mais transportáveis dos equipamentos, que nos permitem estar na Internet e podem associar essa localização a dados, para disponibilizar um enorme conjunto de serviços. Tal como outras tecnologias digitais, estas capacidades trazem benefícios, mas também preocupações, pois conhecer a localização de alguém levanta sérias questões de privacidade, segurança física (entre ser-se seguido até ser-se preso), mas a maior parte das pessoas abraçaram os S.B.L. (Serviços Baseados em Localização) sem pensarem muito nos perigos, como a gestão dos dados pelos fornecedores ou roubo dos dados por *hackers* (Lawson, 2012).

Embora não seja evidente, para a larga maioria dos utilizadores, existem até 10 sistemas diferentes em uso nos *smartphones*, ou a serem desenvolvidos, que permitem identificar a sua localização, sendo que, em muitos casos, são utilizados vários em conjugação para melhorar o resultado, ou substituindo-se quando um dos sistemas é menos eficaz. Os sistemas disponíveis são os seguintes:

1. GPS - várias redes, GPS (E.U.A.), Glonass (Rússia), Galileo (U.E.) e Beidou (China);
2. GPS assistido – Rede Celular (GSM) e *Wi-Fi*;
3. GPS sintético – software calcula, com dias/ semanas de avanço, localização dos satélites da rede;
4. Identificação de célula – GSM;
5. Wi-Fi – sabe-se onde estão os routers e servidores;
6. Sensores de inércia – Direcção da deslocação, aceleração, mudanças de direcção;
7. Barómetro – conjugada com outros para determinar altitude;
8. Ultra-sónico (RFID e NFC[32]) – Por onde o equipamento vai passando, e.g. dentro de lojas;
9. Balizas *Bluetooth*[33] - localização precisa em ambientes fechados;
10. Transmissores terrestres.

O rastreamento dos equipamentos móveis, estacionários ou em movimento, pode ser feito somente por triangulação dos sinais rádio entre várias antenas (que definem células), pois o sistema GSM baseia-se na identificação da potência do sinal do telefone em relação às antenas, pode ser feito sem existirem chamadas telefónicas, isto implica que a rede sabe, SEMPRE, onde está o telefone, mesmo que tudo o resto esteja desligado (GPS, acesso à Internet, *Wi-Fi* e *Bluetooth*). Graças a este facto, as autoridades conseguem (felizmente) localizar e seguir criminosos e actividades ilícitas, ou salvar e resgatar pessoas cujo paradeiro, de outra forma, não se poderia determinar (há inclusive aplicações que permitem saber a localização com base, exclusivamente, no número de telefone).

[32] *NFC - Near Field Communication* - Comunicação por Campo de Proximidade, é uma tecnologia que permite a troca de informações sem fio e de forma segura entre dispositivos compatíveis que estejam próximos um do outro. Ou seja, logo que os dispositivos estejam suficientemente próximos, a comunicação é estabelecida automaticamente, sem a necessidade de configurações adicionais. Estes dispositivos podem ser telefones celulares, *tablets*, cartões e qualquer outro dispositivo que tenha um chip NFC (quase todos os *smartphones* têm) (Wikipédia, 2019).

[33] *Bluetooth* – Especificação de rede sem fios, para troca de informação entre dispositivos, via rádio, segura e que funciona a pouca distância.

Percebe-se facilmente que esta informação é altamente pessoal e delicada, pois sem qualquer consentimento da pessoa pode-se seguir toda a sua vida quotidiana, sendo que estes dados deveriam ser tão ou mais protegidos que outros dados recolhidos e que fazem parte da pegada digital individual, é uma questão de Geoprivacidade. A entidade que gere o sistema GPS dos E.U.A. (GPS.gov, 2018) chama a atenção para o facto de o sistema ser unidireccional, não podendo rastrear nada nem ninguém no solo, limitando-se a enviar sinais que os receptores captam e processam. Destacando casos judiciais relativos à privacidade da localização, lembra que a 4ª Emenda à Constituição protege os cidadãos e a sua privacidade, mas declara que não é claro se o uso de tecnologia GPS, sem mandato, para rastrear e perseguir criminosos, é ou não uma violação deste direito. Não obstante, uma decisão do Supremo Tribunal de 2012, declarou ser necessária a existência de um mandato judicial antes de se colocar um dispositivo de rastreamento GPS no veículo de um suspeito.

Mas para se ter melhor noção deste tipo de informação, é essencial analisar qual é, efectivamente, o grau de precisão destes sistemas nos equipamentos móveis, que trazem incorporado um Chip GPS que é concebido sobretudo para: optimizar o consumo de energia, ser rápido a fixar os satélites e optimizar a precisão. Segundo um teste feito para a ESRI há seis anos (Shaner, 2013), com vários equipamentos, a precisão com céu aberto (sem prédios, nem obstáculos verticais significativos, em relação à linha de horizonte) foi em 99% dos casos inferior a três metros. Utilizando antenas exteriores (*Bluetooth*), emparelhadas com os *smartphones* 99% das posições estavam abaixo de três metros de precisão, mas 70% estavam abaixo de um metro. Por último, ligando o equipamento a uma antena de alta precisão, 92% das posições estavam abaixo de um metro de precisão, mas isto foi há seis anos…

Segundo Pesyna, Heath, & Humphreys, (2015), utilizando certas antenas exteriores ao telefone, foi possível atingir precisões centimétricas, até porque os próprios modelos de órbita, atmosfera e relógio foram melhorados e, entretanto, apareceram mais sistemas GPS. Mas o problema maior, nos equipamentos "normais" acontece com a degradação de sinal em ambiente urbanos, a "selva urbana", com muitas obstruções da linha de horizonte e limitação da proporção de céu aberto. Num teste feito nos E.U.A. (Buczkowski, 2016), em 150 localizações em centros urbanos, concluiu-se que a precisão da localização média rondava os 30 metros, podendo variar (consoante as condições), entre um mínimo de um metro e um máximo de 204 metros. O valor médio depende do "volume" e densidade de edifícios (Nova Iorque, 87 metros de precisão média, Boston, 51 metros, Chicago, 10 metros), mas outros factores são responsáveis pela variação: fontes (GPS, *WiFi* e GSM), dentro ou fora de portas e uso pessoal (grau de acesso no telefone, tipo de aplicação, sistema operativo e modelo).

Visto que esta variabilidade e precisões médias deixavam, nalguns caso, algo a desejar, a indústria conjugou esforços para melhorar os Chipsets[34] GPS nos *smartphones*, tirando também partido da existência de mais e melhores sinais, tendo como objectivo atingir precisões da ordem dos 30 centímetros, em equipamentos a partir de 2018 (Kastrenakes, 2017). Estes equipamentos recebem melhor os sinais, de mais constelações GPS, bem como informação adicional que podem utilizar para "refinar" a posição, sendo sobretudo muito mais eficazes em ambientes urbanos. Actualmente, há investigação utilizando *smartphones* actuais, combinando sinais dos diferentes sistemas GPS, que podem chegar a centímetros de precisão (University of Otago, 2018), como se pode ver na Figura 8.

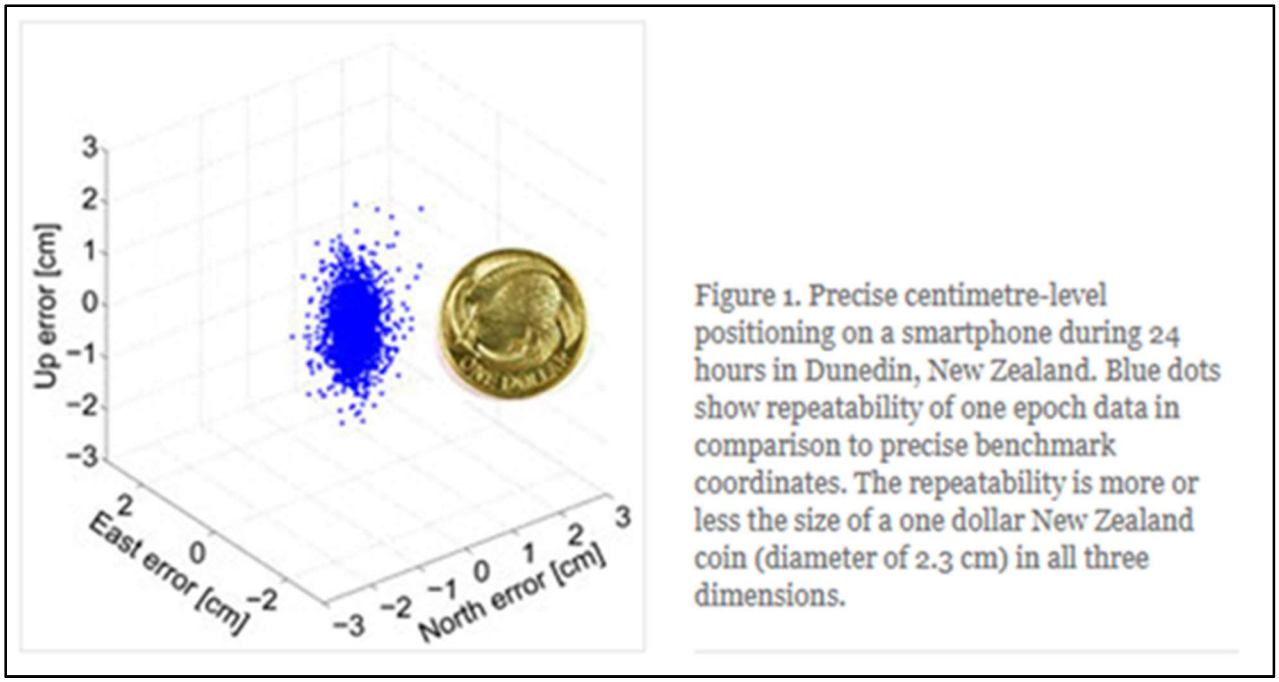


Figura 8 – Posicionamento a nível centimétrico, em três dimensões, utilizando um *smartphone*, ao longo de 24 horas, ao lado de uma moeda de 2.3 cm para efeitos de escala (University of Otago, 2018).

A quase total ubiquidade de *smartphones*, o seu uso também para acesso à Internet, chamadas e mensagens de texto, levanta questões importantes de segurança às pessoas e actividades que desenvolvem, pois não foram pensados nem concebidos para segurança e privacidade. Um dos rastreamentos mais fáceis de fazer é, precisamente, o da sua localização, mesmo com uma baixa margem de precisão espacial, ou interceptar as comunicações, o que, como em tudo, pode ser bom (para "apanhar os maus"), ou péssimo se for para nos espiar e seguir. Acresce o facto de se ter muito menos controlo, num equipamento móvel quando comparado com um computador,

[34] Chipset - Conjunto de componentes electrónicos, num circuito integrado, que gerem o fluxo de dados entre o processador, memória e periféricos. É normalmente encontrado na placa mãe (*motherboard*) do equipamento (Wikipédia, 2019).

sobre as opções, software e forma como utiliza os recursos e sistema operativo, entre outros (SSD, 2018). Tal como outros equipamentos electrónicos, os telefones podem ser "infectados" com *malware*[35]

Por isso, muitos criminosos, ou pessoas que querem simplesmente fugir às possibilidades de rastreio, utilizam telefones descartáveis (*burner phones*), geralmente o mais simples possível e com o mínimo de extras e possibilidades de ligação. Não basta trocar de equipamento, é preciso mudar de número, substituindo o SIM, as redes sabem que SIM's foram utilizados em que equipamentos, podendo seguir ambos, em conjunto ou separados. Convém também lembrar que as comunicações móveis são feitas via radio, não encriptadas, podendo, portanto, ser facilmente escutadas com equipamento de escuta rádio. Além desta informação os operadores registam e sabem, naturalmente, quem liga ou envia mensagens para quem, o que disseram ou escreveram, bem como o tráfego de e para a Internet. Ainda bem que assim é, esperando-se, como já referido, que somente com ordem judicial se possa ter acesso a essa informação e por razões "válidas".

No fundo, faça-se o que se fizer, há quem saiba sempre onde o equipamento está, mas acreditamos que essa informação não é acedível pelo público em geral, portanto desligando os serviços de localização do telefone, só os operadores ou alguém com capacidade especiais de rastreio, pode localizar o equipamento. Mas não é bem assim, segundo um estudo realizado nos E.U.A. (Kaplan, 2016), cerca de 90% das pessoas mantêm a função dos serviços de localização sempre ligada nos seus *smartphones*. Isto porque dependem dos equipamentos para se orientarem e navegarem, ou utilizarem serviços vários que dependem da sua localização, os S.B.L. Neste estudo, 90% das pessoas utilizavam os telefones para localização, 67% para ouvir música, 47% para videochamadas e 30% para ver conteúdos de entretenimento. Por alguma razão, a Google diz que as buscas por "locais perto de mim" aumenta cerca de 150% por ano, o que certamente é ajudado pelo "*auto complete*" na barra de procura.

É evidente que a geolocalização tem riscos, mas tem, também, muitos e importantes benefícios, por isso a banalização e uso maciço, mas esta informação, tal como a pegada digital em geral, pode ser recolhida de uma forma activa ou passiva, cruzando e correlacionado informação do utilizador. Com uma estimativa de mais de dois mil e quinhentos milhões de *smartphones* no mundo em 2019 e mais de dois milhões de aplicações Android e iPhone no mercado, a prevalência de tecnologia de geolocalização só continuará a aumentar (Estes, 2016). Vejamos então quais são as três principais categorias de dados de geolocalização, Figura 9.

[35] *Malware - malicious software*, é software destinado a infiltrar-se num sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações. Pode aparecer na forma de código executável, *scripts* de conteúdo activo e outros tipos de softwares. "Malware" é um termo geral utilizado para referir uma variedade de formas de software hostil ou intrusivo (Wikipédia, 2019).

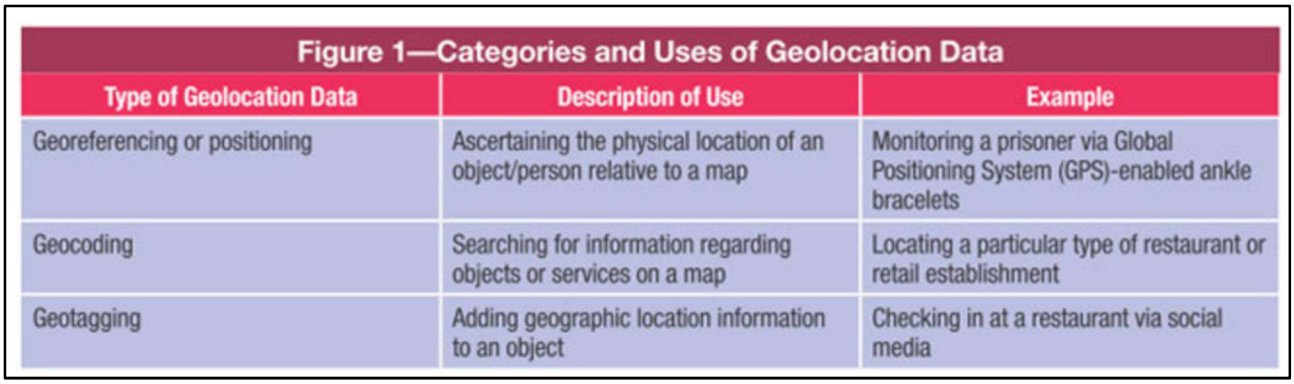


Figure 1—Categories and Uses of Geolocation Data

Type of Geolocation Data	Description of Use	Example
Georeferencing or positioning	Ascertaining the physical location of an object/person relative to a map	Monitoring a prisoner via Global Positioning System (GPS)-enabled ankle bracelets
Geocoding	Searching for information regarding objects or services on a map	Locating a particular type of restaurant or retail establishment
Geotagging	Adding geographic location information to an object	Checking in at a restaurant via social media

Figura 9 – Principais categorias e usos de dados de geolocalização (Estes, 2016).

O tipo de dados mais mencionado e explorado até aqui é, pura e simplesmente, a georreferenciação ou posicionamento, localização exacta, física, de um objecto ou pessoa relativamente a uma base cartográfica, que é feita directamente ou de uma forma assistida sobretudo por GPS. Mas existem também a geocodificação, a transformação da descrição de um endereço físico numa localização num mapa, uso muito comum: ver onde é ou fica algo (morada, serviço, objecto). Por último, há ainda o *geotagging*, o processo de adicionar informação de localização a um objecto, quando se atribui coordenadas geográficas a uma fotografia ou se identifica, numa rede social, o local onde se está. Todos, os que têm uma vida *online*, podem reconhecer nestes três tipos de dados de geolocalização, práticas e procedimentos comuns e quotidianos.

Além das vantagens para os utilizadores, a geolocalização traz grandes (e chorudos) benefícios aos negócios, estando a ser alavancada por todos os tipos de empresas, manufactura, retalho, serviços financeiros, seguros, transportes, utilidades e governos. Para muitos negócios, o uso de geolocalização e tecnologias móveis é crítico, pois em conjugação com aplicações através de várias plataformas, providencia a base para fundir informação de localização, redes sociais em serviços de contexto enriquecido (Estes, 2016). Alguns dos usos e benefícios da geolocalização, para os negócios, incluem:

- Publicidade direccionada;
- Gestão de entregas e frotas;
- Personalização e optimização de conteúdos e entregas;
- Realidade aumentada;
- Veículos autónomos;
- Detecção e prevenção de fraude;
- Gestão em tempo real de incidentes.

Mas, segundo o mesmo autor, os factores de risco da recolha destes dados estendem-se muito para lá dos indivíduos, até às empresas e famílias, levantando questões de privacidade e segurança: que dados são recolhidos? Quem é que está a recolher os dados e quem é que os está a utilizar? Com quem podem os dados ser partilhados e quanto tempo ficam guardados? A partilha acidental ou involuntária de dados de localização pode resultar em incómodo, embaraço ou perigo para a segurança do individuo? Há dois caminhos para mitigar o risco da geolocalização: através de salvaguardas tecnológicas e (sobretudo) através do utilizador.

Na prática, como referem Valentino-DeVries, Singer, Keller, & Krolik, (2018), "As suas aplicações sabem onde esteve ontem à noite". Pois dezenas de empresas utilizam as localizações que o *smartphone* regista para ajudar sobretudo os publicitários (mas não só), dizendo que os dados são anónimos, embora eles mostrem quão impessoais são. Segundo um estudo, referido pelos autores, pelo menos 75 companhias recebem dados anónimos, com informação de localização precisa, de aplicações que ligam os serviços de localização dos *smartphones* para obter notícias locais e previsões meteorológicas. Algumas destas empresas afirmam seguir até 200 milhões de dispositivos móveis nos E.U.A., sendo que uma amostra desta informação expunha as deslocações diárias das pessoas, com um erros de metros, nalguns casos actualizada até 14.000 vezes por dia.

Estas companhias vendem, usam ou analisam os dados, para os fornecer a anunciantes, procurando compreender os hábitos dos consumidores, é um mercado "em brasa", atingindo uns estimados 21 mil milhões de Dólares em 2018, tendo a IBM entrado no mercado ao comprar as aplicações do Weather Chanel. É todo uma economia de dados de localização, em que as aplicações formam a espinha dorsal do negócio, bastando seguir o dinheiro para se perceber que a publicidade direccionada é o uso mais comum da informação. Valentino-DeVries, Singer, Keller, & Krolik, (2018) referem ainda que "a Google e Facebook, que dominam o mercado móvel de anúncios, também lideram na publicidade baseada em localização. Ambas as companhias recolhem dados das suas próprias aplicações. Dizem que não os vendem e os guardam para si, para personalizarem os seus serviços, vender anúncios direccionados na Internet e saber se os anúncios levam a vendas efectivas".

Mas como é possível que os *smartphones* recolham, utilizem e partilhem tanta informação? O que se pode fazer para evitar isto? Como vimos antes, há inúmeros sensores e sistemas a produzir dados de localização, mas sabe-se que mesmo desligando aplicações, GPS e outros sistemas, a localização pode ser conhecida, aliás a Google foi "apanhada" a rastrear dados dos utilizadores mesmo com tudo desligado (Misra, 2018). O problema é que estes computadores de bolso, carregados de sensores, fornecem quantidades assombrosas de informações às aplicações, quer sejam do sistema ou instaladas pelos utilizadores, enviando-as ao fabricante do equipamento, do próprio sistema operativo (Google ou Apple), etc. Junta-se a isto todas as pesquisas, os dados

rastreados pelos navegadores, pelos sítios visitados e, sobretudo, onde e quando se está a fazer isso (Nield, 2018).

Para se ter uma ideia do acesso que as aplicações têm aos dados é ir às definições do telefone, aplicações e notificações (no Android), escolher uma APP e ver as permissões, é de se ficar estarrecido com as que não parecem ser necessárias para o funcionamento da aplicações ou utilização do serviço. Mas rapidamente se percebe que, depois de ver que dados são recolhidos e depois como podem ser usados ou passados a terceiros, não é fácil compreender quais as políticas, pois estão salvaguardadas em ambiguidade e cláusulas de difícil percepção, para defender os fabricantes e produtores. Já houve um artista (Dima Yarovinsky), que fez uma instalação de arte ("I agree") com os "user agreements" (termos e condições) que todos devíamos ter lido, mas não lemos[36].

Cada vez mais anunciantes utilizam publicidade "consciente da localização", anúncios que aparecem quando estamos perto de certos negócios ou empresas, o que se pretende é um registo completo de onde se está a toda a hora. Segundo Webster (2018), um exemplo deste mercado é a WeatherBug, uma aplicação que requere a localização do utilizador para fornecer actualizações da previsão meteorológica, mas que é propriedade da GroundTruth, uma empresa de publicidade, além de toda a informação que a APP necessita para funcionar, também é vendida a terceiros. A GroundTruth tem a possibilidade de extrair informação de "mais de mil" outras aplicações que integraram parte do seu código de software, seguindo diariamente, nos E.U.A., cerca de 70 milhões de pessoas: onde estão, quando saem para o trabalho, por onde, quando voltam para casa, quando vão a eventos públicos, etc.

Portanto, muitas empresas vendem a informação de localização dos utilizadores de *smartphones*, segundo Garen (2018), nos E.U.A. as empresas de marketing gastaram em 2017, 16 mil milhões de Dólares em anúncios direccionados à localização, cerca de 40% de toda a despesa com anúncios em equipamentos móveis, esperando que este valor duplique até 2021. "O espião está no nosso bolso", mesmo desligando os serviços de localização e revogando os privilégios das aplicações, existem inúmeras formas de rastreio, por vezes as mais invasivas são as mais fáceis (basta pensar na forma como, voluntariamente, partilhamos *online* dados da nossa localização em redes sociais…). Cada *smartphone* é como um farol, que emite continuamente dados, mesmo que não toque, que não se navegue, que o GPS esteja desligado, há sempre aplicações a recolher e enviar dados, por isso essa informação vale tanto dinheiro para Wall Street" (Dezember, 2018).

Segundo um estudo realizado no Canadá (Tomlinson, 2017), o utilizador de *smartphone* tem 18 aplicações instaladas em média, de redes sociais a *Fitness*, compras e jogos, portanto inventaram uma aplicação, um simples horóscopo, para testar até que ponto os utilizadores revelavam dados

[36] https://gizmodo.com/these-giant-scrolls-are-the-hellish-user-agreements-you-1825822690

pessoais quando instalavam aplicações. Todas as pessoas abordadas, para descarregar a aplicação, deram acesso à localização, câmara do telefone, até ao microfone. Algumas das aplicações mais populares requerem estas autorizações, além dos contactos, mensagens, etc., podendo, além de seguir os movimentos da pessoa, activar a câmara ou o microfone, o que é, no mínimo, perturbante. Os consumidores têm, efectivamente, que estar cientes de que dados e em que quantidade estão a oferecer, percebendo que estão a pagar com a sua privacidade muitos serviços, que geralmente são, talvez também por isso, gratuitos.

Uma forma mais indirecta, tanto voluntária como involuntária, de se acrescentar dados da localização à pegada digital de quem está *online* é através do *geotagging*. Segundo a Wikipédia (2019) *geotagging* é o processo de acrescentar metadados com informação geográfica a vários tipos de média, como a fotografias, vídeos, sítios web, mensagens de texto, códigos QR[37], entre outros. Os dados consistem geralmente em coordenadas de latitude e longitude, mas também podem incluir altitude, rumo (azimute), distâncias, dados de precisão, nomes de locais e uma indicação temporal. Esta informação pode ser obtida por um, ou vários, dos sistemas mencionados anteriormente, produzindo dados de elevada precisão.

Quer isto dizer que, quando se usa um *smartphone* para tirar fotografias (muitas máquinas fotográficas "clássicas" também o permitem), está-se automaticamente a incluir dados de geolocalização (de elevada precisão) nas imagens e vídeos, o que muitos utilizadores desconhecem e tem sérias implicações em termos de privacidade. Várias celebridades denunciaram, assim, a localização das suas casas e locais de férias, a localização de bens precisos (animais em vias de extinção, espécies raras, locais protegidos), já para não mencionar questões de segurança de ordem militar. Segundo Rodewig, (2012), em 2007, no Iraque, quatro helicópteros Apache da USAF foram destruídos no solo por tiros de morteiro, graças a fotos com localização que vários soldados partilharam em redes sociais.

As fotos em formato JPEG[38], partilhadas no Twitter, Facebook, Instagram, WhatsApp, Snapchat, ou simplesmente armazenadas no telefone (e partilhadas com a Google através do Google Photos…), têm as coordenadas exactas do lugar onde foram tiradas. Esta informação está guardada nos metadados EXIF[39] do ficheiro e, uma vez mais, a ideia é boa, saber todos os parâmetros técnicos da imagem (máquina usada, diafragma, velocidade de obturação, data e hora, resolução, etc.), podendo-se também usar os outros dados para catalogar, organizar e classificar. Mas haverá mesmo perigo? Segundo Schiffner (2013), por exemplo, num caso que se tornou emblemático, em

[37] Código QR - *Quick Response Code*, código de barras matricial, bidimensional.
[38] JPEG - *Joint Photographic Experts Group* (jpeg.org)é um método comum usado para comprimir imagens fotográficas. O grau de redução pode ser ajustado, o que permite escolher o tamanho de armazenamento e seu compromisso com a qualidade da imagem (Wikipédia, 2019).
[39] EXIF - *Exchangeable image file format*, norma utilizada para imagem, vídeo e som, em câmaras digitais, scanners, etc. (Wikipédia, 2019).

Setembro de 2010 três ladrões assaltaram mais de 18 casas na área de Nashua, New Hampshire, nos E.U.A., seguindo os movimentos dos proprietários *online* e, quando estes estavam fora, entrando nas casas e levando mais de 100.000 dólares de bens.

Segundo o mesmo autor, 78% de ex-assaltantes condenados, disseram que as redes sociais estão a ser utilizadas para escolha de alvos, 74% referindo, enquanto "especialistas", que o Google Street View desempenha um papel essencial em muitos dos assaltos a casas actualmente. O mais elementar bom senso dirá que, partilhar fotos de bens valiosos, dentro ou fora de casa, georreferenciados, é mesmo estar a convidar os ladrões. Os principais conselhos decorrentes deste estudo, relativamente a fotografias são:

- Remover / limpar a informação dos metadados ("*sanitize*") utilizando software de edição EXIF[40];
- Não publicar fotografias directamente a partir do telefone, utilizar a câmara sem GPS;
- Fotografias tiradas com o telefone, gravar em formato PNG, não tem dados EXIF, partilhar de um PC;
- Não fazer *posts* em nenhuma rede social a partir do telefone, a ter de o fazer, não autorizar as aplicações a usar dados do GPS.

O problema, uma vez mais, é que muitas pessoas não têm qualquer noção disto, acham que a informação é anónima ou não põe gravemente em questão a sua privacidade e, infelizmente, o bom senso também não é assim tão abundante e bem distribuído como isso. Num artigo sobre as implicações para a privacidade do *geotagging*, Sommer & Friedland (2010), fazem o seguinte ponto da situação;

- **Serviços de geolocalização** – Cada vez mais serviços *online* recolhem, fornecem e analisam informação geográfica, encorajando até constantemente a partilha da localização, para por exemplo encontrar amigos nas imediações, lojas com descontos, mostrar onde se esteve, comeu, etc.;
- **Privacidade da localização** – os S.B.L. (Serviços Baseados em Localização) têm diferentes abordagens à privacidade, na maior parte das aplicações as opções por defeito incluem, quase sempre, fornecer dados de geolocalização (nos iPhones sempre, no Android tem de se ligar);
- **Triangulação GPS e *WiFi*** – Quase todos os *smartphones* têm GPS, juntando as possibilidades de incremento da precisão, através das redes *WiFi* e GSM, obtêm-se sempre uma localização ou muito elevada precisão nas coordenadas;
- **Metadados** – A vantagem original, como já foi referido, é a facilidade de catalogação e organização, mas os dados EXIF não são visíveis directamente e a maioria dos utilizadores não os conhece.

[40] https://listoffreeware.com/free-exif-editor-software-windows/

Os autores realçam que não advogam deixar de se utilizar a geolocalização, em geral, ou o *geotagging* em particular, pois é uma tecnologia maravilhosa, mas sentem que há uma falta clara de educação e informação, bem como de concepção de sistemas que protejam ao máximo a privacidade. Nesse artigo demonstram como, facilmente, utilizando os dados EXIF de uma fotografia, procurando essas coordenadas no Google Maps ou Earth e depois com o Google Street View, se chega a um metro de distância de onde a fotografia foi tirada, ver Figura 10.

Figure 1: Photo of a bike taken with an iPhone 3G and a corresponding Google Street View image based on the stored geo-coordinates. The accuracy of the camera location (marked) in front of the garage is about +/−1 m. Many classified advertisements come with photos of objects offered for sale, with geo-tags automatically added.

Figura 10 – Foto de bicicleta e imagem Google *Street View* correspondente, baseada nas coordenadas dos Metadados (Sommer & Friedland, 2010, p. 5).

Vários investigadores e analistas independentes de segurança *online* (auto-apelidados "*white hat hackers*"), têm desenvolvido esforços no sentido de aumentar a consciencialização acerca dos *geotag*, produzindo estudos e apresentações (Murphy, 2010). Há artigos interessantes, por exemplo Choi, Larson, Li, Li, Friedland & Hanjalic, (2017), avaliaram como os filtros das câmaras dos *smartphones* podem ajudar a proteger a privacidade, alterando as fotos e metadados. Alguns sítios, como o Flickr, têm dado passos para dificultar o acesso aos dados de geolocalização das images e, actualmente, o Twitter retêm-nos, mas não os divulga[41], o Facebook retira os dados[42], mas o Instagram não se percebe[43].

Há efectivamente formas de diminuir a pegada digital, neste caso geográfica, aumentando a geoprivacidade dos utilizadores, embora nunca de uma forma directa, mas num futuro próximo, 2020 talvez, com o advento da próxima geração de comunicações móveis (5G), vai ser muito mais difícil manter – tentar ter essa geoprivacidade. Actualmente a triangulação entre GPS e rede 4G

[41] https://help.twitter.com/en/using-twitter/tweeting-gifs-and-pictures
[42] https://www.facebook.com/help/community/question/?id=10201464422674131
[43] https://www.techjunkie.com/instagram-remove-exif-data-images/

permite uma grande precisão, acrescida com mais sistemas GPS e melhores *chipsets*, excepto quando as condições de operação são péssimas (combinação de sinal fraco e muito mau tempo). Com a 5G a precisão aumentará mais de 10 vezes, pois as torres das células que permitem esta nova tecnologia serão muito mais numerosas (Bosnjak, 2019), assim, por exemplo, os dispositivos Android podem verificar periodicamente as suas coordenadas, mesmo com a localização desligada.

Como é que a privacidade da localização se vai degradar tanto? Cada vez que um dispositivo liga a uma torre, a rede móvel sabe a que distância ele está da torre, na 4G isso dá uma "resolução" de cerca de um quilómetro e meio, mas como as torres 5G vão ter que estar em "todo o lado" e o dispositivo se liga, de cada vez, a uma torre, a rede saberá com enorme precisão onde se está, prédio-a-prédio (Grothaus, 2019). Além desta profusão e proximidade de antenas, tem havido crescente preocupação com a possibilidade de formas de vigiar o tráfego, nomeadamente por parte dos fabricantes de equipamento, como a chinesa Huawei, o que tem levado a tensão entre os E.U.A. e o resto do mundo (Halpern, 2019).

Acresce ainda, que ao deslocar-se, o operador pode cartografar o trajecto com um elevado grau de precisão, pois salta-se de torre para torre em muitíssimo menores distâncias. A questão põe-se caso os operadores de comunicações vendam os dados, sobretudo para serviços de publicidade e dados altamente orientados para localização de alta precisão. Enquanto começa a instalação da 5G, já se planeia a 6G (2030), mais rápida (1 Tbps e 1 ms de latência) e virada para a optimização da inteligência artificial (McCaskill, 2018).

A geolocalização tornou-se, portanto e como parte da mais abrangente pegada digital de cada pessoa, uma das mais sofisticadas ferramentas de negócio da era digital, produzindo volumes extraordinários de informação e estando, embora não exclusivamente, ligada ao próprio conceito de *Big Data*, aqui definida como tecnologia de informação, grandes conjuntos de dados, resultantes do aumento exponencial de informação no mundo digital, (Wikipédia, 2019), Figura 11.

A sinergia da geolocalização com o *Big Data* está a modificar as rotinas quotidianas, estes dois sistemas mudaram a forma como se concebem estratégias de marketing digital, lojas de retalho, recrutamento e muitas outras áreas de negócio. Quais são então, de acordo com Ryan (2018), os seis modelos de *Biga Data* na geolocalização:

- ***Geofencing*** – Perímetro virtual para uma área, alerta as empresas, através de sinais rádio ou GPS, quando consumidores alvo entram num determinado território ou localização, isto dá às companhias a possibilidade de enviar mensagens, em tempo-real, acerca de descontos, ofertas ou promoções que resultam frequentemente em compras. Além deste benefício, a *Big*

Data analisa a informação recolhida pelo *geofencing* e detecta padrões de compra e hábitos dos clientes dentro das lojas;

Figura 11 – Os 10 V's da *Big Data* (Daniel, 2017).

- **Tecnologia de balizas**[44] – Envia notificações acerca dos últimos produtos, mais vendidos, promoções ou descontos, de acordo com um estudo, mais de 70% dos retalhistas conseguem rastrear e compreender os padrões dos consumidores desta forma. Isto só é possível com *Big Data*, permitindo comunicar as melhores ofertas, cruzando imensa informação e agir proactivamente quando entram ou estão perto dos seus pontos de venda;
- **Publicidade** – O marketing contemporâneo não se baseia em mensagens genéricas, os consumidores modernos exigem cada vez mais uma abordagem personalizada, visto que todas as pessoas deixam uma enorme pegada digital na Internet, toda essa informação requer uma análise *Big Data* para prever e calcular as necessidades dos utilizadores em todas as localizações;
- **Recursos humanos** – Muitos empregos são "sensíveis" e dependentes da localização, sendo necessário procurar candidatos em cidades e regiões específicas. A tarefa é muito mais facilitada pois pode direccionar espacialmente os anúncios de empregos e saber a origem geográfica dos candidatos;
- **Transportes** – Os transportes e logística actuais não seriam sustentáveis sem *Big Data* e geolocalização. Grandes sistemas como redes ferroviárias e aeroportos não poderiam funcionar sem actualizações constantes de velocidades de veículos, distâncias, condições meteorológicas e muitas outras indicações. Mesmo os transportes pessoais dependem de *Big*

[44] *Beacon* no original, em Inglês.

Data, por exemplo, recebemos notificações constantes e em tempo real sobre o estado do trânsito, melhores caminhos, obras em curso, etc. sendo todos pequenos detalhes, mas que tornam a nossa vida quotidiana mais confortável;

- **Cuidados de saúde** – O *Big Data* tem potencial para diminuir drasticamente os custos, um dos aspectos mais óbvios está relacionado com a prevenção da hospitalização, pois os médicos podem controlar as condições físicas dos pacientes, à distância, em qualquer localização (lembram da *IoT* e dos seus sensores?). Um fluxo constante de informação médica torna possível prever problemas potenciais ou lembrar aos pacientes consultas marcadas, procedimentos médicos, eliminando muitas intervenções presenciais.

O mesmo autor, Ryan (2018), conclui que, "embora a geolocalização não seja uma tecnologia nova, ela é amplificada drasticamente com o surgimento do *Big Data*. Hoje é possível analisar volumes gigantescos de informação e utilizá-la para direccionamento em função da localização em todo o mundo. As companhias exploram esta tecnologia no retalho, logística e em todos os tipos de indústrias".

Assim, depois de se abordar a geolocalização nos seus aspectos técnicos, como se obtém, como pode ser melhorada, como a partilhamos (activa ou passivamente) e como o *Big Data* enquanto método e abordagem podem alavancar e optimizar a sua utilização, enquanto parte (mais uma) da nossa pegada digital, convém abordar a geolocalização em termos exclusivamente de privacidade, a geoprivacidade propriamente dita.

Geoprivacidade

A única definição de geoprivacidade que se consegue encontrar *online*, em Wiktionary[45], é "manter privada a localização geográfica de uma pessoa, especialmente a restrição de dados geográficos mantidos por equipamento pessoal electrónico". Será que ela é assim tão importante? Num artigo de Kounadi & Leitner (2014), em que foram analisadas, no período 2005-2012, 19 Revistas Científicas relacionadas com SIG, Geografia, análise espacial de crime e Geografia da saúde, foram identificados 41 artigos com informação (geográfica) confidencial e 16 artigos em que a informação foi protegida com uma máscara geográfica, tendo o número de artigos com informação a "descoberto" aumentado ao longo do período, com um total de 68.000 endereços a serem revelados. Foi a área temática da Geografia que publicou mais de metade (57.9%) dos artigos com informação confidencial apresentada em mapas.

Se isto se passa a nível académico, já a título pessoal estamos constantemente a partilhar activa, ou passivamente, dados directos ou indirectos da nossa localização, na maioria dos casos graças a e através de *smartphones*, por via de vários tipos de aplicações. Para se controlar os dados de localização basta, em primeira instância, não os partilhar, ou só os partilhar com pessoas conhecidas, em circunstâncias específicas, verificando se o histórico de localizações do sistema está ligado ou não e apagando, eventualmente, os dados passados. Mas será que esta informação é assim tão diferente de outos tipos de informação que partilhamos?

Não propriamente, como Spangrud (2019) refere, "partilhar os nossos pensamentos, opiniões, sonhos, aparecimentos, ou o facto de que se gosta de ananás na pizza não nos impacta no mundo físico. […] Mas a localização importa. Se os detalhes de localização deixam de ser privados, qualquer ataque digital pode facilmente tornar-se físico. A IPL (Informação Pessoal de Localização) é cada vez mais regulada [legalmente], mas a localização é um factor chave da informação pessoal que ainda não é devidamente salvaguardado". Há muitas razões, nos dias de hoje, para partilharmos a nossa localização, sendo a maioria inofensiva a nível pessoal. No entanto, como a localização é persistente e pode ser relacionada com outros tipos de dados, pode-se saber muita informação sobre determinada pessoa.

Como se viu antes, os consumidores têm pouca protecção de privacidade por via da difusão de localização GPS dos seus *smartphones*, ou porque ela é automaticamente adicionada às suas fotografias digitais. Como sintetiza Schwartz (2012):

1. Electrónica de consumo guarda informação de localização – GPS, *geotagging* das fotos (EXIF);
2. Não há informação de partilha dos dados GPS aos consumidores, pelo sistema e/ou aplicações;

[45] https://en.wiktionary.org/w/index.php?title=geoprivacy&oldid=51797105

3. Os países têm abordagens diferente à privacidade de dados GPS, U.E, Artigo 29º declara que faz parte dos dados pessoais[46];
4. A FTC [47] tem instado o Congresso a proteger os dados GPS e outros dados móveis de localização;
5. Várias leis no Congresso dos E.U.A., para definir padrões claros para privacidade dos dados GPS;
6. Malware ligado a dados GPS, para aumentar a autenticidade dos *mails* de *phishing*[48] e outros;
7. Polícia pode ter acesso aos dados GPS de um *smartphone* e até activar o rastreio remotamente.

O problema é grande porque as pessoas estão, constantemente, a partilhar experiências de lugares com fotos que têm dados "embebidos" de localização, segundo Kiliç (2017), "a literatura académica sugere que os utilizadores de redes sociais estão preocupados com a privacidade da sua localização *online*, tendo também uma atitude cautelosa quanto a partilhar informação pessoal e de localização. No entanto, os utilizadores continuam a partilhar a sua informação de localização, a utilizadores amigos e serviços das aplicações, apesar das suas preocupações. Esta dicotomia entre preocupação e comportamento de divulgação é conhecida como paradoxo da privacidade".

O mesmo autor refere, nesse estudo, que o paradoxo da privacidade não se aplica a quem faz *geotagging* em redes sociais, pois raramente o fazem e quando fazem é em ocasiões especiais ou viagens. De 149 participantes, 37.6% assumiram que não faziam *geotagging* por precaução em partilhar informação de localização ou para permanecerem anónimos e 62.4% admitiram que o faziam nas redes sociais, utilizando pontos de interesse ou adicionado localização. Além disto, concluiu-se que os utilizadores não têm controlo sobre os dados de localização e seu fluxo, nem para que efeitos estão a ser utilizados, ou que terceiros têm acesso e estes dados pessoais, pois as "companhias ligadas às redes sociais são muito opacas quanto à monetarização que fazem dos dados" Kiliç (2017). Segundo o autor, o ideal seria as companhias tornarem clara a informação acerca de: (1) que informação de localização é recolhida, (2) como e onde é guardada e (3) que terceiros utilizam, processam e reutilizam esta informação.

A preocupação crescente com a privacidade dos dados pessoais, em geral, tem sido muito amplificada pelas fugas de informação relativas a espionagem maciça dos cidadãos, através de meios informáticos, de toda o tráfego da Internet e comunicações móveis (ver Taylor, 2019), ataques a dados, *ciberguerra*, entre outros, aos quais se junta muita paranóia e teorias da conspiração. O que é paradoxal, é que neste "caldo" de preocupação e dúvida, as pessoas são

[46] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en Declara que, entre outros, o endereço de email, os dados de localização, o endereço IP, a ID de um *cookie* são dados pessoais e estão protegidos. Claro está que, nos E.U.A., onde estas empresas (quase) todos têm sede, não…
[47] Federal Trade Commission dos E.U.A., organismo de protecção dos consumidores.
[48] *Phishing*, significa pesca, é uma forma de fraude electrónica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais (Wikipédia, 2019).

voluntariamente ignorantes, ou não têm cuidado nenhum com a informação que partilham, sobretudo dados de localização, mesmo que indirecta e passivamente, sobretudo através de redes sociais.

Segundo Armstrong, Tsou & Seidl (2018), a "geoprivacidade é uma «construção» relativamente nova, que surgiu com a emergência e confluência de novas tecnologias (SIG, GPS, *smartphones* e redes sociais) que são capazes de capturar e transformar informação acerca do movimento de indivíduos no espaço. […] A capacidade de utilizar mapas para construir interligações entre vários tipos de informação não é nova. O que mudou, dramaticamente, é a fluência (a facilidade e capacidade de realizar uma tarefa) e o fluxo (volume e fluxo de informações) que permitem realizar tais tarefas. […] Muitas pessoas com menos de 25 anos «nasceram digitais» e têm a sua localização controlada e seguida durante grande parte da sua vida. Efectivamente, nesta era de *Big Data*, a privacidade da localização talvez seja um ponto discutível". No artigo, os autores conseguem determinar o espaço de actividades de uma pessoa, construindo perfis de comportamento que detalham as deslocações para o trabalho e outras localizações, com base em dados partilhados, ver exemplo na Figura 12.

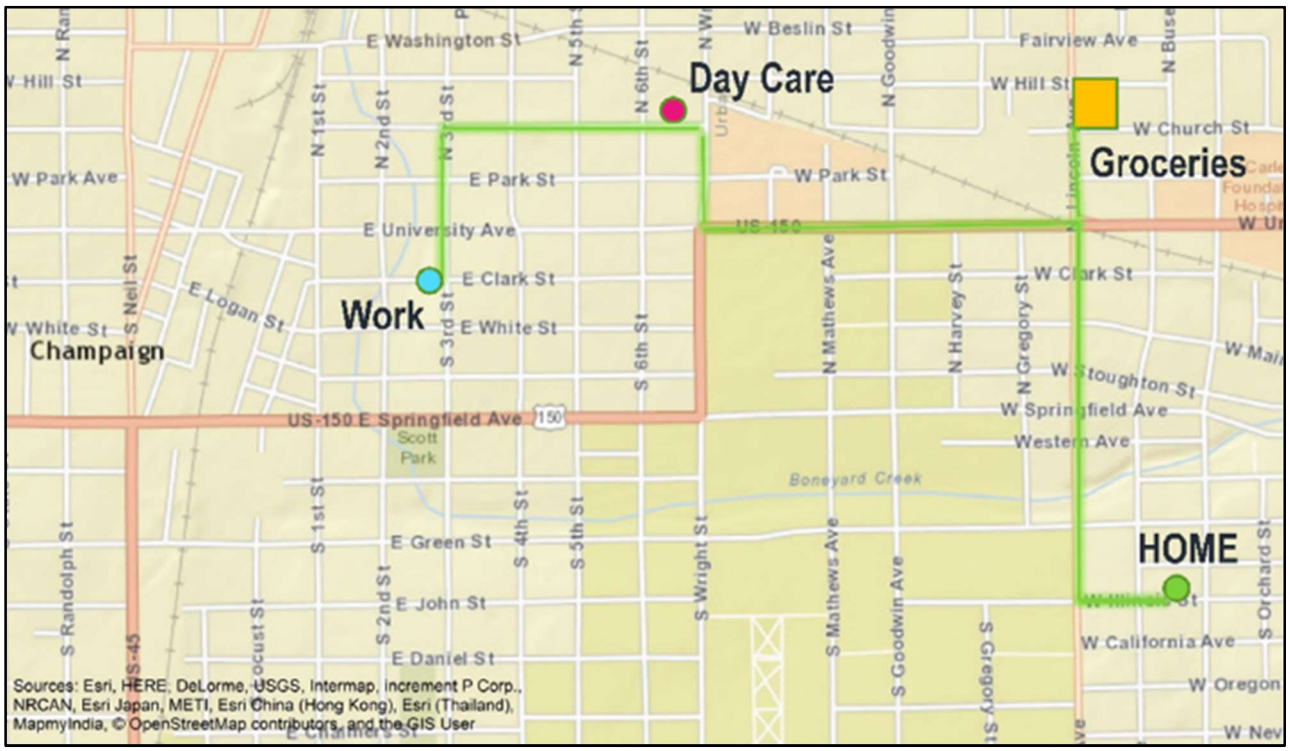


Figura 12 – Um exemplo de uma mapa de espaço de actividade que pode ser construído a partir de transacções de um *smartphone* e redes sociais (Armstrong, Tsou & Seidl, 2018).

Mas a geoprivacidade vai para além das coordenadas geográficas, o desejo de partilhar informação é tal, que muitos outros elementos da pegada digital que continuamente criamos, podem gerar informação que denuncia a localização de um utilizador, aquilo a que se chama

assinaturas semânticas e que são "minadas"[49] em milhões de *check-ins* geosociais (McKenzie, Janowicz & Seidl, 2016). Segundo os autores, quando se discute geoprivacidade, as pessoas pensam sobretudo em coordenadas e tecnologias de posicionamento, mas existem muito mais possibilidades de inferir a localização de um individuo e algumas, em termos de geoprivacidade, podem ser até mais reveladoras que as coordenadas geográficas por si só, são as "indicatividades":

1. Espaciais – e.g. Publicar que se está num restaurante Mexicano em determinado bairro;
2. Temporais – e.g. Indicar a hora a que se está num lugar, pode mostrar o tipo de lugar;
3. Temáticas – Palavras e linguagem utilizadas para falar das actividades, podem designar o lugar.

Além dos dados, directos e indirectos, relativos à localização de uma pessoa, que são recolhidos pelos *smartphones* ou partilhados voluntariamente, o problema está claramente do lado das aplicações, pois estas estão a reportar dados pessoais a terceiros, companhias que rastreiam os utilizadores, como a Google Analytics ou a Facebook Graph API. Uma aplicação não recolhe somente dados para utilizar no telefone propriamente dito, as aplicações de cartografia, por exemplo, enviam a informação para um servidor gerido pela empresa que desenvolve a aplicação para calcular direcções do local onde se está para um destino desejado.

Segundo Vallina-Rodriguez & Sundaresan (2017), 70% das aplicações que estudaram, têm ligação, pelo menos, a um *tracker* [rastreador] e 15 ligavam a cinco ou mais. Um em cada quatro *trackers* recolhia, pelo menos, um identificador do equipamento, tal como o número de telefone ou o IMEI[50] de 15 dígitos". Rastrear os utilizadores nos seus *smartphones* é só parte de um problema muito maior, pois "mais de metade das aplicações que fazem rastreio também seguem e registam a navegação dos utilizadores por sítios da Internet. Graças a esta técnica de rastreio cruzado, estes serviços podem construir um perfil muito mais completo da *persona online*". Segundo os mesmos autores e ainda mais perturbante, detectaram rastreadores em aplicações destinadas a crianças, tendo testado 111 aplicações, observaram que 11 recolhiam e transmitiam o endereço MAC[51] do *router WiFi* a que estavam ligados.

Existem efectivamente riscos, neste rastreio de dados de localização, embora grande parte deste dados seja "anonimizado" antes de ser guardado ou vendido, mas embora os dados possam parecer inócuos, basta um algoritmo para reconhecer padrões e combiná-los com outra informação dos utilizadores. Este facto torna-se particularmente alarmante quando se descobre, em detalhe, a forma como os dados são recolhidos e guardados: em 2011 os clientes de iPhones e

[49] *Data Mining* – o processo de descobrir padrões em grandes bases de dados (*Big Data*) envolvendo métodos na intersecção de *machine learning*, estatística e sistemas de bases de dados (Wikipédia, 2019).
[50] IMEI - International Mobile Equipment Identity, número de identificação global e único para cada telemóvel (Wikipédia, 2019).
[51] Ver nota de rodapé Nº 29.

iPads descobriram que a Apple estava a seguir os seus movimentos, há mais de um ano, tendo os ficheiros guardados perigosamente à vista de todos [52].

McIntosh (2017), dá vários exemplo dos riscos, para a privacidade, do rastreio de dados de localização:

1. **Dados de geolocalização, obrigatório para perseguidores** [*stalkers*] – Por vezes é difícil deixar de ser seguido por pessoas indesejáveis, más companhias, relações que deram para o torto, pessoas que não reconhecem que a sua atenção é indesejada, etc. Num inquérito realizado no Canadá em 2009, pelo organismo nacional de estatísticas, foram reportados 20.000 casos de *stalking*, 59 casos por 100.000 pessoas, mas convém lembrar que é uma estimativa baixa, pois segundo o mesmo estudo, somente três em cada dez pessoas contactaram a polícia. Pensemos, em Portugal, em todos os crimes contra mulheres, muitas delas escondidas e em casas abrigo, o assédio e perseguição que existem e o perigo que o acesso a dados de localização pode implicar, a todos os níveis, para estas pessoas;
2. **Ashley Madison 2.0[53] – A sua mulher sabe onde está?** – Recentemente houve um caso judicial em França contra a Uber, em que uma mulher "apanhou" o caso extraconjugal do marido, graças a um *bug*[54] no software, que enviava alertas e detalhes do transporte para o seu telefone. A Uber já tinha sido acusada, em 2014, de ter um modo que permitia seguir os utilizadores em tempo real, tendo empregados seus utilizado este serviço para seguir celebridades e antigas relações[55];
3. **Já se envolveram numa manifestação?** – As autoridades podem saber que esteve lá. Em 2016, a Geofeedia, uma plataforma que utilizava dados de redes sociais como o Facebook e Twitter, transformou os dados em controlo baseado na localização, dados que foram usados para seguir manifestantes em eventos, chegando a haver 500 forças da autoridade nos E.U.A. que utilizavam os seus dados para vigilância policial[56]. Posteriormente a Facebook, Instagram e Twitter bloquearam os acesso aos dados pela plataforma;
4. **Os patrões podem estar a vigiar** – Há muitos argumentos a favor e contra o controlo dos empregados, sobretudo com a facilidade e baixo custo das tecnologias actuais. Do ponto de

[52] https://www.wired.com/2011/04/iphone-tracks/

[53] Ashley Madison - era um sítio comercial que permitia aos utilizadores registados procurar, ter e gerir casos extraconjugais, tendo sido atacado e visto os dados de clientes expostos em Julho de 2015, 25 Gb de dados, com pormenores dos utilizadores e suas contas. Ashley Madison Data Breach - https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

[54] Bug de software – erro, falha ou defeito, num programa ou sistema de computador, que leva à produção de um resultado incorrecto ou inesperado (Wikipédia, 2019)

[55] https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/ ou https://www.cosmopolitan.com/lifestyle/a8495499/uber-using-god-view-tool-to-spy-on-celebs/

[56] https://slate.com/technology/2017/03/the-geofeedia-controversy-shows-why-social-networks-need-clearer-tos.html ou https://www.nbcnews.com/tech/internet/facebook-twitter-instagram-block-geofeedia-tool-used-police-surveillance-n664706

vista dos empregadores é valioso saber onde estão os empregados: gerir entregas, saber quando uma equipa chega a um lugar ou quem está mais próximo numa emergência, por exemplo em Portugal, em 2019, as chamadas para o 112 vão passar a ser georreferenciadas (com vantagens óbvias)[57]. Mas os empregados podem não ficar tão satisfeitos, o rastreio da localização erode a confiança e tudo se complica quando o rastreio continua para lá do dia de trabalho;

5. **Publicidade em localizações específicas** – Quando se vai a guiar numa estrada, ou andar numa rua, através do rastreio dos hábitos de navegação no *smartphone*, o equipamento "sabe" que se gosta de determinado produto, ou tipo de consumo a determinada hora (e.g. café, bolo, almoço), assim os anunciantes podem "bombardear" os consumidores com indicações de proximidade, para produtos ou serviços, basados na localização e/ou trajecto que se está fazer.

Depois de estes, poucos, exemplos e outros casos referidos antes, sabendo-me a "mecânica" de funcionamento e os dados disponíveis, percebe-se o leque de problemas potenciais com os dados e rastreio da geolocalização, contudo e só por si isto não uma coisa má. Há inúmeros impactos, altamente benéficos, do uso da tecnologia, "incluindo encontrar amigos quando se está em determinada área, design urbano baseado no movimento da população, ajudar as pessoas a encontra o caminho e chegar ao destino, entre outros. Um uso particular da geolocalização que pode salvar vidas vem dos sectores dos cuidados de saúde: aplicações como a PulsePoint[58], que liga pessoas que dominam a reanimação cardio-respiratória com vítimas próximas, em situação de paragem cardíaca. Contudo, deve depender sempre do utilizador escolher se quer partilhar a localização, ou escolher se está a ser rastreado e para que é que esses dados podem ser utilizados. Privacidade significa respeito pelo espaço e saber que, às vezes, mesmo quando não se sente que faça mal, se deve verificar antes de assumir que os utilizadores querem ser seguidos".

Será que é possível garantir a privacidade da informação, a geoprivacidade num mundo de redes sociais? Embora a privacidade da localização seja um conceito pouco claro, ele pode ser definida, como "a capacidade de impedir outrem de conhecer a nossa posição actual ou passada, ou, a capacidade de um individuo se deslocar no espaço público com a espectativa de que, sob condições normais, a sua localização não será, sistemática e secretamente registada para uso posterior (Kar & Ghose, 2014). Os mesmos autores citam várias definições de privacidade pessoal: "a qualidade ou estado de se estar à parte de companhia ou observação, ou, liberdade de intrusão indesejada, ou ainda, o direito a estar sozinho".

No caso Português, a Constituição da República, nos Direitos, Liberdades e Garantias, consagra no Artigo 26º - Outros direitos pessoais[59]:

[57] https://24.sapo.pt/atualidade/artigos/chamadas-para-o-112-vai-ser-mais-facil-localizar-pedidos-de-ajuda-e-cidadaos-surdos-terao-uma-aplicacao-propria
[58] https://www.pulsepoint.org/
[59] https://dre.pt/web/guest/legislacao-consolidada/-/lc/337/201904191549/127985/diploma/indice

1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.

2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.

O Regulamento Geral de Protecção de dados (RGPD[60]), que será abordado posteriormente, no âmbito de outras questões ligadas à geoprivacidade, especificamente as legais, específica, no seu Capítulo I -Disposições Gerais, Artigo 4ª – Definições[61]:

1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

Legalmente parece claro, em termos de privacidade no sentido mais lato, que a privacidade é um direito fundamental, que os dados pessoais fazem parte dessa privacidade e que os dados relativos à localização fazem parte dos dados pessoais. Contudo, a ubiquidade das tecnologias permitidas pela geolocalização, a partilha crescente da nossa localização, com cada vez mais serviços externos, levam a uma preocupação crescente na sociedade, onde a maior parte desconhece o funcionamento das tecnologias e o uso que é feito dos dados, que é difícil de enquadrar em termos legais, sobretudo quando as principais empresas que recolhem, guardam, processam e vendem esses dados estão "algures", geográfica e juridicamente.

[60] https://protecao-dados.pt/o-regulamento/
[61] https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf

A geoprivacidade, para ser devidamente enquadrada e perspectivada, deve ser vista de uma forma multifacetada, tecnológica, ética, legal e educativa. Keßler & McKenzie (2017) construíram um manifesto pela geoprivacidade, com esta abordagem, baseado em 21 teses, que sumarizam um conjunto de argumentos, partindo de que "a informação relativa à localização é diferente dos outros tipos de informação pessoal, em combinação, que a geoprivacidade deve ser protegida e não ser uma mera ilusão. [...] As perspectivas tecnológica e ética têm de ser combinadas e integradas, com os aspectos educacionais e legais deste problema, que diz respeito a quase todos os indivíduos na mundo desenvolvido".

O documento é muito extenso e denso, baseado num casal ficcional, para dar exemplos positivos e negativos, neste contexto vai-se tentar sintetizar e resumir as 21 teses apresentadas:

Espacial é especial

1. A informação sobre a localização de um individuo é substancialmente diferente de outros tipos de informação identificável pessoalmente – A questão central é o controlo pessoal da informação de localização, como, quando e até que ponto se quer comunicá-la a outrem.

Acesso à informação de localização

2. A ubiquidade de dispositivos de localização e facilidade de uso das API's[62] tornam a informação sobre as pessoas muito mais fácil de capturar que outros tipos de informação identificável – Acesso à informação de localização. Em 2015 68% dos adultos em países desenvolvidos tinham *smartphone*s, 54% em países emergentes/em desenvolvimento, juntando *wearables* (monitores de actividade física, *smartwatches*[63], relógios desportivos), pode-se afirmar que há milhares de milhões de dispositivos no mundo, que estão quase sempre com os donos, junta-se *WiFi* ou *Bluetooth*, o que aumenta, ainda mais a população rastreada, isto para não referir a *IoT*. Os navegadores da Internet, através de HTML5, Java e outros *scripts* também determinam a localização do utilizador. O desenvolvimento de software e hardware torna, portanto, fácil, barata e absolutamente generalizada, a recolha de dados de localização, mais do que outros tipos de dados sobre os utilizadores (na sua pegada digital).

Utilidade da informação de localização

3. Os utilizadores de serviços de informação têm um incentivo substancial a partilharem a sua localizam, com quem providencia o serviço, pois a informação de localização pode melhorar

[62] API *Application Programming Interface* - conjunto de rotinas e padrões estabelecidos pelo software para a utilização das suas funcionalidades por aplicações que não pretendem envolver-se em detalhes da implementação do software, mas apenas usar os seus serviços (Wikipédia, 2019).

[63] *Smartwatch* - relógio de pulso computadorizado com funcionalidades que vão além de mostrar as horas, com frequência comparado com os assistentes digitais pessoais (PDA). Enquanto os primeiro modelos podem somente executar tarefas simples, como cálculos, tradução e jogar videojogos, os relógios inteligentes modernos são efectivamente computadores "vestíveis" [*wearables*] (Wikipédia, 2019). Por exemplo: https://www.wareable.com/smartwatches ou https://www.techradar.com/news/wearables/best-smart-watches-what-s-the-best-wearable-tech-for-you-1154074

significativamente a qualidade do serviço e torná-lo mais útil – Muitos dos produtos ou serviços que procurarmos estão ligados à nossa localização;

4. Os utilizadores partilham, frequentemente, a sua localização sem o saberem – Já foram dados muitos exemplos, sobretudo a nível de aplicações, algumas coercivamente e sem necessidade aparente de conhecerem a localização do utilizador.

Deduções baseadas na localização

5. Ter acesso ao histórico de localização do utilizador, permite um vasto campo de deduções baseadas na localização, tal como informação sobre a saúde, comportamento de consumo ou estatuto social – Deduções baseadas na localização. Sobretudo durante longos períodos;
6. Deduções baseadas na localização podem revelar informação que o utilizador nunca pretendeu, ou autorizou partilhar com um serviço – Pode-se ser rico vivendo num bairro pobre, ter saúde sem nunca ir a um ginásio, a forma como a informação é trabalhada e reconstruída, as deduções são quase adivinhas;
7. Deduções incorrectas baseadas na localização podem ter efeitos adversos severos - Em casos extremos pode estender-se a utilizadores que nem usam serviços de localização, basta o endereço IP do equipamento com que se acede à Internet.

Valor económico da informação de localização

A perspectiva das empresas

8. Conhecer a localização de um cliente é um activo económico para um negócio – É o núcleo do negócio da Google ou Facebook, dado o seu sucesso fica claro o valor, embora seja difícil de o quantificar.

A perspectiva do utilizador

9. Os utilizadores valorizam a sua própria informação de localização com base no nível de detalhe e casos de utilização – Têm consciência do seu valor, de que pode ser usada contra si, pois muitos recusam partilhá-la.

Um mercado Emergente

10. Está a emergir actualmente um novo mercado no qual as empresas e utilizadores trocam informação de localização de nível pessoal – Um exemplo são as companhias de seguros venderem apólices, com base nos GPS que os clientes instalam nos carros, para traçar o perfil de condução dos mesmo, só pagando o tempo e distância que guiam (incentivo);
11. Descontos para clientes que concordam em partilhar a sua localização com uma empresa, o que está efectivamente a penalizar os que se recusam a fazê-lo e que pode erodir o princípio da solidariedade e segurança colectiva.

Salvaguarda da geoprivacidade

Recolha e tratamento de dados que respeita a privacidade

12. Preservar a geoprivacidade envolve mais do que ofuscar as coordenadas geográficas. A localização pode ser deduzida de informação não explicita geograficamente, tal como interesses, actividades ou dados sociodemográficos – O tipo de linguagem, interesses, parte da pegada digital.

Avaliar a geoprivacidade

13. Quaisquer serviços, com base na localização, oferecidos ao utilizador são limitados pela quantidade de informação que este está disposto a partilhar – O conceito é graduado, depende de uma análise custo-benefício, entre a utilidade do serviço prestado e o grau de intrusão, ver Figura 13.

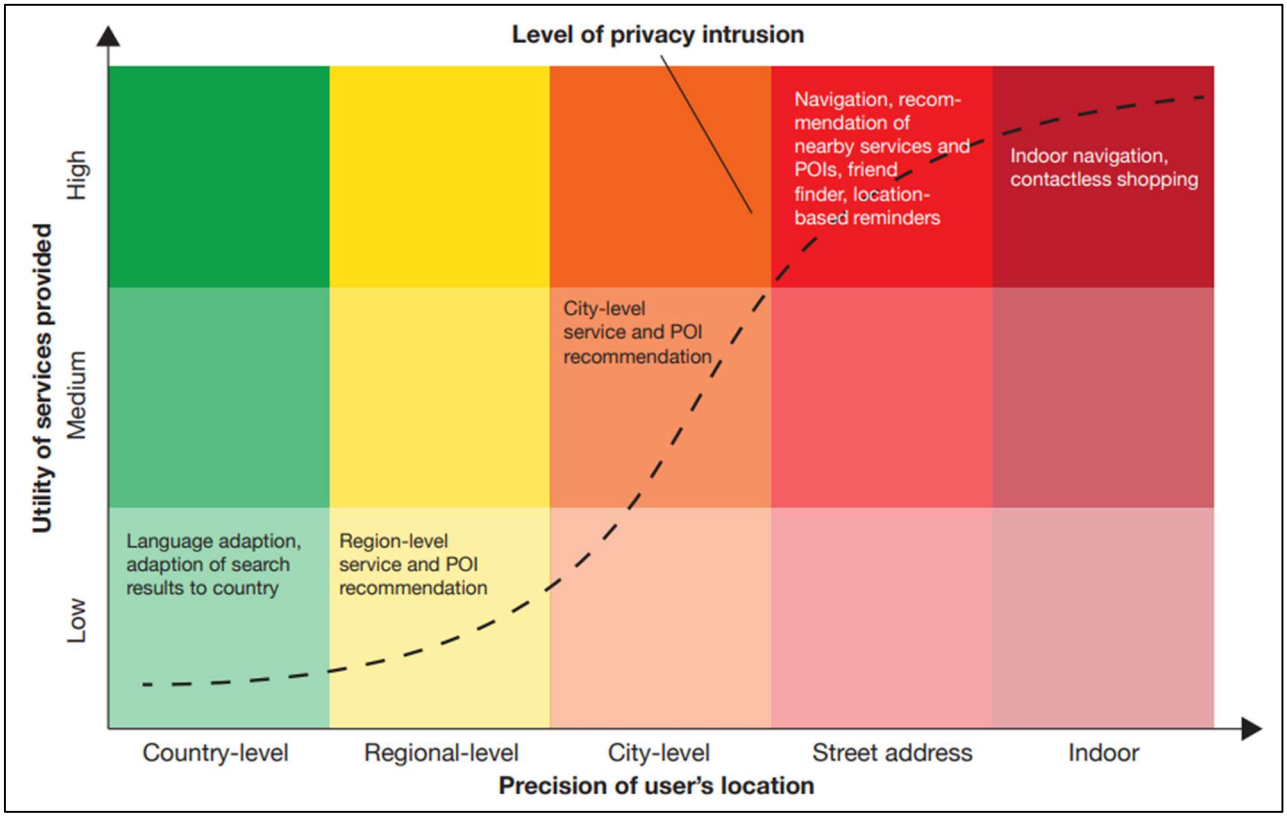


Figura 13 – O serviços mais úteis, baseados na localização, dependem do conhecimento da localização precisa do utilizador. Quanto mais útil o serviço, mais severa é a intrusão na geoprivacidade do utilizador (Keßler & McKenzie, 2017, p. 12).

14. Os mecanismos de controlo, dos sistemas de operação móveis, têm falta de mecanismos de controlo de grão fino, limitando assim grandemente o grau de controlo que os utilizadores podem ter sobre a sua informação de localização – Autorização de partilha de localização com as aplicações, é feita aplicação a aplicação? Pode-se, pura e simplesmente, desligar? Para todas? Mesmo quando é necessário?
15. O grau de geoprivacidade de um individuo não pode ser avaliado de uma forma fiável, porque é impossível saber a que informação auxiliar uma terceira parte tem acesso.

Aspectos legais e éticos

16. As ramificações éticas dos avanços na tecnologia activada pela localização são frequentemente vistas como uma reflexão tardia e os aspectos e preocupações legais em relação à privacidade ficam para trás, em relação aos avanços tecnológicos;

17. A geoprivacidade como tópico de investigação situa-se no campo de tensão entre aspectos tecnológicos, éticos, económicos, legais e educativos que, até agora, só têm sido abordados separadamente – Falta uma abordagem holística.

Geoprivacidade como um campo de tensão

"Olhando para a Figura 14, pode-se ter ideia dos principais aspectos que afectam a privacidade de um utilizador, no centro estão o utilizador e as **ferramentas** com que interage, tais como as aplicações móveis e monitores de actividade. Estão ligados através da **utilidade** oferecida pela ferramenta, que o utilizador procura. Para se alavancar esta utilidade, o utilizador necessita de fornecer a sua **localização** com uma determinada **precisão**, onde a própria utilidade depende dessa mesma precisão" (Keßler & McKenzie, 2017, p. 15).

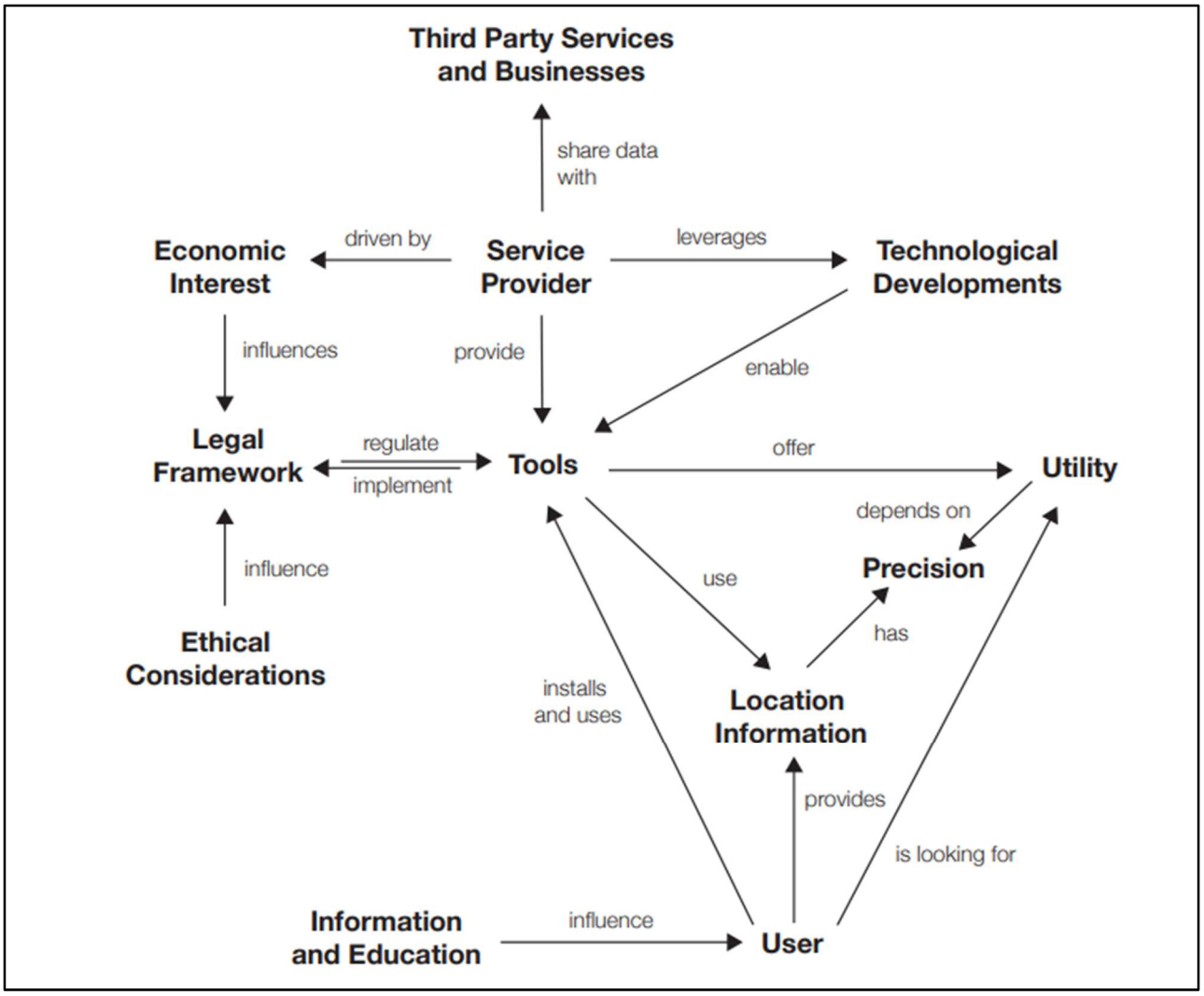


Figura 14 – A geoprivacidade é influenciada por um número de aspectos diferentes, criando um campo de tensão que torna difícil abordá-la como um todo (Keßler & McKenzie, 2017, p. 16).

18. Os utilizadores não têm forma de verificar se os serviços, "conscientes" da localização e equipamentos que a usam, actuam dentro do quadro ético e legal e estão de acordo com a descrição aceite de política de privacidade – Este facto depende, muito, da educação e informação que o utilizador possui;
19. Um nível elevado de educação do utilizador, na área de rastreio de posição e serviços baseados em localização é requerida para se poder tomar decisões mais informadas sobre as ferramentas e serviços que se está a utilizar – A maioria das pessoas não sabe (imagina?) como está constantemente a ser seguida, ou pode sê-lo, com relativa facilidade, mesmo que não queira;
20. Uma base de utilizadores mais educada, pode fazer pressão para uma legislação mais restritiva e forçar os fornecedores de serviços a serem mais transparentes, acerca das suas políticas de recolha e utilização de dados.

Conclusões

21. A vigilância constante da localização dos cidadãos pode ser utilizada como uma ferramenta para a opressão e para limitar a liberdade de expressão, mesmo em democracias – Pensemos nas inúmeras aplicações para seguir constante os filhos (crianças ou não), por mais boa intenção que tenham, às que permitem seguir os empregados, na facilidade de saber quem esteve em protesto e manifestações, a encontrar-se com pessoas perseguidas em regimes ditatoriais. Mesmo em países democráticos, estar no sítio errado à hora errada pode ter efeitos nefastos.

Depois de apresentar este conjunto de teses, que não devem dispensar uma leitura completa do artigo de onde foram retiradas, caso ainda não se tivesse tornado claro, penso que não restam muitas dúvidas quanto à importância vital da questão da geoprivacidade. Como os autores referem no final, "Embora estas não sejam, de forma alguma, novas observações, ainda não há uma ampla discussão, quanto mais consenso, na sociedade, acerca de que usos da informação de localização são aceitáveis e onde está a linha vermelha que não deve ser ultrapassada. Áreas como a saúde, ou a finança, já estão a ver regulações mais rigorosas, em relação à utilização de IIP [Informação de Identificação Pessoal] e, ainda mais importante, têm aumentado a consciência quotidiana dos utilizadores. Tópicos que só tinham interesse para especialistas de segurança, tais como a autenticação de dois factores ou encriptação de ponta-a-ponta, são agora discutidas nos *media* convencionais. Esperamos que este texto contribua para este debate, bem como para a manifestação do direito à privacidade (da localização) como uma conquista da civilização moderna e não só um mero ponto na história humana" (Keßler & McKenzie, 2017, p. 18-19).

Depois da definição, justificação e estruturação da questão da geoprivacidade e apresentação de um manifesto em sua defesa, seria interessante apresentar exemplos de vantagens da utilização da geolocalização, interesse didáctico, pedagógico, plástico, mas também perigos e, sobretudo, casos em que a revelação deste dados criou ou podia ter criado sérios problemas.

Geolocalização, exemplos e casos…

Provavelmente muitos utilizadores de *smartphones* nem se apercebem, mas muitas das aplicações que todos os dias utilizam dependem da geolocalização, ou fornecem serviços relacionados com ela, sinteticamente e para se ter uma ideia dos grandes grupos (até porque seria impossível e indesejável tentar ser mais exaustivo):

1. **Navegação e mapas** – Google Maps e Earth, Bing Maps, Waze, OsmAnd, HERE WeGo Maps;
2. **Encontrar amigos e família** – Glympse, Find my friends, Family Locator, GeoZilla, MeetMe, MyKids;
3. **Astronomia** – Skymap, SkyEye, Skyview, StarChart, StarTracker, Mobile Observatory;
4. **Meteorologia** – WindGuru, Windfinder, Windy, MeteoEARTH, AccuWeather, Weather Channel;
5. **Jogos** – Pokemon GO, Landlord, Geocaching, Ingress, Zombies: Run;
6. **Fitness** – Movescount, Strava, Endomondo, Fitbit, Nike+, Mapmyfitness, MyTracks;
7. **Viagens e comida** – Uber, Cabify, AirBNB, Booking, Trip Advisor, Yelp, Zomato, Foursquare;
8. **Redes Sociais** – Facebook, Twitter, Snapchat, Instagram (Geotag), Flickr (Geotag);
9. **"Encontros"** – Tinder, Grindr, Happn, OkCupid, MeetMoi, Nearify.

Muitas destas aplicações, além de dependerem da geolocalização também produzem muita informação, como já discutido, que pode ou não ser recolhida e/ou tratada e/ou passada a terceiros. Talvez as mais conhecidas são as ligadas ao *Fitness* e a outros desportos ao ar livre, que registam o movimento dos utilizadores, seja exclusivamente com o *smartphone*, seja com pulseiras, relógios ou GPS. Várias marcas destes equipamentos disponibilizam, *online*, *heat maps*[64] com os dados que foram carregados para a nuvem, o que, como se verá a seguir, já criou sérios problemas de segurança e privacidade. Este tipo de cartografia, além de ter interesse plástico, didáctico e geográfico, permite análises *Big Data* impossíveis de realizar doutra forma. Pode ver-se nas Figuras 15 e 16 exemplos da Strava e Garmin, que podem ser explorados e com elevado grau de interactividade, óptimos, portanto, para utilizar no âmbito no ensino da Geografia.

Claro está que, quem partilha, sempre voluntariamente, este tipo de informação está a abdicar da sua geoprivacidade e a aumentar a sua pegada digital, não é difícil compreender alguns dos géneros de riscos associados a este tipo de informação, sobretudo depois dos vários aspectos debatidos até aqui. Claro está que, algumas pessoas, utilizam estas funcionalidades para se divertirem, transmitir mensagens, ou criar "arte", ver Figura 17, até existem *online* artigos sobre como fazer e aprimorar esta possibilidade[65].

[64] *Heat Maps* – Representação gráfica de dados, em que os valores individuais contidos numa matriz são representados como cores, variando as tonalidades em função da densidade ou valor absoluto (Wikipédia, 2019)

[65] https://www.outsideonline.com/1978066/how-make-gps-art ou https://www.buzzfeed.com/robinedds/things-you-can-draw-using-gps-that-will-make-excercising ou

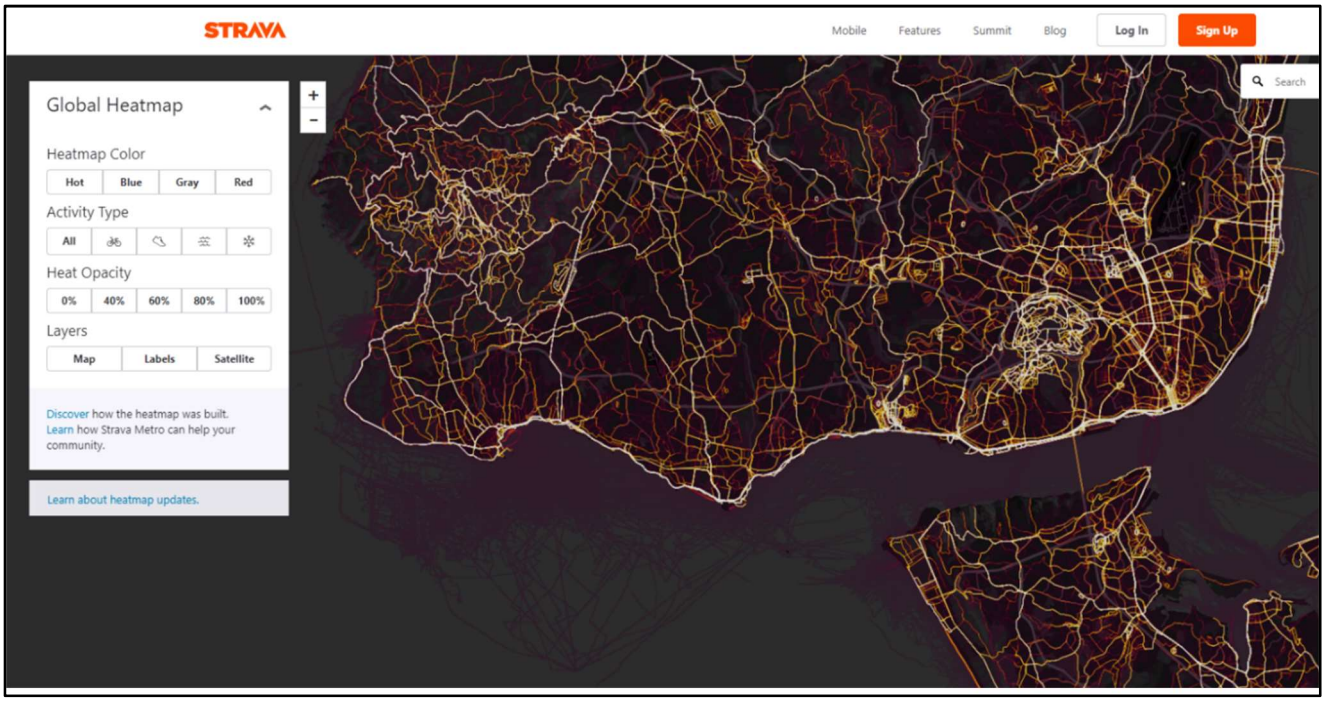


Figura 15 – *Heat Map* da Strava, para vários tipos de actividades físicas, o tom dos traçados varia consoante a quantidade de trajectos registados, site da Strava[66].

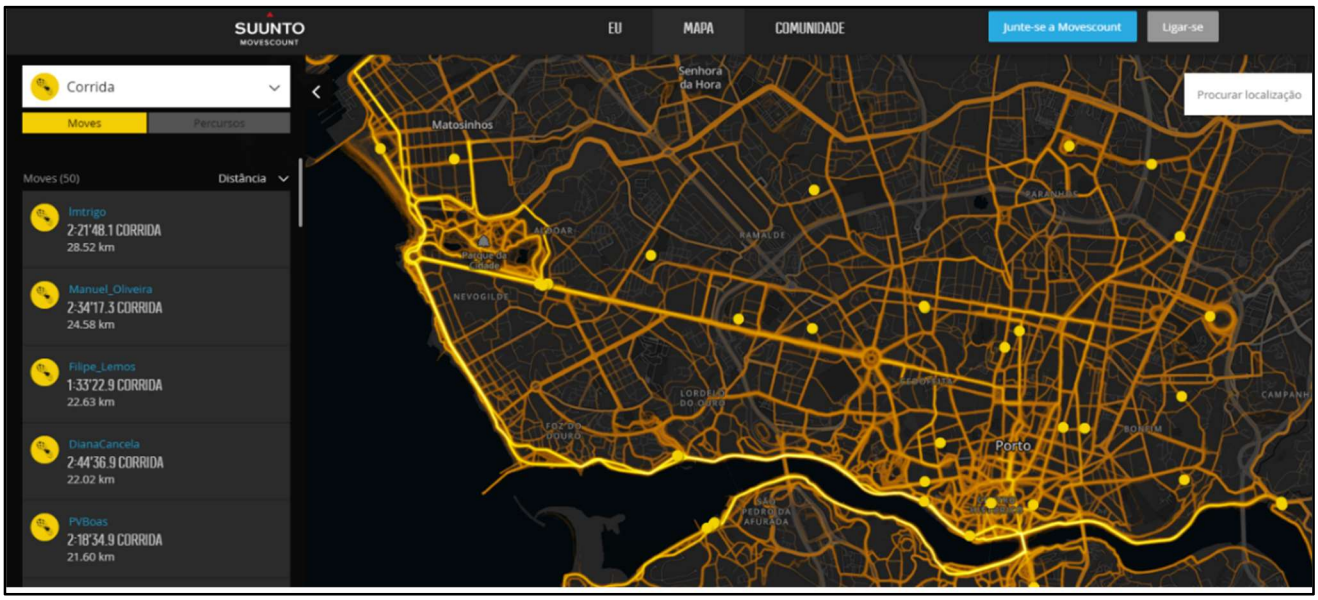


Figura 16 – *Heat Map* da aplicação Movescount da Suunto [67].

https://www.boredpanda.com/bike-gps-doodle-stephen-lund/?utm_source=duckduckgo&utm_medium=referral&utm_campaign=organic

[66] https://www.strava.com/heatmap#11.50/-9.31959/38.75346/hot/all

[67] http://www.movescount.com/pt/map?lat=41.16071061691093&lon=-8.658200128441706&zoom=13.623714515318 48&activity=3&heatmap=true&style=suunto-dark

Figura 17 – *Figure Running*, novo "desporto" que encoraja os corredores a serem criativos[68].

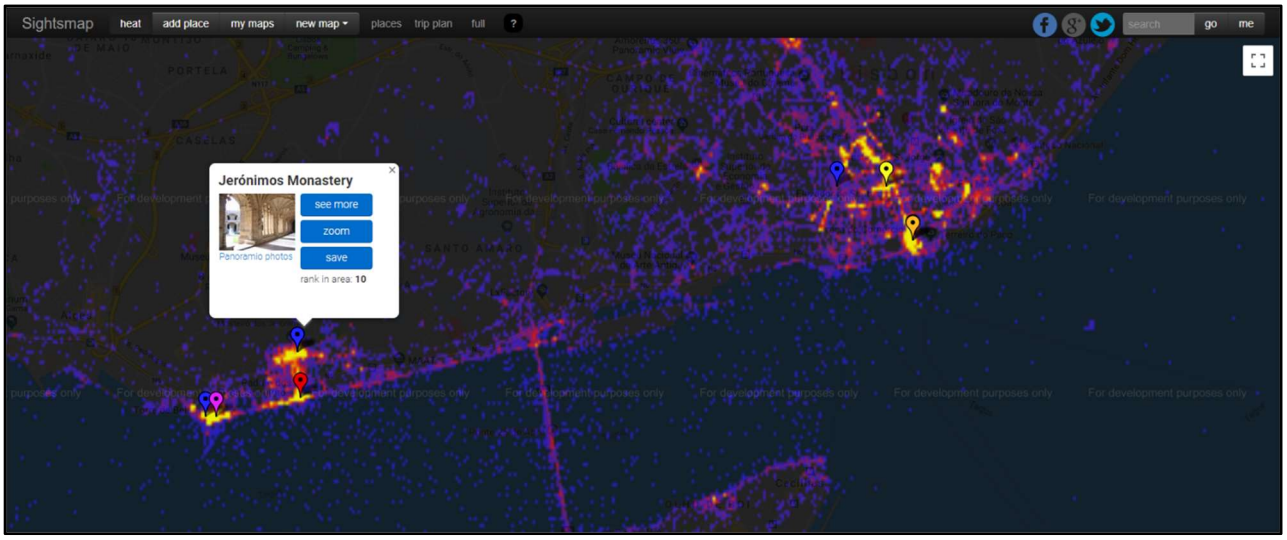


Figura 18 – Heat *Map* com os locais de que as pessoas mais gostam, em todo o mundo, com base no número de fotografias Panoramio, quanto mais vermelho e depois amarelo, mais imagens existem[69].

[68] https://blog.adafruit.com/2016/12/27/create-gps-art-with-these-apps/
[69] http://www.sightsmap.com/#

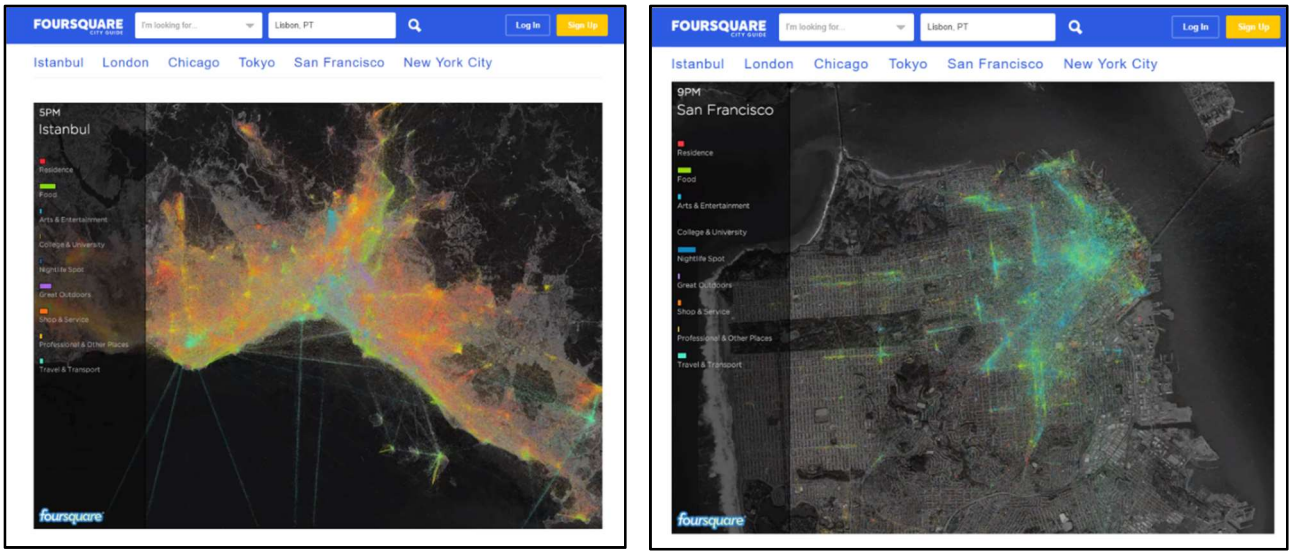


Figura 19 – Heat *Map* Foursauqre, ao longo do dia (vídeo), para várias actividades em várias cidades do Mundo[70].

As variantes são numerosas, como os utilizadores partilham muitas fotos de comida, localizando-as, também se pode ver quais as "comidas mais comidas" nas cidades do mundo (Capitais da Comida no Instagram, Ver Figura 20), ou o índice de felicidade gay mundial, com base na Rede Planet Romeo[71], ver Figura 21.

Figura 20 – Capitais da Comida no Instagram, por tipos de comida[72].

70 https://foursquare.com/infographics/pulse
71 https://classic.planetromeo.com/
72 https://cewe-photoworld.com/instagram-food-capitals/

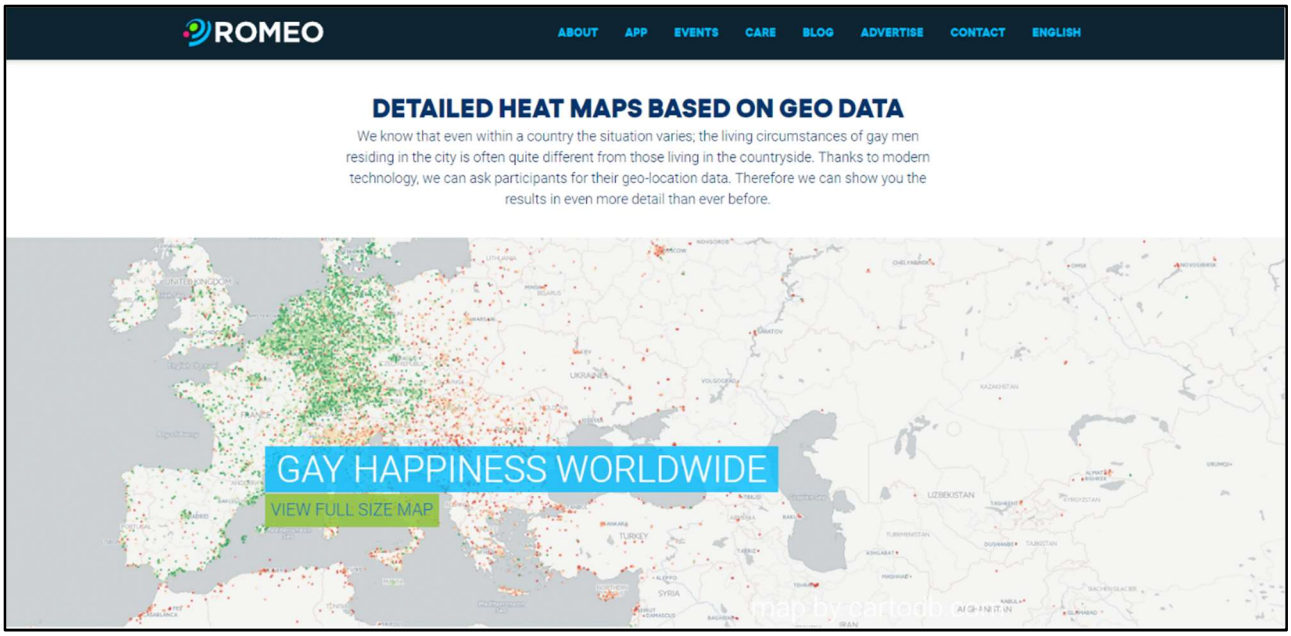


Figura 21 – Mapa da Felicidade Gay no mundo[73].

Outra utilização interessante dos dados geolocalizados, neste caso do Twitter, permitiu construir uma "geografia do ódio" nos E.U.A., com base no estudo de mensagens de ódio, postadas na rede social, divididas em categorias: racistas, homofóbicas, contra deficientes e deficiências, etc. podendo-se procurar, também, por palavras chave contidas nos *tweets* (Bean, 2013). As manchas no mapa interactivo, ver Figura 22, dão uma gradação de maior ou menor discurso de ódio, em função da localização dos *smartphones* utilizados para fazer os *tweets*.

Uma utilização comum dos dados de geolocalização, que se pressupõe seja feita dentro dos limites da lei e por razões de segurança para as pessoas e para o estado, é a realizada por forças da autoridade. Os dados de localização e seu histórico, que a Google mantém (potencialmente) em todos os dispositivos Android, as pesquisas feitas ou a previsão meteorológica local têm ajudado a resolver crimes e a encontrar dispositivos perto de cenas do crime (Khandelwal, 2019). Não só ajuda a localizar quem utilizava o *smartphone*, como pode identificar todos os dispositivos que passaram pelo local em determinada janela temporal, a base de dados onde está a informação é conhecida, internamente, por *Sensor Vault*, com registos de centenas de milhões de telefones em todo o mundo (Nieva, 2019). Graças aos dados pode-se definir o "espaço de actividade" de suspeitos (Schmitz, P. & Cooper, A. 2019), ou estudar *gangs* e o seu relacionamento em redes sociais (Ferrara, E., De Meo, P., Catanese, S. & Fiumara, G., 2014).

O objectivo desta base de dados é recolher informação para melhor direccionamento de anúncios, mas a pegada digital registada é muito mais vasta, podendo fornecer inúmeros

[73] https://www.planetromeo.com/en/care/gay-happiness-index/

elementos às investigações policiais, incluindo o histórico de localização (para quem o tem ligado). Esta utilização tem levantado frequentes, contantes e recentes questões de legalidade, uma das quais é a violação de privacidade de pessoas inocentes, muitas vezes somente porque estavam "perto" de acontecimentos, tornando-se essa informação "circunstancial", no caso de processos.

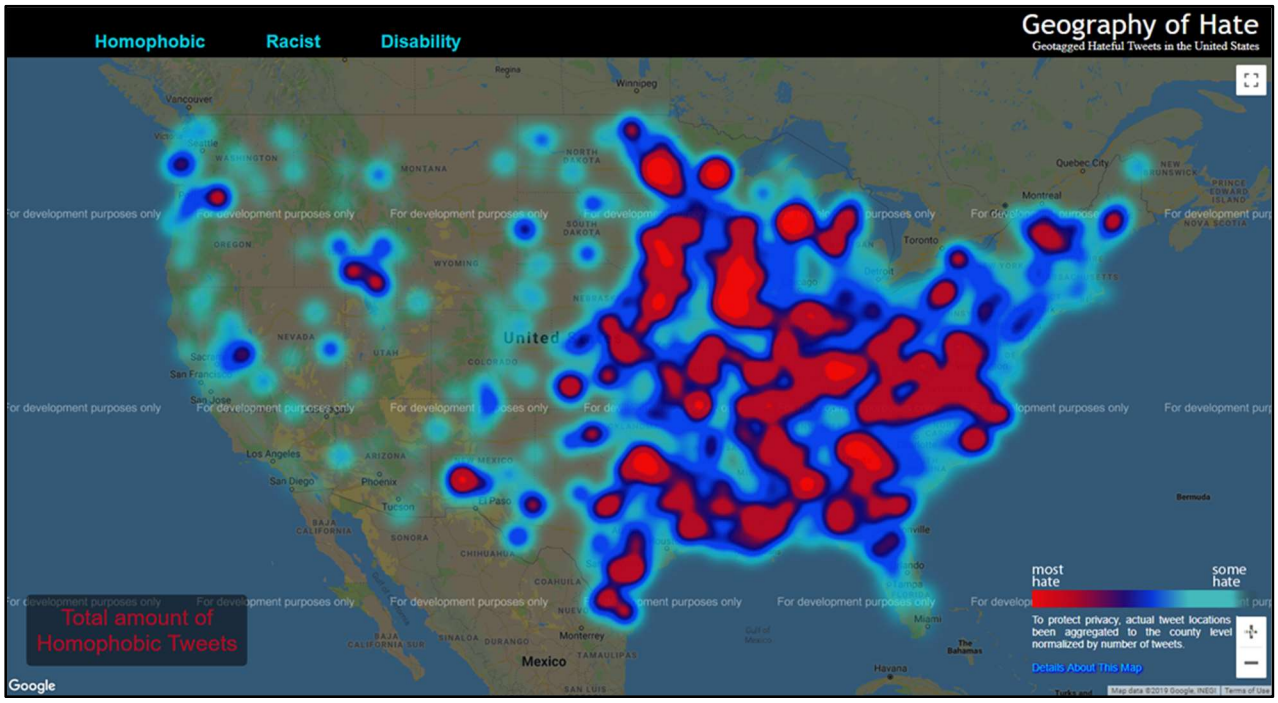


Figura 22 – Mapa da localização de *tweets* de ódio, nos E.U.A., em função da localização[74].

Em áreas do mundo menos desenvolvidas, onde os direitos são menores e os perigos maiores, em estados frágeis e áreas de conflito, estas tecnologias ajudam a salvar pessoas, como no Uganda, onde este tipo de dados foi utilizado para prever onde a guerrilha poderia atacar, ajudando a salvar vidas (Henley, 2013).

Uma utilização ligada à criminalidade, é a cartografia de crime em tempo mais-ou-menos real, com base nos dados de geolocalização: ver Figura 23 *Crime Reports* para o Norte de Miami, ou os mapas gerados pela aplicação *Safe and the City*, utilizada por mulheres para reportar e denunciar assédio, piropos ou crimes na via pública, ver Figura 24. No entanto, estas aplicações podem alimentar uma falsa percepção das taxas de crime, ao contrário dos dados reais, pois alimentam o medo, tornando muito mais visível este tipo de informação e levando à sua partilha, em esquema tipo rede social (Molla, 2019).

Há, também, a possibilidade de utilizando métodos de análise de *Big Data*, separar as fotografias ou *tweets* feitos pelas população local dos turistas, com base na informação dos *smartphones* e

[74] https://users.humboldt.edu/mstephens/hate/hate_map.html#

dados de geolocalização, o que permite visualizações muito interessantes e didácticas, sobretudo a nível das diferentes percepções dos distintos grupos, além de destacar as áreas mais relevantes e "interessantes" geograficamente para esses grupos, ver Figura 25 (dados de imagens no Flickr) e Figura 26 (dados do Twitter).

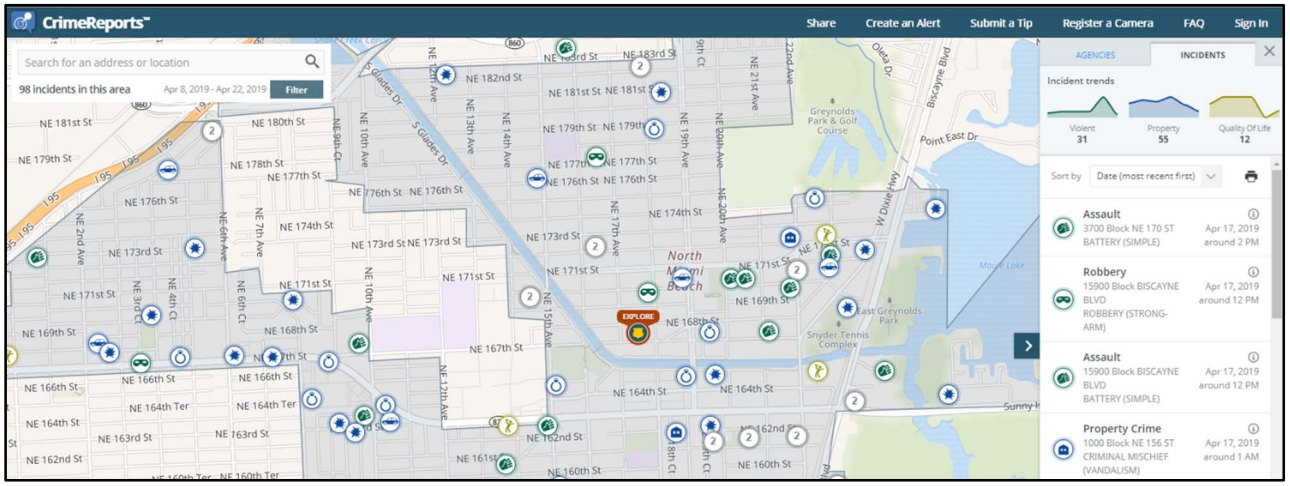


Figura 23 – Mapa de ocorrências criminais, Norte de Miami, Crime Reports [75].

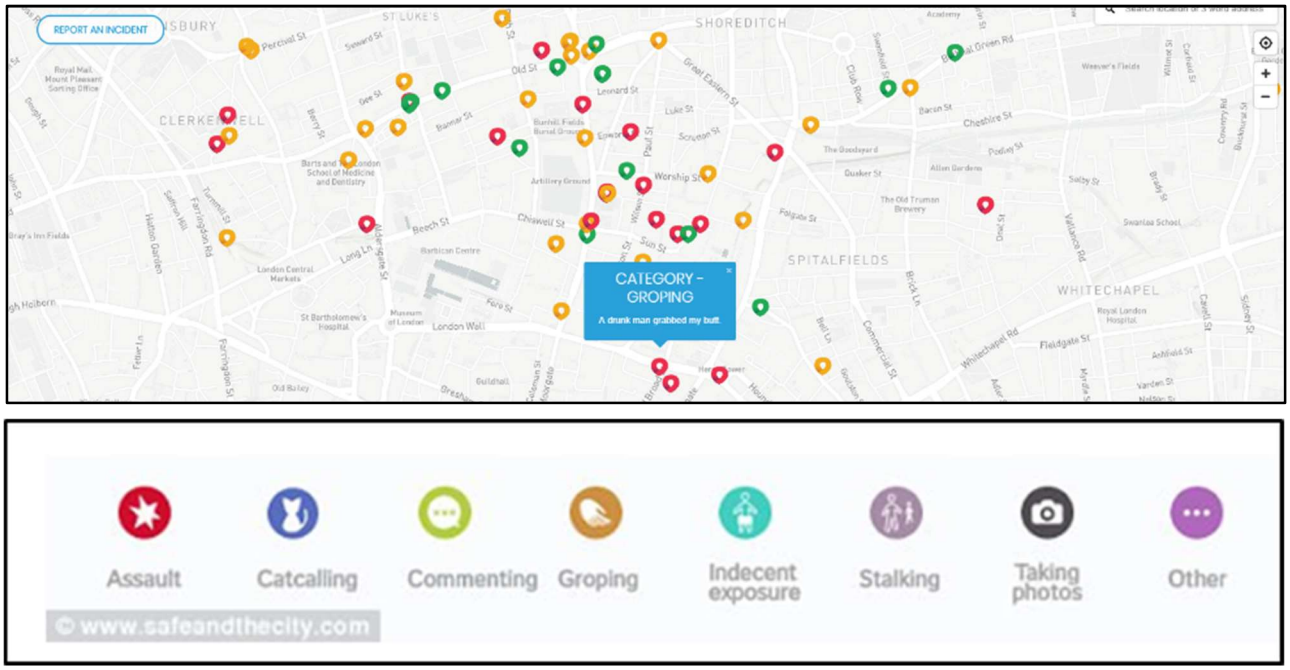


Figura 24 – Mapa da aplicação Safe and the City[76].

[75] https://www.crimereports.com/
[76] https://www.safeandthecity.com/

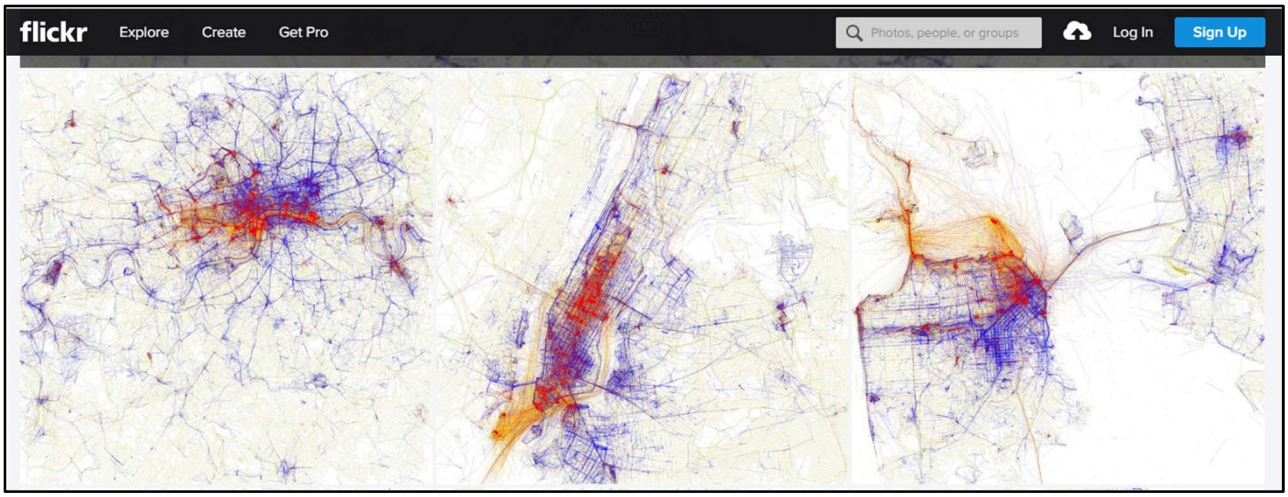


Figura 25 – Fotografias carregadas para o Flickr, por "locais" (azul) e turistas (laranja), há muitas cidades para explorar neste sítio[77].

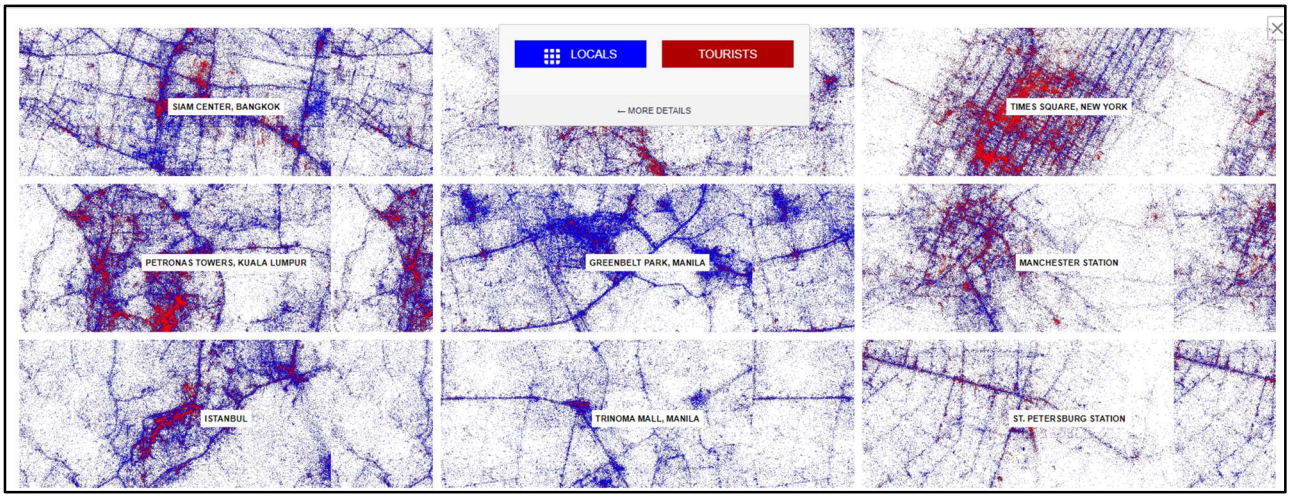


Figura 26 – Mapas dos *tweets* "postados" por "locais" (azul) e por turistas (vermelho), pode-se explorar o mundo ou por cidade[78].

Para terminar, num tom um pouco mais ligeiro: cartografar os gostos musicais nos E.U.A., para os 50 artistas mais populares, com base nas visualizações do YouTube (Katz, 2017), entre Janeiro de 2016 e Abril de 2917, que independentemente da plataforma em que são feitas, são geolocalizadas (Figura 27), tal como as categorias mais procuradas por países, no Pornhub em 2018, (Figura 28). Não é só saber-se tudo o que estamos a fazer, é a partir de onde está a ser feito…

[77] https://www.flickr.com/photos/walkingsf/sets/72157624209158632/detail/
[78] https://labs.mapbox.com/labs/twitter-gnip/locals/#2/-12.2/-271.1

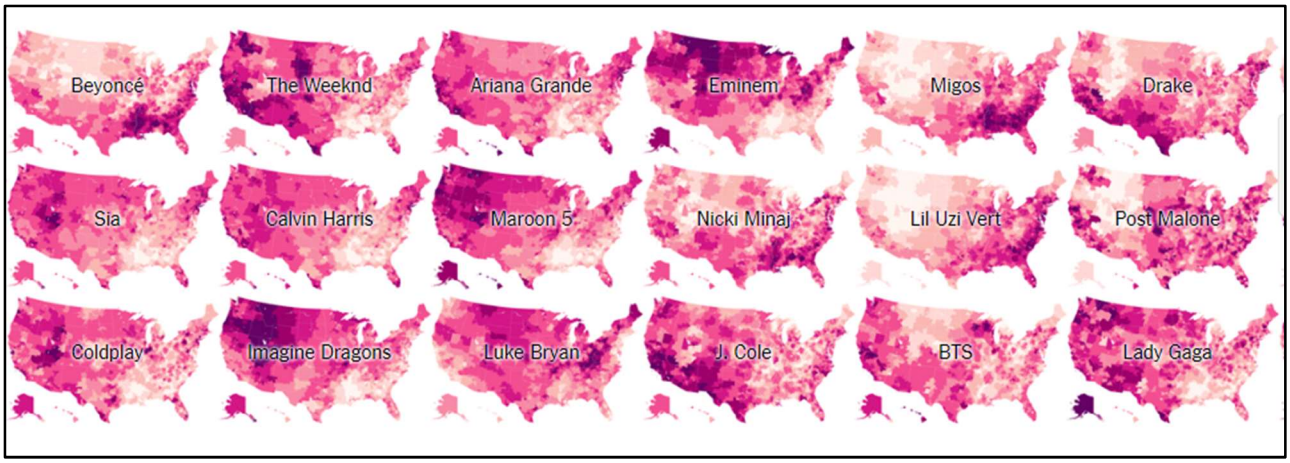


Figura 27 – Visualizações no YouTube dos principais artistas musicais, em função da localização, entre Janeiro de 2016 e Abril de 2017[79].

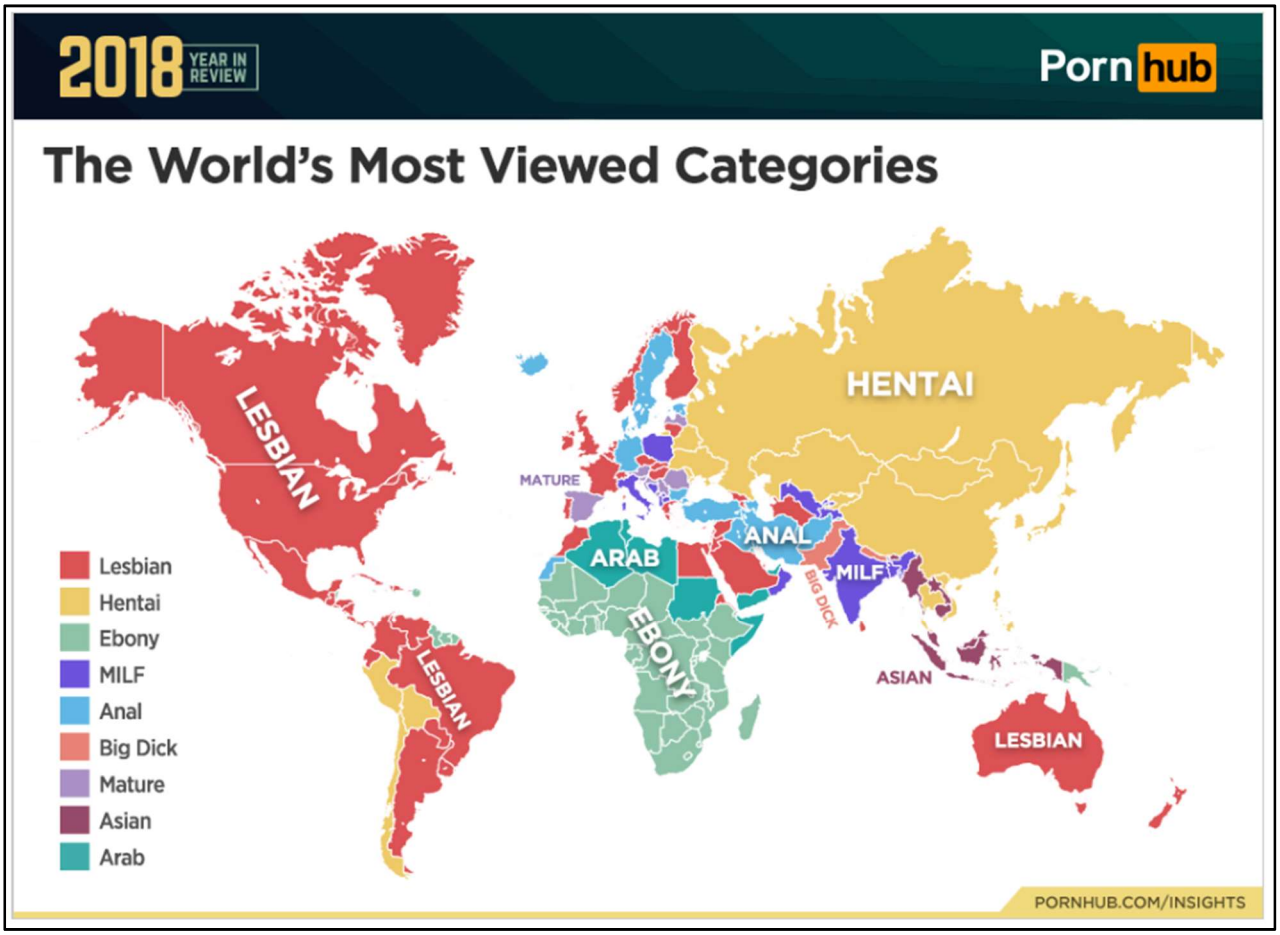


Figura 28 – Categorias mais procuradas, por países, no Pornhub em 2018[80].

[79] https://www.nytimes.com/interactive/2017/08/07/upshot/music-fandom-maps.html
[80] https://www.pornhub.com/insights/2018-year-in-review#searches

Existem exemplos doutros géneros, mas os apresentados têm interesse para serem explorados, a nível pessoal, como material didáctico e no contexto de sala de aula, razão pela qual foram escolhidos, ficando muito para explorar por cada um, mas também para não sobrecarregar visualmente. Convém apresentar mais alguns exemplos, não tão visuais, mas muito interessantes, um deles prende-se com um sistema de moradas global, para resolver um problema complicado, sobretudo em países menos desenvolvidos, falta pura e simples de moradas postais, o que dificulta o contacto com as pessoas, seja postal, pessoal, de emergência ou outro (Adam, 2018).

Apesar de toda a cartografia que existe, muitas áreas não estão cobertas, algumas moradas têm séculos e outras podem ter dias, sobretudo em meios urbanos caóticos, com construção precária e de crescimento explosivo. Este sistema dividiu todo o planeta numa quadricula de 3 X 3 metros, tendo cada quadrícula como referência um conjunto de três palavras únicas, assim qualquer pessoa pode encontrar qualquer localização ou partilhá-la, podendo o serviço ser utilizado com uma aplicação para *smartphone*, mapa *online*, incluída noutra aplicação ou sítio na Internet, chama-se What 3 Words[81] e tem um enorme sucesso fora do mundo "mais desenvolvido", mas com limitações nesse, onde os endereços existentes representam uma hierarquia (Melon, 2019).

Actualmente existem inúmeras aplicações para *smartphones* que permitem rastrear a localização de crianças[82], animais de estimação (que têm de ter localizador), família[83] mas cada vez mais, em virtude do envelhecimento da população e consequente declínio cognitivo e demência, torna-se importante poder localizar pessoas nessas circunstâncias, pois não só se perdem como podem nem saber quem são. Há soluções para *smartphones*, tanto para uso das famílias, como das entidades médicas ou autoridades, embora as ideais sejam dispositivos embebidos na roupa (e.g. sapatos) (Schofield, 2017). Existem tecnologias semelhantes para limitar os movimentos a condenados (i.e., a chamada pulseira electrónica[84]) ou para encontra telefones dentro de prisões[85].

Mas há outro tipo de aspectos, ligados à geolocalização, que interessam à Geografia e às pessoas, um deles é o facto de ela permitir a democratização dos mapas, que sempre foram documentos importantíssimos. Com a tecnologia actual, podemos saber onde estamos em qualquer lugar do mundo, graças aos *smartphones*, podendo conceber e criar os nossos próprios mapas. Segundo Unidad Editorial (2019), "deixou de haver um mapa que explica tudo, cada um concebe o seu próprio mapa de acordo com as suas necessidade. [...] Os sistemas de geoposicionamento funcionam nos dois sentidos. Primeiro consumimos informação geolocalizadas, seguidamente

[81] https://what3words.com/
[82] Por exemplo, Finda my Kids, com perto de 4 milhões de downloads: https://findmykids.org/en/ ou Family GPS tracker KidsControl: https://kid-control.com/
[83] Family Locator https://www.life360.com/ ou https://www.sygic.com/family-locator
[84] https://accidentshappenatty.com/ankle-bracelets-work/
[85] https://www.telegraph.co.uk/news/2019/04/20/heat-technology-prisons-trace-illicit-mobile-phones-precise/

produzimos essa informação. A maior mudança é que passámos a ser *adprosumers*[86]. […] Antes a produção de informação geográfica dependia daqueles que controlavam a tecnologia e o seu conhecimento. Hoje, qualquer um pode fazer um mapa [discutível…], é aquilo a que se chama a neogeografia, significa democratizar os mapas e deitar abaixo não só as fronteiras físicas como mentais".

A geolocalização também pode transformar o design urbano, pois o software que trabalha com esses dados pode analisar o crescimento da cidade de uma forma inovadora e abrir novas possibilidades (Marinova, 2019). Também pode ajudar os gestores dessas cidades, pois extraindo os dados de *posts* de redes sociais várias, bem como outro conteúdo escrito, pode-se saber do que os cidadãos estão a falar, o que estão a ver e a visitar, equipamentos que estão a utilizar em cada bairro ou unidade administrativa, o que permite criara *heat maps* (Jefroykin, 2018), ver Figura 29. Isto possibilita compreender as necessidades dos cidadãos, de acordo com o "onde", de uma forma por vezes muito detalhada espacialmente, o que permite incorporar informação na comunicação por parte de quem gere, promovendo um debate muito mais rico, pois permite compreender muito melhor os cidadãos e responder às suas necessidades da melhor forma possível.

Figura 29 – *Heat map* dos tópicos através da cidade, utilizando a geolocalização de tópicos vários, obtidos a partir de *posts* de redes sociais (Jefroykin, 2018).

Neste contexto, não posso deixar de referir uma série de trabalhos nesta área, desenvolvidos por uma empresa criada, entre outros, por um ex-aluno de Geografia da NOVA FCSH, Miguel Marques, a Mapidea, que tem desenvolvido em Portugal trabalho de análise de dados de Geolocalização e *Big Data*, os vídeos são muito interessantes e elucidativos.[87]

[86] *Adprosumers* – cliente com funções de comprador que participa activamente na promoção e recomendação de um produto. (https://www.foromarketing.com/diccionario/adprosumer/)
[87] https://mapidea.com/videos/

Por último, a geolocalização e os seus dados, que são informações essenciais para direccionar a publicidade e promover formas espacializadas de marketing está, também, ela própria, a transformar totalmente o marketing. Conforme as marcas vão descobrindo o poder dos dados GPS e da realidade aumentada graças a eles (*vide* Pokemon Go), estão também a encontrar novas formas de chegar aos consumidores. Interessa-lhes, não só, saber onde está o consumidor, mas também onde está a sua atenção, sendo que a tecnologia está a tornar isso possível (Kulkarni, 2017).

Segundo o mesmo autor, "cada anunciante sabe onde os consumidores estão, através da forma como os seus dispositivos [*smartphones*] traduzem isso em coordenadas geográficas" e por alguma razão o maior negócio ligado à pegada digital é o marketing e publicidade. Por isso, há 15 formas pelas quais a geolocalização está a mudar totalmente o marketing:

1. Eventos de realidade aumentada [88] - Baseiam-se em dados de geolocalização para manipular a realidade física, os publicitários podem conceber experiências virtuais em torno de marcas ou produtos;
2. Publicidade aumentada – Alargar os limites da publicidade, tecnologia de realidade aumentada pode ser utilizada para realçar a experiência de visão, quando um anúncio aparece em determinado local ou evento;
3. Agrupamento focal – Os anunciantes estão a competir para saber que anúncios estão a atrair a atenção, porquê e que tipo de consumidores. O agrupamento focal pode dar essa informação em muito mais detalhe que antes, graças a dados recolhidos por geolocalização nos *smartphones* e tecnologia *wearable*, podendo identificar muito mais do que a localização física do consumidor, pois permite saber para onde o consumidor está a olhar;
4. Ofertas baseadas na localização vão transformar-se com a análise preditiva – Embora ofertas baseadas na localização não sejam novidade, a inteligência artificial e análise preditiva vão levar a personalização a outro nível, permitindo providenciar ofertas "mesmo a tempo", sensíveis ao contexto, a qualquer pessoa com um *smartphone*. Pode-se enviar uma oferta antes de a pessoa sair de casa ou com base na rotina diária, ou semanal;
5. Novas experiências de visualização para o consumidor – Há tecnologias que permitem aos utilizadores terem múltiplas perspectivas de espectáculos ao vivo, podendo, por exemplo,

[88] Realidade aumentada - integração de elementos, ou informações virtuais em visualizações do mundo real, através de uma câmara e com o uso de sensores de movimento como o giroscópio e acelerómetro. O uso mais popular da realidade aumentada é o entretenimento através dos filtros para fotos em aplicações móveis de redes sociais e jogos como o *Pokemon Go*, porém actualmente a realidade aumentada é utilizada de muitas formas tais como no ensino, design de produtos, acções de marketing ou em treino e suporte em unidades industriais. O uso de vídeos transmitidos ao vivo digitalmente, processados e "ampliados" pela adição de gráficos criados pelo computador, também pode ser considerado como um tipo de realidade aumentada (Wikipédia, 2019).

apontar o dispositivo móvel a um ponto e receber, em *streaming*[89], imagem a partir dessa perspectiva, permitindo controlar a experiência de visionamento de formas até agora impossíveis;

6. Utilizando a geolocalização o comércio electrónico vai poder levar o tráfego até lojas físicas – Os vendedores a retalho estão a lutar para se manterem competitivos no meio da ameaça do comércio electrónico, utilizando a geolocalização podem levar as pessoas até à sua "montra";
7. Os influenciadores digitais serão activados com base na localização – Até à data, os maiores esforços de influência de marketing, a grande escala, aconteceram a nível nacional, o que dificulta a vida aos retalhistas locais. Utilizando a geolocalização os anunciantes podem perfeitamente activar influenciadores locais, permitindo-lhes alinhar com personalidades dos *media* sociais que podem inspirar acção em audiências locais;
8. As balizas [beacons] vão tornar-se comuns – As balizas, que são pequenos sensores colocadas nas áreas de retalho, podem dar às lojas uma imagem detalhada de como os consumidores fazem compras, rastreando o seu movimento, passos e paragens. Podem saber onde na loja as pessoas estão a cada momento, permitindo aos anunciantes "empurrar" mensagens e ofertas, enquanto fornecem dados acerca do comportamento dos consumidores;
9. Marketing de eventos vai melhorar – Qualquer pessoa com experiência de marketing de eventos sabe que levar as pessoas aos eventos é muito mais difícil do que parece, é expectável ver empresas a utilizar a geolocalização, como os anúncios direccionados do Facebook, informando os clientes quando localizações próximas vão ter eventos especiais e fazendo ofertas para os fazerem atravessar as portas;
10. Marketing local limitado por tempo para aumentar as vendas – Vai haver negócios a atrair clientes, nas proximidades, através de marketing temporal limitado, cupões especiais so disponíveis numa janela temporal;
11. Controlo de tendências por *drone*[90] - Tecnologia para compreender e estudar multidões, forma como se deslocam e comportam no espaço, sobretudo em áreas comerciais, para melhor gerir esse espaço e direccionar determinados tipos de anúncios;
12. Incentivar a recolha de dados – As marcas há muito que compreendem como é importante a informação acerca de consumo das pessoas em todos os aspectos do marketing, mas os consumidores não abrem mão da sua privacidade facilmente. Utilizando transacções especiais e regalias de filiação, em conjunto com dados de geolocalização, isso permitirá melhorar muito a recolha local de informações, versão melhorada de cartão cliente com muitos metadados;

[89] *Streaming* - Transmissão contínua, também conhecida por fluxo de média, é uma forma de distribuição digital, em oposição à descarga de dados. A difusão de dados, geralmente numa rede através de pacotes, é frequentemente utilizada para distribuir conteúdo multimédia através da Internet (Wikipédia, 2019).
[90] *Drone* - Veículo aéreo não tripulado (VANT) ou drone (do Inglês, zangão), é todo e qualquer tipo de aeronave que pode ser controlada nos três eixos, não necessitando de pilotos embarcados para ser guiada. Estes tipos de aeronaves são controlados à distância por meios electrónicos e informáticos, sob a supervisão de humanos, ou mesmo sem a sua intervenção, por meio de Controladores Lógicos Programáveis (CLP) (Wikipédia, 2019).

13. Check-In instantâneo – Check-ins são uma ferramenta de marketing muito importante, mas os clientes são relutantes em fazê-lo, pois acrescenta mais um passo à sua experiência, mas se esse check-in estiver incorporado em aplicações de compras, melhora a experiência do consumidor e ganham-se dados valiosos dos seus hábitos de consumo;
14. *Geofencing* – Perímetro virtual de uma área, cria uma zona à volta de um negócio para direccionamento de publicidade, por exemplo um cliente pode estar a ler um artigo no telefone, na fila para pagar, recebendo um anúncio direccionado da loja ou empresa ao lado, pois está nessa zona de *Geofencing*;
15. Publicidade baseada na localização de previsões meteorológicas – Com base nos dados meteorológicos, para anunciar produtos específicos, em função do estado de tempo que os consumidores têm na sua localização, e.g. dia de calor, porque não entra para um refresco, ou comprar um chapéu, ou protector solar.

Foram até este ponto e neste bloco apresentados exemplos e casos ligados aos dados de geolocalização, todos eles com interesses vários, inovadores, globalmente positivos, ou relevantes para a sociedade e indivíduos, mas há um lado negro da geolocalização, fuga e roubo de dados, bem como consequências nefastas e, até, perigosas, ligado a essa informação e aos dispositivos que utilizamos quotidianamente, como extensão de nós próprios e com os quais criamos uma enorme pegada digital. Um exemplo disso é o próprio *smartphone* "alimentar uma relação abusiva" (Pequenino, 2019e). Segundo a autora, num artigo sobre violência doméstica, estes equipamentos são regularmente utilizados para monitorizar a localização de companheiros ou ex-companheiros, para ler mensagens, para seguir os relacionamentos nas redes sociais, triando a pegada digital.

Nesse artigo, a autora revela, a propósito de histórias de violência doméstica que chegam à APAV (Associação Portuguesa de Apoio à Vítima[91]), que "Há pessoas que contactam a associação com receios de estarem a ser espiadas pelos companheiros ou ex-companheiros através do telemóvel ou de outros dispositivos electrónicos. Por vezes, são as próprias vítimas (alvo de pressão psicológica) que divulgam as palavras-passe ou pins dos seus equipamentos. Em algumas histórias, como a de Maria, há telemóveis escondidos nos carros das pessoas, para as monitorizar, seguindo-as com a função de GPS. Outras vezes são usados programas informáticos – que custam algumas dezenas

[91] **Serviços telefónicos de apoio a vítimas de violência doméstica**

APAV - Linha de Apoio à Vítima - 116 006 (dias úteis das 9h às 21h)
apav.sede@apav.pt / https://apav.pt/apav_v3/index.php/pt/contactos

CIG - Comissão para Igualdade de Género - 800 202 148 (24 horas por dia) - Serviços de apoio em qualquer ponto do país em http://www.guiaderecursosvd.cig.gov.pt

Associação de Mulheres Contra a Violência (AMCV) - 21 3802160 / sede@amcv.org.pt

de euros por mês – para espiar à distância". Refere ainda que a preocupação é internacional, por exemplo, na Austrália em 85% dos casos era utilizado um telemóvel para seguir e espiar pessoas que se queixaram, nos E.U.A. 72% dos que contactaram a rede de apoio à violência doméstica, referem que estão a ser perseguidos através de uma aplicação móvel ou GPS".

Existem aplicações e programas para espiar as pessoas (*stalkerware e spyware*), que segundo a autora são fáceis e baratos de arranjar, muitos estão disponíveis nas Lojas *online* da Google e Apple, permitindo interceptar mensagens, dar informação GPS em tempo real, recolher histórico de navegação na Internet, activar a câmara ou o microfone. Claro está que este tipo de soluções existe, também, para controlar trabalhadores e crianças, mas as consequências mais trágicas estão relacionadas com a violência doméstica e de género. Basta ter acesso à conta Google de uma pessoa com quem se tem, ou teve, um relacionamento, para poder activar a localização e seguir todo o histórico na linha cronológica. A autora lembra que "além de crimes de violência doméstica, os agressores também estão a cometer crimes informáticos. É sempre aconselhável a denúncia destas situações à unidade de Cibercrime da Polícia Judiciária. […] Se existem fortes indícios que algum dispositivo está comprometido, a vítima deve arranjar um segundo telemóvel «limpo», de modo a que possa contactar as autoridades e essa conversa não seja interceptada".

Num ano em que, até ao dia 7 de Março (2019) já tinham sido mortas 12 mulheres[92], em que muito se discute a forma como os jovens se relacionam, a pegada digital e vida *online* acaba, infelizmente, por ser um elemento central. Segundo Gomes (2019), "A ameaça via telemóvel (com mensagens como "eu sei onde estás e quero explicações, ou nas redes sociais preocupa", embora a principal forma de violência seja psicológica, passa muito por controlar o que o outro faz *online*, com quem comunica, por onde anda, sendo também as ameaças, vingança e pressão feitas *online*. Segundo um estudo da UMAR (União de Mulheres Alternativas e Resposta), feito a 4600 jovens, referido por Branco (2018): 18% foram vítimas de violência psicológica, 12% de violência através das redes sociais, onde o comportamento violento mais frequente é entrar na conta sem autorização (20%), partilhar conteúdos íntimos sem autorização (4%) ou proibição de falar com amigos (21%). Portanto e infelizmente, a pegada digital é usada para controlar e para agredir, não respeitando a privacidade (geoprivacidade incluída).

Existem mesmo aplicações, concebidas e usadas, para controlar as mulheres, duas irmãs da Arábia Saudita, que fugiram do país, estão a pedir à Google e Apple que retirem uma aplicação, "desumana, que permite aos homens controlar e verificar as viagens de familiares femininos, pois ajudar a aprisionar raparigas em famílias abusivas. […] Dá os homens controlo sobre as mulheres, tem de ser retirada [das lojas *online* Google e Apple]" (Bacchi, 2019). Esta aplicação, Absher[93],

[92] https://www.jn.pt/justica/interior/-ja-morreram-12-mulheres-vitimas-de-violencia-domestica-em-2019-10653066.html
[93] https://play.google.com/store/apps/details?id=sa.gov.moi&hl=en

permite utilizar inúmeros serviços governamentais na Arábia Saudita (informação de passaportes, autorizações de viagem, reportar crimes, concorrer a empregos, licenças e documentação variada), mas na prática permite controlar as mulheres, no sistema de tutela masculina do país – "em novilíngua do reino, permite aos guardiões monitorizar as suas protegidas" (Shifter, 2019). As duas empresas comprometeram-se a analisar a questão, mas, entretanto, a Google já disse que não vai retirar a aplicação[94].

Num registo diferente, relacionado com a geoprivacidade, houve um caso muito falado recentemente (2018), em que o carácter público dos *heat maps* da Strava (ver Figura 15) levantou sérias questões de segurança a forças militares e da ordem, ao permitir identificar instalações militares, bases secretas ou áreas sensíveis, bem como os trajectos, dentro e fora desses perímetros feitos pelo seu pessoal. Quando investigadores e jornalistas começaram a analisar os mapas, partilhados por utilizadores de dispositivos de *Fitness*, conseguiram relacionar bases militares dos E.U.A. no Google Earth, com a actividade de utilizadores: bases militares no Afeganistão (Figura 30), patrulhas militares Turcas na Síria (Figura 31), uma base militar Francesa no Níger Figura 32), uma base militar no Djibouti (Figura 33) e até locais "negros" da C.I.A. (Hsu, 2018). Embora algumas já fossem conhecidas, outras não eram identificáveis directamente no Google Earth e punham, sobretudo, a segurança do pessoal aí destacado, operações civis e militares, de Ocidentais, em países em desenvolvimento.

Figura 30 - 31 – *Heat map* Strava e bases "secretas", à esquerda Kabul, Afeganistão[95], à direita patrulhas Turcas em Manbij, na Síria[96].

[94] https://www.thisisinsider.com/absher-google-refuses-to-remove-saudi-govt-app-that-tracks-women-2019-3
[95] https://dabrownstein.com/2018/02/05/national-security-and-personal-bests/
[96] https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1#a-french-military-base-in-niger-8

Figura 32 - 33 – *Heat map* Strava, à esquerda base Francesa no Níger, Madama (Brown, 2019)[97], à direita base militar dos E.U.A. no Djibouti e possível área "negra" da C.I.A. (Brownstein, 2018)[98].

A Strava defendeu-se dizendo que se pode desligar o registo ou não fazer *upload*, que os dados não eram em tempo real, mas sim padrões de actividade acumulada entre 2015 e Setembro de 2017 (Sly, 2018). Os dados estavam longe de ser, exclusivamente, de forças ocidentais, havendo registo de actividades de Russos, Turcos ou Chineses, que também usam dispositivos como Fitbit, Garmin ou Polar, referindo a Strava que o *Heat Map* global tinha 13 biliões de pontos, sendo que a Strava é só uma de centenas de aplicações e dispositivos quer tornam fácil expor esta vulnerabilidade, "poeira digital" (Seldin, 2018).

Muito rapidamente, o Departamento de Defesa dos E.U.A. baniu o uso de possibilidades de geolocalização, em dispositivos deste género, pelo seu pessoal destacado em certas localizações, pois não só os dados ajudam a reconstituir o "desenho" das instalações, linhas de abastecimento, rotas de patrulha e infra-estrutura interior, como sobretudo permitir compreender como as bases funcionam (McLaughlin, 2018). Nalguns casos, tornou-se possível perceber que havia uma base ou actividades, sem qualquer elemento que o pudesse fazer prever, observando e analisando o Google Earth (Figura 34).

A lista de dispositivos proibidos, em áreas operacionais, incluiu dispositivos de rastreio de *Fitness*, *smartphones*, *tablets*, *smartwatches* e todas as aplicações e software relacionado, segundo um Memorando do Departamento de Defesa (Department of Defense, 2018). Claro que as próprias Forças Militares consideram estes dispositivos populares e úteis, tendo até feito um projecto piloto em 2013, com 2200 soldados, usando rastreadores de *Fitness* como parte de uma campanha de bem-estar e saúde, para controlar quotidianamente o exercício que faziam, as calorias queimadas, distâncias percorridas e padrões de sono (Ward, 2018).

[97] https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1#a-french-military-base-in-niger-8
[98] https://dabrownstein.com/2018/02/05/national-security-and-personal-bests/

Figura 34 – *Heat map* Strava, base Sarrin, a Sul de Kobane na Síria, sem que a base fosse perceptível em imagens de satélite[99].

Houve problemas semelhantes, artigos e impacto na opinião pública, no Reino Unido, onde se conseguiu não só ver os trajectos que as pessoas faziam nas bases e à sua volta, neste caso a base de submarinos nucleares de Clyde, de altíssima segurança, onde estão os submarinos com misseis de ogiva nuclear Trident, como os nomes, ritmos cardíacos, do pessoal que lá trabalha (Burgess, 2018) (Figura 35).

Figura 35 – *Heat map* Strava, no interior e em redor da base nuclear da Marinha Real de Clyde[100].

[99] https://thedefensepost.com/2018/01/30/fitness-tracker-strava-opsec-risk/
[100] https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military

Mas as preocupações de segurança não ficaram por aqui, pois muito pessoal publicava *online* fotografias, com *geotagg*, o que permite verificar no Google Earth as localizações, ou simplesmente tinham cópia dessas imagens na nuvem, *online,* onde podem ser "atacadas" e expostas, segundo um artigo do Jornal da Defesa dos E.U.A.: "Want to send your location to ISIS There's an app for that" (Burke, 2018). Um dos exemplos mais conhecidos já foi referido, a propósito do *geotagg* das fotografias, quando em 2007 quatro helicópteros (AH – 64 Apache) novos foram destruídos no Iraque, tendo sido localizados com base em fotos "postadas" por soldados. Num documento dos Exército dos E.U.A. (US Army, s.d.) é explicado, detalhadamente e com exemplos, por que razão não se deve geolocalizar fotografias e partilhá-las em redes sociais, exemplos de como graças a uma fotografia de um carro um apresentador (MythBusters) revelou, inadvertidamente, a localização da sua casa (Murphy, 2010), ou como ao ver uma desconhecida, num parque, a tirar uma fotografia com um *smartphone*, se conseguiu facilmente chegar a outras fotos tiradas pela mesma pessoa, através do mapa do Flickr, a fotos do interior da sua casa, do seu quarto, da sua cozinha, descobrindo-se a sua morada (Honan, 2009).

O documento do exército explica que as aplicações, que permitem partilhar fotografias geolocalizadas, permitem seguir e rastrear as deslocações diárias e encontrar padrões, sabendo-se o que as pessoas fazem, a que horas e onde, expondo até indivíduos à distância (a família do pessoal destacado no estrangeiro), tornando a população militar num alvo potencial. Lembra que nunca se deve permitir localização geográfica nas fotografias, "postar" fotografias que exponham localizações geográficas específicas, usar redes sociais baseadas na localização pessoal, desligar a função GPS de todos os dispositivos que o permitam e que tudo é, também, uma questão de bom-senso e percepção situacional (Brownstein, 2018). Facilmente se entende que a nível individual, qualquer pessoa aceitará como válidas estas recomendações, para a sua vida quotidiana, como forma de defender a sua privacidade e segurança, mas a maioria esmagadora dos utilizadores destes dispositivos e aplicações, não parece ter noção disso (como se viu com as tropas dos E.U.A. e outros países).

Um factor que torna ainda mais fácil localizar, em mapas e plataformas como o Google Earth, as coordenadas embebidas nas fotografias, é a existência de cartografia de alta resolução como o OSM (Open Street Map)[101]. Esta plataforma de cartografia apareceu como um projecto de colaboração aberto (tipo Wiki), a Open Street Map Foundation[102], com o objectivo de criar e fornecer dados geográficos, como mapas de ruas, a toda a população, por considerar a cartografia um direito universal, que não pode ficar não mãos de empresas privadas, organizações ou estados. Uma das formas de criar o "melhor mapa do mundo" é permitir que toda a comunidade (potencialmente toda a população do mundo, basta registar-se), possa participar (ver Figura 35).

[101] https://www.openstreetmap.org/#map=7/39.602/-7.839
[102] https://wiki.osmfoundation.org/wiki/Main_Page

Todos podem "desenhar" o mapa, ficando registado quem fez as edições, pode-se corrigir, editar, discutir, sendo esta plataforma um recurso didáctico geográfico interessantíssimo, pois permite introduzir conceitos básicos de cartografia, fotointerpretação, conhecimento do território, sendo desenhado e construído, pelo utilizador, sobre imagens Bing Maps, podendo carregar e utilizar pontos, linhas ou polígonos recolhidos com dispositivos que possuam geolocalização (Figura 36).

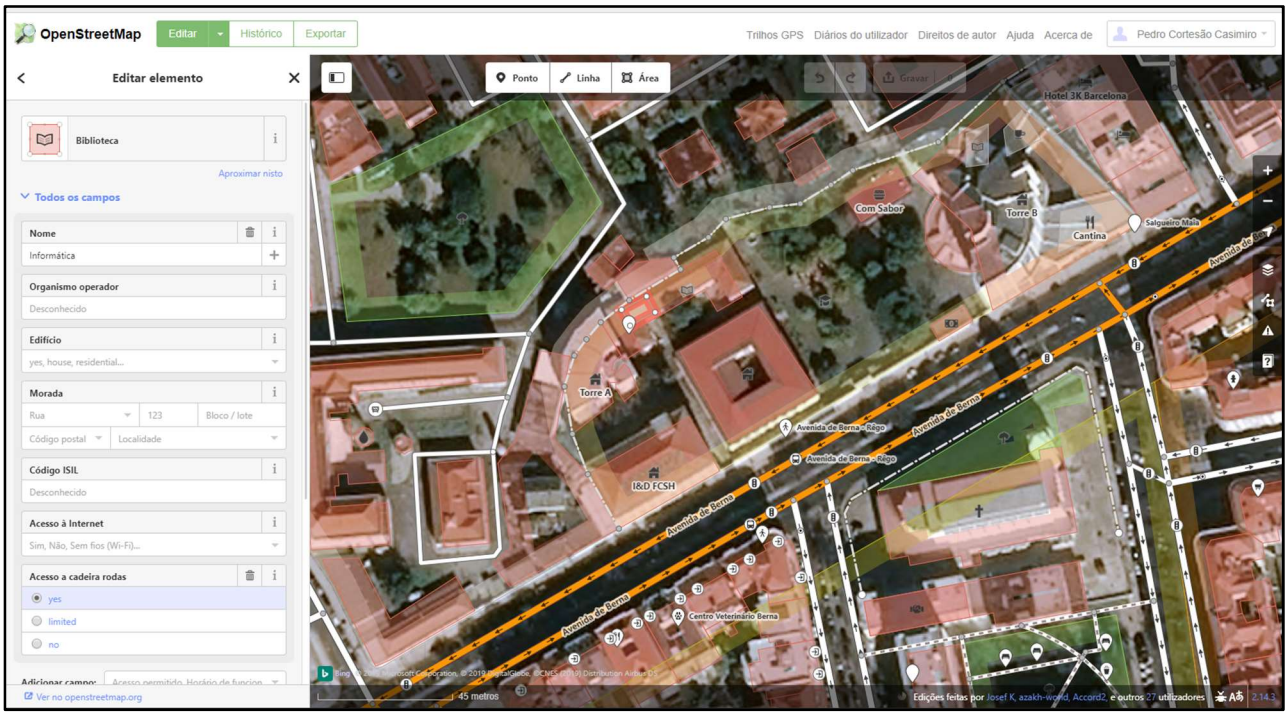


Figura 36 – Open Street Map em modo de edição, FCSH – Nova, Avenida de Berna, Lisboa[103].

Neste momento tem mais de dois milhões de utilizadores registados, sendo um exemplo proeminente de informação geográfica voluntária (ver descrição e mais informação em OSM - Wikipédia[104]). O esforço da comunidade, em casos de catástrofes naturais, tem sido importantíssimo para dotar as agências, ONG's e pessoal de apoio, socorro e salvamento no terreno, sobretudo em áreas sem cartografia, sendo recorrentes e comuns os apelos a cartografia urgente[105].

A cartografia e dados, por sua vez, podem ser descarregados livre e gratuitamente, para todo o tipo de dispositivos que tenham funcionalidade de geolocalização, permitindo navegação *offline* em tempo real, sobretudo em áreas e países para os quais não há, de todo, informação cartográfica comercial, detalhada ou não. Isto implica que, com dados de geolocalização da

[103] https://www.openstreetmap.org/login?referer=%2Fedit#map=18/38.74012/-9.15159
[104] https://en.wikipedia.org/wiki/OpenStreetMap
[105] https://wiki.openstreetmap.org/wiki/Humanitarian_OSM_Team e https://www.facebook.com/hotosm

pegada digital de uma pessoal, se pode encontrar, identificar e conhecer, melhor ainda, o contexto geográfico do utilizador[106].

A conjugação dos dados de geolocalização, recolhidos por dispositivos vários, a sua análise e localização potencial com plataformas como o Google Earth e OSM, leva a que haja guias e manuais *online* para tornar anónimos esses dados, retirando-os, de certa forma, à pegada digital de cada um (Loufgran, 2018). Se pensarmos bem, os dados do Strava, por exemplo, permitem muito mais do que saber a localização e trajecto, podem revelar entre outras coisas: qual a actividade praticada (correr, andar, nadar, bicicleta), que material se utiliza (caso se identifique a bicicleta), com quem se faz as actividades, quando não se está em casa, como se vai para os pontos de partida e chegada dos trajectos, a forma em que se está, se se está a melhorar ou piorar, quando e para onde se viaja no mundo, entre outras.

Uma forma fácil de diminuir a pegada digital destas actividades é dar o mínimo de pormenores, não utilizar o nome real, convidar aqueles com quem se fazem as actividades a seguir os mesmos procedimentos, nunca começar ou acabar os registos em locais reais importantes em termos de privacidade (emprego, escola, casa). O problema é que a maior parte das pessoas, por gosto, vaidade ou falta de conhecimento (ou uma mistura de todos os factores), ao gostarem de "postar" estas actividades, tornam os dados o mais visíveis e pessoais possível, sendo que assim a pegada digital é completamente voluntária.

O problema é quando o fazemos de forma completamente involuntária, para mais proporcionado lucro às empresas que o fazem, como a Google, que regista a localização e o seu histórico, mesmo quando se desliga esta função, o que deveria evitar que o Google Maps ou as simples buscas, fossem geolocalizadas, embora continuem a ser: sempre que se abre o Google Maps é registada a localização, o mesmo quando se procura a previsão meteorológica ou faz uma busca (Schroeder, 2018). Como esta opção está ligada por defeito, TODOS os utilizadores de um *smartphone* Android, estão continuamente a fornecer dados de localização, o que não respeita a sua geoprivacidade. Estima-se que existam, a funcionar, mais de dois mil milhões de dispositivos Android e centenas de milhões de iPhones que utilizam o Google, para cartografia e buscas, que partilham este problema de privacidade (Nakashima, 2018).

Sabe-se que, mesmo sem os serviços de localização ligados, sem quaisquer aplicações instaladas e sem cartão SIM no telefone, o sistema regista dados das torres da rede celular próximas e, mal o telefone tenha ligação à Internet, envia esta informação para a Google. Isto aconteceu mesmo com equipamentos a que se fez um *reset* de fábrica, também usando ligações *WiFi* para obter a localização e enviar os dados e embora a Google diga que não utiliza os dados, permitem aos

[106]https://help.openstreetmap.org/search/?csrfmiddlewaretoken=yijgDlPh1cApzorSAyxOiHBeGHgXCE9M&q=download+for+gps&Submit=search&t=question

anunciantes utilizá-los, para por exemplo saber em que lojas ou áreas comerciais esteve um dispositivo Android, o que permite direccionar a publicidade (Collins, 2017).

Quem queira aprofundar um pouco mais a questão da Google e da sua hegemonia, com o devido filtro crítico e algumas cautelas, embora essa abordagem seria toda uma outra conversa, pode começar por um extracto do Livro de Julian Assange, disponível na Wikileaks, "Google is not what is seems" (Assange, 2014), onde nas considerações finais (p. 37), refere: "Quer esteja a ser só uma empresa [a Google] ou «mais do que só uma empresa», as aspirações da Google estão firmemente entrelaçadas na agenda política estrangeira da maior superpotência do mundo. Conforme o monopólio da Google de pesquisa e serviços da Internet cresce, enquanto alarga o seu cone de vigilância industrial para cobrir a maior parte da população mundial, dominando rapidamente o mercado de telefones móveis mundial e acelerando para estender o acesso à Internet no Sul global, a Google está a *tornar-se*, para muitas pessoas, na própria Internet. A sua influência nas escolhas e comportamento da totalidade dos seres humanos, traduz-se no poder real para influenciar o curso da história. […] Se o futuro da Internet é ser a Google, isso deveria ser uma séria preocupação para as pessoas em todo o mundo […] para quem a Internet encarna a promessa de uma alternativa à hegemonia cultural, económica e estratégica dos E.U.A. […] Um império do não ser mau ["don't be evil empire" no original] não deixa de ser um império".

A Google tem tido processos em tribunal, por rastrear a localização dos utilizadores sem o sem consentimento e contra a sua vontade expressa (Lucas, 2018), acresce o facto de cerca de 75% das aplicações terem rastreadores de localização, "um estudo de 2014 feito pelo Governo Francês [CNIL organismo de protecção ao consumidor], mostrou que entre um terço e um quarto das aplicações tinham acesso à localização do telefone. […] Um estudo da Universidade de Yale descobriu que três quartos das aplicações para Android utilizavam rastreadores de localização, geralmente contendo publicidade. […] O estudo do CNIL mostrou, também, que algumas aplicações rastrearam a localização do telefone mais do que um milhão de vezes durante um período de três meses – acedendo à informação cerca de uma vez por minuto".

Embora possa não parecer importante, ou passível de permitir identificar claramente os utilizadores dos dispositivos, um estudo dos dados de mobilidade, sobre meio milhão de utilizadores, durante 15 meses, permitiu compreender quão únicos são os padrões de deslocação das pessoas (Montjoye, Y., Hidalgo, C.A., Verleysen, M. & Blondel, V.D., 2013). "Efectivamente, num conjunto de dados onde a localização de um individuo é especificada a cada hora, sendo a resolução espacial igual às células da rede de antenas dos operadores, quatro pontos espácio-temporais são o suficiente para identificar 95% dos indivíduos. […] o carácter único dos rastos de mobilidade decai aproximadamente com a potência 1/10 da sua resolução. Consequentemente, mesmo conjuntos de dados menos detalhados permitem pouco anonimato".

Considerando que, o uso da Internet nos *smartphones* actuais amplifica o carácter único dos indivíduos, as tecnologias modernas alargam os desafios tradicionais da privacidade. O problema é que, no passado, somente os operadores de comunicações móveis tinham acesso a estes dados, mas hoje há inúmeras aplicações, constituindo um grande proporção nos *smartphones*, que recolhem, enviam e partilham estes dados (ver Figura 37).

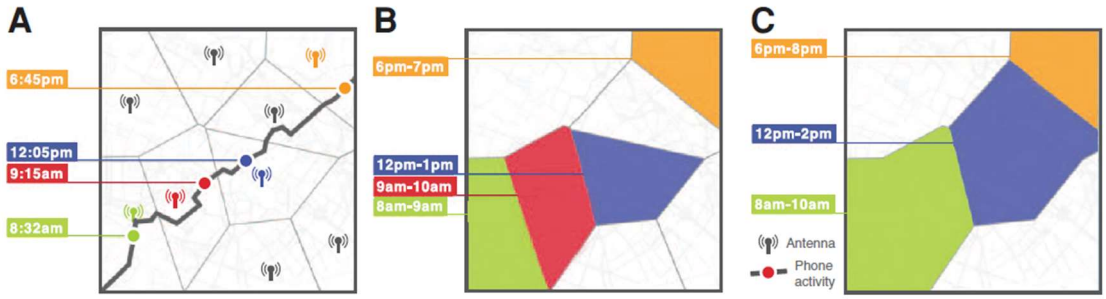


Figure 1 | (A) Trace of an anonymized mobile phone user during a day. The dots represent the times and locations where the user made or received a call. Every time the user has such an interaction, the closest antenna that routes the call is recorded. (B) The same user's trace as recorded in a mobility database. The Voronoi lattice, represented by the grey lines, are an approximation of the antennas reception areas, the most precise location information available to us. The user's interaction times are here recorded with a precision of one hour. (C) The same individual's trace when we lower the resolution of our dataset through spatial and temporal aggregation. Antennas are aggregated in clusters of size two and their associated regions are merged. The user's interaction are recorded with a precision of two hours. Such spatial and temporal aggregation render the 8:32 am and 9:15 am interactions indistinguishable.

Figura 37 – (A) Rasto anónimo do utilizador de um telemóvel durante um dia, os pontos representam tempos e localizações em que o utilizador fez, ou recebeu, uma chamada, de cada vez que existe uma destas interacções a antena mais próxima que encaminha a chamada é registada. Em (B) o mesmo rasto na base de dados móvel, dados recolhidos hora-a-hora. Em (C) o mesmo rasto, mas com a resolução espacial menor (Montjoye, Hidalgo, Verleysen, & Blondel., 2013, p. 2).

Mas se, até aqui, se falou de criar, voluntária ou involuntariamente, uma pegada digital extensa, com destaque para a geolocalização de informações várias, falta abordar a parte obscura, menos conhecida e eventualmente ilícita da questão: que informação existe e circula na *deep* e *dark web*? Que informação foi roubada e posta à venda? Como foi lá parar? Comecemos então pelas definições, segundo Reilly (2017):

Deep Web – Antes de mais, não deve ser confundida com a *Dark Web*, refere-se a qualquer parte da Internet que é não "descobrível" através de motores de busca (i.e. Google, Bing, Yahoo, DuckDuckGo, etc.), não querendo isso dizer que seja suspeita, há potencialmente muitos sites que se visitam diariamente e estão nesta categoria. Quando se vai a serviços bancários *online*, quando se navega para um endereço que não tenha sido fornecido por um motor de busca, passa-se o mesmo com subpáginas de serviços de correio electrónico (i.e., *webmail*, e.g. Gmail, Outlook, Hotmail, etc). É difícil estimar quão grande é a *Deep Web*, mas a pesquisa mais frequentemente citada dá-lhe uma dimensão cerca de 400 a 550 vezes maior que a "*surface web*" (ver Figura 38).

Dark Web – Se a *surface web* é a ponta do iceberg e a *Deep Web* é o que está debaixo de água, então a *Dark Web* é aquilo se se encontra nas águas profundas mais escuras. A *Darknet* é a rede *peer-to-peer*[107], que permite as ligações ao conteúdo na *Dark Net*. A palavra chave aqui é anonimato, denúncias, activistas, hackers e dissidentes que querem obscurecer a sua localização e "postar" anonimamente, a questão é que este grau de secretismo leva a que este espaço seja, também, utilizado para actividades ilegais e criminosas (venda de drogas, armas, dados roubados, tráfico de pessoas, prostituição, etc.).

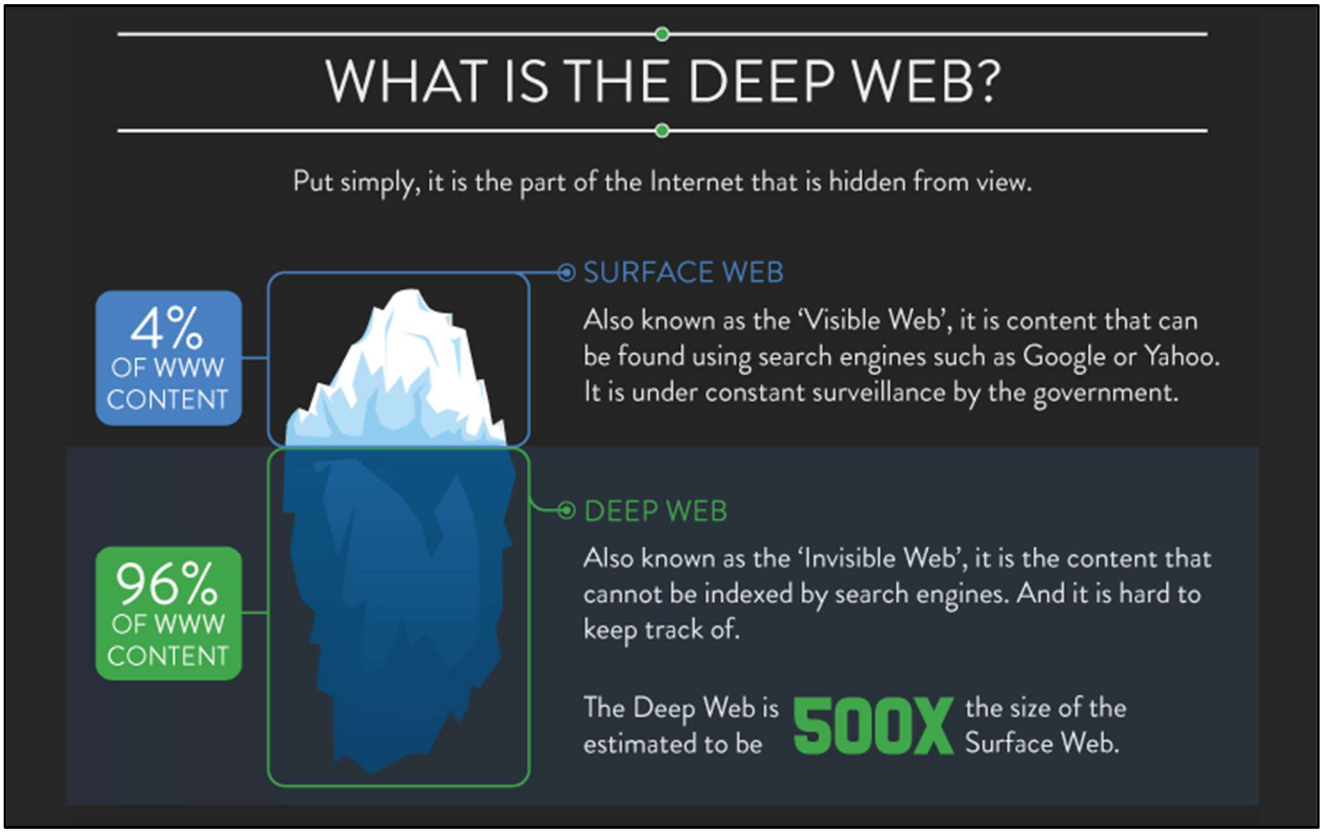


Figura 38 – Dimensão e conteúdo da *Deep* Web (Deepweb, 2016).

Esta rede não está indexada e exige determinado tipo de *software* para se poder ter acesso[108], anonimamente, recorrendo a ligações VPN[109], as transacções financeiras são feitas, exclusivamente, em criptmoedas, como a Bitcoin, que está indelevelmente ligada à *Dark Web* e

[107] *Peer-to-peer* - Arquitectura de redes de computadores onde cada um dos pontos, ou nós da rede, funciona tanto como cliente quanto como servidor, permitindo compartilhar serviços e dados sem a necessidade de um servidor central. As redes P2P podem ser configuradas em casa, em empresas e ainda na Internet (Wikipédia, 2019).

[108] TOR – The Onion Router, https://www.torproject.org/

[109] VPN – Virtual Private Network, rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros, a VPN cria uma conexão segura e criptografada, que pode ser considerada como um túnel, entre o computador e um servidor operado pelo serviço (Wikipédia, 2019).

Silk Road (loja de venda de droga) (Bradbury, 2019). Há quem diga que a sua dimensão e importância têm sido exageradas, pela comunicação social (Cox, 2015), sendo que a maior parte dos utilizadores se limita a recorrer a ela para efeitos de privacidade[110].

Como se pode imaginar, algures na obscuridão da *Dark Web*, há muita informação pessoal a circular e à venda, num grau tal que pode ser considerado perturbante. Segundo Patterson (2019), a cada violação de dados [*data breach*], os dados das vítimas aparecem na Internet escondida e encriptada (*Dark Web*), como cada vez mais companhias capturam e guardam informação pessoal, roubá-la [*hacking*] tornou-se uma profissão altamente lucrativa. Um *Hacker* conhecido como Gnosticplayers roubou, alegadamente, mais de 840 milhões de registos de utilizadores, tendo libertado 26.42 milhões desses registos por 1.2431 Bitcoin[111]. Segundo o autor, "a *Dark Web* forneceu as matérias primas, de que estes especialistas em fraudes necessitavam, para construírem impérios criminais escaláveis. Estamos a falar do roubo de dados de identidade de milhões de pessoas, incluindo crianças".

Naturalmente que as autoridades, todas elas, andam em força (espera-se) pela *Dark Web* "à caça" das actividades criminosas várias, sobretudo em tempos de insegurança global, ligados ao terrorismo e todo o tipo de tráficos abjectos, que encontram aí local seguro para as suas actividades e, sobretudo, comunicações. Assim, há constantes operações (algumas tornadas públicas) para combater as actividades criminosas[112] .

O problema é que, de cada vez que é anunciada uma vitória, a *Dark Web* reconstrói-se: "a história ensinou-nos que este ecossistema é muito, muito resiliente, é parte de um ciclo, estamos na parte caótica do ciclo. Teremos de ver como recupera. Mas se tivesse de apostar, diria mais depressa que iria recuperar do que mudar (Greenberg, 2019). Um exemplo destes ciclos, dado pelo autor, foi o derrube da *Silk Road*, mercado de droga da *Dark Web*, a que logo se seguiu o aparecimento de cerca de uma dúzia de alternativas, para responder à procura de drogas *online*. Será sempre mais fácil comprar drogas, armas, ou outros produtos ilícitos *online*, sob anonimato, que num beco escuro, a um vendedor que não se conhece.

---

[110] Ver https://www.wired.com/tag/dark-web/, ou https://darkwebnews.com/help-advice/access-dark-web/, ou https://www.quora.com/What-is-the-deep-dark-web-and-how-do-you-access-it, ou ainda https://www.publico.pt/2017/08/08/tecnologia/perguntaserespostas/o-que-e-a-dark-web-1781702

[111] https://bitcoin.org/en/ uma Bitcoin (XBT) vale 4883.62 Euros (24-04-2019, https://www.xe.com/currencyconverter/convert/?Amount=1&From=XBT&To=EUR)

[112] Ver: https://www.wired.com/story/hansa-dutch-police-sting-operation/ , https://www.policeone.com/dark-web/ , https://motherboard.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web , https://www.welivesecurity.com/2019/03/27/global-police-arrest-dark-web-sting/ , https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web , https://www.truthfinder.com/infomania/dark-web/5-worst-dark-web-criminals/, https://algarvedailynews.com/news/16348-portuguese-police-join-international-team-in-dark-web-arrests

Um caso curioso, porque está relacionado com *geotagging* de fotos e geoprivacidade, segundo (Khandelwal, 2016), dois estudantes de Harvard descobriram 229 traficantes de armas e droga com a ajuda das fotografias, tiradas pelos próprios e utilizadas como anúncios em mercados da *Dark Web*, das 223.471 imagens que recolheram, 229 tinham dados EXIF de geolocalização. Felizmente, neste caso, parece ser um erro comum por parte de criminosos, pois as autoridades recorrem cada vez mais a esta informação nas suas investigações e esforços de identificação[113].

Embora seja, virtualmente, impossível saber a quantidade e valor dos dados roubados, disponíveis, vendáveis ou efectivamente vendidos, a dimensão do problema do roubo de identidades é enorme. É fácil assumir que muitos dados das pegadas digitais podem, fazem, parte destas grandes massas de dados, sobretudo se foram "perdidos", mal protegidos ou roubados a quem os recolhe e deveria guardar. Segundo ISN (2018), há várias formas de os *hackers* fazerem dinheiro com dados roubados:

- **Criam um repositório de dados roubados** – Quando o inventário está criado, a informação é empacotada e vendem dados pessoais, como nomes, endereços, números de telefone e endereços de *email*, quanto mais recentes os dados, mais valiosos;
- **Apontam para dados que valham mais dinheiro** – Depois da informação pessoal, listas de credenciais de autenticação e contas lucrativas. Endereços governamentais e militares, de companhias e empresas, dados e *email* e palavras-passe, como muitas pessoas repetem as palavras-passe, conseguem atingir outras contas das mesmas vítimas. Este tipo de ataque é comum;
- **Venda de informação de cartões de crédito** – Informação financeira vendida em pacotes, centenas, milhares, testam com compras falsas, compram cartões de oferta, para depois poderem ser utilizados anonimamente em compras directas. Segundo a McAfee[114] um cartão de crédito (ou dados), com o código CVV2[115], vale entre 5 e 8 Dólares Americanos, mas se também tiver o número de identificação do banco, pode valer 15 USD, se tiver toda a informação da vítima, pode valer até 30 USD (McAfee, 2015);
- **Descarregamento dos dados restantes a granel** – Ao fim de meses, venda a preços de desconto, pois a maior parte das credenciais possivelmente já não valem nada, pois a violação de dados foi (potencialmente) descoberta. Por exemplo, uma base de dados de TODAS as credenciais do Linkedin[116] ainda está disponível, mas a maior parte não tem grande valor;

[113] https://timesofindia.indiatimes.com/city/hyderabad/geo-tagging-helps-to-nab-43-criminals/articleshow/56366911.cms ou https://link.springer.com/article/10.1186/s40163-015-0017-6
[114] Uma das principais empresas mundiais de segurança informática, https://www.mcafee.com/pt-pt/index.html
[115] CVV2 – Código de segurança do cartão, no verso, para validar compras não presenciais, https://www.cvvnumber.com/
[116] LinkedIn – Rede social de negócios e empregos, https://www.linkedin.com/

- **Receber reembolsos fraudulentos de impostos** – Organizações criminosas utilizam as identidades roubadas e entregam declarações falsas de impostos, tentando receber reembolsos, segundo a entidade fiscal dos E.U.A., as perdas por esta fraude diminuíram 14% no último ano [2017] mas representam, ainda, perdas de 783 milhões de USD;
- **Práticas médicas fraudulentas e reembolsos fraudulentos** – o Governo dos E.U.A: estima que 10% do dinheiro gasto no Medicare[117] é perdido para fraude e desperdício. O registo médico completo de uma pessoa pode valer 250 USD no mercado negro, utilizam-nos para pedir reembolsos de pequenas quantias, para se diluírem nas contas dos contribuintes;
- **Venda de propriedade intelectual** – As companhias do mundo industrializado gastam anualmente milhões de dólares em pesquisa e desenvolvimento, dinheiro que não existe noutros locais do mundo, roubam-se segredos industriais, projectos, filmes, músicas, por vezes para pedir resgates, há casos registados com a Disney[118], HBO[119] ou a SONY[120].

Oficialmente, se é que assim se pode dizer, "os dados roubados são a «mercadoria» que mais depressa se vende na *Dark Web*" Richard (2017). Segundo o relatório "The Hidden Data Economy" (MAcAFee, 2015), "Os dados são o «petróleo» da economia. O mercado comercial para dados pessoais está em florescimento, com grandes bases de dados de informação de subscritores levando a enormes valorizações das companhias que os possuem, mesmo que algumas ainda tenham de dar lucro. Consoante cresce o valor comercial dos dados pessoais, os cibercriminosos[121] construíram há muito, uma economia baseada no roubo de dados, a qualquer pessoa com um navegador da Internet e meios de pagamento".

Ora, assim, torna-se claro que as principais companhias que dependem e vivem da recolha maciça de dados, pegada digital para a qual contribuímos voluntariamente ou não, sabendo-o ou não, são dos alvos mais apetecíveis para roubo de dados, mesmo e sobretudo quando lhes confiamos os nossos dados pessoais, de todos os tipos. Quase todas as grandes empresas têm sido alvo de roubos, mas convém perceber a dimensão, mecânica e gravidade destes roubos/violações de dados [*data breaches*].

Segundo Schroeder (2017), "embora pensemos que os nossos dados estão seguros, por vezes fornecemos a terceiros grandes quantidades de informação, sem termos conhecimento adequado de como essa informação é guardada e utilizada. Também não temos uma única pista acerca da coisa mais importante de todas, como é que as companhias mantêm os nossos dados seguros. […]

[117] Seguro de saúde estatal - https://www.medicare.gov/
[118] https://eu.usatoday.com/story/money/2017/05/15/reports-hackers-demand-ransom-stolen-disney-movie/101726832/
[119] https://www.washingtonpost.com/news/morning-mix/wp/2017/08/08/hackers-post-stolen-hbo-game-of-thrones-scripts-*online*-demand-bitcoin-ransom/?noredirect=on&utm_term=.b98752cbee36
[120] https://www.samaa.tv/culture/2014/12/script-of-new-bond-film-stolen-in-sony-attack/
[121] Cibercriminoso - pessoa que recorre a sistemas electrónicos e às novas tecnologias de informação para cometer crime(s), https://www.infopedia.pt/dicionarios/lingua-portuguesa/cibercriminoso

descobriu-se que eles não estão tão seguros como pensávamos. A Yahoo [empresa de fornecimento de acesso à Internet, conteúdos e motor de busca], viu em 2013 e 2014, 1.5 mil milhões de contas de clientes terem todos os tipos de dados pessoais comprometidos, nomes reais, palavras-passe, *emails*, datas de nascimento, telefones, etc.".

Podem-se considerar as fugas/roubo/violação de dados em dois grandes conjuntos, "em instituições a quem as pessoas escolhem confiar os seus dados – como retalhistas e bancos – e fugas ou roubos de entidades que adquiriram secundariamente esses dados – como empresas de crédito e de marketing" (Newman, 2018). É difícil manter a informação a salvo, por vezes é impossível não partilhar dados, especialmente com organizações governamentais, bancos, companhias de seguros e muitas vezes, quase sem reparamos, aceitamos nos termos e condições, que partilhem informação com terceiros.

Pode-se ver na Figura 39, os riscos de roubo/violação de dados de localização, convém termos noção que, "se souberem o nosso nome, palavra-passe, *email*, telefone ou informação do cartão de crédito, os *hackers* têm ferramentas para tornar a nossa vida num inferno, mas podemos evitar tudo isso se notificados a tempo. As palavras-passe podem ser mudadas, pode-se fazer uma nova conta de *email*, activar verificação em dois-passos[122], cancelar cartões, etc. [...] Mas, tendo dados sobre a localização, espacialmente morada de casa, pode ser verdadeiramente perigoso. Não podemos mudar de morada facilmente e é simplesmente impossível, para a maioria da população" Schroeder (2017).

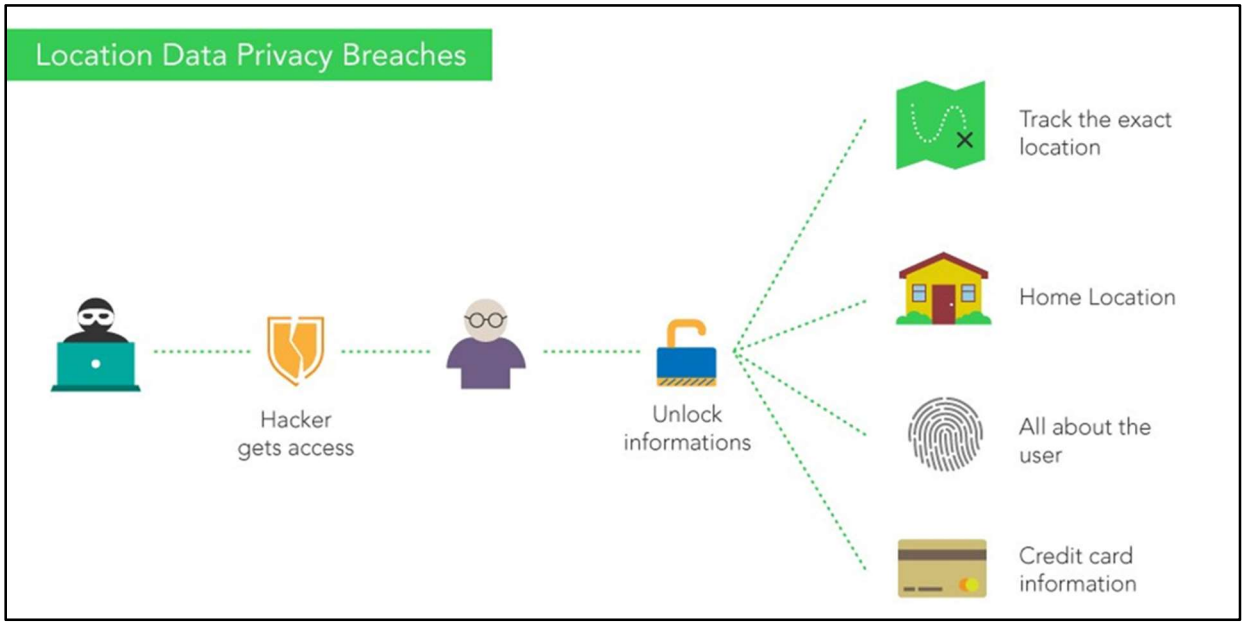


Figura 39 – Riscos de roubo/violação de dados de localização (Schroeder, 2017).

[122] Segunda camada de segurança depois da validação inicial, geralmente por outro meio/dipositivo.

Segundo o mesmo autor, sintetizando, alguns dos roubos/violações de dados de localização recentes foram os seguintes:

- **540.000 dados de rastreio de GPS**[123] - guardados no serviços da nuvem da Amazon S3 (Mathews, 2017), incluíam IMEI[124] do dispositivo, nome de utilizador, palavras-passe, *email*, moradas, matrículas de carros em que os dispositivos estavam instalados, bem como o registo completo dos GPS 's;
- **Pouca segurança do Grindr** (aplicação gay masculina para encontros) – A aplicação liga os utilizadores através da sua localização, usa, portanto, a localização exacta para funcionar, mas os dados não estavam seguros;
- ***Hack* do mSpy** – Aplicação de rastreio com vários serviços, entre eles localização, utilizado para controlar a actividade de crianças pelos pais, para isso usa mensagens de texto, WhatsApp, *email*, e outras funções, tudo dados altamente sensíveis, mas *hackers* conseguiram roubar centenas de Gigabytes de informação da base de dados, tendo a base de dados acabado por aparecer num servidor Tor;
- **Sprint dá dados de GPS à polícia Federal** – Operador de comunicações, a pedido do FBI ou outras agências governamentais, entregava dados GPS dos clientes;
- **Accuweather** – Sítio e aplicação de previsão meteorológica, tal como as outras ABL (Aplicações Baseadas na Localização), está constantemente a recolher dados de localização, esta era partilhada com outras empresas, incluindo router *WiFi*, endereço AMC e dados públicos;
- **McDonalds da India e dados de localização dos utilizadores** – Aplicação móvel McDelivery tinha uma API que permitia roubar informação, foram expostos dados de 2.2 milhões de utilizadores, moradas, coordenadas exactas, telefones, *email* e perfis de redes sociais;
- **Runkeeper partilha dados de localização com terceiros** – Aplicação de fitness e rastreio de localização, regista dados de localização, movimento e dados pessoais, mesmo depois de desinstalada, neste caso os dados parecem estar seguros;
- **Foursquare publica *online* dados de localização dos utilizadores** – Aplicação de partilha de localização, milhões de utilizadores, uma falha de segurança permitia ver os *check-ins* de TODOS os utilizadores, a falha foi resolvida;
- **Uber e o rastreio após as viagens** – A Uber introduziu, na aplicação, a possibilidade de recolher informação da localização dos clientes (Conger, 2018), fora da prestação do serviço de transporte, até cinco minutos depois, tinham assim acesso a rotinas diárias dos clientes, a companhia aceitou encriptar estes dados quando eram enviados para os seus servidores e entre eles. Alguns empregados utilizaram os dados para seguir ex-namorados e namorados, bem como algumas celebridades;

[123] https://www.forbes.com/sites/leemathews/2017/09/22/data-from-540000-vehicle-tracking-devices-leaked-online/#57027068274b

[124] Ver nota de rodapé Nº 50.

- **Snapchat com práticas de segurança fracas** – Aplicação de comunicação multimédia, em 2014 4.6 milhões de utilizadores foram afectados por uma fuga de informação, que expôs os seus nomes, números e localizações. Quando lançou a SnapMap, que permitia ver num mapa os amigos, como é uma rede social , leva a que muitos amigos não se tenham efectivamente e fisicamente encontrado, quando se combina muitos amigos que nunca se viram, com um mapa, isso é um problema, a informação da localização é partilhada com todos os utilizadores;
- **Uma aplicação que revela as localizações dos utilizadores do Tinder** – Aplicação para "encontros", a mais famosas de todas, encontra combinações em função da vizinhança/proximidade, uma aplicação (Tinderfinder) conseguia encontrar e marcar todos os utilizadores num mapa, a sua localização exacta, pois os dados não estavam encriptados.

Concluindo, a geoprivacidade é importantíssima, valiosa e deve ser preservada, dependendo de cada utilizador tomar as devidas precauções para a salvaguardar. Verificar se as aplicações registam a localização, se e a quem a enviam, se é encriptada, como é guardada, o que é difícil de saber em muitos casos. Deixando as fugas/roubos/violações de dados, exclusivamente, de localização e passando para os dados pessoais, segundo a Business Insider, Leskin, (2018), os roubos de dados mais assustadores de 2018 incluíram (em função dos utilizadores afectados, o que foi afectado e como):

- **British Airways** (companhia aérea) – 380.000 utilizadores afectados, pagamentos com cartões, *hack* que afectou as reservas feitas no sítio da Internet e aplicação;
- **Orbitz** (viagens) – 880.000, informação de cartões e dados pessoais (moradas, telefones, *email*), *hack* das reservas no servidor do sistema;
- **SingHealth** (cuidados de saúde, Singapura) – 1.5 milhões, nomes, moradas, história clínica, medicamenstos, etc., ataque à base de dados;
- **T-Mobile** (comunicações móveis, Alemanha) – 2 milhões, palavras-chave encriptadas e dados pessoais, números de contas, informação de facturação e *emails*, *hack* dos servidores através de uma API;
- **my Personality** (APP do Facebook) – 4 milhões, dados pessoais *via* Facebook, quem usou a APP, que levou os utilizadores a partilhar (voluntariamente) informação;
- **Saks and Lord & Taylor** (cadeia de retalho, E.U.A.) – 5 milhões, pagamentos cartões, *hack*;
- **SheIn.com** (moda feminina) – 6.42 milhões, *emails*, palavras-passe encriptadas, ciberataque;
- **Cathay Pacific** (companhia aérea) - 9.4 milhões, números de passaporte, cartões de identidade, cartões de crédito, acesso sem autorização;
- **Careem** (chauffeur *online*) – 14 milhões, nomes, moradas, telefones e dados das viagens, *hack*;
- **Timehop** (aplicação de efemérides pessoais) – 21 milhões, nomes, moradas, telefones, credencial de acesso comprometida;
- **Ticketfly** (eventos) – 27 milhões, dados pessoais, moradas, telefones e *emails*, *hack*;

- **Facebook** (rede social) – 29 milhões, dados altamente sensíveis, **localização** detalhes de contacto, estado das relações, buscas recentes, dispositivos usados para se ligar, *hack*;
- **Chegg** (livros *online*) – 40 milhões, dados pessoais, nomes, *emails*, moradas, *usernames* e palavras-passe de contas;
- **Google +** (rede social) – 52.5 milhões, informação privada de perfis, nomes, empregos e título, *email*, aniversário, idade, etc.;
- **Cambridge Analytica** (consultoria política) – 87 milhões, perfis do Facebook e identificadores de dados dos utilizadores, preferências e interesses, uma aplicação passou dados dos utilizadores, os dados foram utilizados por uma empresa que apoiou a campanha de Donald Trump[125] (e Granvile (2018)). 270 mil utilizadores do Facebook instalaram a aplicação, voluntariamente, mas em virtude das políticas de partilha de dados na época, a aplicação recolheu dados de milhões dos seus amigos;
- **MyHeritage** (plataforma de genealogia *online*) – 92 milhões, *emails*, palavras-passe encriptadas, dados estavam num servidor fora da companhia;
- **Quora** (sítio de perguntas e respostas, conhecimento) – 100 milhões, informação das contas, incluindo nomes, *emails*, palavras-passe encriptadas, dados de contas, perguntas e respostas de utilizadores, acesso malicioso;
- **MyFitnessPal** (aplicação para exercício e dieta) – 150 milhões, nomes, *emails*, palavras-passe encriptadas, acesso fraudulento;
- **Exactis** (marketing) – 340 milhões, informação detalhada compilada de milhões de pessoas e empresas, incluindo telefones, moradas, interesses pessoais, características e muito mais, base de dados com quase todos os cidadãos dos E.U.A., deixada num servidor com acesso público;
- **MarriotStarwood** (hóteis) – 500 milhões, informação de hóspedes, incluindo telefones, *emails*, números de passaporte, datas de reservas, informação de cartões de pagamento, *hack*;
- **Aadhar** (número de identidade oficial da India) – 1.1 mil milhões, informação provada de residentes na India, nomes, número de identificação (12 dígitos), informação de serviços ligados, como contas bancárias, fuga graças a uma API.

Quando se vê uma lista destas, pode-se imaginar aquilo que nunca se soube, saberá ou não foi ainda detectado, há várias empresa ligadas à recolha de dados e sua venda para efeitos de publicidade, entre outros, como a Google e a Facebook. Um exemplo recente, relativo à Google, assumido publicamente a 21 de Maio de 2019, os dados de utilizadores empresariais, G Suite, incluindo palavras-passe, estiveram guardadas desde 2005, sem qualquer encriptação, num servidor da empresa (Newman, 2019a). A Facebook e Twitter tiveram problemas semelhantes, que, entretanto, foram corrigidos. Se começarmos a pensar em todos os sítios, formulários e informações pessoais, que já nos foram pedidas ou fornecemos *online*, tudo isto se torna perturbante e assustador

[125] Dossier do Público, sobre o caso, com vários artigos: https://www.publico.pt/caso-cambridge-analytica e https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram e ainda https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

e se neste ponto do texto, quem lê, não pensa de outra forma na privacidade dos seus dados, então tem um problema…

O ponto a que se chegou, em relação ao Facebook, levou a uma multa potencial de três a cinco mil milhões de Dólares, à Federal Trade Comission dos E.U.A[126], por violação dos termos do acordo de 2011 com a agência, relativo â uma melhor protecção dos dados dos utilizadores (Vogelstein, 2019). Se o valor da multa representa, somente, entre sete e onze por cento das reservas financeiras da companhia, já simbolicamente é muito significativa, sobretudo no seguimento do caso Cambridge Analytica e dados de 50 milhões de utilizadores que foram expostos no ano passado. Segundo o mesmo artigo, "a União Europeia já multou a Google em oito mil milhões de Dólares, em três ocasiões[127], por violações *antitrust* [combate a práticas monopolistas] e violações de privacidade. […] A maior multa anterior, contra uma companhia de tecnologia, foi contra a Google em 2012, 22.5 milhões de Dólares, por falhas de privacidade no navegador Safari".

No Canadá, os reguladores de privacidade determinaram que o Facebook violou as leis locais de mau tratamento dos dados dos utilizadores e que levaram, portanto, a empresa a tribunal, para a forçar a mudar a forma como protege a privacidade dos consumidores (Kelly, 2019). Segundo o comissário da privacidade do Canadá, "a recusa da Facebook em actuar com responsabilidade é profundamente perturbante dada a enorme quantidade de informação sensível que os utilizadores confiam à companhia. […] O quadro de privacidade era vazio e os seus termos vagos eram tão elásticos, que não eram significativos para a protecção da privacidade"[128].

A Facebook tem estado sob grande pressão, num extenso artigo (Thompson & Vogelstein, 2019) abordam os vários escândalos, traições, demissões, lucro e bombas relógio. Os receios prendem-se, sobretudo com a ameaça e perigos que podem deitar abaixo uma empresa com lucros de 55.8 mil milhões de Dólares em 2018: os regulamentos anti monopólio nos E.U.A. (separar Instagram, WhatsApp e Facebook), a repressão federal pelas falhas de privacidade (fugas várias e partilha com outras empresas), os reguladores europeus (caso já referido na Alemanha e RGPD da U.E. de que se falará a seguir) e, por fim, embora um quinto do globo use o Facebook todos os dias, o número de utilizadores tem estagnado nos adultos e declinado significativamente entre adolescentes (embora muitos migrem para o Instagram).

[126] https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html
[127] https://en.wikipedia.org/wiki/European_Union_vs._Google
[128] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/

Vida *online*…

Smartphones

Há alguns aspectos, relacionados com a *vida online*, que devem ser abordados porque ajudam a compreender e enquadrar o que até aqui foi aludido. O primeiro aspecto está ligado aos *smartphones*, à sua massificação e difusão, se navegar e "viver" na Internet cria uma pegada digital significativa, os telefones são o que, hoje, permite fazê-lo continuamente, em qualquer lugar (ou quase) e a qualquer hora, mas será que esta extensão digital de nós próprios não terá mudado, já, o nosso comportamento em sociedade?

Os "*smartphones* permitem ligação, comunicação e conhecimento, tendo passado a fazer parte das nossas identidades. Não é de admirar [portanto] que as violações de privacidade nos incomodem tanto" (Lynch, 2016). Pode dizer-se que os telefones não nos ajudam a conhecer e lembrar, mas que o conhecimento e recordações são constituídos, de facto pelo telefone, se não conhecimento, pelo menos sensação de conhecimento. Por essa razão cria tanto desconforto não termos acesso a eles, nem a uma forma de os ligar à Internet. "Sejamos ou não os nossos telefones, identificamo-nos cada vez mais com eles. Cada vez mais os vemos e à vida digital que levamos com eles, como constituindo parcialmente quem somos psicologicamente".

Segundo um estudo[129] recente, 49% das pessoas com menos de 35 anos e 35% com mais de 35 anos estão preocupadas com a sua confiança nos seu telefones, 43% disseram que examinam a informação que recebem mal ela chega, voltando depois a ela, 63% acreditam que os seus *smartphones* e *tablets* lhes permitem alcançar e realizar mais, porque a informação guardada digitalmente lhes permite libertar o cérebro para outras coisas (Fegan, 2016). Os utilizadores também usam os telefones para guardar lembretes e notas (53%), 30% enviam notas e *emails* a si mesmos como lembretes e 32% usam um calendário *online* para guardar e armazenar informação.

"Descarregando a responsabilidade de recordar informação para os dispositivos, as pessoas podem libertar os seus cérebros para lidar com tarefas mais importantes e lidar melhor com o enorme volume de informação que é empurrado na sua direcção. […] Nas nossas vidas digitalizadas, utilizamos a nossa memória de uma forma diferente. Parecemos lembra-nos de menos informação, mas lembramo-nos mais sobre como encontrar essa informação" (Fegan, 2016). Pode dizer-se que a forma fácil como acedemos a informação está, efectivamente, a remodelar a forma como pensamos.

[129] Feito pela Kaspersky Lab., uma empresa de Ciber Segurança, a 6000 pessoas entre 16 e 65 anos, em seis países da União Europeia.

O que permite este acesso fácil é a Internet, o que permite aceder-lhe em qualquer lugar, a qualquer hora, é o *smartphone*, passou a haver uma "descarga cognitiva" no telefone, motor de busca ou GPS. Segundo (Perry, 2016) este processo existe há muito tempo, com calculadoras, calendários, mas nada se compara à Internet, levando a questionar o que todo este processo está a fazer aos nossos cérebros. Argumenta-se que, visto termos capacidades limitadas, o uso destes dispositivos nos permite subverter os nossos limites cognitivos, mas será que isso não vai tornar as experiências de vida menos vívidas nas nossas memórias? Numa experiência, registou-se que as pessoas que, num museu, podiam utilizar câmaras fotográficas, se lembravam de muito menos detalhes dos quadros, mas lembravam-se melhor de objectos que não tinham fotografado.

A facilidade com que se encontra muita e boa informação na Internet (tendo espírito crítico), utilizando motores de busca, levou Car (2008) a questionar se o Google nos estaria a tornar estúpidos? Segundo o autor, quanto mais utilizava a *web*, navegando, procurando, saltitando, percebeu que havia um preço, "os meios não são só um canal de informação, eles fornecem o alimento ao pensamento, mas também modelam o processo de pensamento", o que o levava a dizer que a Internet estava a diminuir a sua capacidade de concentração e contemplação, a sua mente esperava assimilar informação da mesma forma que a rede a distribui.

Parece haver uma diminuição da capacidade de ler e absorver conteúdos longos, podendo a forma como "estamos" na Internet, estar de facto a mudar a forma como lemos e pensamos, "é claro que os utilizadores não estão a ler *online* no sentido tradicional do termo; há de facto sinais de que estão a emergir novas formas de «leitura», quando os utilizadores navegam [*power browse* no original] horizontalmente pelos títulos, páginas de conteúdos e resumos para uma «vitória» rápida. Quase parece que estão *online* para evitar ler no sentido tradicional" Car (2008). Se pensarmos que, actualmente, muita desta leitura é feita em telefones e *tablets*, em função da sua dimensão esta adaptação ainda será mais sensível.

Mas o que é que os *smartphones* estão a mudar no nosso cérebro? Cerca de 81% das pessoas têm os telefones quase sempre ao seu alcance, uma em cinco pessoas (jovens) admite verificar / examinar os ecrãs a cada cinco minutos, Faithfull-Williams (2017). Segundo a autora, as consequências são: estarmos cada vez mais dependentes dos telefones, pois consultamos a Internet para tudo a toda a hora, estamos a ficar simbióticos com eles; desenvolvemos mais um membro, pois o telefone parece uma extensão do nosso braço, ou de nós próprios (há quem sinta vibração fantasma do telefone, sem o ter, ou sinta perda de identidade quando são separados dele); a nossa ansiedade tem ansiedade, a presença de um telefone à vista, mesmo que não seja o nosso, torna-nos mais ansiosos; temos pensamentos em registo de fogo-rápido, a barragem de notificações, mensagens de correio, de texto, links de *clickbait*[130] são exactamente a forma como

[130] *Clickbait* - Termo pejorativo que se refere a conteúdo da internet que é destinado à geração de receita de publicidade *online*, normalmente à custa da qualidade e da precisão da informação, por meio de

a tecnologia sobrecarrega o nosso cérebro, embora essa fonte de informação seja boa, tem um custo emocional elevado.

Outra discussão que percorre a Internet, sob vários aspectos, é se a própria sexualidade humana está a mudar em função dos *smartphones*? Além da relação íntima entre as pessoas e os seus telefones, um em cada dez Americanos usam o telefone durante o sexo, dois em cada 10 jovens adultos usam o telefone durante o sexo. "Em termos práticos, os *smartphones* são como amplificadores/transmissores/receptores/memórias externas para o nosso id[131]" (Apt No 7, 2013). Efectivamente, a presença deste equipamento na nossa vida e a sua importância é tal, que pode estar a "estragar" a vida sexual dos seus utilizadores, segundo Langham (2019) são várias as formas como isto está a acontecer:

- Pornografia – Acesso fácil, ubíquo, criação de expectativas irrealistas, ansiedade, não tem mal nenhum, é uma questão de quantidade e *timing*;
- Redes sociais – Fácil ficar viciado e obcecado, vivem-se vidas em função do que os outros acham/pensam/anseiam e daquilo que se expõe (falso ou não, exagerado ou não), leva a desconcentração, desinteresse e ansiedade;
- Aplicações de "encontros" - Tudo, até os encontros e "engates" pode ser feito *online*, não pessoalmente, cara-a-cara, as pessoas procuram parceiros potenciais para sexo, falta a ligação;
- Mensagens de texto – Muitas pessoas fazem-no continua e doentiamente, não param ou interrompem o que estão a fazer para escrever.

Sem aprofundar mais o impacto dos telefones na vida sexual dos utilizadores, há quem tenha estudado a fundo as alterações numa geração, os pós-*millennials* (nascido entre a metade dos anos 1990 a 2000), que estão mais confortáveis *online* do que em festas ou em carros, são mais seguros que todos os outros adolescentes antes deles, mas estão à beira de uma crise de saúde mental (Twenge, 2017). A forma como vêem o mundo é diferente, a forma como passam o tempo também, as experiências que têm quotidianamente são radicalmente diferentes e tudo aconteceu [nos E.U.A.] quando se ultrapassou a proporção de 50% da polução com *smartphones* (em 2017 três em cada quatro adolescentes tinham um).

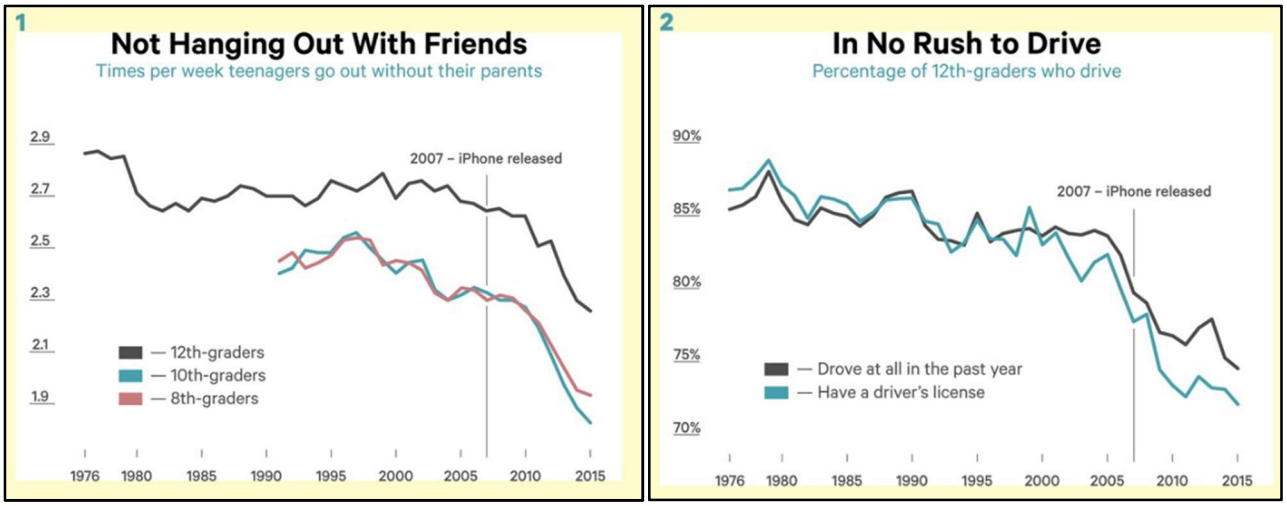
Primeiro com o telefone, depois com o *tablet*, aumentou brutalmente o "tempo de ecrã", transversalmente ao nível socioeconómico, étnico, nas cidades, subúrbios e pequenas vilas, "onde

manchetes sensacionalistas e/ou imagens em miniatura chamativas para atrair cliques e incentivar o compartilhamento do material pelas redes sociais (Wikipédia, 2019).

[131] Id – Na teoria psicanalítica é uma das três estruturas do modelo triádico do aparelho psíquico. O id seria a fonte da energia psíquica. É formado pelas pulsões - instintos, impulsos orgânicos e desejos inconscientes. Funciona segundo o princípio do prazer, ou seja, procura sempre o que produz prazer e evita o que é desagradável (Wikipédia, 2019).

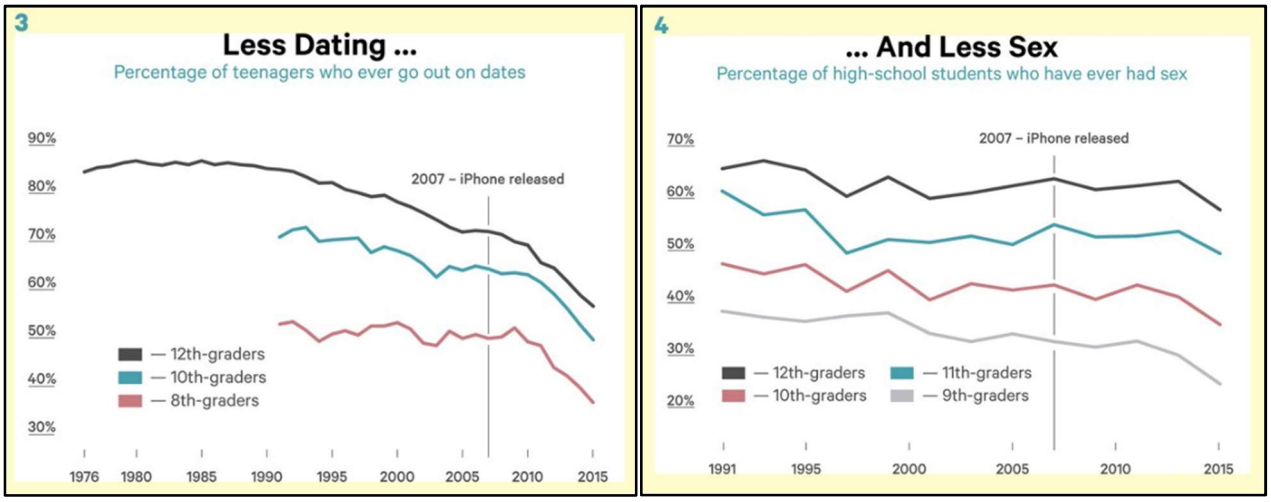
há uma antena da rede celular, há adolescentes vivendo as suas vidas nos *smartphones*". Os níveis de depressão aumentaram, saem menos de casa, namoram menos, começam a sua vida sexual mais tarde, guiam menos, trabalham menos para terem dinheiro e independência, estão menos com os amigos, claro está que a conjuntura também mudou, como tudo à sua volta, mas agora podem estar no seu telefone, no seu quarto e muitas vezes angustiados. Apesar de todo o poder para ligar os jovens, as redes sociais e todas as outras formas de comunicação, permitidas pelos telefones e suas aplicações, também exacerbam a sensação (preocupação) tão adolescente de ser deixado de fora.

Neste longo artigo (Twenge, 2017), além da discussão e casos apresentados, são apresentados dados estatísticos para os E.U.A. muito interessantes, para esta "geração do *smartphone*", onde a "presença da Internet, particularmente as redes sociais, está a mudar o comportamento e atitudes dos adolescentes", ver Figuras seguintes.



Figuras 40 - 41 – Vezes por semana que os adolescentes saem sem os pais, percentagem de alunos do 12º ano que guiam (Twenge, 2017).

Os gráficos mostram que o aparecimento e, posteriormente, generalização dos *smartphones* têm impactos marcados, em vários aspectos da vida dos adolescentes, menos convívio directo com amigos, menos namoros e sexo, menos actividades exteriores, solidão, exclusão e menos sono. Segundo o autor, quando perguntou aos seus alunos na Universidade o que faziam com o telefone à noite, as respostas foram um "perfil em obsessão: quase todos dormiam com o telefone, debaixo da almofada, no colchão, ou à distância de um braço da cama. Verificavam as redes sociais antes de dormirem, procuravam o telefone assim que acordavam (todos o utilizavam como despertador). O telefone era a última coisa que viam antes de adormecer e a primeira que viam depois de acordar. Se acordavam a meio da noite, frequentemente, acabavam por olhar para o telefone. […] Viam o telefone como uma extensão do corpo, ou até como um amante: «ter o meu telefone mais perto de mim enquanto durmo é um conforto»".



Figuras 42 - 43 – Percentagem de adolescentes que namoram e que já iniciaram a sua vida sexual (Twenge, 2017).

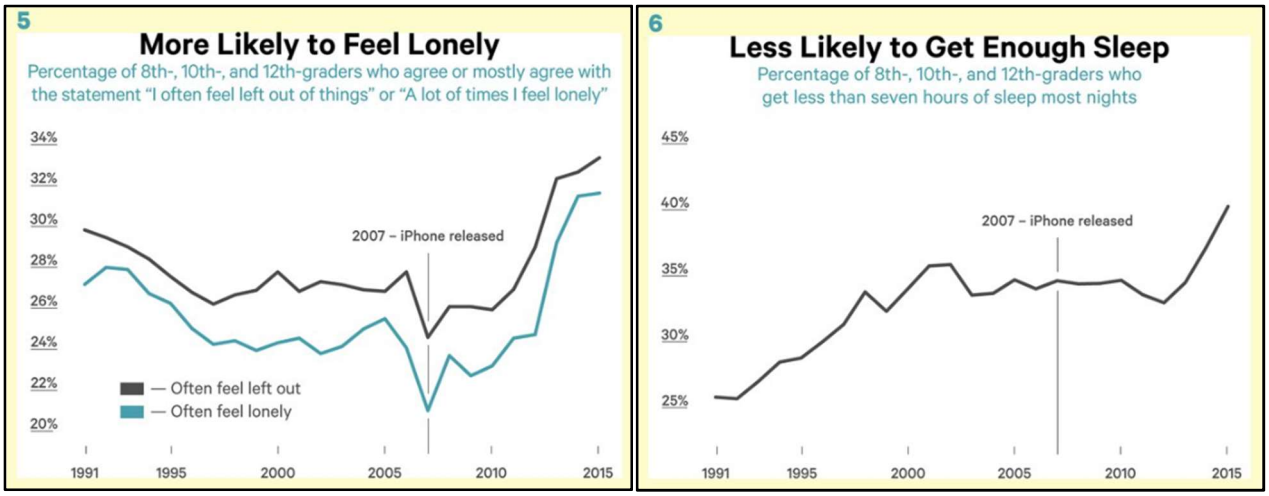


Figura 44 - 45 - Percentagem de adolescentes que se sentem excluídos e sozinhos e percentagem de alunos que dormem menos de sete horas por noite (Twenge, 2017).

Se passarmos dos adolescentes para os mais novos, em geral, a indústria tecnológica está a "fazer uma guerra às crianças", utilizando a psicologia como uma arma (Freed, 2018), levando-as a desenvolver uma ligação fortíssima e doentia com os *smartphones*, que também são porta de acesso aos jogos e redes sociais. Segundo o autor, "Os pais não fazem ideia de que, espreitando por trás dos ecrãs e telefones das suas crianças, estão uma multidão de psicólogos, neurocientistas e especialistas em ciências sociais, que utilizam o seu conhecimento das vulnerabilidades psicológicas, para conceberem produtos que capturem a atenção das crianças em nome do lucro da indústria. O que estes pais e a maior parte do mundo têm, ainda, de compreender, é que a psicologia – uma disciplina que associam a cura – está agora a ser usada como uma arma contra as crianças".

Esta "tecnologia persuasiva", que configura máquinas digitais e aplicações – *smartphone*s, redes sociais e videojogos - para alterar os pensamentos e comportamentos humanos, constrói "máquinas concebidas para mudar os humanos". Esta tecnologia funciona, criando ambientes digitais que os utilizadores sentem como preenchendo os seus desejos e objectivos, melhor que as alternativas no mundo real. "As crianças ficam horas *online* em redes socias e jogos em busca de *likes*, «amigos», pontos ou níveis – porque isso é estimulante, acreditam que isso os torna felizes e bem-sucedidos, além de isto ser mais fácil do que fazer as importantes, mas difíceis, actividades de desenvolvimento da infância".

Estes produtos criam dependência, como se de drogas se tratassem, manipulam psicologicamente, tentam absorver completamente a pessoa e afastá-la do mundo real, prendendo-a a tecnologias de entretenimento (segundo o autor, um estudo refere que nos E.U.A. as crianças passam cinco horas e meia por dia neste ambiente, jogos, vídeo, redes sociais). Pode-se ver esta ligação constante ao ecrã na vida quotidiana, muitas vezes com a "ajuda" dos pais, em espaços públicos, restaurantes, no trânsito, quando estão em conjunto: as raparigas mais ligadas às redes sociais, os rapazes, aos jogos. "Há pessoas que se preocupam com a inteligência artificial. Perguntam como podemos maximizar o seu potencial sem prejudicar os interesses humanos. Mas a inteligência artificial já aí está. Chama-se Internet. Libertámos esta caixa negra, que está sempre a desenvolver novas formas de nos persuadir a fazer coisas, deslocando-nos de uma transe para a próxima" (Leslie, 2016).

Segundo um estudo da ERC[132] (Entidade Reguladora para a Comunicação Social), referido por Ponte & Castro (2019), as crianças começam cada vez mais cedo a ter imenso tempo de ecrã, sejam jogos, *streaming* de vídeo ou televisão. Todas vêm televisão, metade joga jogos digitais e 38% usam a Internet (estamos a falar de crianças entre 3-8 anos de idade), gerem já uma imensa pegada digital, sem se aperceberem. Os pais começam cedo, todos o vimos em espaços públicos, consultórios, restaurantes, a expor os filhos aos ecrãs, para os calar, sossegar, distrair.

Os pais partilham, também e desde cedo, fotos dos filhos, o *sharenting* "fotografias captadas para um dado momento de conexão, não para passarem de geração em geração. O seu uso efémero contrasta com a possibilidade de permanência trazida pelo digital, mas talvez a maior mudança decorra da pressão para a partilha, como se quem não (se) mostra na rede não tenha existência. O termo *sharenting* – que dá conta do abuso da partilha (*share*) de comentários ou imagens dos filhos nas práticas dos pais (*parenting*) […] Num recente questionário feito em Portugal, 28% das crianças e jovens (9-17 anos) assinalaram que os pais tinham publicado coisas sobre eles sem lhes

[132] Crescendo entre ecrãs – Usos de meios electrónicos por crianças (3-8 anos), http://www.erc.pt/documentos/Crescendoentreecras/mobile/index.html#p=1

perguntarem se antes concordavam [metade pediu aos pais para o retirarem]" Ponte e Castro (2019).

Concluindo, por mais que se aponte o dedo à dependência e uso constante de *smartphones* pelos jovens e crianças, os pais foram vítimas do mesmo" encantamento" e criaram, sem o consentimento dos filhos, enormes pegadas digitais deles, mesmo antes de os próprios terem acesso à Internet. Os pais, portanto, devem ter uma série de cuidados para evitar expor os filhos, identificá-los, violar a sua privacidade, antes de eles se tornarem cidadão digitais munidos dos seu próprios *smartphones*.

Outro problema associado aos *smartphones* é o facto de eles conterem uma enorme quantidade de informação, altamente sensível e pessoal, a todos os níveis, bem como as chaves de acesso a inúmeros serviços *online* (bancos, redes sociais, contas de *email*, serviços de *backup* na nuvem, etc., etc., etc.). Acedendo-se a um telefone, legalmente, pela força ou roubando-o, acede-se a TODA a vida *online* de qualquer pessoas, à sua pegada digital, à sua vida, *tout court*. Por essa razão, no contexto dos tempo securitários (necessários) em que vivemos actualmente, e que para "muitos" convém prolongar e manter, alguns países, como os E.U.A. e o Canadá, passaram a poder "pedir" (exigir) acesso aos *smartphones* (tablets e portáteis) de cidadãos à entrada das suas fronteiras, bem como acesso a contas de redes sociais[133].

Imagine, o que tudo o que tem nos seus dispositivos digitais diz sobre si, o que diz e faz *online*, por aí a fora. O argumento de que "quem não deve não teme" não pode ser levado a estes extremos, sendo fácil encontrar na Internet "sugestões" para contornar esta violação de privacidade[134]. Também se encontra bastante informação relativamente aos direitos das pessoas nessas circunstâncias, mas o simples facto de ser legalmente possível deveria levar-nos a pensar, seriamente, em privacidade e no uso que cada um faz do seu *smartphone*.

Embora se percebam as boas intenções, a polícia também passou a exigir (nalguns países) acesso aos telefones de vitimas de crimes, no Reino Unido causou revolta e indignação (Maio de 2019), uma regra que obriga vitimas de violação a dar acesso total aos *smartphones* e contas de redes sociais, sob pena de não serem consideradas as queixas[135], o que é revoltante.

---

[133] https://www.cbc.ca/news/business/cbsa-boarder-security-search-phone-travellers-openmedia-1.5119017, https://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746 , https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html

[134] https://privacysos.org/blog/social-media-privacy-at-the-border/ , https://www.eff.org/press/releases/digital-privacy-us-border-new-how-guide-eff , https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/ https://www.theverge.com/2017/2/15/14629022/border-search-customs-data-privacy-encryption

[135] https://www.theguardian.com/society/2019/apr/29/new-police-disclosure-consent-forms-could-free-rape-suspects?fbclid=IwAR06rJX2BFNBo4pUHPH_8o%E2%80%A6 , https://edition.cnn.com/2019/04/28/uk/rape-claimants-phones-police-gbr-intl

Um último aspecto a ter em conta, relativamente aos *smartphones*, resultante da sua dimensão, versatilidade e de se ter tornado um prolongamento digital das pessoas, no seguimento do que até aqui foi discutido, é o perigo real de roubo, seja o roubo físico, seja "entrar" no telefone e ter, assim, acesso a tudo o que ele contém e tudo aquilo a que dá acesso. Por um lado estes dispositivos têm preços muitos elevados (500-1000€ na maior parte dos casos), levando os compradores a racionalizarem um conjunto (mais ou menos válido) de razões para justificar a sua compra, "o telefone é o meu computador, preciso dele para o meu trabalho/emprego, dividindo o custo pelo uso que tem vale a pena, estou a testar o futuro, quero o melhor, posso pagá-lo" (Goode, 2019).

Os *smartphones* são, efectiva e comprovadamente, um alvo altissimamente apetecível para cibercriminosos, pois são "uma parte central da nossa vida e permitem-nos fazer todo o tipo de tarefas quotidianas, facilitando a nossa existência diária e tornando-a mais agradável" (ESET, 2017). As razões pelas quais os telefones são um alvo tão apetecível para os criminosos, apontadas por esta empresa de segurança, podem ser resumidos nos seguintes tópicos:

1. **Um *smartphone* sabe tudo sobre nós** – A quantidade de informação guardada é gigantesca, tem aumentado e continua a aumentar, a conectividade das aplicações significa que fornecemos quase toda a informação possível sobre nós, sejam detalhes de contas bancárias, ou preferência do tipo de pizza. Para um cibercriminosos que queira, potencialmente, praticar roubo de identidade, um *smartphone* é uma mina;
2. **É uma forma de aceder a empresas e organizações** – A práticas de incentivar o uso dos dispositivos pessoais em empresas é generalizado globalmente [BYOD – *Bring Your Own Device*[136]], num estudo de 2015, 74% das empresas a nível mundial já tinham adoptado ou planeavam adoptar esta política, assim, os cibercriminosos vêm estes dispositivos como uma porta ideal para aceder e roubar informação empresarial, ou das organizações;
3. **A segurança pode ser relaxada** – O aumento da política de BYOD trouxe inúmeras dores de cabeça a um grande número de empresas em várias indústrias, sobretudo pela dificuldade em ter uma abordagem unificada à segurança. Num recente inquérito a executivos e trabalhadores das tecnologias de informação, 45% responderam que os dispositivos móveis constituíam o maior risco para a infra-estrutura das empresas, sendo a natureza fragmentada de muitas plataformas citada como razão principal;
4. **O autopreenchimento tornou-se o nosso melhor amigo** – Uma das razões pelas quais os *smartphones* (mas não só) carregam cada vez mais informação pessoal consigo, deve-se ao nosso desejo de conveniência, com tantos serviços e aplicações, existem cada vez mais dados e detalhes de autenticação. Consequentemente, é fácil ser preguiçoso, decidindo muitos de nós activar os sistemas de autopreenchimento de formulários de todos os tipos, o que na maior parte dos casos aumenta os riscos de segurança;

[136] https://www.thebalancecareers.com/bring-your-own-device-byod-job-policy-4139870

5. **É um caminho para a nossa carteira** – Os telefones podem ser utilizados para transferir dinheiro, pagar contas e, até, como método de pagamento, como tal são uma alvo apetecível, sobretudo com a banalização desse tipo de aplicações e do seu uso**;**
6. **Os telefones sabem onde estamos e onde trabalhamos** – Como já referido, as vantagens obtidas com a geolocalização e S.B.L. são grandes, maximizando a utilizada de aplicações e dados, ter acesso a toda essa informação pode ser muito perigoso;
7. ***Bluetooth*** - A facilidade com que se liga um telefone a outros dispositivos por *Bluetooth*, nos carros em modo sem-mãos, a colunas, computadores, cria também uma linha de acesso, que pode ser explorada para obter informação privada (*Bluebugging e Bluesnafing*[137]). Actualmente, a exploração deste tripo de métodos, tem-se tornado mais difícil;
8. **Alguns casos são específicos dos dispositivos móveis** – Por exemplo infecções com *malware*, que levam o telefone a fazer chamadas com custos elevadíssimos, estas tramóias são muito lucrativas e facilmente disseminâveis a um grande número de dispositivos;
9. **São uma grande forma de enviar *spam*[138]** - Todas as pessoas detestam *spam*, menos os cibercriminosos, por várias razões, mas os *smartphones* são a plataforma ideal para o fazer, pois é muito difícil aos ISP rastrear quem são e bloqueá**-**los;
10. **Os utilizadores são ignorantes relativamente aos perigos** – Muitos dos utilizadores de tecnologia conhecem (ou deviam) as melhores práticas para o uso de computadores ou portáteis, mas os *smartphones* descem na lista de prioridades, o que em muitos casos é surpreendente, pois são cada vez mais alvos (fáceis).

GPS

O sistema GPS mudou completamente a forma como cartografamos o mundo, como nos deslocamos e como vivemos (Massey, 2019), mas será que o uso, generalizado e banal, de dispositivos com capacidade de geolocalização está a mudar a nossa sensibilidade à importância dessa informação? Será que está a mudar os nossos cérebros, sentido de orientação e percepção do espaço? Tornámo-nos cartógrafos? Vamos tentar aflorar estas questões, caras para os geógrafos e que são uma consequência directa, uma vez mais, da existência de *smartphones* que se conseguem "localizar" por vários meios.

As possibilidades dos equipamentos transformaram os dados de localização, "num produto em si. No reino dos criadores de software, o espaço-lugar foi reduzido e discretizado a um conjunto de coordenadas, desprovido de experiência humana e significado" (Rzeszewski & Luczys, 2018). Isto

[137] Bluebugging – forma de ataque através de *Bluetooth*, causada frequentemente por falta de noção de quem mantém ligações abertas, num raio de 10-15 metros, permitindo controlar o dispositivo e aceder a informações, ouvir chamadas, etc. (Wikipédia, 2019).

[138] Spam - pode ser um acrónimo derivado da expressão em inglês "Sending and Posting Advertisement in Mass", traduzido em português "Enviar e Postar Publicidade em Massa", ou também Stupid Pointless Annoying Messages que significa mensagem ridícula, sem propósito, e irritante (Wikipédia, 2019).

levou as pessoas a, resignadamente, desvalorizarem a importância destes dados, aceitando entregá-los como moeda de troca por aquilo que se obtém em S.B.L. (Serviços Baseados em Localização). Num complexo estudo feito pelos autores, há vários tipos de atitudes dos utilizadores, quanto ao uso de dados de geolocalização quotidianamente, que podem ser agrupados nos "temas" seguintes;

- **Utilidade** – Atitudes positivas ou entusiásticas em relação a S.B.L., geralmente pessoas com conhecimento tecnológico, desconhecendo quase totalmente o papel da geolocalização nos serviços móveis e apropriação de dados. Não se preocupam com as consequências ou perigos de partilhar a sua localização, na sua perspectiva a tecnologia só traz avanços e utilidade, não vendo razão para reflectir sobre o assunto. As opiniões expressas são estereotipadas, e.g. associar exclusão digital com idosos e pobres. Usam e frequentemente produzem conteúdo de redes sociais geolocalizado alegremente e sempre que possível;
- **Programabilidade** – Atitude emocional neutra, semelhante à utilidade, as pessoas neste grupo não temem as consequências da divulgação da localização, mas sentem muito menos a necessidade de utilizar essa possibilidade. Percepcionam os S.B.L. como só mais uma inovação tecnológica que têm ao seu dispor, uma ferramenta, mas não um brinquedo. Não "brincam" com dados geolocalizados nas redes sociais, se usam S.B.L. é para efeitos muito concretos e terra-a-terra, e.g. navegação. Não reflectem no papel da apropriação de dados de geolocalização e possuem pouco conhecimento de tecnologia, não surpreendentemente, quase nunca produzem conscientemente conteúdo geolocalizado;
- **Cabeça e coração** – Neste tema agrupam-se pessoas que que mostram uma atitude emocional positiva, mas também possuem um muito maior grau de conhecimento do que nos temas anteriores. Reflectem muito mais frequentemente no papel dos S.B.L. na sociedade, esta reflexão pode ser descrita como cautelosamente optimista, com a tecnologia de localização a ser percepcionada como problemática, mas bastante promissora. Este ponto de vista, contudo, não os leva a participar na produção de conteúdo geolocalizado;
- **Actividade** – Neste caso, a produção de conteúdo forma o eixo principal em torno do qual o tema é criado. As pessoas neste tema têm uma atitude emocional predominantemente positiva e um nível de conhecimento tecnológico sobretudo alto, mas misto. Têm uma boa compreensão dos mecanismos dos S.B.L. e utilizam-nos para objectivos específicos. Este tema é marcadamente diferente da programabilidade porque há um aspecto emocional envolvido na equação – a ligação com os S.B.L. Estes serviços e aplicações desempenham um papel muito importante nas actividades quotidianas destas pessoas, têm o conhecimento de como utilizar S.B.L. para os seus objectivos e sentem que têm tudo sob controlo. A reflexão está presente, embora não em todos os tipos de atitudes que formam este tema, o qual não está associado a nenhum tipo de atitude emocional particular;
- **Privacidade** – Este tema é drasticamente diferente dos outros quatro porque consiste, unicamente, em atitudes que são emocionalmente negativas em relação aos S.B.L. As pessoas

neste tema não produzem conscientemente conteúdo geolocalizado e optam, activamente, por não utilizar serviços que permitam ou exijam partilha de informação de localização. Também temem o que pode ser feito, com os dados que involuntariamente fornecem. Esta ansiedade é sobretudo associada à falta de conhecimento sobre o funcionamento técnico dos serviços de localização e as práticas empresariais dos seus criadores e fornecedores. Contudo, neste tema também se encontram pessoas que têm conhecimento técnico moderado ou até avançado. Pessoas que usam API's[139] de geolocalização na sua vida diária e têm experiência em SIG[140] podem pertencer a este grupo, se têm uma atitude negativa, ela é motivada pelas suas experiências de apropriação de dados.

O leitor, pertence a que grupo? Só a um deles? A vários? Encontra-se entre temas ou completamente num deles? A sua atitude é sempre a mesma, ou varia consoante os S.B.L.? Essa atitude foi sempre a mesma? Mudou quando? Porquê? Enfim, muitas questões de resposta altamente pessoal e que pressupõem, certamente concordarão, uma reflexão séria, ponderada e com tempo.

Uma das questões preocupantes, para a maioria dos utilizadores de *smartphones* e S.B.L., é saber que muitos dos escândalos de fugas – roubo de dados de geolocalização podiam ser evitados, ou combatidos, num mundo com menos desregulamentação e estados mais fortes. Segundo Bode (2019), os E.U.A. são um *wild west* em termos de privacidade dos consumidores, não havendo leis verdadeiramente da era da Internet relativas a privacidade, depois de vários escândalos[141], estando o resto do mundo (desenvolvido) na mesma ou pior. O autor refere que a maior parte da afronta é contra o Facebook, mas refere que os operadores móveis têm práticas tão, ou mais, graves, para rastrear os utilizadores na Internet.

Os dados de geolocalização são usados pelas autoridades, para gerar lucro, roubados, deixados à vista, mas, no fundo, quanto menos informados e mais apáticos estiverem os consumidores, com menos consciência do que se passa melhor para as empresas. "Um consumidor informado, com poder, tem muito mais probabilidade de não permitir a recolha de dados e sua monetarização, custando milhares de milhões às empresas" (Bode, 2019).

Sabemos que o sistema GPS e dispositivos associados mudaram, até, a forma como pensamos acerca do planeta, graças ao seu uso no domínio da geodesia, os mapas têm um rigor e precisão

[139] API – Aplication Programming Interface – como a API do Google Maps, ver nota de rodapé Nº 62.
[140] SIG - Sistemas de Informação Geográfica - Sistema de hardware, software, informação espacial, procedimentos informáticos e recursos humanos que permite e facilita a análise, gestão ou representação do espaço e dos fenómenos que nele ocorrem (Wikipédia, 2019).
[141] O autor dá três exemplos: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win , https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning , https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

nunca vistos e até o movimentos das placas ou as deslocações verticais da litosfera, provocadas por sismos, podem ser medidas com um rigor enorme (Blitz, 2017). Convém lembrar a importância do sistema nestes domínios, embora fora do âmbito deste texto, pois a maioria esmagadora das pessoas utiliza dispositivos GPS exclusivamente para se localizar e/ou orientar. Visto que isso é, agora, possível de uma forma continua e ubíqua, graças aos *smartphones*, mesmo sem rede móvel disponível, estará a nossa capacidade de orientação a mudar? A nossa percepção do espaço? Os nossos cérebros? Isso representa um perigo real?

Segundo Milner (2016a), a maior parte dos incidentes com GPS não leva à morte (há excepções[142]), "são acidentes ou viagens acidentais resultantes duma aceitação acrítica dos comandos *turn-by-turn* do GPS: os turistas japoneses na Austrália guiaram o carro para o oceano enquanto tentavam chegar a uma ilha[143]; o homem que conduziu um BMW, por um caminho estreito no Yorkshire[144], quase caindo de uma arriba; a mulher em Bellevue, Washington, que guiou o seu carro para dentro de um lago que o GPS dizia ser uma estrada; o casal sueco que pediu ao GPS para os guiar até à ilha de Capri no Mediterrâneo, mas que ao invés disso chegaram à cidade industrial de Capri, no norte da Itália[145]; a idosa na Bélgica que tentou usar o GPS para a levar a Bruxelas, a 145 km da sua casa, mas acabou percorrendo centenas de quilómetros até Zagreb, só percebendo o erro quando reparou que toda a sinalização era em Croata[146]".

Um outro caso, que tornou um turista conhecido na Islândia (Kushner, 2016), resultou de uma informação mal introduzida no GPS, que vinha com o carro de aluguer e que o levou a centenas de quilómetros do destino desejado, tendo-se perdido completamente, levantando a questão de como tal é possível. Será que o uso, tão banalizado e constante do GPS, diminuiu as nossas capacidades de observação e estreitou o nosso mapa cognitivo[147]?

Um estudo inglês de 2006 revelou que os cérebros dos taxistas de Londres, cuja obtenção de licença exigia demonstrarem que conheciam cerca de 25 mil nomes de ruas, pontos de referência e de interesse, tinham mais matéria cinzenta na região do hipocampo, responsável pela complexa representação espacial, que os cérebros dos condutores de autocarros, ou seja, o volume de

[142] https://www.interculturalnews.com.br/2015/10/o-caso-da-jornalista-que-foi-morta-apos.html , ou https://www.sacbee.com/entertainment/living/travel/article2573180.html ou https://www.methodshop.com/2016/12/death-by-gps.shtml ou https://www.mirror.co.uk/news/world-news/man-watches-wife-burn-alive-5435575

[143] https://abcnews.go.com/blogs/headlines/2012/03/gps-tracking-disaster-japanese-tourists-drive-straight-into-the-pacific/

[144] http://news.bbc.co.uk/2/hi/uk_news/england/bradford/7962212.stm

[145] http://news.bbc.co.uk/2/hi/europe/8173308.stm

[146] https://www.telegraph.co.uk/news/worldnews/europe/belgium/9798779/GPS-failure-leaves-Belgian-woman-in-Zagreb-two-days-later.html

[147] Tipo de representação mental, que serve para um individuo adquirir, armazenar, relembrar e descodificar informação acerca das localizações relativas e atributos dos fenómenos nos eu ambiente espacial quotidiano ou metafórico. O conceito foi introduzido em 1948 por Edward Tolman. (Wikipédia, 2019).

matéria cinzenta diminuía quando a capacidade não era utilizada (Milner, 2016a)(ver Figura 46). Será que o uso do GPS pode levar a isto?

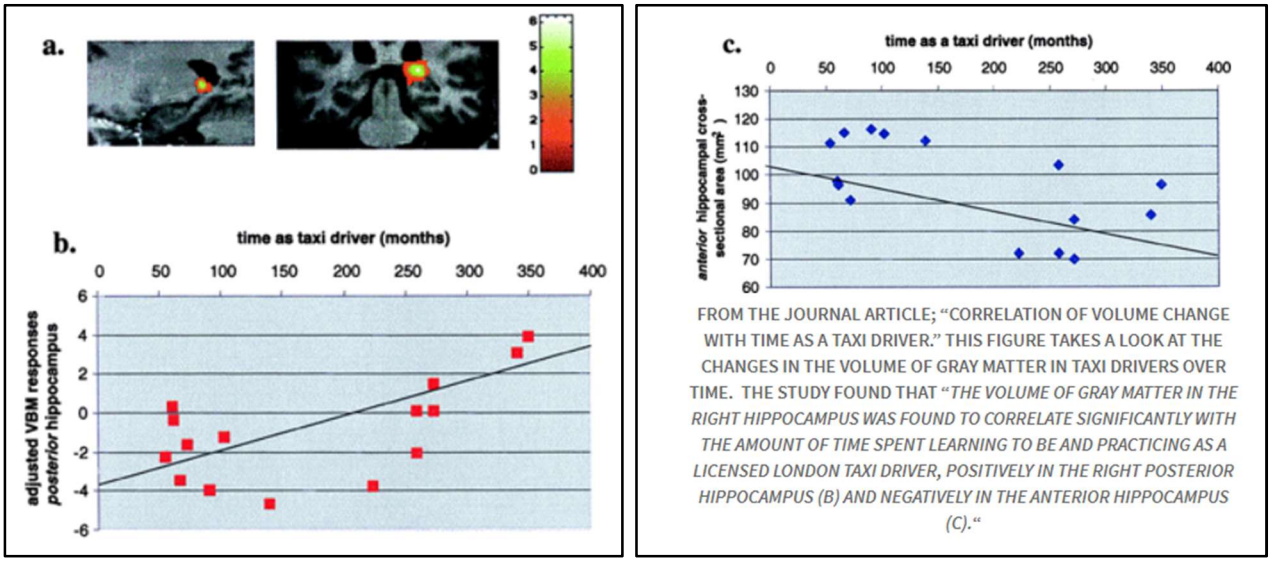


Figura 46 – Correlação entre a mudança do volume de massa cinzenta, como taxista, com o tempo como taxista, positiva no hipocampo posterior direito, negativa no hipocampo anterior (Maxwell, 2013).

Segundo o mesmo autor, vários estudo confirmam esta hipótese: um estudo no Japão, em 2008, demonstrou que entre três grupos de caminhantes numa cidade, um aprendeu directamente o caminho, outro tinha GPS o terceiro um mapa, o grupo com GPS tinha a menor capacidade de encontrar o caminho, caminhavam mais devagar e faziam mais paragens para se reorientar. Acresce que, depois das tarefas, eram o grupo com pior classificação, na memória da configuração e topologia da rota. Outro estudo, feito pela Universidade de Cornell em 2008, analisou o efeito em condutores e chegou às mesmas conclusões: falta de envolvimento com o ambiente, pois o GPS eliminava grande parte da necessidade de prestar atenção ao que se passa na envolvência.

Se o GPS faz tudo por nós, deixamos de construir mapas cognitivos, deixamos de ter de decidir, não registamos pontos de referência no caminho. "Num nível humano fundamental, nós necessitamos de mapas. Um estudo alemão descobriu que a capacidade das pessoas para apontar na direcção de pontos de referência era maior quando estamos virados para Norte. As pessoas estavam, de facto, a organizar as relações espaciais como num mapa de papel, que geralmente tem o Norte no topo. Os mapas físicos ajudam-nos a construir os mapas cognitivos" (Milner, 2016b).

Uma outra abordagem ao mesmo problema, indica que se o *smartphone* é o nosso segundo cérebro, quando seguimos indicações de navegação graças ao GPS, a parte do nosso cérebro que trata da navegação fica em descanso (Gholipour, 2017). O GPS interno do cérebro é uma das

suas maravilhas, o estudo das células nervosas especializadas, que registam nos ratos a sua localização no espaço, levou ao Prémio Nobel da Fisiologia ou Medicina em 2014, essas células estão no hipocampo.

Numa experiência de navegação simulada[148], no Soho em Londres, com a actividade cerebral de 22 participantes medida e controlada, naqueles que navegavam por si, sem GPS, a actividade do hipocampo e do córtex pré-frontal era muito maior e ligada ao planeamento e tomada de decisões (Condliffe, 2017). "Crianças que crescem com os seus *smartphones* podem desenvolver um conjunto diferente de capacidades, em relação às gerações de pessoas que aprenderam, primeiro a navegar naturalmente nas suas redondezas, ou a memorizar informação em vez de procurar tudo *online*" (Gholipour, 2017). É uma questão, também de bom-senso e pensamento crítico, bem como de capacidade de observação que se perde com a facilidade em procurar,

Mas e a velha questão de género, relativamente à capacidade de orientação e navegação? Vários estudos demonstram que os homens e mulheres utilizam estratégias diferentes quando tentam navegar (Maxwell, 2013). Num estudo feito na Holanda, em que se pediu a homens e mulheres para encontrar o caminho para os seus carros, num parque de estacionamento cheio, os homens tendiam a utilizar mais termos relacionados com distâncias, enquanto descreviam a rota, enquanto as mulheres mencionavam também pontos de referência. Embora os homens costumem ser melhores a ler e utilizar mapas, as mulheres costumam chegar primeiro ao seu destino, pois são melhores a lembrar-se de pontos de referência e, consequentemente, têm menos probabilidades de se perder.

Segundo o mesmo autor, outros estudos demonstram que os homens e mulheres desenvolvem diferentes métodos de navegar e se orientarem no ambiente espacial, por causa dos diferentes papéis de caçadores e recolectores, o que poderia explicar "a razão pela qual os homens se perdem em supermercados, enquanto as mulheres encontram o caminho em minutos. [...] Os homens são melhores a encontra objectos escondidos, enquanto as mulheres são melhores a lembrarem-se onde esses objectos estão" (Maxwell, 2013).

No início, os dispositivos GPS eram muito para o mar, caminhadas, desertos, depois estradas, mas a inclusão nos *smartphones* foi o que permitiu, verdadeiramente, o seu uso generalizado em meio urbano. Um dos aspectos interessantes, a que se dá pouca importância, é a capacidade de orientação automática e auto-centragem dos dispositivos (Grabar, 2014) e que define as capacidades de direccionamento *online* e com GPS. A orientação automática (se se escolher essa opção no equipamento), corresponde à perspectiva do utilizador enquanto se desloca, o que é muito diferente de estar orientado a Norte; o mapa auto centrar-se leva à organização em torno da localização do utilizador e isto elimina uma grande parte do esforço mental de leitura de mapas.

[148] https://www.nature.com/articles/ncomms14652

Claro está que, centrar os mapas onde se está, é comum e prática corrente, o célebre "você está aqui" com um circulo e/ou ponto, além da tendência ancestral de central mapas-mundo na posição do cartógrafo, mas esta capacidade é prática e permite que naveguemos sem andar a rodar mapas a cada esquina, ou com o topo para baixo e todo o texto ao contrário com difícil legibilidade. "Já não temos que «ler» mapas como fazíamos. Mas é quase certo que passamos muito mais tempo a olhar para eles. Para cada cientista cognitivo, a observar a conectividade a diminuir os nossos talentos de percepção, conhecimento e resolução de problemas, há muitos mais miúdos a explorar a Terra nos seus computadores [ou *tablets*, ou *smartphones*]" (Grabar, 2014).

Convém ter noção de um problema potencial, segundo Truscot (2019), "o uso do GPS em vez de mapas é a troca de tecnologias com mais consequências na história, os mapas não podem ser pirateados [*hacked*], mas os GPS sim. Pagaremos por isso um dia". Há menos mapas à venda, menos (ainda menos…) pessoas a comprar mapas, a saber lê-los e utilizá-los então nem é bom pensar. Quando o serviço militar era obrigatório, pelos menos os rapazes eram forçados a saber localizar-se, orientar-se e navegar com cartas militares. Sabe-se que se pode bloquear e interferir com os sinais GPS, há aparelhos baratos para o fazer, inibindo a determinação de posição num determinado raio[149], a China[150], a Correia do Norte[151], a Rússia[152] fazem-no, bem como os donos do sistema, os E.U.A.[153].

Um sistema sofisticadíssimo, caro, mas que é vulnerável a ameaças de baixo custo (pelo menos a nível local), este facto aplica-se a todos os sistemas, sejam o dos E.U.A., da Rússia, da China ou da U.E., estes países têm testado e usado estas técnicas em conflitos regionais um pouco por todo o mundo, durante exercícios militares ou em testes mais ou menos reconhecidos oficialmente (Cebul, 2018). Os satélites passaram a ser, inclusive, alvo eventual de *hackers* (Gruss, 2018), "um número crescente de actores não estatais tem examinado sistemas de satélites comerciais e descoberto ciber-vulnerabilidades que são semelhantes em natureza às encontradas em sistemas não espaciais".

[149] https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955 , https://www.gps.gov/spectrum/jamming/, https://www.economist.com/international/2013/07/27/out-of-sight , https://www.thesignaljammer.com/categories/GPS-Jammers/

[150] https://rntfnd.org/2016/09/26/china-jamming-us-forces-gps/, https://www.linkedin.com/pulse/china-jamming-us-forces-gps-dana-a-goward

[151] https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/ , https://www.bbc.com/news/world-asia-35940542

[152] https://www.thedrive.com/the-war-zone/20034/the-russians-are-jamming-us-drones-in-syria-because-they-have-every-reason-to-be , https://edition.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html , https://sputniknews.com/military/201903271073573254-russia-gps-spoofing-capabilities/

[153] https://www.theregister.co.uk/2016/06/07/us_military_testing_gps_jamming/ , https://theaviationist.com/2019/02/08/basically-carrier-strike-group-4-is-jamming-gps-across-u-s-southeast-coast/ , https://www.gpsworld.com/u-s-air-force-jamming-gps-in-southwest-sky-this-week-and-next/

Pode-se, facilmente, imaginar os perigos para a navegação aérea, marítima, equipas de socorro, autoridades, etc., tanto a esfera militar como civil são, potencialmente, afectadas. Pode-se até dizer as "Guerras do GPS chegaram, pois, os S.B.L. [Serviços Baseados na Localização] são universais, críticos e horrivelmente vulneráveis" (Braw, 2018). Os bloqueadores de sinais GPS, basicamente, sobrecarregam os receptores com sinais errados (*junk*), impedindo o receptor de captar os sinais reais, uns metros no caso de dispositivos pessoais, regiões no caso dos sistemas testados por países. Ora, com mapas tradicionais e navegação tradicional isto não acontece, mas não deixaria de ser um enorme retrocesso.

A tecnologia GPS acaba, também e consequentemente, por afectar a nossa percepção do espaço e a forma como o cartografamos. Será que a frase "o que interessa é a viagem e não o destino" faz menos sentido, quando a experiência da viagem está a diminuir por causa do GPS? Segundo Altawell (2018), como os dispositivos móveis se transformaram em ferramentas confortáveis e o uso das tecnologias de localização quase uma "segunda natureza", tornando-se praticamente parte de nós, também diminuíram o nosso "sentido de lugar e experiências que, de outra forma, teríamos se navegássemos através de um lugar até ao nosso destino. [...] os dispositivos indicam-nos, geralmente, o caminho mais rápido, mas outras experiências podiam ter um impacto positivo no viajante. [...] A navegação GPS está sobretudo concentrada em evitar aborrecimentos, que nos atrasam, mas não seleccionam as coisas que podem enriquecer a nossa experiência com um local" (ver Figura 47).

A forma como nos envolvemos com os lugares, a experiência que temos do local, também dependem do meio que utilizamos para o explorar, estudos mostram que os mapas promovem mais esse empenho e comprometimento, o que se reflecte em benefícios físicos e mentais, que controlam em absoluto a forma como vivemos e experimentamos os lugares (Altawell, 2018 e Poon, 2015) (ver Figura 48). Segundo o autor, "o que o uso do GPS mostra, é que está a distanciar-nos das experiências do mundo real, que poderiam ter em nós efeitos a longo prazo. Por um lado, isto pode representar que temos experiências menos ricas, mas por outro lado, também pode ter consequências na nossa saúde e bem-estar. As experiências que temos na nossa envolvência enriquecem-nos claramente".

Em função das modificações da percepção do espaço, orientação e capacidades de navegação (juntamente com a comunicação que os *smartphones* permitem), qual é hoje a sensação de se estar perdido, num mundo de mapas digitais e GPS? Beck (2018) resolveu entrevistar várias pessoas que se tinham perdido, antes e depois do uso do GPS, para tentar compreender qual é a sensação, pois mesmo com um dispositivo há erros de cartografia, não há cartografia para a área ou pode não haver rede para carregar mapas *online*.

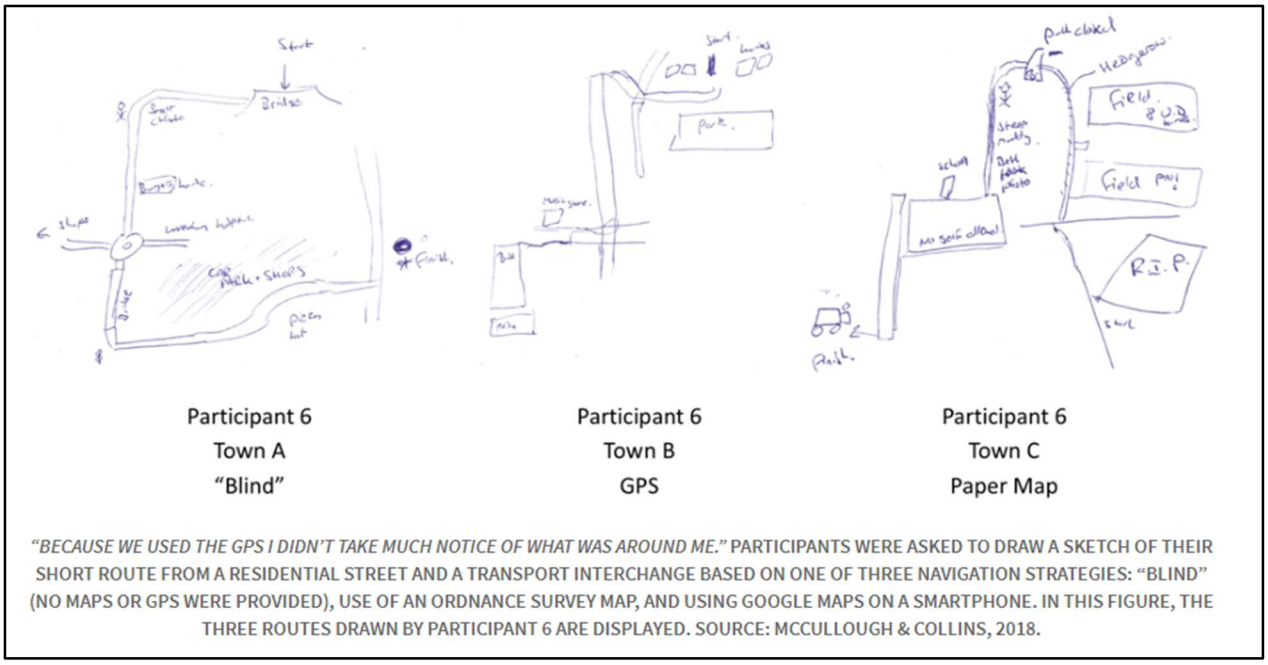


Figura 47 – Mapas mentais de um trajecto urbano, baseados em três estratégias de navegação: cega (sem mapas ou GPS), com mapa e utilizando Google Maps num *smartphone* (Altawell, 2018).

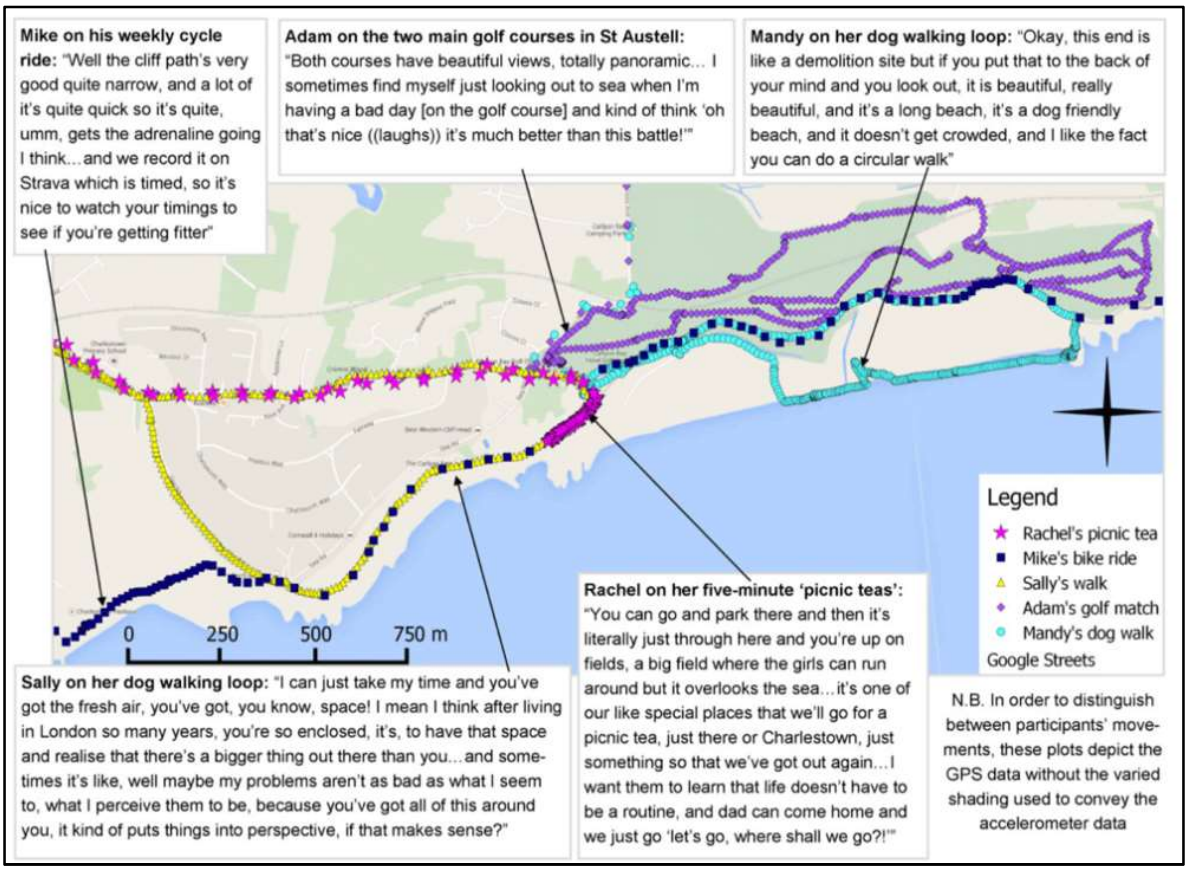


Figura 48 – As diferentes experiências de bem-estar, valorizadas por diferentes participantes numa área (Altawell, 2018).

A conclusão a que a autora chegou foi: "há muitas formas de nos perdermos. Algumas diminuíram com a tecnologia; outros nasceram agora. Mas em cada situação, estar perdido é estar vulnerável. A vulnerabilidade é assustadora, por vezes perigosa, mas também traz ligação – às pessoas [onde as há…] e aos lugares. Os mapas que as pessoas levam nos bolsos podem ser barreiras a essa ligação, mas também são redes de segurança. É mais fácil dar um salto em frente quando sabemos que há algo, em baixo, para nos apanhar".

Um aspecto interessante, outro, e diferente quanto ao uso generalizado de dispositivos com GPS, é o que nos transforma em "cidadãos sensores" (Foody et al, 2017). Como se referiu, quando foi abordado o Open Street Map, os mapas são um bem essencial para inúmeras actividades quotidianas, cada vez mais, necessitando ser actualizados, rigorosos e estarem disponíveis. Se até há pouco tempo, somente autoridades governamentais e agências internacionais os podiam produzir, os desenvolvimentos tecnológicos no domínio da geoinformação e a proliferação de dispositivos altamente móveis, baratos e precisos, permitiu a emergência de uma comunidade de cartógrafos amadores, do cidadão como fonte de dados geográficos. Ao longo dos vários artigos do livro supracitado, pode-se reconhecer todo o potencial existente, mas principalmente as preocupações, sobretudo com a qualidade, rigor e motivação subjacente à recolha dos dados.

Este novo mundo levanta questões quanto a esta Informação Voluntária Geográfica (I.V.G.), pois quase todos os conteúdos gerados por utilizadores se podem situar no contexto geográfico, mas voltam a aparecer, novamente, as questões ligadas à privacidade desses dados. A questão que a IVG levanta, segundo Mooney, Olteanu-Raimond, Touya, Juul, Alvanides & Kerle (2017), é que "quando esta informação é recolhida e subsequentemente disseminada, ela pode ser reutilizada, exposta, integrada e transformada numa miríade de formas. O modelo para compreender o que acontece com os dados, uma vez que são partilhados pelo individuo, ou o que significam, é, portanto, fluído e incerto". Acresce ainda que os cidadãos têm, geralmente, pouca capacidade para compreenderem as relações entre dados e as consequências e questões subjacentes, à recolha de I.V.G., porque este conceito e o de dados abertos [*open data*] são relativamente novos.

Esta capacidade crescente, de cada vez mais pessoas poderem contribuir com informação geográfica e consumirem-na, tem levado os geógrafos a aplicar a teoria crítica, para examinar as implicações de privacidade associadas com o uso constante de dispositivos capazes de geolocalização. Segundo Ricker, Schuurman & Kessler (2014), os geógrafos têm muita esperança de que este uso de *smartphones* seja utilizado para revelar e transmitir conhecimento sobre fenómenos espaciais, através de I.V.G., combinada com S.B.L. (Serviços Baseados em Localização) e mapas interactivos. Para já, as pessoas estão sobretudo a usar os telefones para consumir S.B.L., mais do que para I.V.G. e não o fazem por receios ligados à privacidade.

Mas esse uso, se massificado e centralizado, pode levar a um panóptico[154], "prisão onde o guarda está no centro e pode, ou não, olhar para os prisioneiros em qualquer altura, mas estes sentem-se constantemente observados, metáfora da sociedade em, que hoje vivemos" (Ricker, Schuurman & Kessler, 2014), "big brother is watching you[155]".

Big Brother

Quando Edward Snowden[156] revelou a postura da NSA[157]: "Recolher tudo, processar tudo, explorar tudo, cheirar [*sniff* no original] tudo, conhecer tudo" (Cole, 2014, acerca do livro de Glenn Greenwald), houve quem tivesse ficado espantado, revoltado, preocupado, mas o facto é que a Internet e toda a comunicação ter passado a ser exclusivamente digital, permite um grau de vigilância, intromissão e recolha gigantescos. Os dados são tantos que pressupõem uma análise *Big Data*, por parte de organismos centrais, que levam a: "uma reconceptualização da geoprivacidade e «segurança algorítmica». A geoprivacidade é revelada como uma montagem geopolítica, em vez de algo que se pode possuir, sendo parte de uma política emergente de tecnologia e mercados neoliberais. A segurança tornou-se cada vez mais algorítmica e biométrica" (Crampton, 2015).

Imaginemos então, que além de toda esta vigilância, um país resolve utilizar TODOS os dados da pegada digital dos seus cidadãos, atribuindo pontos a factores ligados: ao crédito, confiança, amigos, actividade física, *posts* feitos em redes sociais, *likes*[158], etc.? A China já o está a fazer, criando um sistema de social de pontuação dos cidadãos, para recompensar ou castigar indivíduos ou empresas dando-lhes (ou não) acesso a serviços públicos, como saúde, viagens e emprego (Samuels, 2019). Mais, aqueles que têm elevada pontuação passam a estar num "corredor verde", tendo acesso mais fácil a oportunidades sociais, enquanto quem tem acções consideradas reprováveis, pelo Estado, ficam paralisados (Sheperd, 2018).

---

[154] Termo utilizado para designar uma penitenciária ideal, concebida pelo filósofo e jurista inglês Jeremy Bentham em 1785, que permite a um único vigilante observar todos os prisioneiros, sem que estes possam saber se estão ou não a ser observados. O medo e o receio de não saberem se estão a ser observados leva-os a adoptar o comportamento desejado pelo vigilante (Wikipédia, 2019).

[155] Big Brother – personagem do livro 1984, de George Orwell, líder de uma estado totalitário, onde os cidadãos estavam sob constante vigilância (Wikipédia, 2019). https://upload.wikimedia.org/wikipedia/commons/6/6b/1984-Big-Brother.jpg

[156] Empregado da CIA e que denunciou informações da NSA (ver nota seguinte), relativamente a um vasto programa de vigilância em conjunto com a vários países, companhias de comunicações e governos da Europa, ver, por exemplo: https://mashable.com/2014/06/05/edward-snowden-revelations/?europe=true

[157] NSA – National Security Agency dos E.U.A., responsável pela monitorização, controlo, recolha e processamento de informação e dados de espionagem e contra-espionagem estrangeiras (Wikipédia, 2019). https://www.nsa.gov/

[158] Likes – manifestações de gosto, feitas em redes sociais várias.

Pensemos, nesse caso, em toda a pegada digital que geramos, Google (ou Apple), Facebook e outras redes sociais, além de buscas feitas *online*, juntemos informação bancária, compras *online*, Amazon, Ebay, etc., tudo junto numa plataforma e controlado por um Estado, de partido único. Não é uma visão distópica, possível, futura, tipo 1984 e o Big Brother, é real. Uma colaboração, assumida, entre empresas de *Big Data* e agências de vigilância governamentais, no ocidente, como seria?

O melhor é olhar primeiro, melhor, para o sistema em vigor na China, um sistema experimental de *ranking* social. Graças aos *smartphones*, os pagamentos foram substituídos por aplicações (Alipay e WeChat Pay), para se poder pagar deve-se agregar cada vez mais informação à conta (carta de condução, matrícula do carro), dados médicos, contas de gás, electricidade, água, Internet, dados bancários, cartões de crédito, etc. (Hvistendahl, 2017). Estas aplicações, por sua vez, ligam-se a outras (tipo AirBnb, Uber, partilha de bicicletas), concentrando ainda mais informação, criando um perfil digital enorme, actualizado continuamente, permitindo (ou não) concessão de crédito (com outra aplicação) em função do "crédito pessoal". Através de códigos QR[159], em lojas, pedintes, campas, serviços, os utilizadores podem ligar a sítios, perfis de redes sociais, fazer pagamentos, ligando de uma forma nunca vista o mundo *online* e *offline*.

O objectivo é ter, até 2020 e para todos os cidadãos chineses, um ficheiro com todos os dados pessoais da pessoa, incluindo dados biométricos, o objectivo deste sistema de crédito social é "uma tentativa de alcançar um sistema autoritário, mais suave e invisível. […] levando as pessoas a ter comportamentos «melhores»". (Hvistendahl, 2017). Juntando dados fiscais, multas, impostos, se são pagos ou não, imagine-se o poder que o sistema tem para "avaliar" o cidadão. O assustador é que o sistema também avalia a pessoa em função das amizades, permitindo subir ou descer na escala, o que entra no domínio da engenharia social, "marcando" a pessoa como estando algures muito ou pouco aquém do seu "potencial". Toda esta informação inclui, também e como é óbvio, dados de geolocalização, que em conjunto com os biométricos permitem reconhecimento facial (permite enviar multas em tempo real, controlar os movimentos, encontrar "criminosos").

Os créditos que são atribuídos inicialmente a cada pessoa podem aumentar ou diminuir, "bom comportamento (desde cuidar da sogra acamada após a morte do marido até andar ou correr x milhares de passos diariamente para manter a forma, oferecer uma televisão a um centro cívico ou ter um filho a fazer serviço militar no Tibete) ou as "perdas" por "comportamento incorreto" (desde cuspir na rua até atravessá-la fora da passadeira, passar muitas horas no computador sem ser a trabalhar, ter amigos "errados" nas redes sociais, demorar demasiado tempo a pagar as dívidas, viajar sem bilhete, passear um cão sem trela, fumar num recinto fechado)" (Moura, 2019).

[159] Ver nota de rodapé Nº 37.

Na sequência desta avaliação, pode-se publicar a pontuação, por exemplo em plataformas de encontros (Mota, 2019), o que permite encontrar cidadãos modelo, alguns são retratados em enormes imagens na via pública, dando conta dos bons exemplos. Na prática este sistema já impediu, por exemplo, 23 milhões de pessoas de comprar bilhetes para viajar (Kuo, 2019), pois estavam em listas negras. A China tem, também, utilizado esta tecnologia e sistema de vigilância maciço para controlar a minoria muçulmana Uyghur, que consideram ser separatistas e terroristas potenciais, impedindo que sejam contactados a partir do exterior, seguindo as suas aplicações de *smartphone*, comunicações, reconhecimento facial e, até, recolha de DNA para construir perfis (Cockerell, 2019).

A meio de Maio de 2019, a Cidade de São Francisco, nos E.U.A., baniu o uso de reconhecimento facial, por agências da cidade, no que se tomou a primeira medida deste género no país (Barber, 2019). Outros estados devem seguir-se, pois o ponto a que a ligação entre dados recolhidos, inteligência artificial e análise *Biga Data*, chegou implica, de facto, vigilância em tempo real dos cidadãos. Vários estudos indicaram que a tecnologia era menos precisa a identificar não brancos, o que a tornava tendenciosa.

No entanto, também nos E.U.A., várias cidades avançam neste momento (Maio de 2019), para sistemas de reconhecimento facial, em tempo real, por exemplo Chicago e Detroit (Barber & Simonite, 2019). Estes sistemas analisam continuamente imagens vídeo, pondo em causa o anonimato em espaços públicos, por exemplo, Chicago tem 20.000 câmaras em ruas e de trânsito. Há várias organizações com muitas dúvidas e receios, o que é natural, pois são os direitos civis dos cidadãos que estão ameaçados com estas tecnologias, sendo que consideram ser tarde demais para impedir a sua proliferação (Newman, 2019b).

Muitas pessoas concordarão com as ideias, bondosas, subjacentes a esta tentativa de classificar os comportamentos sociais dos cidadãos, ou pelo menos penalizar os maus cidadãos, mas conseguem imaginar este grau de controlo? A junção de Estado, tecnologia, pegada digital e *Big Data*? Será que têm noção que estamos todos, em parte, já a "colaborar" activamente?

Leis

Falta abordar um último aspecto, ligado à vida *online* e privacidade: que quadro legal existe? Funciona? Deve sequer existir? Um dos primeiros passos para o debate deveria ser, pelo menos, quem tem uma vida *online* ter noção dos dados que fornece, voluntariamente ou não, da forma como são utilizados e por quem, o que é difícil. Num estudo (WWW Foundation, 2018), feito sobretudo a jovens em países em desenvolvimento, onde a quase totalidade do acesso à Internet se faz em dispositivos móveis, incorporando dados de geolocalização na gigantesca pegada digital

criada, concluiu-se que o uso de redes sociais era generalizado e a quantidade de dados pessoais recolhidos era gigantesco.

Segundo o estudo, os inquiridos, além de verificarem diariamente, pelo menos uma vez, as suas contas nas redes sociais, permitem acesso aos dados sem restrições, não tendo conhecimento que, quando as utilizam, estão a partilhar dados muito além dos que introduzem directamente. A maior parte vê os termos de serviço, mas não os entendem e/ou não os consideram importantes, além disso consideram que a informação e divulgação dos seu dados é um "preço a pagar" pelos serviços e vantagens proporcionados. Paradoxalmente, acham que a privacidade é importante, que a sua informação pessoal é dos dados mais importantes que existem, sentem-se em risco, mas sem serem capazes de se proteger. Ou seja, esta conclusão aplica-se perfeitamente a (quase) todas as pessoas com uma vida *online*.

Será que, como referido por Brookshire (2017), nas redes sociais (especificamente) a privacidade deixou de ser uma escolha pessoal? É que mesmo tomando várias precauções, com o que se publica, quem e o que se identifica, o objectivo e lógica das redes é encontrar amigos e, para o fazer, um dos primeiros passos é importar para as aplicações as listas de contactos: do telefone, do correio electrónico, de outras aplicações ou de outras redes sociais. Esta informação parece inócua, mas a rede social passou a tê-la, quer quem a forneceu tenha concordado em partilhá-la ou não e permite prever detalhadamente uma quantidade enorme de informação que, originalmente, pode não se querer partilhar (e.g. estado civil, localização, afiliação politica ou orientação sexual).

Eventualmente, temos de repensar como entendemos a privacidade, "estamos habituados a ter um espaço privado. Pensamos que temos um quarto com chaves e que deixamos entrar algumas pessoas. [mas uma melhor imagem será] …imaginarmo-nos cobertos na tinta fresca da nossa informação pessoal. Se tocamos alguém, deixamos uma impressão. Quanto mais tocamos outras pessoas, mais marcas deixamos" (Brookshire, 2017), portanto olhando para essas pessoas pode-se chegar à "tinta que nos cobre". Como deixámos de controlar a privacidade, este é um problema que não podemos resolver sozinhos, é um problema de todos.

Começando a questão das leis pelos dados de localização, como se podem implementar Serviços Baseados na Localização (S.B.L.) que respeitem a privacidade? O Regime Geral de Protecção de dados (RGPD), já referido a propósito da pegada digital e direitos dos cidadãos, harmoniza as leis na Europa, mas não explica, a quem concebe e cria as aplicações, como construir sistemas que o respeitem. Por definição, a privacidade é o "direito de um individuo determinar que informação sobre si mesmo deve ser conhecida por outrem. […] Importando também como é obtida e como é utilizada. [podendo ser abordada a três níveis] Nível político, sociocultural e individual. Obviamente, diferentes sistemas políticos e filosofias irão variar, em termos da valorização que dão

à liberdade individual quanto à vigilância, *versus* manter a ordem pública [*vide* China]. Os quadros legais, como o RGPD, são meios pelos quais estes diferentes valores podem ser expressos (Ataei, Debelo, Kray & Santos, 2018).

No caso dos E.U.A., a Quarta Emenda à Constituição, protege a privacidade os indivíduos "direito a estarem seguras nas suas pessoas, casas, papéis e efeitos, contra buscas e apreensões despropositadas" (EPIC.org, 2019), implicando que a forma como se deslocam em espaços públicos e privados está protegida e que, portanto, não devem ser seguidas e vigiadas. Contudo, os dispositivos actuais permitem, largamente e facilmente, recolher, guardar e transmitir esta informação, o que tem consequências quanto aos seus direitos, sobretudo quando nos E.U.A., em 2019, cerca de 90% dos utilizadores de telefones, com mais de 18 anos, recorrem a S.B.L. Tal como na União Europeia, a recolha de dados de geolocalização dos utilizadores, sem os informar ou dar opção de aceitar ou não, é uma ameaça (ilegal) ao direito à privacidade e protecção dos dados pessoais.

Como se discutiu antes, acerca das formas de minimizar os dados de geolocalização, as empresas deviam oferecer a hipótese de não registar ou apagar esses dados, a Google anunciou (1 de Maio de 2019) que ia, "brevemente", incluir uma opção de "auto-apagar" os dados de localização e actividade a cada 3 ou 18 meses (Porter, 2019). Mas os utilizadores devem sempre defender-se, pois a anonimização dos dados pelas empresas (quando é feita) não resolve tudo, podendo (Berzinya, 2018): desligar a localização quando as politicas de privacidade são pouco claras ou específicas; pesar os benefícios, que por vezes não cobrem os riscos associados; só usar a localização para objectivos específicos, desligando-a em seguida; ter muito cuidado com as aplicações que podem aceder à localização; ler e compreender as politicas de privacidade.

A maior parte das empresas que recolhe, trata e vende dados (directa ou indirectamente) estão sediadas nos E.U.A, legalmente, pois para efeitos fiscais estão "por aí", onde mais convém, o que cria problemas a nível de aplicação da legislação. Será razoável esperar, enquanto cidadãos, que a geoprivacidade seja respeitada por empresas e operadores na U.E.? Segundo a Directiva Europeia 2002/58/EC (Privacidade e comunicações electrónicas), Artigo 2(c), dados de localização são: "quaisquer dados processados numa rede de comunicações, indicando a posição geográfica do equipamento [terminal] de um utilizador de um serviço de comunicações electrónico disponível publicamente" (Nouwt, 2008). O preâmbulo da Directiva explica que os dados de localização podem ser tanto longitude e latitude, como direcção de deslocação, nível de rigor da informação de localização, identificação da célula em que o terminal está registado e o tempo e localização do registo (a localização de quem envia e recebe pode ser considerada "dados de tráfego").

Ou seja, a nível de geolocalização, a lei protege o utilizador, mas é importante não confundir privacidade com protecção de dados, que envolve as regras de tráfego (Directiva 95/46/EC),

Comunicações Electrónicas (Directiva 2002/58/EC) e Retensão de Dados (Directiva 2006/24/EC), i.e., os S.B.L. estão abrangidos pela lei SE os dados estiverem a ser processados. Segundo Nouwt (2008), o Tribunal Europeu dos Direitos Humanos reconheceu o direito à privacidade em lugares público, logo, quando a informação é recolhida em lugares públicos, os "governos devem entender que os cidadãos têm expectativas legitimas quanto ao uso da geoinformação".

No entanto, no espaço público há, também, espaços privados, os dados dos utilizadores estão nos equipamentos e em servidores privados, que têm de reter os dados por um certo período, por razões ligadas à segurança, justiça e ordem pública. O problema pode estar aqui, "a distinção entre público e privado pode falhar [...] mas no caso dos dados de geolocalização esta dúvida pode funcionar ainda melhor, pois a privacidade protege as pessoas e não os lugares" (Nouwt, 2008). Nos E.U.A. também há várias directivas, ligadas às comunicações, fraude e privacidade, que protegem os dados recolhidos pelos *smartphones*, num quadro legal, em termos gerais, semelhante à U.E. (Privacy Rights Clearinghouse, 2017).

Qual é o ponto da situação, neste momento em Portugal, quanto aos dados pessoais e sua protecção? Os dados pessoais são (Oliveira & Costa, 2018): qualquer informação que permita identificar um individuo, localização incluída, há dados mais sensíveis e que, portanto, têm protecção acrescida - origem racial ou étnica, opiniões políticas, religião, dados genéticos, orientação sexual, dados sobre saúde (em regra geral o tratamento destes dados é proibido). O que mudou verdadeiramente foi o consentimento, que antes era tácito, com base nas listas ininteligíveis e agora tem que sere explicitamente pedido (daí a vaga que houve de pedidos de confirmação / aceitação de autorização para receber *mails*, newsletters, informação comercial).

A ideia é cada um ter maior controlo sobre os dados, podendo-se pedir para ter acesso aos dados (direito de acesso), pedir para os transmitir a outrem (portabilidade, como nas contas dos operadores móveis), o direito ao "esquecimento", pedir para apagar os dados e a autoridade a quem uma pessoa se pode queixar é a Comissão Nacional de Protecção de Dados[160]. Ainda segundo Oliveira & Costa (2018), o regulamento prevê que haja um atenção especial relativamente às actividades especificamente dirigidas às crianças: para usarem sítios de jogos ou redes sociais as crianças com menos de 13 anos necessitam do consentimento dos pais — o regulamento prevê o limiar dos 16 anos, mas dá aos Estados-membros liberdade para tomar essa decisão. O Governo português defendeu os 13 anos na proposta de lei apresentada, apesar da CNPD e outras entidades preferirem os 16 anos. A questão não está decidida e só deve ficar resolvida com a aprovação da lei que vai adaptar o regulamento à realidade nacional".

Mas será que o RGPD fez ou vai fazer diferença? Segundo Martins (2018) "A resposta mais provável é: não, se não se fizer mais nada. O RGPD impõe novas regras de manipulação e segurança dos

[160] CNPD - https://www.cnpd.pt/

dados pessoais dos empregados e clientes das empresas tradicionais. Isso é positivo pois impõe melhores práticas de segurança que vão ser a pouco e pouco incorporadas nos sistemas empresariais. Mas seria um desperdício inútil impor às pequenas e médias empresas uma transição abrupta, porque a mesma é cara, apressada e provavelmente ineficaz. Naturalmente, a questão é bastante mais sensível para as grandes empresas, com milhares de clientes, e é muito mais relevante para os organismos do Estado que lidam com dados privados dos cidadãos. Consciente da dificuldade de mudar todos os sistemas de uma só vez, o Estado isentou-se *a priori* de multas, o que não deixa de ser digno de alguma hipocrisia".

Segundo o autor, tudo muda de figura com as empresas cujo modelo de negócio depende da Internet, "nomeadamente os media, os serviços de vendas *online*, as plataformas de intermediação (hotéis, viagens, táxis, aluguer de casas, pesquisa de preços, leilões, música, etc.) assim como as grandes plataformas mundiais da Internet: motores de busca, redes sociais, serviços de correio, etc. […] O modelo de negócio vigente na Internet impõe a quebra da privacidade dos utilizadores, a partilha de informações com os anunciantes, a utilização de sistemas de análise de dados que escrutinem o maior número possível de características de cada um de nós. Tempo é dinheiro foi substituído por "conhecer-te bem é dinheiro" e o modelo de negócio vigente conduziu a uma troca de valor profundamente desigual: dá-me os teus dados que eu forneço-te serviços "gratuitos".

Segundo um estudo da Kaspersky (DN Insider, 2019), feito a 11 mil consumidores Europeus, "39% dos utilizadores na Europa estaria disposto a receber dinheiro, retirando algum benefício do "sacrifício" da privacidade. Deste bolo, são os mais novos, entre os 16 e os 24 anos, quem mais estaria disposto a vender os próprios dados (50%). […] Mas também há quem aceite apenas ceder os seus dados para receber algo gratuito em troca – um em cada cinco indivíduos […] 26% dos inquiridos relata que já viu os seus dados serem acedidos por terceiros, sem consentimento. Este valor aumenta consideravelmente quando se fala dos mais jovens (31%)".

Para os utilizadores fica o consentimento prévio, mas o RGPD só exige que seja informado e aceite a recolha de dados. Será que há uma "«revolução silenciosa» ou a ilusão de controlo sobre os nossos dados"? como diz Gonçalves (2019). "Não é difícil deduzir que as tecnologias de *Big Data* dificultam extraordinariamente a observância de princípios fundamentais do RGPD como o consentimento prévio do titular dos dados, a limitação do fim ou a minimização dos dados, pois a essência do *Big Data* reside precisamente na reutilização de dados para fins diferentes dos que presidiram à sua recolha, apoiando-se numa acumulação ilimitada de dados".

Ou seja, embora as empresas e operadores de telecomunicações tenham mais obrigações, existem imensas formas de indirectamente recolher informação, como se referiu no início (*cookies*, *scripts*, registo de actividade, etc.). Uma vez mais, é dever do habitante digital, na sua vida *online,* estar o mais informado possível. Um ano depois da entrada em vigor do RGPD, que balanço se pode fazer?

Segundo Barros (2019) a ameaça que as empresas sentiam tornou-se uma oportunidade, são mais cuidadosas com os termos de uso que redigem, a forma como se relacionam com os clientes/consumidores mudou, respeitando mais a ideia de consentimento prévio, o que aumentou a confiança e segurança do público.

Mas não sejamos ingénuos, as grandes empresas que vivem, dependem e lucram com a colheita da pegada digital têm muito poder, por exemplo a Facebook fez chantagem com a U.E. para não haver regulação europeia sobre o negócio da publicidade *online*. Segundo Pena (2019), "o modelo de negócio é ganhar dinheiro à medida que as pessoas clicam, é por isso que a desinformação se dissemina [o que liga a questão também à disseminação de *fake news*]. Havia um outro problema, se olharmos para as pessoas do grupo de peritos, é também bastante surpreendente que a maioria tenha uma fonte de financiamento comum: a Google. Isso fez com que tivessem fracassado as tentativas de incluir no debate mecanismos de controlo *antitrust*, regras para a competição (num mercado que funciona em duopólio, tendo o Google e o Facebook mais de 80% das receitas publicitárias *online*)".

Mais recentemente, a propósito da Directiva dos Direitos de Autor[161], sem querer entrar especificamente nessa questão, ficou claro como é difícil tentar resolver os "problemas" que a Internet e a vida *online* criam. Há razões válidas para os dois lados da questão, o parlamento Europeu e os parlamentos nacionais estiveram divididos, como quase todas as pessoas que tentaram perceber o que estava em jogo, mas a vida *online* será irremediavelmente mudada. Ao tentar regular a Internet e as grandes empresas tecnológicas, primeiro com as questões de protecção de dados e agora com os direitos de autor, acabaram por nivelar os gigantes (como a Google) com todos os sítios na rede.

Segundo Ball (2019), "o Artigo 11, que exige aos motores de busca e similares, pagamento aos editores quando são reproduzidos pequenos extractos do seu material. [Implica] que serão somente algumas firmas a receber a maior parte da receita. E, porque a Google e outros não querem pagar, mostrarão muito menos informação de sítios onde cobram. […] No fim ficam todos a perder, motores de busca, editores (menos tráfego) e utilizadores". O artigo 13, o mais controverso, aumenta a responsabilidade dos sítios da Internet, pela disponibilização de material que viola direitos de autor (e.g. Youtube), o conteúdo é culpado até se provar que é inocente (há excepções como conteúdo humorístico e a Wikipédia). Na prática isto vai incentivar filtros automáticos, que podem acabar por funcionar como censura, pois por precaução muito material será bloqueado. Isto tudo foi feito com muito boas intenções, mas muito contra o utilizador da Internet.

[161] Site da U.E. https://ec.europa.eu/portugal/news/directive-copyrights-faq_pt, notícia https://www.publico.pt/2019/02/20/tecnologia/noticia/conselho-ue-define-texto-final-directiva-direitos-autor-votacao-parlamento-1862726

Soluções, reduzir a pegada digital, controlar a privacidade

Depois de tudo o que foi abordado até aqui, compreende-se o que está em questão quando se fala de pegada digital, mal nos ligamos à Internet, usamos um *smartphone*, *tablet,* PC ou qualquer outro dispositivo digital ("ligável" à rede) e deixamos um rasto, intencional ou não. Não foram referidos alguns aspectos, mais específicos, mas que também contribuem: os jogos que se jogam (nos dispositivos e *online*), com quem, onde e quando se jogam, que vídeos se vê *online*, o que se compra *online*, onde e como, toda a correspondência de correio electrónico, chamadas telefónicas (telefone, Skype, WhatsApp, etc.), as noticias que se lêem (quais, onde, como). Toda esta informação está algures, se nalguns casos já está agregada e constitui um perfil, noutros casos está disseminada e pode ser agregada, acaba por ser um cenário assustador, se pensarmos em sistemas de vigilância como o que está à beira de ser instituído para todo o território da China.

Além de tudo o que foi discutido há, também e ainda, uma questão eminentemente filosófica, quem somos *online*, como é que o nosso comportamento *online* nos define? Será que "como afirma o existencialismo, só podemos ser definidos pela nossa existência actual, logo pelas nossas acções – pelas quais somos responsáveis" (Warburton, 2019). O autor argumenta que, conforme as nossas vidas migram do analógico para o digital, como cada acção que temos é uma declaração que nos define como indivíduos, elas moldam quem somos individualmente e colectivamente. "Há uma liberdade, que induz a angústia, quando coloca nas nossas mãos o poder total de nos definirmos a nós e à humanidade através da contribuição, viciante, que todos fazemos para o grande mar do *Big Data*. […] tudo o que fazemos acresce ao *stock* digital que nos define. […] Com grande poder vem uma grande responsabilidade […] nestes dias de interligação, a nossa responsabilidade como agentes está a aumentar".

Até aqui pressupôs-se que se deve reduzir a pegada digital, mas há que ver a questão pelo lado oposto, e se o objectivo for aumentar essa pegada? Trabalhá-la? Aumentar e melhorar a visibilidade *online*? Esse é um objectivo normal para empresas, políticos, figuras públicas, faz parte da sua natureza e muitas empresas oferecem esse serviço – marketing digital. Então, quase tudo deve ser feito ao contrário, maximizar o rasto que se deixa, "*posts* em Blogs, páginas nas redes sociais, sítios *web*, vídeos, comentários de utilizadores [há quem pague para se comentar], análises e críticas" (Wilde, 2018). Um dos pontos importantes é colocar a empresa/nome/produto tão acima quanto possível nos resultados dos motores de busca, a palavra Google deu origem ao verbo "Googlar"[162], "é tudo uma questão de ter muitos *hits*, o máximo, positivos, na primeira página. Vários estudos de marketing indicam que 90% das pessoas não passa da primeira página de buscas no Google" (Gurling, 2017).

[162] Googlar - verbo transitivo e intransitivo, pesquisar (palavra, expressão) na internet utilizando o motor de busca Google, o inglês Google®+-ar, pelo verbo inglês to google, «idem» (Infopédia – Porto Editora - https://www.infopedia.pt/dicionarios/lingua-portuguesa/googlar

Há muitas empresas a dar sugestões e vender serviços neste domínio, a pessoas, empresas, partidos políticos, a quem quiser se mais "visível". Segundo Media Leaders (2018), depois de consultados vários especialistas, a melhor forma de aumentar a pegada *online* é:

1. Colocar vídeos no sítio *web* [da empresa/entidade] e partilhá-los nas redes sociais, cada vez mais consumidores procuram este tipo de conteúdo [facilidade?];
2. Criar uma estratégia de marketing de entrada, criar conteúdos que as pessoas queiram ler e estejam facilmente acessíveis para a audiência nicho (*links* e *tags* também funcionam);
3. Escrever um artigo de "investigação" utilizando dados internos, assegurar que é um tópico que teve *likes* e *links* no passado, incluir gráficos, fazê-lo chegar a influenciadores e jornalista da área;
4. Emular as marcas que se admira, ver quem tem *links* para elas, porquê e quais são os artigos mais populares. Quando se tiver percebido, criar conteúdo semelhante ou melhor;
5. Publicar em plataformas externas, criando blogs onde publicar, regularmente, estabelecer "conversas" nas redes sociais, pôr a "audiência" a produzir o conteúdo;
6. Concentrar na optimização da experiência de busca, optimizar todos os canais e pontos de contacto, com que os clientes possam estabelecer ligação;
7. Criar alertas Google para a marca, o serviço permite receber alertas quando uma marca é mencionada *online*, pode-se controlar as marcas maiores e contactar quem menciona;
8. *Postar* histórias no Instagram, barato para arranjar "espaço mental", fotografias efémeras, segmentadas e vídeos, podendo-se acrescentar ligações;
9. Optimizar os perfis de redes sociais com palavras-chave, pois há sempre janelas de procura, assegurar que as palavras-chave coincidem com as do sítio da Internet.

Um dos métodos mais aconselhados, para garantir resultados, é procurar frequente e regularmente por nós próprios (a empresa, pessoa, entidade) na Internet, garantir que se existe, que a imagem encontrada é boa, sendo que isto se aplica a qualquer pessoa, pois cada vez mais as empresas pesquisam informação, em todos os meios, relativa a futuros potenciais empregados, muitas vezes com consequências catastróficas com as "coisas", pessoais, que as pessoas põem *online*. Segundo Smith (2019), deve-se; "ter um *website* ou blog, que dão uma âncora à pegada digital; ser activo nos comentários *online*, o que eleva o perfil; partilhar informação útil *online*, o que faz as pessoas voltarem; criar conteúdo de dimensão adequada, para tornar a mensagem digerível; esconder-se *online* é tão 2002, ser visto é o futuro".

No fundo, tudo o que é sugerido acima é, basicamente, o contrário daquilo que o autor acha que se deve fazer e que, realmente, está na base da tentativa de criar este ensaio – como reduzir a pegada digital, como garantir o máximo (possível) de privacidade, a todos os níveis, quando se leva uma vida *online* activa. No entanto, não referir e lembrar que há, até, uma "ciência" e um modelo de negócio oposto, não seria correcto nem demonstraria, por oposição, aquilo que se quer

– aumentar e melhorar a consciência das consequências do que se "põe" na Internet, voluntariamente ou não. Vamos então tentar apresentar, de uma forma hierarquizada, os princípios gerais da gestão e diminuição da pegada digital, as escolhas técnicas a nível de navegação, aplicações e serviços e, por fim, como desaparecer (ou quase) da Internet, o que é praticamente impossível.

Seria quase impossível ser exaustivo, relativamente aos sistemas operativos (não conheço iOS nem utilizei alguma vez um iPhone), navegadores da Internet, aplicações ou redes sociais. Contudo, tendo noção do tipo de opções que existem, a todos os níveis, a ideia é tornar mais fácil explorar e encontrar as soluções possíveis, podendo cada um decidir que tipo e grau de privacidade quer implementar na sua vida *online*. O objectivo deste ensaio é informar, alertar, ajudar a perceber como a nossa pegada digital é criada, para a poder controlar e reduzir (caso se queira…), mas sobretudo geri-la melhor e ter noção dos riscos. A partir daí cada um fará o seu trajecto, as suas escolhas e investigação acerca deste mundo, além de o poder (dever) transmitir a outros, menos avisados e informados.

Um passo preliminar (Trend Micro, 2019), que pode ser fastidioso e levar algum tempo, é avaliar o perfil digital de cada um: tentar listar (apontando), quais os *websites*, aplicações e formulários onde se introduziu informação pessoal, bancária, etc. Pode-se começar por ver as credenciais, no Windows "procurar > Gerir Credenciais Web", ficando-se a saber quais os dados de registo e palavras passe guardadas para navegar na Internet (e não só), podendo-se decidir quais actualizar, apagar ou mudar. A escolha das palavras-passe deve ser criteriosa, longas, complexas, com uma mistura de letras, números e símbolos, maiúsculas e minúsculas, o ideal seria mudá-las frequentemente. Quase todos os navegadores da Internet (Chrome, Edge, Firefox) têm, também, opções para gerir palavras-passe e formulários.

Seguidamente há considerações de carácter geral, manter o software o mais actualizado possível, forçando a sua actualização, seja no computador, tablet ou *smartphone*, pois uma parte significativa das actualizações lidam e resolvem falhas de segurança. Basta procurar no Windows > Windows Update (na lupa que está na barra de tarefas, à esquerda), no iOS > Preferências do sistema > actualização de software. Nos telefones Android, nas definições > Actualizações de Software, no iOS, Definições > Geral > Actualização de software.

No computador deve-se ter um antivírus e *firewall* activos, no caso do Windows vêm integrados no sistema (procurar Segurança do Windows), ou pode-se recorrer a terceiros (e.g. Symantec, McAfee, Kaspersky[163]). As principais marcas têm, também, soluções para *smartphones*, o que é importante, oferecem vários serviços (protecção dos dados, encontrar o telefone, bloqueá-lo, etc.) e não são caros, é explorar. Convém ter em atenção que muita da oferta, sobretudo gratuita, não detecta

[163] https://www.symantec.com/ , https://www.mcafee.com/pt-br/index.html , https://www.kaspersky.pt/

nem garante segurança por aí além[164], pode-se procurar testes comparativos em revistas ou sítios da especialidade (e.g. PC Magazine[165], C NET[166] ou PC World[167]).

Procurar por mim na Internet…

O primeiro passo efectivo, para saber qual é, afinal, a pegada digital de cada um é procurar por nós próprios na Internet, utilizando vários motores de busca: Google (https://www.google.com/), BING (https://www.bing.com/), Yahoo (https://www.yahoo.com/), The Internet Archive Search (https://archive.org/search.php), ASK.com (http://www.ask.com/) e quaisquer outros que se conheça, incluindo um de que se falará adiante (DuckDuckGo - https://duckduckgo.com/). Deve-se procurar: o nome, completo e variantes várias, números de telefone, moradas e endereços de correio electrónico (para saber se "andam por aí"), procurar também combinações do nome pessoal com a empresa, entidade ou qualquer organização, a que se esteja ou tenha estado associado, procurar família e amigos e ver se se aparece associado. Pode e deve fazer-se o mesmo nas redes sociais, procurando pelo nome próprio e variantes, alcunhas conhecidas, amigos e família, etc.

Depois de se fazer isto, de uma forma organizada e mais ou menos exaustiva, fica-se geralmente chocado com o que se encontra, em quantidade, diversidade e, nalguns casos, antiguidade e que, potencialmente, nunca mais sairá da Internet. Haverá dados e informação que cada um "lançou" voluntariamente *online*, alguma informação que não se sabe como apareceu e outra que é institucional, mais ligada ao mundo profissional de cada um. Caso se detecte informação gravosa, incorrecta, comprometedora ou embaraçosa deve-se tentar resolvê-la, caso seja possível. É neste ponto que se compreende como se construiu uma reputação *online*, visível por todos, por vezes involuntariamente.

Sistemas operativos

Depois do choque, maior ou menor, pode-se passar à acção para controlar a privacidade, através do sistema operativo, Windows e Android (lamento o desconhecimento do iOS, como já referi, aconselho começarem pela própria Apple[168]), não esquecendo as contas pessoais da Microsoft e Google. As hipóteses e opções são múltiplas, algumas complicadas, seria demasiado cansativo e pesado percorrer tudo, mas pelo menos convém saber como ir até estas opções, estudá-las A

[164] https://www.zdnet.com/article/two-thirds-of-all-android-antivirus-apps-are-frauds/ ou https://www.av-comparatives.org/tests/android-test-2019-250-apps/
[165] https://www.pcmag.com/roundup/256703/the-best-antivirus-protection
[166] https://www.cnet.com/news/the-best-antivirus-protection-of-2019-for-windows-10/
[167] https://www.pcworld.com/article/3219792/best-antivirus-for-windows-pc.html
[168] https://www.apple.com/privacy/

SÉRIO, procurar informação sobre aquelas para as quais se tem dúvida e tomar as decisões adequadas ao perfil de privacidade que se quer ter.

No Windows 10, indo às definições ou procurando (lupa na barra à esquerda ou botão Windows + S), deve-se ir para Privacidade. Nessa página (ver Figura 49) pode-se controlar as Permissões do Windows e Permissões da Aplicação, havendo sempre ligações para páginas *online* sobre todas as opções e política de privacidade (deveria ser visto e analisado atentamente). Convém ver-se, ponto por ponto, opção por opção, quais as hipóteses, o que representam, que limitações implicam (caso sejam ligadas/desligadas), quem tenha receio de "escolher mal" pode tomar notas para depois desfazer as opções. É complicado, moroso, muitos acharão que talvez não valha a pena, mas se chegaram até aqui, depois de tanto texto e acham a privacidade importante, mesmo que não mexam, pelo menos devem explorar.

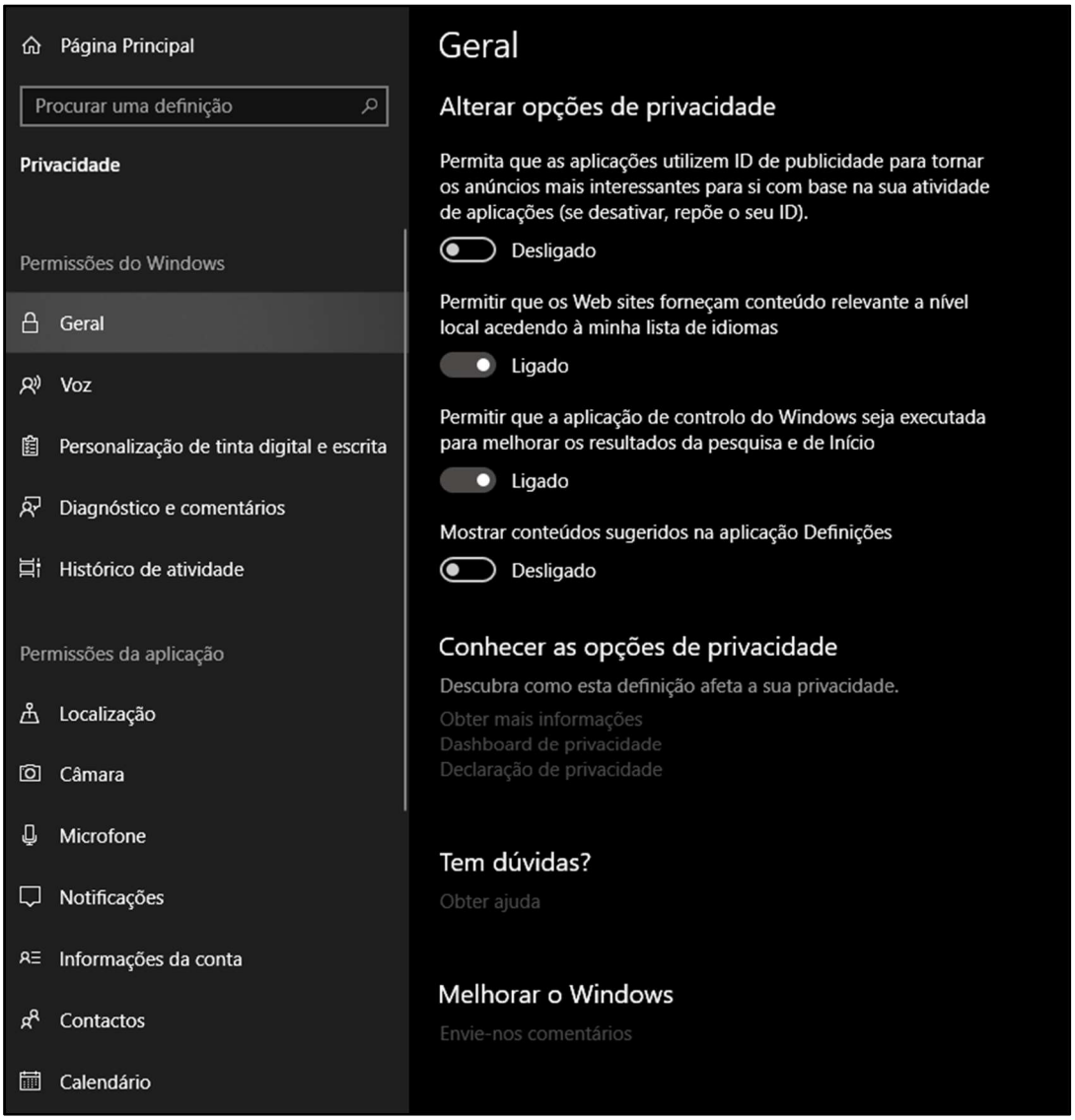


Figura 49 – Página de opções de Definições de Privacidade no Windows 10.

Depois de percorrer e analisar as Permissões gerais, deve-se passar para as permissões dadas às aplicações, com destaque para a localização, câmara e microfone, entre outras. Poderão verificar, certamente, que muitas aplicações têm permissões que "não lembram ao diabo", por mais úteis que possam parecer (são-no em muitos casos). Convém, uma vez mais, estudar, investigar e decidir: deixar tudo na mesma, mudar, desligar. Para já, cada um pode ter assim noção da quantidade de informação que a Microsoft recebe, de todos os equipamentos com Windows, o que permite gerir, melhorar e corrigir, mas não só…[169]

Não obstante, esta é só parte da questão, pois quase todos terão uma conta Microsoft, com todas as vantagens associadas, a que podem aceder em https://account.microsoft.com/ . Aí poderão encontrar toda a informação pessoal que forneceram à Microsoft e controlar o acesso, mas também uma parte relativa a Privacidade (ver Figura 50), depois de entrar pode-se ver que há uma descrição e explicação da política de privacidade (a ler atentamente) e percebe-se que são recolhidos: o histórico de navegação, de pesquisas, de localização, actividade de voz, actividade multimédia, etc., etc. e que, no fundo da página, acrescem, ainda, outras definições de privacidade (Xbox, Skype, Publicidade, Office…).

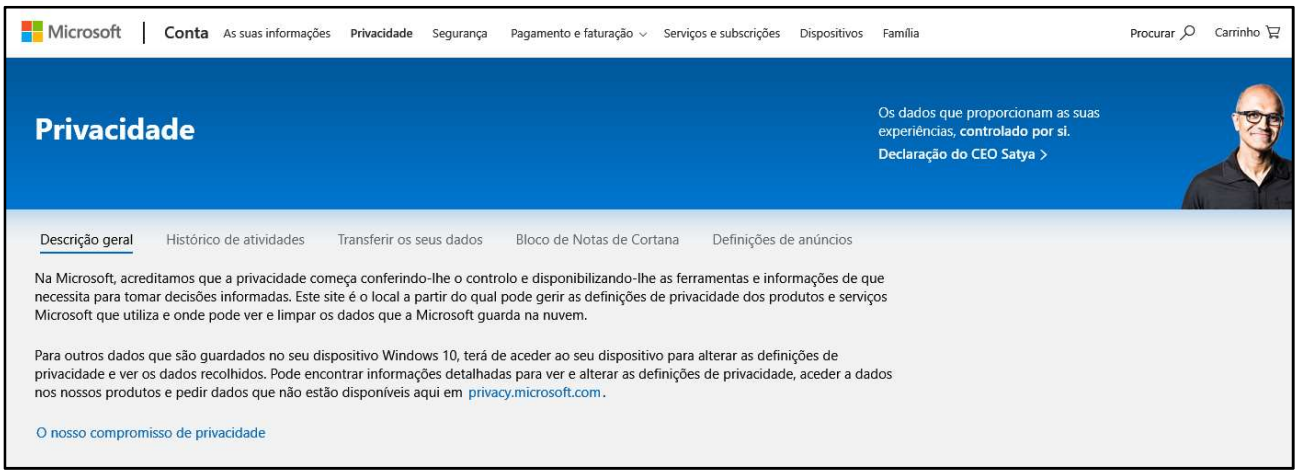


Figura 50 – Conta Microsoft, acesso às definições de privacidade (https://account.microsoft.com/privacy/)

Percorrendo todos os tópicos e todas as opções fica-se a saber a quantidade assombrosa de dados que, por defeito, são recolhidos e enviados, sempre, claro está, com a melhor das intenções e para melhorar a experiência. Cada um deve, de uma forma documentada, pensada e objectiva, decidir o que quer deixar recolher e partilhar, sabendo de antemão que algumas coisas poderão funcionar de uma forma diferente (pior). Chamo a atenção para a quantidade de informação, honesta, de

[169] https://www.computerworld.com/article/3188235/windows-10-data-collection-what-you-need-to-know.html ou https://www.theverge.com/2017/4/5/15188636/microsoft-windows-10-data-collection-documents-privacy-concerns ou https://wccftech.com/windows-10-data-collection-microsoft/

qualidade, que está disponível no "fim-do-fim" da página, abordagem à privacidade, declaração e pedidos ao governo. Como se verá adiante, a recolha não acabou aqui, o seu controlo pode ser feito a três níveis: Windows, Conta Microsoft e depois no navegador que se utiliza (se for o Edge ou o Internet Explorer é mais informação que vai para a Microsoft), mas os navegadores e navegação serão abordados a seguir. Acrescem serviços digitais da Microsoft, como o Outlook (correio), Skype, OneDrive (nuvem) ou MSN, toda a actividade associada a uma conta é recolhida.

O que se passa, então, com o Android? Todos os dispositivos que o utilizam (*smartphones* e *tablets*, das televisões e assistentes não se falará), estão associados a uma conta, pessoal, da Google, podendo-se controlar alguns parâmetros no telefone e a maior parte, *online*, na conta Google. Começando pelo telefone, naturalmente todos os utilizadores deverão ter PIN, bloqueio de ecrã, boas palavras-passe, antivírus, encriptação de dados (ou não) e comunicações, etc., mas isso é para proteger o telefone e a utilização que fazemos dele.

Uma das principais definições que se controla, directamente no telefone, é a opção de ter os serviços de localização ligados, bem como o *WiFi* e o *Bluetooth*, como se discutiu antes, estes três serviços servem para produzir/melhorar/improvisar dados de geolocalização, portanto desligá-los ajuda (um pouco adiante discutiremos, especificamente, as questões da mitigação dos dados de geolocalização). Convém ter noção que com a localização desligada se perdem vários serviços (encontrar o telefone, saber onde se está, chamar um Uber, etc.).

O passo seguinte, moroso e fastidioso, é procurar nas definições a opção Aplicações e percorrê-las, uma a uma, vendo que permissões é que têm: acesso a localização, câmara, microfone, *Wi-Fi*, agenda, contactos, etc. Nas versões mais recentes de Android (Pie, 9), há uma opção para ver "permissões da aplicação", que mostra por serviço, quais as aplicações que o usam, sendo muito mais fácil ligar ou desligar as permissões. Será provável encontrar-se permissões abusivas, mas também algumas óbvias e incontornáveis, como uma aplicação que faz chamadas pela Internet ter de aceder aos contactos e microfone, ou uma de mapas poder aceder ao GPS.

Contudo, se este levantamento for exaustivo, poder-se-á chegar à conclusão de que algumas (muitas, poucas) permissões são abusivas, devendo-se considerar seriamente se vale a pena ou não desligá-las, em função do tal perfil de privacidade que consideramos e definimos como ideal, *a priori*, para a nossa vida *online*. Mas, tal como com a Microsoft, esta é só parte da questão, pois a Google também tem (pelo menos), três níveis de controlo de privacidade: opções no dispositivo, conta Google e informação recolhida pelo seu navegador, o Chrome.

Quando se vai à conta Google *online* (https://myaccount.google.com/) (ver Figura 51), há um mundo de informações e definições para escolher, que estão sempre, por defeito, a recolher tudo e mais alguma coisa que se faz na Internet, navegando no Chrome ligados à conta e nos

dispositivos Android associados a essa conta. Todos os utilizadores deveriam, pelo menos uma vez, estudar detalhadamente todos os parâmetros da sua conta, aconselho começarem pela Privacidade e fazerem o gerir/ver histórico de tudo. Pode-se verificar que TODA a actividade da *web* e aplicações é registada e enviada, as localizações e o seu histórico, todo o uso do dispositivo, actividade de voz e áudio, pesquisas no Youtube, visualização, etc.

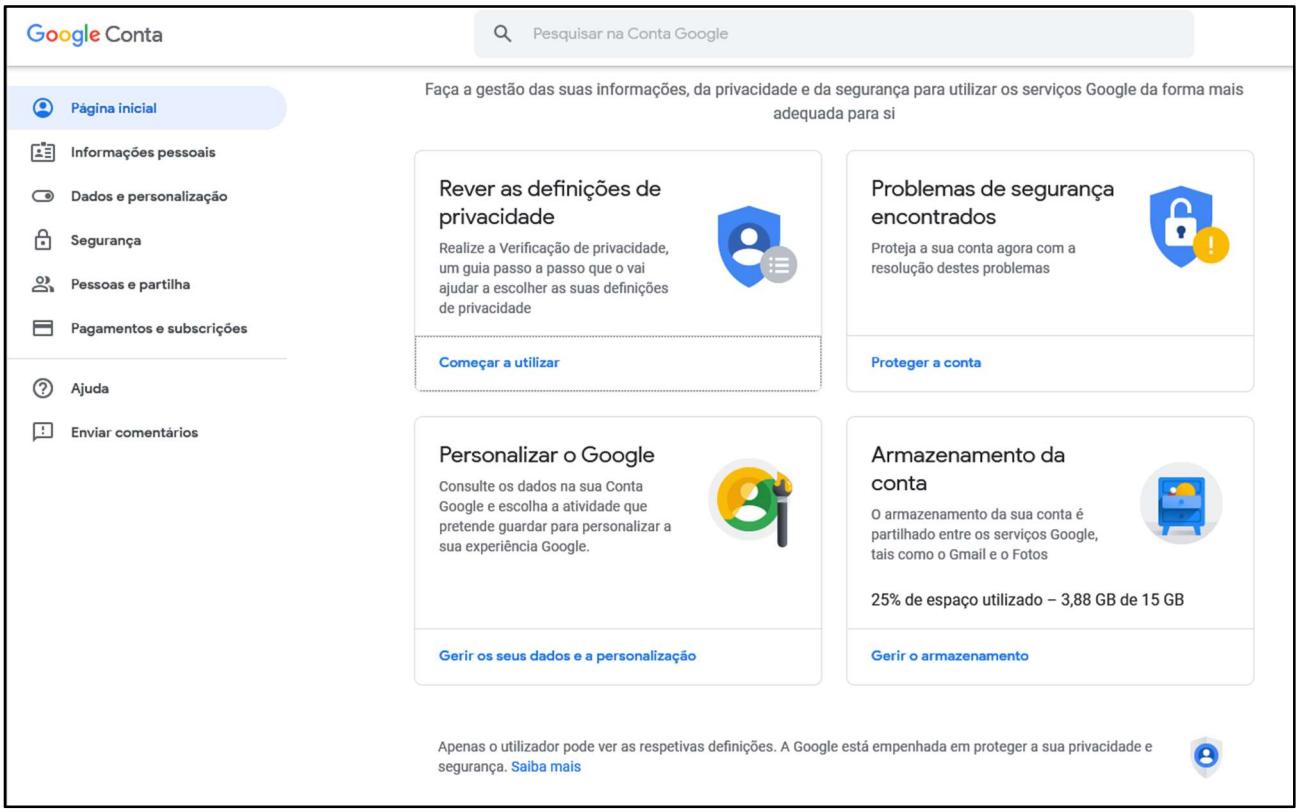


Figura 51 – Conta Google, acesso às definições (https://myaccount.google.com/).

Este é somente o Tópico 1, para personalizar a experiência Google, mas descendo há outras definições, para o Youtube, Google Photos, Publicidade etc. Convém ter noção que todas as aplicações e serviços do universo Google (Drive, Gmail, Photos, Agenda, Contactos, Mapas, Notícias, Calendário, Tradutor) estão ligadas, ou seja, fornecemos as "nossas" fotos, mensagens, ficheiros, contactos, agenda, localizações, enfim… TUDO o que fazemos e somos digitalmente, à Google. Parte é voluntário ou por desconhecimento das opções de controlo disponíveis, por isso este texto, outra parte involuntariamente, é ver de seguida a parte Dados e Personalização. Sabe-se hoje, por exemplo, que a Google "varre" todo o conteúdo dos *emails* das contas Gmail (Graham, 2019), para saber que compras *online* foram feitas pelos utilizadores, esta informação (difícil de apagar) pode ser consultada em https://myaccount.google.com/purchases.

É interessante tentar imaginar, a cada segundo, de cada minuto, de cada hora, de cada dia, o volume transcendente, brutal, de dados que estão a ser recolhidos, formando uma base de dados de tudo o que se faz *online*, pessoa a pessoa. Depois do que se discutiu, é fácil imaginar e perceber

o que isto pode representar, se em muitos casos lucramos (verdadeiramente) com melhores serviços prestados, dando os nossos dados no tal *trade-off* paradoxal, não devemos, contudo, deixar de nos questionarmos se queremos "participar" nisto voluntariamente. Aconselho a exploração cuidada, séria e sistemática do que é, efectivamente, uma conta Google, depois cada um pode decidir o que fazer, até onde ir na tentativa de controlo da privacidade[170]. Convém lembrar que, para além de tudo o que é transparente, legal e conhecido, sabe-se que há, também, práticas fraudulentas, vendas, fugas e escândalos, alguns dos quais mencionados antes, portanto a dimensão, diversidade e replicação da totalidade ou partes, da pegada digital de cada pessoa anda "por aí" e dificilmente é apagável ou controlável.

Navegação

Depois das questões gerais (prévias e estruturais), do sistema e mecânica montados pela *troika* sistema operativo – conta de serviços – navegador, mesmo tendo só aflorado a ponta do iceberg dos dados recolhidos, pode-se passar então para a navegação propriamente dita. Independentemente do dispositivo, sistema operativo, ou navegador, o simples acto de "navegar" na Internet implica a recolha de muitos dados, que podem ser associados (ou não) a cada utilizador, como foi sinteticamente descrito no início do texto.

Também neste caso há vários níveis de "defesa", pois há várias possibilidades e origens de recolhas de dados: primeiro o ISP (*Internet Service Provider*), a empresa que está a dar-nos acesso à Internet, no PC, tablet ou *smartphone*, seja comercial e paga pelo utilizador (NOS, MEO, VODAFONE), seja num equipamento de uso público, no emprego, por cabo, *WiFi*, ou outro meio. Toda e qualquer busca, página aberta, ou seja o que for, introduzido no navegador, vai do equipamento ao servidor do ISP e daí para a Internet, logo, pode ser interceptado e visto antes de lá chegar (facílimo em redes *WiFi* abertas), sendo que o ISP sabe sempre que tráfego cada "cliente" faz, estuda e trabalha estes dados e pode, inclusive, vendê-los. Como é que isto se resolve? Encriptando a comunicação a partir do nosso equipamento, utilizando uma VPN (Virtual Private Network), de que se falará depois, nem o ISP nem quem intercepte sabe o que está no tráfego, só sabe de onde vem e para onde vai, não o consegue "ler".

A segunda linha de recolha de dados é feita pela empresa que criou o navegador, se o utilizador iniciar aí sessão: utilizando o Edge, a Microsoft associa toda a navegação (como se viu) ao utilizador com conta Microsoft, utilizando o Chrome, a Google associa toda a navegação (como também se viu) ao utilizador com conta Google. Como é que isto se resolve? Num computador pode-se usar os navegadores sem iniciar sessão, contudo, num telefone Android, mal este é ligado, está-se

[170] Quem esteja no mundo Apple tem um "problema" semelhante, computador, tablet e telefone, acrescidos de conta *online*. "Certamente" a Apple disponibiliza acesso, explicação e possibilidades de controlar e escolher o que é recolhido.

"dentro" da conta Google e, portanto, toda a actividade é associada ao utilizador. Qual é a alternativa? Utilizar outros navegadores, que não recolhem dados, nem estão associados a conta nenhuma, há alguns (Vivaldi[171] e Opera[172] ou o DuckDuckGo para Android[173]).

A terceira linha de recolha de dados, como se referiu (também) no início, está relacionada com as páginas que se visita e com os *cookies* que elas colocam no equipamento, além dos *scripts* que executam, tendo por objectivo conhecer todo o tipo de comportamento do utilizador. Aqui há várias soluções, dependendo do grau de protecção de privacidade, situação em que se navega e "trabalho" que se está disposto a ter:

1. No navegador que se está a utilizar, desligar (pelo menos) a opção não monitorizar (não seguir, *do not track*), o que impede que um sítio *web* siga o que fazemos noutros, até depois de sairmos desse sítio;
2. No navegador, desligar a opção aceitar *cookies* de terceiros (*third party cookies*), um sítio colocar *cookies* de outro domínio;
3. Dependendo do navegador que se utiliza, procurar extensões que permitam controlar os *scripts* que são executados, o que, contudo, torna complicado e cansativo, por vezes, navegar, dois exemplos são NoScript[174] e ScriptSafe[175] (também descarregáveis nas Lojas *Online* – Microsof Store no Windows e Chrome Web Store);
4. Usar bloqueadores de anúncios, *Ad Blockers*, não só tornam a experiência de navegação melhor (sem publicidade), também impossibilitam a monitorização e rastreio, por exemplo Adblock Plus[176] ou AdBlock[177] (convém ter noção que, também aqui, muitos sítios nos vão dificultar a vida, complicar o acesso à página ou pedir para desligar o bloqueio);
5. Embora possa parecer uma questão lateral, somente os sítios HTTPS têm encriptação (vê-se essa informação, a URL, na janela com o endereço no topo do navegador e um cadeado), o tráfego entre o navegador e o sítio, se for interceptado, não pode ser lido, portanto só se deve navegar em sítios protegidos. Por si só isto impede parte da recolha de dados pelo ISP, e.g. sabe que estamos na Amazon, mas não sabe o que compramos. Existem extensões para navegadores que "forçam" a navegação a só aceitar sítios HTTPS, por exemplo HTTPS://everywhere[178] (ver Figura 52);
6. Utilizar motores de busca anónimos, que não criam uma bolha de resultados, com o tempo, em função das nossas buscas e/ou interesses comerciais (i.e., anúncios). A vantagem, entre outras, é que diferentes pessoas, em diferentes momentos, obtêm sempre os mesmos resultados, o

[171] https://vivaldi.com/
[172] https://www.opera.com/
[173] https://duckduckgo.com/app
[174] https://noscript.net/getit
[175] https://www.andryou.com/scriptsafe/
[176] https://adblockplus.org/
[177] https://getadblock.com/
[178] https://www.eff.org/https-everywhere

melhor deles é o DuckDuckGo[179], vale a pena visitar o sítio e estudar as vantagens que oferece, há também o SartPage[180] e o Qwant[181]. Claro que têm limitações, idiossincrasias e não "nos conhecem" como o Google ou Bing, que sabem o que procuramos, fazemos e compramos;

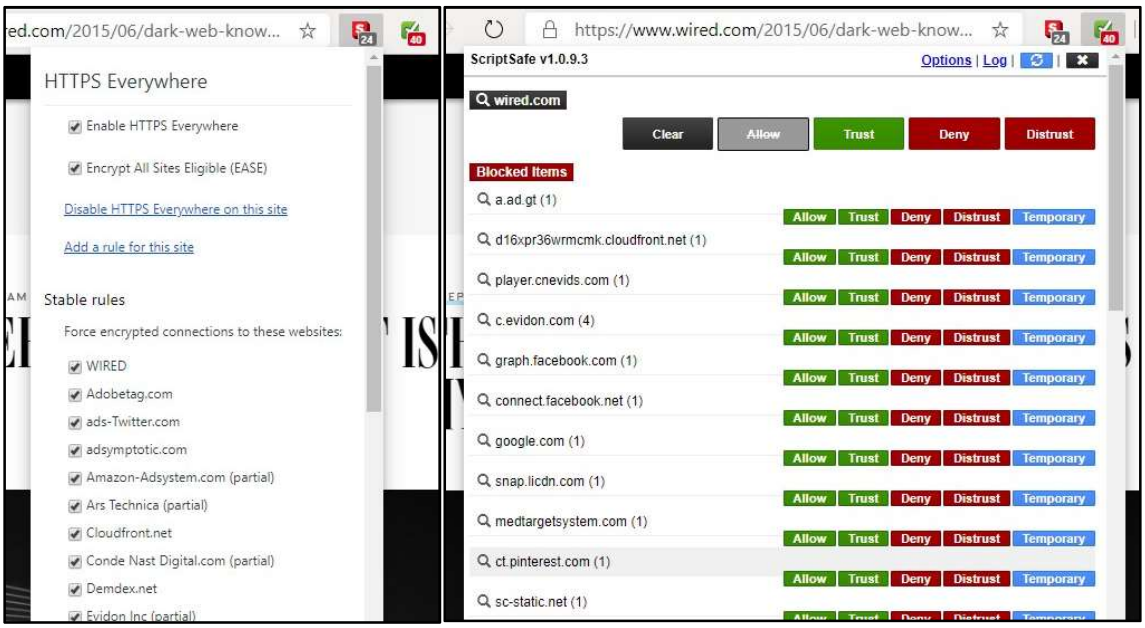


Figura 52 – Um exemplo do que "não se vê", sítio da Wired (https://www.wired.com/), extensão HTTPS está a encriptar a comunicação com 24 sítios e a extensão Script Safe detecta 40 *scripts* na página, vários ligados a publicidade, ao Google, Twitter, Amazon, etc.

7. Alternativas ao Google Maps mais concentradas na privacidade, se não se quer dar a conhecer todas e quaisquer buscas cartográficas à Google, pois já se demonstrou que, até depois de desligar o histórico de localização e as opções de localização, a Google continua a seguir as pessoas e registar as pesquisas. Alternativas, com limitações, idiossincrasias, questões várias, algumas vantagens além de anónimas: HERE WeGo[182], Sygic Maps and Navigation[183], OpenStreetMap[184] e Maps.Me[185];
8. Quando se navegar num equipamento público, ou que não é nosso, utilizar SEMPRE o modo incógnito/privado e fechar o navegador depois de terminar. O que é que este modo garante? Que a actividade do *navegador* não é guardada localmente (histórico, buscas, transferências), evita a criação de *cookies* e/ou apaga-os quando se sai, para não se ser seguido/rastreado. Convém ter noção que este modo não protege de vírus e *malware*, não esconde os dados do

[179] Declaração de interesses, é o que utilizo: https://duckduckgo.com/
[180] https://www.startpage.com/
[181] https://www.qwant.com/
[182] https://wego.here.com/
[183] https://www.sygic.com/gps-navigation
[184] https://www.openstreetmap.org/#map=7/39.602/-7.839 e aplicações https://wiki.openstreetmap.org/wiki/Android
[185] https://maps.me/ e https://maps.me/download

ISP, governos, *hackers* ou publicitários e, menos ainda, torna a navegação segura em redes *Wifi* públicas;

9. Regularmente e (muito) frequentemente limpar todos os dados de navegação: *cookies*, histórico e transferências.

Aplicações

Embora possa parecer redundante, porque já foi referido para o Windows e Android, deve-se ter atenção às permissões das aplicações porque, um dos acessos mais desejados por algum tipo de *software*, é precisamente aos dados de navegação. Por mais que se tente proteger e controlar a privacidade de navegação, permitir a aplicações de terceiros acesso a esses dados é, neste contexto, "entregar o ouro ao bandido".

Encriptação

Embora não tendo de ver directamente com pegada digital, tem tudo a ver com privacidade, no caso de roubo ou "entrada" num *smartphone*, a única forma de proteger toda a informação é encriptar[186] o seu conteúdo, havendo várias soluções para tal, tanto no sistema Android[187] como iOS[188]. Convém estudar e ponderar bem esta opção, tem vantagens e desvantagens, mas é a mais segura, inclusive porque nem as autoridades conseguem (facilmente) aceder ao que está no equipamento, como ficou provado quando a Apple recusou desbloquear um iPhone[189].

Também se pode encriptar, guardar e gerir credenciais de autenticação[190], salvaguardando as contas a que se tem acesso a partir do *smartphone*, existem várias soluções e aplicações, pagas e gratuitas, também aqui convém estudar bem as opções disponíveis, os seus custos, garantias e grau de protecção[191].

---

[186] https://www.wired.com/2013/10/keep-your-*smartphone*-locked/ , https://gizmodo.com/why-you-should-be-encrypting-your-devices-and-how-to-ea-1798698901

[187] https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/ , https://www.techrepublic.com/article/encrypt-your-android-*smartphone*-for-paranoid-level-security/ ,

[188] https://www.cnet.com/news/iphone-android-encryption-fbi/ , https://www.lifewire.com/encrypt-the-data-on-your-android-phone-or-iphone-2377707

[189] https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties , https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html , https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

[190] https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/ , https://ithemes.com/why-you-should-use-password-manager/ , https://www.washingtonpost.com/technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one/?utm_term=.0c9ff3afcc60

[191] https://www.lifewire.com/free-password-managers-2626175 , https://www.pcmag.com/roundup/300318/the-best-password-managers ,

Facebook

O exemplo do Facebook é paradigmático, pois recolhe muita informação da pegada digital (voluntária e involuntária), desde comércio, serviços, compras, questões políticas, religiosas, pessoais delicadas, por vários meios. Mesmo que "tratem" bem, guardem e respeitem esta informação (foram dados vários exemplos de como, regularmente e repetidamente, não o faz), o potencial destes dados para governos, agências e *hackers* é gigantesco e irresistível. Imagine-se, no contexto do que se está a passar na China, ou quando é pedido para entrar num país, como já é feito nos E.U.A.[192]. Portanto, é importantíssimo ter noção dos dados que se autoriza recolher e que se podem, efectivamente, controlar. O exemplo dado é do Facebook, pela sua dimensão e ubiquidade, mas certamente que as outras redes sociais também permitem algum grau de controlo da pegada digital, no entanto seria difícil e não faria sentido, falar de várias neste contexto (ver Figura 53).

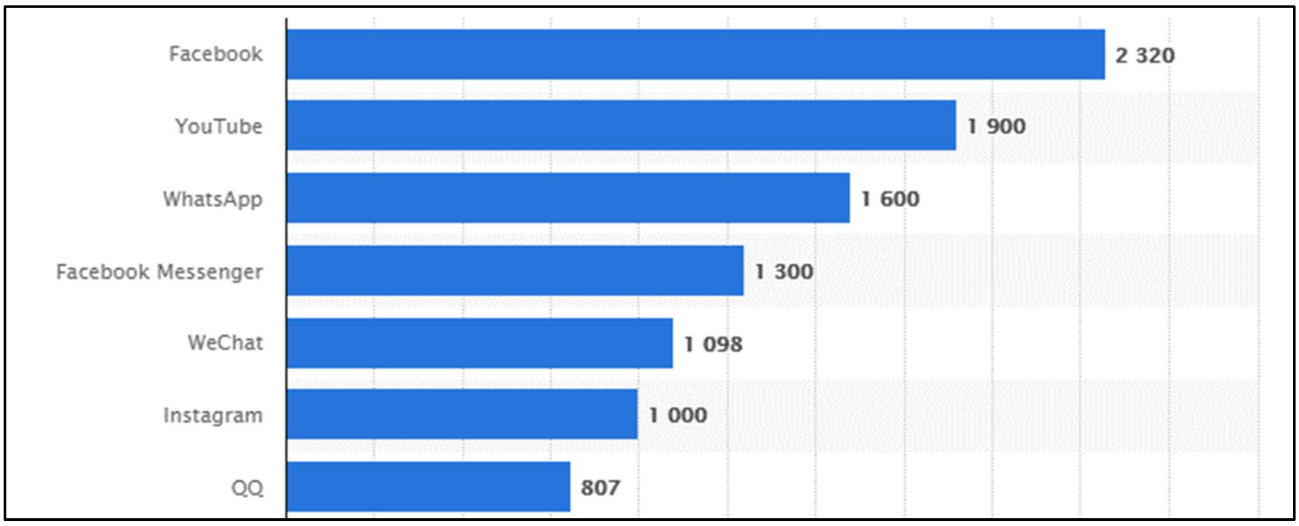


Figura 53 - Redes sociais mais populares a nível popular, Abril de 2019, ordenadas pelos de utilizadores (milhões) (Statista[193]).

No entanto, há muitos mais parâmetros que podem ser controlados, estão agregados em vários tópicos das definições, com particular destaque para Privacidade[194] (ver Figura 55). Aqui pode-se controlar a nossa visibilidade, a informação pessoal, mas vale a pena analisar, atentamente, várias das outras definições e explorar a documentação oferecida, para perceber o mecanismo, sem ter

https://www.androidauthority.com/best-password-manager-apps-android-353684/ , https://www.cnet.com/news/the-best-password-managers-directory/

[192] https://www.bbc.com/news/world-us-canada-43601557 , https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/ , https://www.theverge.com/2016/12/22/14066082/us-customs-border-patrol-social-media-account-facebook-twitter , https://www.nytimes.com/2016/06/29/us/homeland-security-social-media-border-protection.html , https://www.theguardian.com/world/2016/dec/26/us-customs-social-media-foreign-travelers

[193] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[194] https://www.facebook.com/settings?tab=privacy

grandes ilusões de que ser anónimo numa rede social não só é impossível, como contrário à própria existência e objectivos da mesma. Vale a pena ver Haselton (2017) com uma descrição de como saber o que o Facebook sabe de nós[195].

Figura 54 – Preferências de publicidade do Facebook (ver Nota de Rodapé Nº 196).

A primeira coisa que se pode fazer, se se é um utilizador do Facebook, é saber que informação a plataforma tem sobre nós, indo às Preferências de Publicidade[196] (Ver Figura 54). Podem-se percorrer os "interesses", que foram deduzidos da actividade na plataforma (e removê-los todos, só custa a primeira vez, depois é fazer regularmente e "pasmar" com os interesses que aparecem). No quadro seguinte estão os Negociantes e Negócios com que se interagiu, também se podem remover, bem como a possibilidade de receber publicidade direccionada, na secção "As tuas Informações". Nas definições de publicidade pode-se, pura e simplesmente, não permitir nada (não implica deixar de se receber, completamente, anúncios). Por último, podem-se ocultar, por períodos de seis meses, um ano ou permanentemente, certos tópicos de publicidade, além de, no fundo da página, haver informação sobre a publicidade no Facebook. A primeira vez que alguém vê esta informação costuma ficar, no mínimo, espantada, mas é aqui que se pode controlar parte da pegada.

[195] https://www.cnbc.com/2017/11/17/how-to-find-out-what-facebook-knows-about-me.html
[196] https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen

Figura 55 – Definições do Facebook, Privacidade (ver Nota de Rodapé Nº 194).

Como ponto da situação, pode-se dizer que, seguindo os passos referidos até aqui, nos sistemas operativos, contas *online*, navegadores e procedimentos de navegação, motores de busca alternativos e controle da privacidade nas plataformas sociais, pelo menos, há controle da informação que é recolhida da nossa actividade. Não obstante, o essencial é compreender que "tudo depende de se terem bons hábitos na Internet, na vida *online* como cidadãos digitais, ninguém nos pode salvar de nós próprios, pois a melhor segurança ou anonimato não ajudam se se cair num «cambalacho» ou decidir partilhar informação privada numa rede social. Deve-se ter a certeza que se percebem as ferramentas que utilizamos *online* e onde os dados dados podem acabar, quando os partilhamos" (Kilpatrick, 2018).

Geolocalização

A recolha de dados de geolocalização é um aspecto, entre outros, da pegada digital, mas muito específico e que levanta problemas sérios de privacidade e segurança, como foi discutido, pois existe um número absurdo de aplicações que recolhem, guardam e partilham a localização dos terminais. Quanto aos operadores de comunicações móveis pouco ou nada há a fazer (somente utilizar telefones descartáveis), nos computadores e equipamentos sem GPS pode-se desligar a localização (no sistema operativo), mas sabendo-se o endereço IP através do ISP sabe-se, de uma forma grosseira, onde se está (só usando uma VPN que esconde o nosso endereço IP), mas nos

smartphones pode-se desligar os serviços de localização, como já se explicou (ver Valentino-DeVries, Singer, Keller, & Krolik (2018)[197], sobre como o fazer em iOS e Android).

No caso específico do Google, pode-se desligar o histórico de localização na conta *online*, apagar os dados que estão guardados e deixar de os recolher, como também já se explicou parcialmente (para uma descrição mais detalhada, para iOS e Android ver Steele, & Cohen (2018)[198]. Em Maio de 2019 a Google anunciou que ia acrescentar uma opção, não disse quando, para os dados de actividade e o histórico de localização se auto-apagarem, a cada três meses ou dezoito (Khandelwal, 2019)[199], um assunto importante a seguir.

Se os *smartphones* não tiverem estes dados disponíveis, nem *WiFi*, nem *Bluetooth*, as aplicações não têm como recolher dados de localização. Há grupos a desenvolver aplicações, especificamente para inibir a recolha de dados de localização, aumentando a geoprivacidade dos utilizadores (e.g. Fawaz & Shin, 2014).

Quando se abordou a geoprivacidade, mais concretamente a questão do *geotagging* das fotografias que se partilha, sugeriram-se formas de o evitar, convém explicar que além do formato do ficheiro que se partilha (sem dados EXIF), utilizando *software* para editar ou remover essa informação[200], há opções nos *smartphones* para impedir a associação de coordenadas às fotografias (ver Klein, 2017)[201].

Tentar controlar e maximizar a geoprivacidade é importante, mas há casos em que é necessário, essencial até, usar a geolocalização nos *smartphones*. Segundo Siciliano (2019) há alguns aspectos a ter em conta:

- **Não se deve utilizar a geolocalização em casa** – Ligar a qualquer conta *online* com a localização ligada mostra que se está em casa, além de mostrar "onde" é a casa;
- **Não utilizar a geolocalização em casa de amigos e família** – Aplica-se a mesma regra que acima;
- **Ter cuidado com as pessoas que se seguem em redes sociais** – Nalguns sítios e plataformas, os seguidores, amigos e fãs vêm muita informação, se quiserem seguir uma pessoa, atacá-la, incomodá-la ou, simplesmente, serem inconvenientes, podem "encontrar" facilmente quem partilhe a sua localização nestas plataformas;

[197] https://www.nytimes.com/2018/12/10/technology/prevent-location-data-sharing.html
[198] https://www.pcmag.com/article/345340/how-to-get-google-to-quit-tracking-you
[199] https://thehackernews.com/2019/05/google-web-location-history.html?fbclid=IwAR3F3Yo4cCyX9HQU_0is8GgSYCv5r3sfo2hmARWfx4FreQTqYE%E2%80%A6
[200] https://www.maketecheasier.com/best-apps-remove-exif-data-from-images/ ou https://gadgets.ndtv.com/apps/features/remove-location-data-from-photos-view-edit-exif-android-windows-mac-iphone-1821872
[201] https://www.howtogeek.com/203592/what-is-exif-data-and-how-to-remove-it/

- **Evitar desenvolver um padrão** – Tendo rotinas especificas que relacionem um determinado momento do dia/semana/ano com determinadas localizações pode expor, desnecessária e perigosamente, uma pessoa;
- **Educar a família** – Pesquisar cuidadosamente acerca dos perigos de usar S.B.L. nos telefones, debater, explicar e acertar uma política de geoprivacidade conjunta, de família;
- **Estudar e aprender como as aplicações funcionam** - Algumas necessitam, efectivamente, da geolocalização, mas outras não.

Há situações em que a geolocalização pode salvar vidas[202], como em pedidos de ajuda e socorro, como também se referiu antes, além de permitirem um enorme conjunto de serviços, a que muitos utilizadores de *smartphones* já se habituaram e de que não prescindem. Chen (2017), testou durante duas semanas inúmeros S.B.L., apresentando as seguintes sugestões quanto ao uso e partilha de dados de geolocalização:

Utilizar Geolocalização

- Quando se planeia encontrar amigos nalgum lugar, através do iMesage, Google Maps ou Facebook Messenger por exemplo, para difundir a nossa própria localização, mas durante um curto período, estritamente necessário para se encontrarem e seguirem o trajecto dos outros (se isso for importante), depois desligar;
- Utilizar o mesmo tipo de aplicações, ocasionalmente, com parceiros românticos, por consideração pelo espaço e tempo do outro;
- Quando há preocupações de segurança em relação a crianças, podendo-se saber onde andam ou andaram, dependendo das circunstâncias em que se acede a esta informação. Numa emergência faz sentido ver *online* o histórico (Google) tendo acesso à conta, fazê-lo quotidianamente é uma violência e uma invasão de privacidade, tudo depende de muitos factores;
- Em eventos de multidão, ao ar livre, pode-se combinar *a priori* um ponto de encontro, partilhado pelo grupo, ou usar as aplicações que o permitem, encontrando as pessoas no meio da multidão.

Não utilizar Geolocalização

- Em espaço fechados, comerciais ou não, o rigor dos dados é mínimo;
- Em espaços abertos, mas onde a inexistência de rede móvel, ou pouca qualidade, impedem a partilha;

[202] Ver nota de rodapé Nº 57, relativa às chamadas para o 112 e activação da geolocalização.

- Não deixar as crianças e jovens partilhar dados da sua geolocalização com estranhos, ou pessoas que os podem incomodar (*bullying*), há opções para controlar esta partilha nos *smartphones* em controlo parental e nas contas *online*;
- Por razões de segurança, evitar partilhar publicamente a nossa localização, o Google, por exemplo, torna fácil partilhar um *link* com a nossa localização em tempo real, pode ser interessante ou útil, mas nunca colocado em redes sociais e aberto ao público;
- Conhecer os nossos limites, usar bom-senso, se nos queremos esconder não podemos andar a publicar onde estamos.

VPN

Uma VPN – Virtual Private Network (Rede Privada Virtual) – já referida em várias circunstâncias, permite garantir a privacidade das nossas comunicações e vida na Internet, mas como funciona e que vantagens tem? Qualquer comunicação entre dispositivos, utilizando a Internet, pressupõe tráfego entre o equipamento que se está a utilizar (PC, *tablet* ou *smartphone*) e um servidor (ISP, PROXY numa empresa, ou rede *WiFi*, o que a VPN faz é, digamos assim, criar um túnel dentro da rede pré-existente, onde o tráfego é encriptado, entre o utilizador e um servidor VPN, saindo depois desse servidor para a Internet (ver Figura 56).

A primeira consequência é o ISP não poder ver (ler) o tráfego que existe entre o nosso dispositivo e o seu servidor, sabe de onde vem, o servidor VPN para onde vai, mas não sabe daí para onde parte. No outro extremo, o sítio *web* onde chega o tráfego (um pedido de vista de página, por exemplo), sabe que vem do servidor VPN (o seu endereço IP), mas não quem está na origem do tráfego (nós), se se utilizar EXCLUSIVAMENTE sítios HTTPS, a informação é encriptada entre o utilizador e o servidor VPN, entre este e o sitio *web* e de volta ao utilizador, ninguém (há excepções ao mais alto nível de espionagem) consegue decifrar a informação, mesmo que a interceptem.

As vantagens são óbvias e a vários níveis, o que enviamos e recebemos é confidencial e privado (e.g. dados bancários, palavras-passe, texto, ficheiros, compras, mensagens, etc.), a nossa localização não é conhecida (passa ser a localização do servidor VPN), o que dá total privacidade. Se isto é importante numa rede fixa, quando se utiliza *WiFi*, aberto ou não, ainda é mais importante, pois é fácil interceptar dados e "cheirar" o tráfego[203]. Também é importante para quem viaja, pois há países onde certos serviços estão proibidos (e.g. a China bloqueia o Facebook e tudo o que é Google, Twitter, e jornais vários[204]), usando uma VPN liga-se do país "para fora" a um servidor VPN e daí para onde se quer, sendo que o tráfego é encriptado, por isso há países que proíbem, ou controlam o uso de VPN[205].

[203] Sniffer - https://www.lifewire.com/definition-of-sniffer-817996
[204] https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China
[205] https://thebestvpn.com/are-vpns-legal-banned-countries/

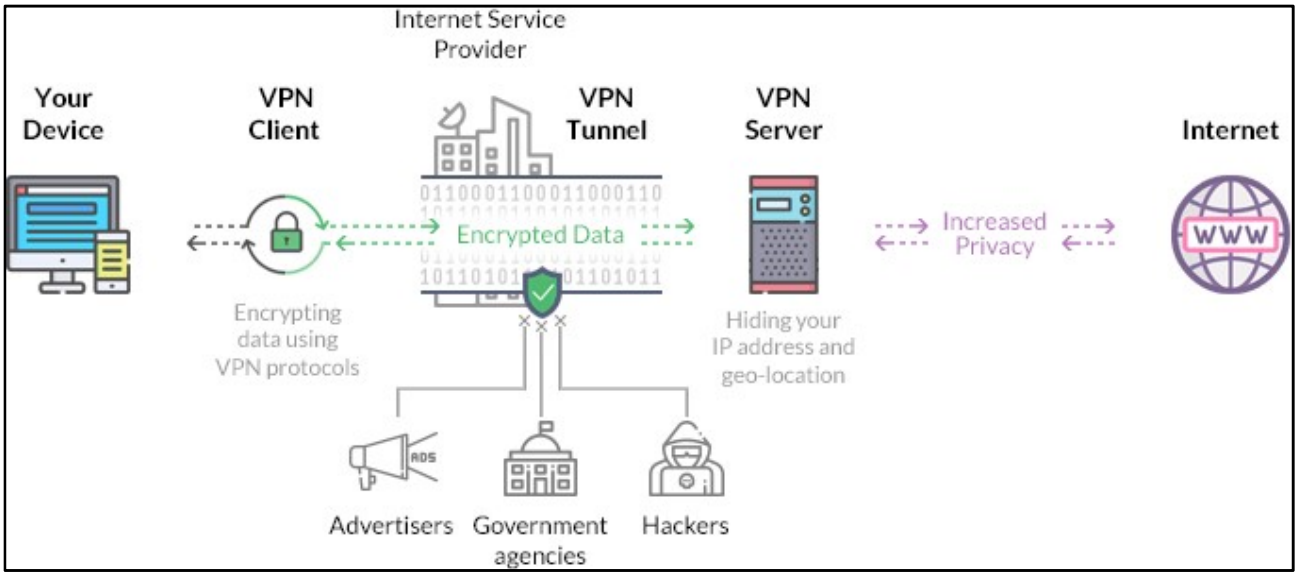


Figura 56 - Esquema de funcionamento de uma VPN[206].

Naturalmente que qualquer delinquente ou criminoso, mas também dissidentes e jornalistas, podem utilizar ligações VPN para se resguardarem (geoprivacidade) e comunicarem confidencialmente, como em tudo, há um lado mais obscuro e outro mais claro na utilização de ferramentas de privacidade. Um dos usos comuns das VPN é aceder a conteúdos *online* que só se encontram disponíveis em certas zonas geográficas, pois pode-se ligar a um servidor VPN nesse país, parecendo ao ponto final de destino que o tráfego vem daí, este uso é comum com plataformas de *streaming* (e.g. Netflix). As vantagens não se ficam por aqui, toda a pegada digital da navegação *online* não pode ser associada ao endereço IP do nosso equipamento, pois o que aparece é o do servidor VPN, por isso os *cookies* que se instalem não conseguem estabelecer o caminho, de publicidade, de volta ao nosso equipamento. Também se pode partilhar ficheiros, em P2P (*peer- to-peer*)[207], tipo Torrent, por exemplo, o que pode ser ilegal, mas não se podendo chegar até quem o fez.

Mas há uma questão, a empresa a quem contratamos o serviço VPN, pode ter registos das ligações que fazemos: sabe quem somos (pois o serviço é pago), não pode ver o conteúdo do tráfego, mas sabe para onde foi. Por essa razão, várias empresas que vendem o serviço garantem não manter registos, mesmo que sejam pedidos judicialmente não os entregam e podem, até, estar sedeadas em países onde a lei internacional não se aplica. Claro que tudo isto é muito bom e interessante, se for por uma "justa causa", a nossa privacidade, mas permite "esconder" muita actividade criminosa.

[206] https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-a-vpn-server-how-does-a-vpn-server-work/
[207] Peer-to-peer - Arquitectura de redes de computadores onde cada um dos pontos, ou nós da rede, funciona tanto como cliente quanto como servidor, permitindo compartilhar serviços e dados sem a necessidade de um servidor central (Wikipédia, 2019).

Há bastante informação *online* acerca das vantagens, limitações, potenciais do uso de VPN, é procurar, a oferta costuma incluir várias ligações (e.g. 6 ligações em simultâneo, sem limites de tráfego, com uma rede global de servidores), o que permite ligar o PC em casa, o portátil, o *tablet* e vários *smartphones*. Convém estudar a oferta, a densidade e velocidade dos servidores (a velocidade desce sempre), os tipos e graus de encriptação oferecidos, se têm *killswitch* (bloqueio total de acesso à Internet sem VPN*),* o regime de registo, que plataformas podem usar (Windows, iOS, Android, Linux), outros serviços oferecidos, etc.

Podem-se ver testes vários, em *sítios* especializados e credíveis da Internet, relativamente à oferta VPN[208], ou aquilo que se deve procurar no serviço[209], mas as principais são[210]:

https://www.expressvpn.com/

https://nordvpn.com/

https://www.cyberghostvpn.com/

TOR

O último e mais elevado grau de privacidade e anonimato, para navegar na Internet, pode ser alcançado utilizando um navegador específico (TOR), que utiliza uma rede própria – a rede TOR (*The Onion Router* – daí o símbolo ser uma cebola[211]), permitindo o acesso à *darkweb*, mas não só. Segundo a documentação (TOR Project, 2019), a rede TOR é constituída por "um conjunto de servidores operados por voluntários, que permite às pessoas melhorarem a sua privacidade e segurança na Internet. Os utilizadores do TOR [navegador] utilizam esta rede ligando-se através de uma série de túneis virtuais em vez de fazerem uma ligação directa [entre si e o servidor final], permitindo assim a partilha de informação, por indivíduos e organizações, em redes públicas, sem comprometerem a sua privacidade. Simultaneamente, o TOR é uma ferramenta efectiva de contorno à censura, permitindo aos seus utilizadores chegar a destinos, ou conteúdos, que de outra forma estariam bloqueados".

Mas qual a origem? Como funciona? O que pressupõe? O princípio de base da rede TOR, *onion routing* (encaminhamento cebola) foi desenvolvido em meados dos anos 1990 no Laboratório de

---

208 https://www.pcmag.com/roundup/296955/the-best-vpn-services, https://www.cnet.com/best-vpn-services-directory/, https://www.techradar.com/vpn/best-vpn, https://www.bestvpn.com/, https://www.lifewire.com/best-vpn-service-providers-4061659, https://www.vpnmentor.com/

209 https://www.computerworld.com/article/3186847/what-to-look-for-in-a-vpn-to-protect-your-privacy.html , https://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/ , https://vpnadviser.com/what-to-look-for-in-a-vpn/, https://www.vpnmentor.com/blog/10-things-look-for-when-buying-vpn/

210 Declaração de interesses, utilizo a NordVPN, contracto a três anos.

211 https://2019.www.torproject.org/index.html.en

Pesquisa Naval dos Estados Unidos[212], por um matemático e um cientista de computadores, para proteger as comunicações de segurança e espionagem dos E.U.A. *online*, tendo sido depois desenvolvido pelo DARPA[213] e depois, lançado ao publico em 2002, sendo o código aberto disponibilizado em 2004[214]. Há muita documentação sobre a origem, desenvolvimento e lógica subjacente à arquitectura da rede e navegador, tanto no sítio do projecto[215], como por toda a Internet.

Tentando simplificar e sintetizar o modo de funcionamento, pode dizer-se o seguinte: quando criamos tráfego na Internet, cada pacote de dados que circula, tem duas partes, uma parte de carga (correio, imagem, música, vídeo) e um cabeçalho, que permite o encaminhamento (*routing*) entre nós e o servidor de destino, onde está a indicação do ponto de origem, destino, dimensão, tempo. Interceptando o cabeçalho, espiando, pode-se saber muitíssima informação. A forma como a rede TOR funciona, digamos, é a seguinte: quando queremos enviar um pacote de dados, utilizando o navegador TOR, essa informação é encriptada, o cliente TOR no nosso dispositivo procura um ponto de entrada na rede e envia-lhe o pacote (ver Figura 57). Como está encriptado ninguém consegue ler o conteúdo, o ISP sabe o ponto de origem (nós) e de entrada na rede TOR, mais nada.

Quando entra na rede TOR, é como que novamente encriptado /daí a imagem das camadas da cebola), de forma que o nó de entrada sabe qual o destino seguinte (outro nó), mas não o destino final. A partir daqui, de uma forma completamente aleatória, cada novo nó acrescenta uma camada de encriptação (camadas da cebola) e faz seguir o pacote, que só conhece o nó anterior e o seguinte, até um nó de saída (o terceiro), entrando então na Internet (sem encriptação) até ao servidor final (ver Figura 58). Quando chega a este, a informação no cabeçalho do pacote, só refere o ponto de saída, não se conseguindo chegar ao ponto de entrada na rede TOR (o primeiro nó, chamado guarda), menos ainda ao ponto de partida inicial, nós. Mesmo que se intercepte e conseguisse desencriptar, o tráfego entre nós da rede, só se saberia o nó anterior e seguinte, nenhum nó conhece o trajecto completo.

Embora esta explicação seja muito simplificada, percebe-se que com esta arquitectura se salvaguarda a privacidade na origem, por isso o sistema é utilizado por jornalistas, denunciantes, ONG's, activistas políticos e, claro está, criminosos, bandidos, terroristas e todos os que têm algo a esconder (como discutido acerca da *Dark Web*). Mas a coisa complica-se, a cada cerca de dez minutos, ou se o utilizador quiser (clicando num botão no navegador), é criado um novo circuito através dos nós (ver Figura 60), o que ainda torna mais complicado (quase impossível), escutar e

[212] United States Naval Research Laboratory - https://www.nrl.navy.mil/
[213] Defense Advanced Research Projects Agency - https://www.darpa.mil/
[214] Tor (anonymity network) – Wikipédia (2019).
[215] https://2019.www.torproject.org/

"cheirar" o tráfego e não permitindo, caso houvesse intercepção, associar as acções (pacotes de tráfego) anteriores às novas.

Quando o servidor de destino, por exemplo o sítio de um jornal, responde, envia para o nó anterior, de onde recebeu o pedido, que é o nó de entrada na rede TOR, esse pacote não é encriptado, pode ser interceptado, mas só sabe que vai para um ponto de entrada na rede TOR, nada mais (ver Figura 59). Nunca é demais referir, como explicado antes, que é ESSENCIAL utilizar somente sítios com HTTPS (encriptados), quando se navega na Internet, sob pena de se poder ver e ler a informação que circula. Soube-se, em Maio de 2019, que o portal do Ministério Público, para apresentar queixas *online*, não era seguro, pois não funciona com HTTPS, sendo inseguro fazer queixas, pois o anonimato não está garantido[216].

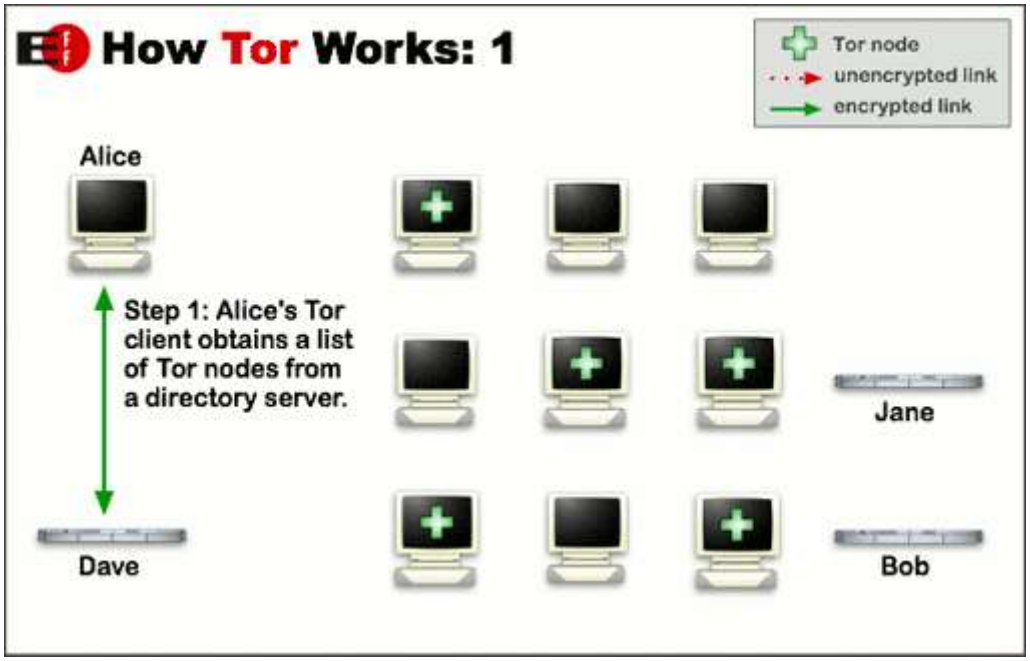


Figura 57 – Como funciona a Rede TOR, rede anónima distribuída (TOR Project, 2019).

Como se pode começar a navegar assim? Visitando o sítio do Projecto TOR, descarregando e instalando o navegador TOR[217], que se baseia no Firefox (há também uma versão para Android[218]), utiliza como motor de busca o DuckDuckGo (porque é anónimo), navegação privada (limpa o histórico todo quando se sai), tendo extensões de controlo de *scripts* bem como HTTPS Everywhere. Pode-se navegar em sítios "normais", mas o navegador e o uso da Rede TOR permitem, também, aceder aos sítios "cebola", que não estão listados e indexados por motores de busca e que

[216] https://www.tugaleaks.com/e-inseguro-apresentar-uma-queixa-no-portal-*online*-do-ministerio-publico.html?fbclid=IwAR3Yoc_vElrH5V1t3DL5X-GBhwYDRkCNVoQXoprrRotsN4Byyi24a_Ca4mo
[217] https://2019.www.torproject.org/download/download-easy.html.en
[218] https://thehackernews.com/2019/05/tor-browser-for-android.html?fbclid=IwAR3nAVPg_3PhOwor97EgqTCbY5GPKIIc6urcd3p0OYgd7ejKrbWXO%E2%80%A6

constituem, efectivamente, a *Dark Web*. Como se compreende, a velocidade de comunicação ressente-se (muito) de tanta volta e encriptação, como se pode ver na Figura 60, os circuitos variam e podem estar em continentes variados. Há, portanto, uma série de usos para os quais o TOR não é adequado, sobretudo grandes volumes de dados (i.e., *streaming*, redes sociais, Torrent, etc.), há muita informação acerca de quando se deve, ou não, utilizar TOR (Selecção de artigos na Nota de Rodapé)[219]. Deve-se ter atenção, cuidado e estudar devidamente o funcionamento, vantagens e perigos de utilizar o TOR, sobretudo se se quiser "andar" pela *Dark Web*, pois como é natural há muitas autoridades à caça por lá (felizmente).

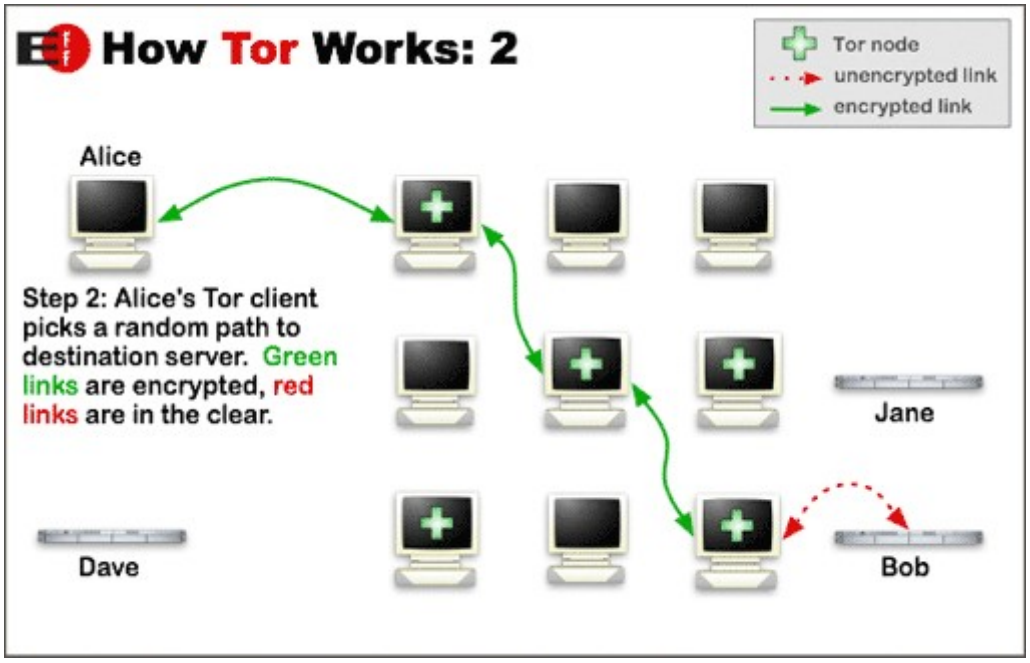


Figura 58 – Como funciona a Rede TOR, tráfego de saída (TOR Project, 2019).

Na *Dark Web*, os endereços são específicos, têm o sufixo ". onion"[220] e não há motores de busca, embora se possam encontrar sugestões e escolhas de sítios (cuidado…[221]), para os visitar têm de utilizar o navegador TOR. Várias empresas e entidades têm endereços ". onion", a Facebook[222], o New York Times[223], a Reuters[224] e outros entidades que, assim, podem receber informação,

[219] https://www.pcworld.com/article/2686467/how-to-use-the-tor-browser-to-surf-the-web-anonymously.html, https://www.hongkiat.com/blog/do-donts-tor-network/, https://gizmodo.com/tor-is-for-everyone-why-you-should-use-tor-1591191905, https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/, https://fossbytes.com/tor-anonymity-things-not-using-tor/, https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-and-why-do-people-use-it/#595f7edf7d75, https://www.howtogeek.com/114004/how-to-browse-anonymously-with-tor/

[220] Pode-se ver um bom resumo em: https://en.wikipedia.org/wiki/.onion

[221] https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/ , https://www.deepweb-sites.com/deep-web-links-2015/ , https://www.deepwebsiteslinks.com/ , https://www.makeuseof.com/tag/find-active-onion-sites/ , https://github.com/alecmuffett/real-world-onion-sites

[222] https://www.facebookcorewwwi.onion/

[223] https://www.nytimes3xbfgragh.onion/

[224] http://xdm7flvwt3uvsrrd.onion/

denúncias, pistas, de uma forma absolutamente anónima. A própria C.I.A. já se "instalou" na Rede TOR, segundo Waite (2019), para as pessoas poderem navegar no sítio da agência, anonimamente, ou enviar informações, até há uma área para crianças[225].

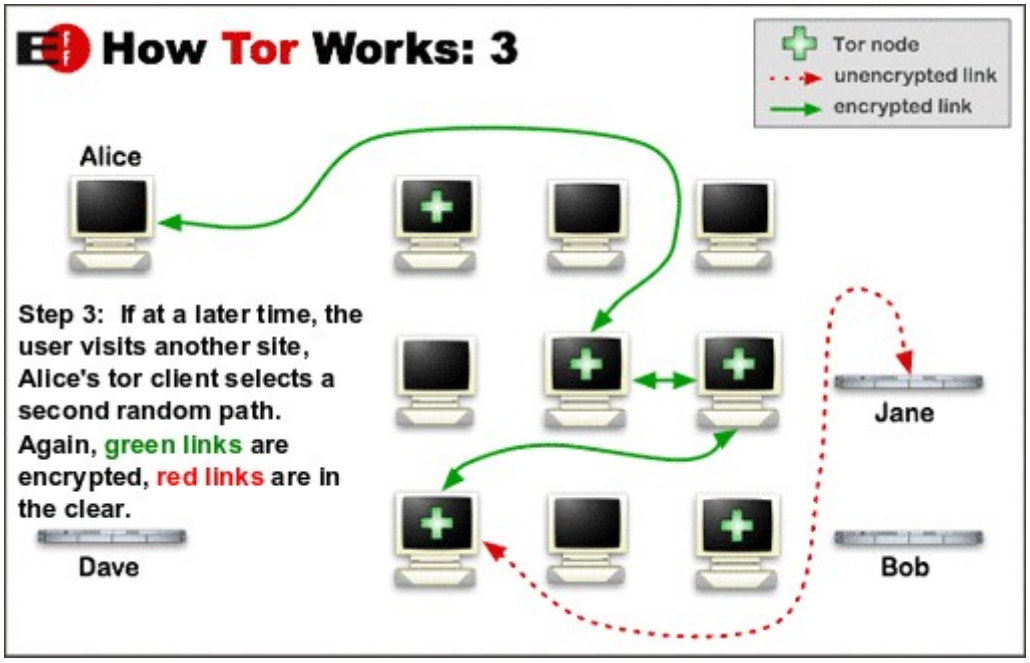


Figura 59 – Como funciona a Rede TOR, outro destino (TOR Project, 2019).

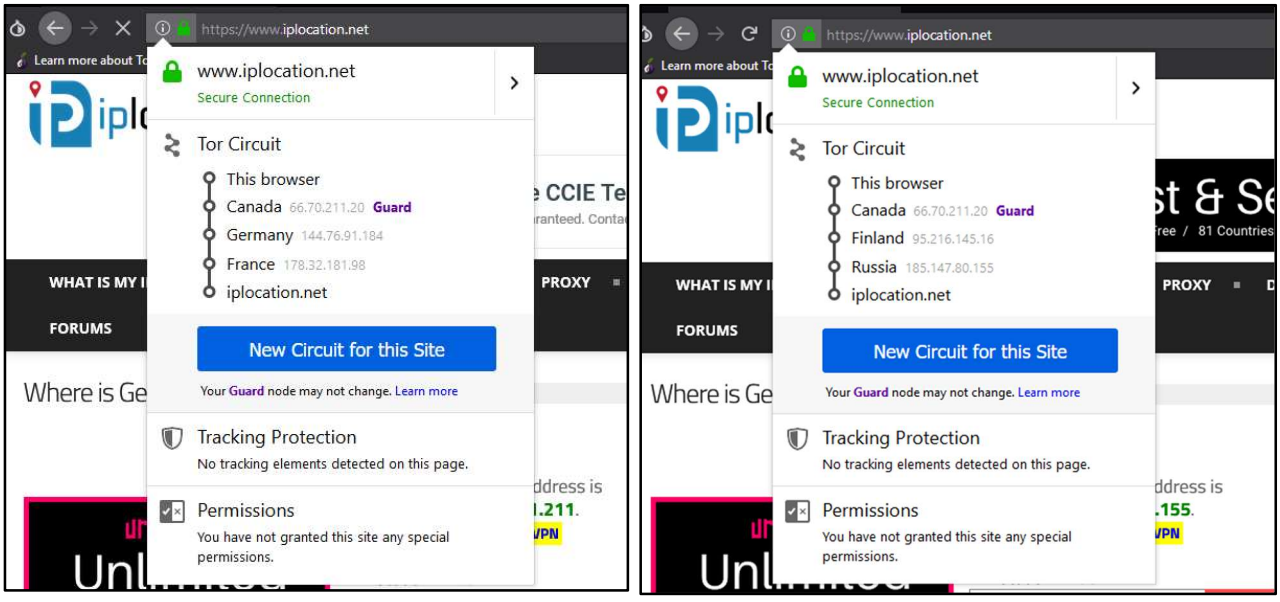


Figura 60 – Circuitos TOR, sítio IP Location, TOR Browser, para o servidor aparecem múltiplos endereços de localização do IP do utilizador, em vários países ou cidades, podendo-se renovar o circuito.

[225] CIA – sítio cebola - http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/index.html

O recurso ao TOR e à Rede TOR deve ser guardado para objectivos, situações e práticas muito específicas (estou, obviamente, a excluir as ilegais), mas é de facto o paradigma da privacidade *online*, embora quase a tocar o exagero, embora esse exagero seja necessário, infelizmente, em muitos locais e situações pelo mundo fora. Embora seja muito complicado explicar, quase tanto como perceber, não é 100% garantido que não se consiga interceptar e descodificar tráfego neste rede, embora isso só seja (teoricamente) possível por organizações secretas, governamentais, de alguns países poderosos, ou alianças de países.

Há um bom resumo dessas fraquezas, embora seja conteúdo muito técnico, na página da Wikipédia[226], mas as principais fraquezas prendem-se com os nós de saída e entrada na Rede Tor, *scripts* de sítios e aplicações (Hoffman, 2017). Parte dessas fragilidades podem ser colmatadas, visitando exclusivamente, sítios HTTPS, não instalando extensões nem diminuindo o nível de segurança no navegador TOR e nunca, mas nunca, gerir ou ser um nó de saída da rede TOR.

Podem-se encontrar na Internet informações, várias[227], sobre a segurança do TOR não ser total, mas para um utilizador normal e sem se ser paranóico, é virtualmente impossível interceptar e ler comunicações e saber a sua origem. Há, no entanto, uma forma de atingir quase os 100% de segurança, utilizando a Rede TOR sobre uma ligação VPN (Figura 61).

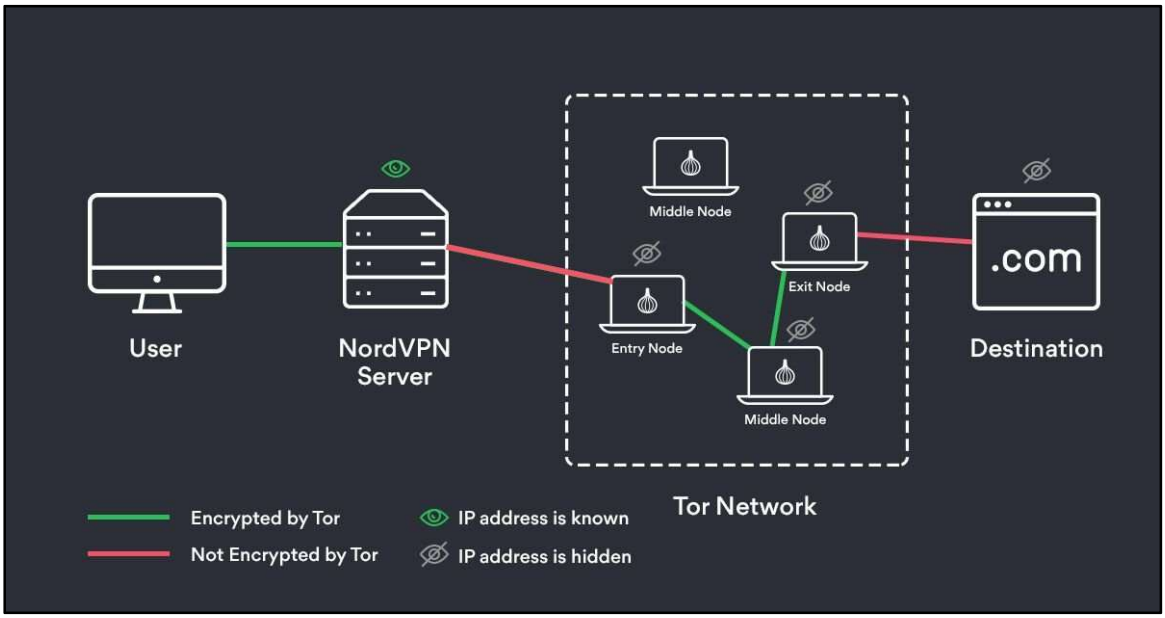


Figura 61 – Esquema de ligação TOR sobre VPN[228], utilizando um navegador TOR, a ligação sai duplamente encriptada do computador do utilizador.

[226] https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Weaknesses
[227] https://thetinhat.com/blog/primers/is-tor-safe.html , https://www.infosecurity-magazine.com/news/tor-is-not-as-safe-as-you-may-think/ , https://securitygladiators.com/tor-isnt-safe-think/ ,
[228] https://blog.bolehvpn.net/tor-over-vpn-vpn-over-tor-which-is-better/

Tentando descomplicar o que, agora, se torna ainda mais complicado, pode-se resumir o funcionamento e vantagens desta forma: o navegador TOR encripta o pacote de dados, que é encriptado pelo cliente VPN (túnel dentro de túnel), viaja passando pelo servidor do ISP (não sabe que é TOR, sabe que vai para VPN), chega ao servidor VPN (que sabe a origem, mas mesmo que quisesse ler o conteúdo não conseguia, pois está encriptado pelo TOR) e faz o pacote chegar ao ponto de entrada na Rede TOR (guarda, que agora não sabe a origem real do pacote, pois ele vem do servidor VPN). Entra na Rede TOR e sai, em direcção ao servidor de destino, que se for HTTPS garante encriptação dupla, até ao nó de entrada, encriptação simples, dentro da Rede TOR, encriptação simples entre o nó de saída e o servidor final. Na pior, das piores hipóteses, para se descobrir a origem (nós), só se chegava ao servidor VPN, se este não mantiver registos (por isso essa questão é tão importante), não se consegue chegar ao utilizador inicial. As vantagens desta solução, TOR sobre VPN, podem ser resumidas da seguinte forma (Crawford, 2016 e Aezean, 2017):

- Esta instalação é fácil de configurar, não requerendo conhecimentos técnicos avançados, basta ter um ISP (sem isso não se navega na Internet), um serviço VPN (que inclui software próprio) e instalar o navegador TOR;
- O ISP não sabe que se está a utilizar a Rede TOR, mas sabe que estamos a utilizar VPN;
- O nó de entrada da Rede TOR não vê o nosso endereço IP verdadeiro, mas sim o do servidor VPN, se quem vende o serviço VPN não tiver registos ou não os ceder, melhor;
- Permite acesso aos serviços escondidos, domínios cebola;
- É a melhor configuração em termos de segurança global.

Esta configuração também tem desvantagens:

- O servidor VPN sabe o nosso endereço IP real, por isso é essencial ter uma política de não registo e estar (idealmente) num território onde as leis internacionais não se aplicam[229];
- O tráfego, ao sair do nó da Rede TOR para a Internet, não está encriptado, mas para resolver isso basta utilizar, exclusivamente, sítios encriptados (HTTPS) e forçar o navegador a não utilizar outros (com extensões como o HTTPS Everywhere);
- Caso a ligação VPN caia, o tráfego TOR podia ficar exposto ao ISP, mas utilizando software VPN com *kill switch* (que desliga qualquer comunicação do PC caso não haja ligação VPN) o problema está resolvido;
- Pode-se ficar sem ligação, pois os nós TOR (alguns) são conhecidos e por vezes bloqueados (raríssimo).

[229] Por exemplo https://nordvpn.com/features/strict-no-logs-policy/ , comparativo em: https://www.vpnmentor.com/ ou https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/ ou https://www.cnet.com/best-vpn-services-directory/

Conclui-se que, com esta configuração e salvaguardando os pontos referidos, o anonimato e privacidade são, na prática, totais. Há outras configurações, muito complicadas e inalcançáveis para leigos, por exemplo ligar a uma VPN depois da saída da Rede TOR e antes do destino, ou ligar à VPN através da Rede TOR, além de não terem uma garantia praticamente total, como a solução apresentada antes. Alguns serviços VPN vendem soluções de ligação directa servidor VPN para a Rede TOR, o que permite utilizar um navegador normal, mas não é tão seguro[230], ou ainda, VPN sobre VPN, que cria um túnel VPN dentro doutro [231].

Como "desgooglar-me", como "apagar-me" da Internet…

Será que é possível desaparecer da Internet? Apagar a pegada digital existente? "Isso é praticamente impossível, mas pode-se tentar" (Ohlheiser, 2017), embora não sirva para (quase) nada se se quiser continuar a ter uma vida *online*, mesmo seguindo várias das soluções e recomendações anteriores, que permitem diminuir a pegada e controlar melhor a privacidade *online*. Mas antes de se tentar apagar a presença na Internet, deve-se ponderar muito bem antes de avançar, pois muito do que pode ser feito, não pode ser desfeito. Além de se perder informação, da presença que se quis desenvolver *online* (o tal marketing digital), pode não se conseguir reabrir contas várias com o mesmo nome (i.e., *email*, comércio *online*, serviços da nuvem, contactos institucionais, etc.).

Segundo WikiHow (2019), como "são medidas drásticas, não devem ser tratadas com leviandade. Considere o que o leva a «apagar-se» completamente. Está a ser perseguido [*cyberstalker*]? É uma má experiência isolada? Está somente farto da invasão na sua vida? Esteja seguro das suas motivações antes de decidir avançar. Há outras formas de resolver o problema, tais como mudar o nome *online* ou utilizar outra conta de *email*, em vez da sua? Por exemplo, se a sua conta corrente de *email* tem associações «desagradáveis» *online*, pode criar outra e usá-la exclusivamente para transacções profissionais. Tenha noção de que não se poderá, sequer, lembrar de parte dos sítios em que se registou, criou contas, participou, etc.".

A primeira abordagem possível, para quem possa, é pagar a alguém para fazê-lo, pois existem empresas especializadas em limpar e gerir a pegada digital, quatro exemplos:

- **DeleteMe**[232] - Gaba-se de ser a melhor, já "limpou" a pegada de vinte milhões de clientes, paga-se e vão removendo continuamente (preços aqui[233]);

[230] Por exemplo https://nordvpn.com/blog/tor-over-vpn/
[231] Por exemplo https://nordvpn.com/features/double-vpn/
[232] https://joindeleteme.com/
[233] https://www.abine.com/deleteme/plans.php

- **Deseat.me**[234] – Limpa as contas não utilizadas e outra informação, procura as contas *online*;
- **Reputation Defender**[235] – Gere a pegada digital, reparando resultados de buscas, limpado imagens e conteúdos negativos, para empresas e indivíduos;
- **Removeyour name**[236] – Retira informação pessoal, "enterra" conteúdo negativo.

Esquematicamente, dando exemplos porque é impossível cobrir todas as possibilidades, deve-se começar por (adaptado, revisto e particularizado a partir de várias, das muitas, fontes *online*[237]):

1. **Apagar contas principais**

   Facebook - https://www.facebook.com/help/delete_account
   Twitter - https://www.twitter.com/ -> settings and privacy -> deactivate account
   Instagram - https://www.instagram.com/ -> privacy -> managing account -> delete
   Google + - https://accounts.google.com/ -> data tools -> account -> delete
   YouTube – mesmo log in que em cima, depois apagar canais e subscrições
   LinkedIn - https://www.linkedin.com/ -> settings and privacy -> close account
   Flickr - https://www.flickr.com/ -> settings -> subscriptions -> delete (descarregar + apagar fotos)
   MySpace - https://myspace.com/ -> settings -> account -> delete
   PayPal - https://www.paypal.com/ -> account -> close
   eBay - https://www.ebay.com/ -> account settings -> close
   Site onde se podem apagar MUITAS contas - https://justdeleteme.xyz/
   ….
   Quando se começa a pensar em todas as contas, em lojas, clubes, organizações, escolas, universidades, sítios de jogos, serviços, etc., etc., etc., fica-se com a ideia da dimensão e, eventual, impossibilidade de fechar tudo. Mas não se deve desanimar nem desesperar, se é este o caminho a seguir, há que ser muito paciente, esperar levar (muito) tempo até se conseguir completar um processo desta natureza, ou até proceder somente a uma "limpeza".

2. **"Factos alternativos", onde não se pode apagar -** Haverá, certamente, contas que não se conseguem apagar, ou que só se conseguem desactivar (o que implica ficar informação no sistema), nesses casos há vários procedimentos possíveis:

---

234 https://www.deseat.me/
235 https://uk.reputationdefender.com/
236 https://www.removeyourname.com/
237 Por exemplo: https://www.dailymail.co.uk/sciencetech/article-2575745/How-DISAPPEAR-internet-9-step-guide-helps-people-vanish-without-trace-surf-anonymously.html, https://www.best-infographics.com/disappear-from-the-internet/ , https://www.cnet.com/how-to/remove-delete-yourself-from-the-internet/ , https://www.washingtonpost.com/news/the-intersect/wp/2017/02/10/erasing-yourself-from-the-internet-is-nearly-impossible-but-heres-how-you-can-try/?noredirect=on&utm_term=.acf9dc91d11f , https://www.whoishostingthis.com/blog/2013/12/12/how-to-disappear-online/, https://www.wikihow.com/Delete-Yourself-from-the-Internet

- Havendo razões pessoais de força maior, por exemplo alguém à procura de anonimato por questões de violência doméstica e com ordens – apoio judicial, contactar directamente os gestores / donos e fazer o pedido;
- Remover TODA a informação que seja possível, editando dados das contas, escrever por cima, pôr em branco, ou preencher com dados totalmente fictícios (não é justo pôr nomes de pessoas conhecidas…). Deve-se considerar usar "lixo" diferente em cada conta, senão está-se a criar um novo perfil, mas falso;
- Criar uma conta de *email* nova, gratuita, com o nome de utilizador mais improvável e informação falsa, associando todas as contas que não se conseguem apagar a este endereço de *email*. Se depois de feito o processo se cancelar o *email*, as contas ficam associadas a um endereço que já não existe;

3. **Fechar sítios pessoais** – Páginas na Internet, Blogs, Grupos, Fóruns, etc.
4. **Empresas** – Verificar e pedir para apagar detalhes pessoais, listas telefónicas, telecomunicações, todas e quaisquer bases de dados de cliente (nalguns casos impossível, água, luz, gás, bancos), mas pelo menos verificar que não estão *online*.
5. **Mailing lists** – Cancelar todas, é facilitado pois nos *emails* recebidos costuma haver instruções e ligações para o efeito. Para quem mantenha um arquivo completo de correio electrónico, uma boa abordagem é ir percorrendo e vendo tudo o que se recebeu, cancelando.
6. **Motores de busca** – Como discutido, acerca de procurar por nós próprios na Internet, deve-se procurar exaustivamente, com todo o tipo de combinações, em tantos motores de busca quantos possível, informação da pegada digital pessoal. Na maior parte das vezes em que não se pode apagar a pegada digital, pelo menos pode-se tentar apagar o resultado que aparece nas buscas. Uma hipótese, no caso de resultados relacionados com *posts* e comentários, é pedir a amigos e/ou conhecidos para os removerem.

   Deve-se ter noção, que dados antigos e referências indirectas e cruzadas, também são mantidos. Pode-se pedir aos motores de busca, oficialmente e com formulários para retirar informação (mais sobre isto adiante). Outra hipótese é contactar, directamente, quem gere os sítios da Internet, caso não haja informação localmente, tipo quem somos ou contactos, pode-se ir a https://www.whois.com/ e procurar que gere o domínio.

   - **Google** – O caso da Google é especial, pois o Tribunal Europeu da Justiça obrigou a Google (Russon, 2014) a "remover dados irrelevantes, inadequados, desactualizados, caso lhe seja

pedido", o direito ao esquecimento[238]. No sítio há Google está explicado como fazê-lo[239], existindo formulário e procedimentos próprios para o fazer[240].

7. **Contas de correio electrónico** – Encerrar, apagar, suspender, se for necessário manter uma conta, usar a fictícia, criada para o efeito. As contas pagas exigem, geralmente, um contacto específico, as gratuitas podem-se fechar e/ou acabam por ser apagadas ao fim de um certo tempo sem utilização. MUITA ATENÇÃO a informação que tenha interesse, deve ser descarregada e guardada antes de ser apagada no servidor e a conta fechada.
8. **Informação falsa e difamatória** – Procurar aconselhamento jurídico.

Depois de toas estas estapas, sabendo que é quase impossível fazer tudo e apagar tudo, há duas hipóteses: nunca mais ligar-se à Internet, não se utilizar qualquer dispositivo electrónico, ou telemóvel, desaparecer do mundo digital; ou então continuar-se *online*, mas com uma conduta de baixo perfil, baixa visibilidade, controlo da privacidade, sem redes sociais, navegação privada, buscas privadas, VPN, sem geolocalização, e/ou outras das sugestões apresentadas e discutidas. A grande questão é: poderemos mesmos desaparecer da Internet? Será que ela "deixa"?

"**Sur-veil-lance Cap-i-tal-ism, n.**

1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction and sales;
2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioural modification;
3. A rogue mutation of capitalism marked by concentration of wealth, knowledge, and power unprecedented in human history;
4. The foundational framework of a surveillance economy;
5. As significant of threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth;
6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy;
7. A movement that aims to impose a new collective order based on total certainty;
8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of people's sovereignty".

Zuboff (2019)

238 https://en.wikipedia.org/wiki/Right_to_be_forgotten
239 https://support.google.com/websearch/troubleshooter/3111061
240 https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf

Referências Bibliográficas

Adam, T. (2018, 23 Junho). The GPS app that can find anyone anywhere. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2018/jun/23/the-gps-app-that-can-find-anyone-anywhere

Aezean (2017, 19 Janeiro). TOR over VPN & VPN over TOR: which is better? *BolehVPN*. Disponível em: https://blog.bolehvpn.net/tor-over-vpn-vpn-over-tor-which-is-better/

Almeida, P. (2019, 8 Abril). Diz-me o que fazes, dir-te-ei quem és. *Público*. Disponível em: https://www.publico.pt/2019/04/08/tecnologia/analise/dizme-fazes-dirteei-es-1868035

Altawell, M. (2018, 1 Novembro). How does GPS technology affect our understanding of place? *GIS Lounge*. Disponível em: https://www.gislounge.com/gps-technology-affect-understanding-place/

Angwin, J. (2015). *Dragnet Nation*. Nova Iorque, E.U.A.: St. Martin's Griffin

Apt No 7 (2013, 13 Novembro). Smartphones are fundamentally changing human sexuality. *Business Insider*. Disponível em: https://www.businessinsider.com/smartphones-are-fundamentally-changing-human-sexuality-2013-11

Armstrong, M.P., Tsou, M.H. & Seidl, D.E. (2018) Geoprivacy. In B. Huang (Ed.) *Comprehensive Geographic Information Systems*. (415-430). Amsterdão, Elsevier. Disponível em: https://www.researchgate.net/publication/308995029_GeoPrivacy

Assange, J. (2014). Google is not what it seems. *Wikileaks*. Disponível em: https://wikileaks.org/google-is-not-what-it-seems/

Ataei, M., Debelo, A., Kray, C & Santos, V. (2018, Novembro). From legal text to implementation of privacy-aware location-based services. *ISPRS Int. J. Geo-Inf. 2018, 7*(11), 442. Disponível em: https://www.mdpi.com/2220-9964/7/11/442/htm

Bacchi, U. (2019, 25 Abril). Saudi sisters call for 'inhuman' woman-monitoring app to be removed by Google and Apple. *The Independent*. Disponível em: https://www.independent.co.uk/news/world/middle-east/saudi-arabia-women-tracking-app-absher-maha-wafa-al-subaie-a8885521.html

Ball, J. (2019, 26 Março). Europe's copyright dispute shows just how hard it is to fix the internet's problems. *MIT Technology Review*. Disponível em: https://www.technologyreview.com/s/613204/europes-copyright-row-shows-just-how-hard-it-is-to-fix-the-internets-problems/?fbclid=IwAR257yBXH7wKqxOtW7Iyu5uL-k1hhXNZ_UDXxiZIWlyCegQkDGLyyTDaBuE

Banafa, A. (2015, 9 Março). Internet of Things (Iot): security, privacy and safety. *DataFloq*. Disponível em: https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948

Bannan, C. (2016, 14 Agosto). The Iot threat to privacy. *TechCrunch*. Disponível em: https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/

Barber, G. (2019, 14 Maio). San Francisco bans agency use of facial-recognition tech. *Wired*. Disponível em: https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/

Barber, G. & Simonite, T. (2019, 17 Maio). Some US cities are moving into real-time facial surveillance. *Wired*. Disponível em: https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance/

Barros, A. (2018, 25 Maio). Um ano depois do RGPD… O que mudou? *DN Insider*. Disponível em: https://insider.dn.pt/opiniao/um-ano-depois-do-rgpd-o-que-mudou/

Bean, D. (2013, 14 Maio). "Geography of hate" maps "racist", "homophobic" tweets. *ABC News*. Disponível em: https://abcnews.go.com/Technology/geography-hate-map-racist-homophobic-tweets/story?id=19178370

Beck, J. (2018, 23 Fevereiro). How digital maps have changed what it means to be lost. *The Atlantic*. Disponível em: https://www.theatlantic.com/technology/archive/2018/02/you-are-here/553997/

Berzinya, A. (2018, 15 Agosto). Privacy experts weigh in on the risks in location data. *Turtler*. Disponível em: https://turtler.io/news/privacy-experts-weigh-in-on-the-risks-in-location-data

Blitz, M. (2017, 18 Abril). How GPS changed the way we think about our planet. *Popular* Mechanics. Disponível em: https://www.popularmechanics.com/science/environment/a26121/gps-earth-science/

Bode, K. (2019, 10 Janeiro). We could easily stop location data scandals, but we cower to lobbyists instead. *Motherboard*. Disponível em: https://motherboard.vice.com/en_us/article/nepx5x/we-could-easily-stop-location-data-scandals-but-we-cower-to-lobbyists-instead

Bosnjak, D. (2019, 3 Março). 5G making smartphone location privacy an even bigger joke. *Android Headlines*. Disponível em: https://www.androidheadlines.com/2019/03/5g-location-privacy-bigger-joke.html

Boyle, A. (2019, 4 Abril). Amazon's Project Kuiper aims to offer satellite broadband access. *GeekWire* Disponível em: https://www.geekwire.com/2019/amazon-project-kuiper-broadband-satellite/

Bradbury, D. (2019, 6 Janeiro). The illicit world of bitcoin and the Dark Web. *The Balance*. Disponível em: https://www.thebalance.com/what-is-a-dark-market-391289

Branco, M. (2018, 14 Fevereiro). Violência no namoro: jovens acham normal perseguir, proibir e abusar. *Revista Sábado*. Disponível em: https://www.sabado.pt/portugal/detalhe/violencia-no-namoro-jovens-acham-normal-perseguir-proibir-e-abusar

Brandon, J. (2016, 1 Junho). Security concerns rising for Internet of Things devices. *CSO Online*. Disponível em: https://www.csoonline.com/article/3077537/security-concerns-rising-for-internet-of-things-devices.html

Brandon, R. (2016, 21 Julho). Police 3D-printed a murder victim's finger to unlock his phone. *The Verge*. Disponível em: https://www.theverge.com/2016/7/21/12247370/police-fingerprint-3D-printing-unlock-phone-murder

Braw, E. (2018, 17 Dezembro). The GPS wars are here. *Foreign Policy*. Disponível em: https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/

Brookshire, B. (2017, 24 Agosto). On social media, privacy is no longer a personal choice. *Science News*. Disponível em: https://www.sciencenews.org/blog/scicurious/social-media-privacy-no-longer-personal-choice

Brown, D. (2019, 29 Janeiro). Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world. *Business Insider*. Disponível em: https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1

Brownstein, D. (2018, 5 Fevereiro). National security and personal bests. [Web Log post] *Musing on Maps*. Disponível em: https://dabrownstein.com/2018/02/05/national-security-and-personal-bests/

Buczkowski, A. (2016, 28 Maio). How accurate is your smartphone's GPS in an urban jungle? *GEO Awesomeness*. Disponível em: https://geoawesomeness.com/how-accurate-is-your-smartphones-gps-in-an-urban-jungle/

Burgess, M. (2018, 30 Janeiro). Strava's data lets anyone see the names (and heart rates) of people exercising on military bases. *Wired UK*. Disponível em: https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military

Burke, C. (2018, 30 Janeiro). Want to send your location to ISIS there's an app for that. *The Defense Post*. Disponível em: https://thedefensepost.com/2018/01/30/fitness-tracker-strava-opsec-risk/

Byler, D. (2019, 11 Abril). Smartphones and the internet gave the Uighurs a sense of their own identity – but now the Chinese state is using technology to strip them of it. *The Guardian*. Disponível em: https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition

Car, N. (2008, Agosto). Is Google making us stupid? What the Internet is doing to our brains. *The Atlantic*. Disponível em: https://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/306868/

Cebul, D. (2018, 16 Abril). High-cost satellites remain vulnerable to low-cost threats. *Defense News*. Disponível em: https://www.defensenews.com/digital-show-dailies/space-symposium/2018/04/16/high-cost-satellites-remain-vulnerable-to-low-cost-threats/

Chaffey, D. (2018, 11 Julho). Mobile Marketing Statistics compilation. *Smart Insights*. Disponível em: https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Chen, B. X. (2017, 12 Julho). When you should (and shouldn't) share your location using a smartphone. *The New York Times*. Disponível em: https://www.nytimes.com/2017/07/12/technology/personaltech/using-location-sharing-apps.html

Choi, J., Larson, M.A., Li, X., Li, K., Friedland, G. & Hanjalic, A. (2017). The geo-privacy bonus of popular photo enhancements. In *Proceedings of the 2017 ACM on International Conference on Multimedia Retrieval*, 84-9. Disponível em: https://www.researchgate.net/publication/317158917_The_Geo-Privacy_Bonus_of_Popular_Photo_Enhancements

Cimpanu, C. (2019, 22 Abril). EU votes to create gigantic biometric database. *ZD Net*. Disponível em: https://www.zdnet.com/article/eu-votes-to-create-gigantic-biometrics-database/

Cockerell, I. (2019, 9 Maio). Inside China's massive surveillance operation. *Wired*. Disponível em : https://www.wired.com/story/inside-chinas-massive-surveillance-operation/

Cole, D. (2014, 12 Maio). 'No place to hide' by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it all'. *The Washington Post*. Disponível em: https://www.washingtonpost.com/opinions/no-place-to-hide-by-glenn-greenwald-on-the-nsas-sweeping-efforts-to-know-it-all/2014/05/12/dfa45dee-d628-11e3-8a78-8fe50322a72c_story.html?utm_term=.b81a5a1bf100

Collins, K. (2017, 21 Novembro). Google collects Android users' locations even when location services are disabled. *Quartz*. Disponível em: https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Condliffe, J. (2017, 22 Março). This is your brain on GPS navigation. *MIT Technology Review*. Disponível em: https://www.technologyreview.com/s/603951/this-is-your-brain-on-gps-navigation/

Conger, K. (2018, Abril). Uber begins background collection of rider location data. *Techcrunch*. Disponível em: https://techcrunch.com/2016/11/28/uber-background-location-data-collection/

Cox, J. (2015, 18 Junho). The Dark Web as you know it is a myth. *Wired*. Disponível em: https://www.wired.com/2015/06/dark-web-know-myth/

Crampton, J.W. (2015, Agosto). Collect it all national security big data and governance. *Geo Journal, Volume 80*, Issue 4, pp 519–531. Disponível em: https://www.researchgate.net/publication/265950222_Collect_it_all_National_Security_Big_Data_and_Governance

Crawford, D. (2016, 26 Fevereiro). How to use a VPN and Tor together. *ProPrivacy*. Disponível em: https://proprivacy.com/guides/using-vpn-tor-together

Daniel, C. (2017, 12 Setembro). Speed, security, and trust for your big data. *SAP*. Disponível em: https://blogs.sap.com/2017/09/21/speed-security-and-trust-for-your-big-data/

Deepweb (2016, 23 Dezembro). How big is the deep web? A complete guide about the deep web. *Deepweb Sites*. Disponível em: https://www.deepweb-sites.com/how-big-is-the-deep-web/

Department of Defense (2018, 3 Agosto) MEMORANDUM - Use of geo location-capable devices, applications, and services. Disponível em: https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES-APPLICATIONS-SERVICES.PDF

Dewey, C. (2016, 19, Agosto). 98 personal data points that Facebook uses to target ads to you. *The Washington Post*. Disponível em: https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?tid=sm_tw

Dezember, R. (2018, 2 Novembro). Your smartphone's location data is worth big money to Wall Street, *The Wall Street Journal*. Disponível em: https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260

Director of National Intelligence (n.d.) Counterintelligence tips – Reducing your digital footprint. Disponível em: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Digitalfootprint.pdf

DN Insider (2019, 27 Maio). Quase 40% dos europeus estaria disposto a vender os dados pessoais. *Diário de Notícias*. Disponível em: https://insider.dn.pt/wow/europeus-estaria-disposto-a-vender-os-dados-pessoais/

Duhigg, C. (2012, 16 Fevereiro). How companies learn your secrets. *The New York Times Magazine*. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp

EDPS (2019, 8 Abril). *EDPS investigates contractual agreements concerning software used by EU institutions*. EDPS – European Data Protection Supervisor. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements_en

Engkehardt, S. (2017, 15 Novembro). No boundaries: exfiltration of personal data by session-replay scripts. *Freedom to tinker: research and commentary on digital technologies in public life*. Disponível em: https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

EPIC.org (2019). Privacy and geotagging. *Locational Privacy*. Disponível em: https://epic.org/privacy/location/

ESET (2017, 28 Fevereiro). 10 reasons why cybercriminals target smartphones. *Welivesecurity*. Disponível em: https://www.welivesecurity.com/2017/02/28/10-reasons-cybercriminals-target-smartphones/

Estes, B. (2016). Geolocation—The risk and benefits of a trending technology. *ISACA Journal, Vol. 5*. Disponível em: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/geolocation-the-risk-and-benefits-of-a-trending-technology.aspx

Evans, D. (2011, Abril). The Internet of Things: How the next evolution of the internet is changing everything. *CISCO – White Paper*. Disponível em: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Faithfull-Williams, K. (2017, 16 Agosto). 4 ways your smartphone is changing your brain. *Netdoctor*. Disponível em: https://www.netdoctor.co.uk/healthy-living/wellbeing/a26303/smartphone-effects-on-brain-health/

Fawaz, K. & Shin, K.G. (2014, 3 Novembro). Location privacy protection for smartphone users. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* 239-250. Disponível em: https://kabru.eecs.umich.edu/papers/publications/2014/ccsfp035-fawaz.pdf

Fegan, J. (2016, 18 Setembro). Digital use changes human behaviour with people using smartphones as extensions of their memories. *Irish Examiner*. Disponível em: https://www.irishexaminer.com/ireland/digital-use-changes-human-behaviour-with-people-using-smartphones-as-extensions-of-their-memories-421437.html

Ferrara, E., De Meo, P., Catanese, S. & Fiumara, G. (2014, 3 Abril). Detecting criminal organizations in mobile phone networks. *MIT Technology Review*. Disponível em: https://www.technologyreview.com/s/526471/how-to-detect-criminal-gangs-using-mobile-phone-data/

Ferreira, V. & Siza, R (2018, 18 Julho). Nova multa recorde ao Google: 4340 milhões de euros por abuso no Android. *Público*. Disponível em: https://www.publico.pt/2018/07/18/economia/noticia/bruxelas-google-android-1838339

Fish, T. (2009). *My Digital Footprint - A two-sided digital business model where your privacy will be someone else's business!* Londres: Futuretext

Foody, G. et al (ed.) (2017) *Mapping and the Citizen Sensor*. Londres, R.U., Ubiquity Press. Disponível em: https://ia800102.us.archive.org/31/items/2017MappingAndTheCitizenSensor/2017_mapping-and-the-citizen-sensor.pdf

Franceschi-Bicchierai, L. (2019, 24 Abril). Hacker finds he can remotely kill car engines after breaking into GPS tracking apps. *Motherboard*. Disponível em: https://motherboard.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps

Franklin, E. (2019, 27 Março). 6 ways to delete yourself from the internet. *C-Net – How to*. Disponível em: https://www.cnet.com/how-to/remove-delete-yourself-from-the-internet/

Freed, R. (20218, 11 Março). The tech industry's war on kids - how psychology is being used as a weapon against children. *Medium*. Disponível em: https://medium.com/@richardnfreed/the-tech-industrys-psychological-war-on-kids-c452870464ce

FTC (2015, Janeiro). Internet of Things: privacy & security in a connected world. *Federal Trade Commission – Staff Report*. Disponível em: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Garcia, J.E. (2019, 18 Janeiro). O valor dos nossos dados. *Público*. Disponível em: https://www.publico.pt/2019/01/18/tecnologia/noticia/valor-dados-1858490

Garen, K. (2018, 5 Março). Your location data is being sold - often without your knowledge. *The intersection of Technology and Humanity* [Web Log post]. Disponível em: https://ubcckengaren.blogspot.com/2018/03/your-location-data-is-being-soldoften.html

Geolocation. (2019). In *Techopedia*. Consultado em 10 de Abril de 2019, disponível em: https://www.techopedia.com/definition/1935/geolocation

Geoprivacy (2019). In *Wiktionary*. Disponível em: https://en.wiktionary.org/w/index.php?title=geoprivacy&oldid=51797105

Gholipour, B. (2017, 21 Março). Using GPS devices may switch off your brain's GPS. *Live Science*. Disponível em: https://www.livescience.com/58348-using-gps-devices-turns-off-brains-gps.html

Gomes, N.R. (2019, 25 Março). "Eu sei onde estás e quero explicações" — para alguns jovens, a violência no namoro é vivida "online". *PÚBLICO*. Disponível em: https://www.publico.pt/2019/03/25/p3/noticia/sei-onde-quero-explicacoes-jovens-violencia-namoro-vivida-online-1866136

Gonçalves, M.E. (2019, 15 Abril). Uma "revolução silenciosa" ou a ilusão de controlo sobre os nossos dados. *PÚBLICO*. Disponível em: https://www.publico.pt/2019/04/15/tecnologia/analise/revolucao-silenciosa-ilusao-controlo-dados-1869189

Goode, L. (2019, 30 Abril). Should I spend $1,000 on a smartphone. *Wired*. Disponível em: https://www.wired.com/story/should-i-spend-1000-on-a-smartphone/

Google (2019). About targeting geographic locations. *Google Ads Help*. Disponível em: https://support.google.com/google-ads/answer/2453995?hl=en

GPS.gov (2018, Outubro). GPS location privacy. *Governance - Privacy*. Disponível em: https://www.gps.gov/policy/privacy/

Grabar, H. (2014, 9 Setembro). Smartphones and the uncertain future of "spatial thinking". *CityLab*. Disponível em: https://www.citylab.com/life/2014/09/smartphones-and-the-uncertain-future-of-spatial-thinking/379796/

Graham, M. (2019, 17 Maio). Google uses Gmail to track a history of things you buy — and it's hard to delete. *CNBC*. Disponível em: https://www.cnbc.com/2019/05/17/google-gmail-tracks-purchase-history-how-to-delete-it.html

Granvile, K. (2018, 19 Março). Facebook and Cambridge Analytica: what you need to know as fallout widens. *The New York Times*. Disponível em: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Greenberg, A. (2019, 9 Maio). Feds dismantle the dark-web drug trade – but it´s already rebuilding. *Wired*. Disponível em: https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/

Grothaus, M. (2019, 1 Março). 5G means you'll have to say goodbye to your location privacy. *Fast Company*. Disponível em: https://www.fastcompany.com/90314058/5g-means-youll-have-to-say-goodbye-to-your-location-privacy

Gruss, M. (2018, 11 Abril). A new target for hackers? Satellites. *Defense News*. Disponível em: https://www.defensenews.com/dod/2018/04/11/a-new-target-for-hackers-satellites/

Gurling, A. (2017, 24 Agosto). Improving your digital footprint—a quickstart guide. *Medium*. Disponível em: https://medium.com/your-brand/improving-your-digital-footprint-535f9846a856

Hadjarbegovic, N. (2015, 25 Novembro). Are we creating an insecure Internet of Things (IoT)? Security Challenges and Concerns. *Toptal – Developers*. Disponível em: https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

Halpern, S. (2019, 26 Abril). The terrifying potential of the 5G network. *The New Yorker.* Disponível em: https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network?fbclid=IwAR1W3CTrQQW4jFPRGnntxNjYJlnhhYAriTZNsCrnNY8Nyd8lQwKR3ud5lVc

Haselton, T. (2017, 19 Novembro). How to find out what Facebook knows about you. *CNBC*. Disponível em: https://www.cnbc.com/2017/11/17/how-to-find-out-what-facebook-knows-about-me.html

Henley, J. (2013, 7 Abril). How geolocation technology is helping save lives in the developing world. *The Guardian*. Disponível em: https://www.theguardian.com/technology/shortcuts/2013/apr/07/geolocation-technology-save-lives-developing-world

Hoffmann, C. (2017, 12 Julho). Is TOR really anonymous and secure? *How-To Geek*. Disponível em: https://www.howtogeek.com/142380/htg-explains-is-tor-really-anonymous-and-secure/

Honan, M. (2009, 19 Janeiro). I am here: one man's experiment with the location-aware lifestyle. *Wired*. Disponível em: https://www.wired.com/2009/01/lp-guineapig/?currentPage=all

Hsu, J. (2018, 29 Janeiro). The Strava heat map and the end of secrets. *Wired*. Disponível em: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Hvistendahl, M. (2017, 14 Dezembro). Inside China's vast new experiment in social ranking. *Wired*. Disponível em: https://www.wired.com/story/age-of-social-credit/

IBM (2017, 17 Novembro). Top 10 IoT security challenges. *IBM Developer*. Disponível em: https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/

Internet Society. (2019). Your digital footprint matters. Disponível em: https://www.internetsociety.org/tutorials/your-digital-footprint-matters/

ISN (2018, 20 Abril). Ways in which hackers make money with stolen data. *Information Security Newspaper*. Disponível em: https://www.securitynewspaper.com/2018/04/20/ways-hackers-make-money-whit-stolen-data/

Jefroykin, S. (2018, 5 Abril). How geolocation technology can benefit city managers. *Zencity*. Disponível em: https://info.zencity.io/blog/how-geolocation-technology-can-benefit-city-managers

Kaplan, D. (2016, 22 Abril). Overwhelming number of smartphone users keep location services open. *GEO Marketing*. Disponível em: https://geomarketing.com/overwhelming-number-of-smartphone-users-keep-location-services-open

Kar, B. & Ghose, R. (2014). Is my information private? Geo-privacy in the world of social media. *CEUR Workshop Proceedings*. 1273. 28-31. Disponível em: http://stko.geog.ucsb.edu/gio2014/gio2014_submission_7.pdf

Kaspersky (s.d.). What are Biometrics: pros and cons of biometrics. *Kaspersky Lab US*. Disponível em: https://usa.kaspersky.com/resource-center/definitions/biometrics

Kastrenakes, J. (2017, 25 Setembro). GPS will be accurate within one foot in some phones next year. *The Verge*. Disponível em: https://www.theverge.com/circuitbreaker/2017/9/25/16362296/gps-accuracy-improving-one-foot-broadcom

Katz, J. (2017, 7 Agosto). What music do Americans love the most? 50 detailed fan maps. *The New York Times*. Disponível em: https://www.nytimes.com/interactive/2017/08/07/upshot/music-fandom-maps.html

Kelly, M. (2019, 25 Abril). Facebook broke Canadian privacy law, according to regulators. *The Verge*. Disponível em: https://www.theverge.com/2019/4/25/18515929/facebook-privacy-law-canada-ftc-eu-gdpr

Keßler, Carsten & McKenzie, Grant. (2017). A Geoprivacy Manifesto. *Transactions in GIS* 22(11). Disponível em: https://www.grantmckenzie.com/academics/GeoprivacyManifesto2017.pdf

Khandelwal, S. (2016, 21 Setembro). Photos on dark web reveal geo-locations of 229 drug dealers - here's how. *The Hacker News*. Disponível em: https://thehackernews.com/2016/09/dark-web-drug-weapon.html

Khandelwal, S. (2019, 15 Abril). Google helps police identify devices close to crime scenes using location data. *The Hacker News*. Disponível em: https://thehackernews.com/2019/04/google-location-tracking.html?fbclid=IwAR3jnAMb2FOinA5ujYGBPIAkJZnKufRdhl3avypySWGFDs6hVTY8q%E2%80%A6

Kiliç, D.L. (2017). *Privacy paradox on geotagging*. (Master thesis). Faculty of Geosciences, Utrecht University, Holanda. Disponível em: https://dspace.library.uu.nl/handle/1874/365864

Klein, M. (2017, 10Julho). What is EXIF data, and how can I remove it from my photos? *How-To Geek*. Disponível em: https://www.howtogeek.com/203592/what-is-exif-data-and-how-to-remove-it/

Korolov, M. (2019, 12 Fevereiro). What is biometrics: and why collecting biometric data is risky. *CSO Online*. Disponível em: https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html

Kounadi, O., & Leitner, M. (2014). Why does geoprivacy matter? The scientific publication of confidential data presented on maps. *Journal of Empirical Research on Human Research Ethics,* 9(4), 34-45. Disponível em: https://www.researchgate.net/publication/264858437_Why_Does_Geoprivacy_Matter_The_Scientific_Publication_of_Confidential_Data_Presented_on_Maps

Kulkarni, C. (2017, 6 Fevereiro). 15 ways geolocation is totally changing marketing. *Fortune*. Disponível em: http://fortune.com/2017/02/06/geolocation-marketing/

Kuo, L. (2019, 1 Março). China bans 23m from buying travel tickets as part of 'social credit' system. *The Guardian*. Disponível em: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system

Kushner, D. (2016, 15 Novembro). Is your GPS scrambling your brain? *Outside*. Disponível em: https://www.outsideonline.com/2135771/your-gps-scrambling-your-brain

LaMonte, T. (2018, 16 Março). What is dark data 7 questions you were afraid to ask. *GetApp LAB – Insights*. Disponível em: https://lab.getapp.com/what-is-dark-data-7-questions-you-were-afraid-to-ask/

Langham, R.Y. (2019). How smartphones impact our sex lives? *Everyday Power*. Disponível em: https://everydaypowerblog.com/how-smartphones-impact-our-sex-lives/

Lawson, S. (2012, 6 Abril). Ten ways your smartphone knows where you are. *PC World*. Disponível em: https://www.pcworld.com/article/253354/ten_ways_your_smartphone_knows_where_you_are.html

Leslie, I. (2016, Novembro). The scientists who make apps addictive. *The Economist*. Disponível em: https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive

Leskin, P. (2018, 30 Dezembro). The 21 scariest data breaches of 2018. *Business Insider*. Disponível em: https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12

Loufgran, S. (2018, 29 Janeiro). Advanced deanonymization through Strava. [Web Log post]. Disponível em: https://steveloughran.blogspot.com/2018/01/advanced-denanonymization-through-strava.html

Lucas, E. (2018, 21 Agosto). Your smartphone is likely tracking your location. *Phys ORG*. Disponível em: https://phys.org/news/2018-08-smartphone-tracking.html

Lynch, M. (2016, 19 Fevereiro). Leave my iPhone alone: why our smartphones are extensions of ourselves. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves

Marinova, E. (2019, 11 Janeiro). How a geolocation tool could transform urban design. *Onoffice magazine*. Disponível em: https://www.onofficemagazine.com/features/item/5484-how-a-geolocation-tool-could-transform-urban-design

Martins, J.L. (2018, 24 Maio). O Regulamento Geral de Protecção de Dados vai fazer a diferença. *Público*. Disponível em: https://www.publico.pt/2018/05/24/sociedade/opiniao/o-regulamento-geral-de-proteccao-de-dados-vai-fazer-a-diferenca-1831340

Massey, A. (2019, 18 Abril). Reveal: How global positioning changed the way we map, move, and live. *ESRI Blog*. Disponível em: https://www.esri.com/about/newsroom/blog/reveal-how-global-positioning-changed-the-way-we-map-move-and-live/

Mathews, L. (2017, 22 Setembro). Data from 540,000 GPS vehicle trackers leaked online. *Forbes*. Disponível em: https://www.forbes.com/sites/leemathews/2017/09/22/data-from-540000-vehicle-tracking-devices-leaked-online/#26151d3f274b

Matsakis, L. (2018, 20 Julho). Facebook confirms it's working on a new internet satellite. *WIRED*. Disponível em: https://www.wired.com/story/facebook-confirms-its-working-on-new-internet-satellite/

Maxwell, R. (2013, 8 Março). Spatial orientation and the brain: the effects of map reading and navigation. *GIS Lounge*. Disponível em: https://www.gislounge.com/spatial-orientation-and-the-brain-the-effects-of-map-reading-and-navigation/

Media Leaders (2018, 1 Fevereiro). How to increase your digital footprint & attract customers. [Web Log post] Disponível em: https://medialeaders.com/blog/increase-digital-footprint/

Meola, A. (2016, 19 Dezembro). How the Internet of Things will affect security & privacy. *Business Insider*. Disponível em: https://www.businessinsider.com/internet-of-things-security-privacy-2016-8

McAfee (2015). The hidden data economy - The marketplace for stolen digital information. *McAfee*. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf

McCaskill, S. (2018, 18 Setembro). Get ready for 6G mobile networks: 1Tbps speeds, microsecond latency and AI optimisation. *TechRadar PRO*. Disponível em: https://www.techradar.com/news/get-ready-for-6g-mobile-networks-1tbps-speeds-microsecond-latency-and-ai-optimisation

McIntosh, V. (2017, 26 Fevereiro). Geolocation data tracking: what are the privacy risks? [Web Log post] de Blog]. Disponível em: https://victoriamcintosh.com/geolocation-data-vs-privacy/

McKenzie, G.D, Janowicz, K. & Seidl, D.E. (2016, Junho). Geo-privacy beyond coordinates. Paper presented at AGILE, Helsinquia. Finlândia. Disponível em: https://www.researchgate.net/publication/301227285_Geo-privacy_beyond_coordinates

McGoogan, C. (2016, 22 Julho). Police 3D print murder victim's finger to unlock his phone. *The Telegraph*. Disponível em: https://www.telegraph.co.uk/technology/2016/07/22/police-3d-print-murder-victims-finger-to-unlock-his-phone/

McLaughlin, E. (2018, 6 Agosto). Defense Department bans geolocation features on tech devices due to security risk. *ABC News*. Disponível em: https://abcnews.go.com/International/defense-department-bans-geolocation-features-tech-devices-due/story?id=57063529

Melon, C. (2019, 26 Abril). Why a geocode is not an address. *Wired*. Disponível em: https://www.wired.com/story/geocode-address-puerto-rico-hurricane-maria/

Milner, G. (2016a, 2 Maio). How GPS is messing with our minds. *Time*. Disponível em: http://time.com/4309397/how-gps-is-messing-with-our-minds/

Milner, G. (2016b, 25 Junho). Death by GPS: are satnavs changing our brains? *The Guardian*. Disponível em: https://www.theguardian.com/technology/2016/jun/25/gps-horror-stories-driving-satnav-greg-milner

Misra, P. (2018, 11 Dezembro). 7 - All the ways in which your smartphone can track you and how to put an end to it. *Entrepreneur EUROPE*. Disponível em: https://www.entrepreneur.com/article/324598

Molla, R. (2019, 7 Maio). The rise of fear-based social media like Nextdoor, Citizen, and now Amazon's Neighbours. *Vox*. Disponível em: https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors

Montjoye, Y., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. (2013). Unique in the crowd: the privacy bounds of human mobility. *Nature, Scientific Reports,* Article number: 1376. Disponível em: https://www.nature.com/articles/srep01376.pdf

Mooney, P, Olteanu-Raimond, A-M, Touya, G, Juul, N, Alvanides, S & Kerle, N. (2017). Considerations of privacy, ethics and legal issues in volunteered geographic information. In: Foody, G, See, L, Fritz, S, Mooney, P, Olteanu-Raimond, A-M, Fonte, C C & Antoniou, V. (eds.) Mapping and the Citizen Sensor. 119–135. London: Ubiquity Press. Disponível em: https://archive.org/details/2017MappingAndTheCitizenSensor

Mota, M. (2019, 9 Março). Não é ficção: a China quer pontuar todos os comportamentos de cada cidadão. *Expresso*. Disponível em: https://expresso.pt/internacional/2019-03-09-Nao-e-ficcao-a-China-quer-pontuar-todos-os-comportamentos-de-cada-cidadao#gs.61pjvm

Moura, M.G. (2019, 16 Abril). Uma abominação que estranhamente parece não estar a incomodar por aí além. *Diário de Notícias*. Disponível em: https://www.dn.pt/opiniao/opiniao-dn/convidados/interior/uma-abominacao-que-estranhamente-parece-nao-estar-a-incomodar-por-ai-alem-10804651.html

Murphy, K. (2010, 11 Agosto). Web photos reveal secrets, like where you live. *The New York Times*. Disponível em: https://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html

Nakashima, R. (2018, 13 Agosto). Google tracks your movements, like it or not, *Associated Press*. Disponível em: https://apnews.com/828aefab64d4411bac257a07c1af0ecb

Newman, L.H. (2018, 7 Dezembro) The Wired guide to data breaches. *Wired*. Disponível em: https://www.wired.com/story/wired-guide-to-data-breaches/?GuideCarveLeft

Newman, L.H. (2019a, 19 Maio). Bluetooth's complexity has become a security risk. *Wired*. Disponível em: https://www.wired.com/story/bluetooth-complex-security-risk/

Newman, L.H. (2019b, 21 Maio). Google has stored some passwords in plaintext since 2005. *Wired*. Disponível em: https://www.wired.com/story/google-stored-gsuite-passwords-plaintext/

Newman, L.H. (2019c, 22 Maio). Facial recognition has already reached its breaking point. *Wired*. Disponível em: https://www.wired.com/story/facial-recognition-regulation/

Nield, D. (2017a, 4 Dezembro). The complete guide to cookies and all the scary stuff websites install on your computer. *Gizmodo*. Disponível em: https://gizmodo.com/the-complete-guide-to-cookies-and-all-the-scary-stuff-w-1794247382

Nield, D. (2017b, 6 Dezembro). Here's all the data collected from you as you browse the web. *Gizmodo*. Disponível em: https://gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304

NIeld, D. (2017c, 6 Dezembro). How to avoid getting tracked as you browse the web. *Gizmodo*. Disponível em: https://gizmodo.com/how-to-avoid-getting-tracked-as-you-browse-the-web-1821008719

Nield, D. (2018, 4 Janeiro). All the ways your smartphone and its apps can track you. *Gizmodo*. Disponível em: https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704

Nieva, R. (2019, 13 Abril). Law enforcement taps Google's Sensorvault for location data, report says. *Cnet*. Disponível em: https://www.cnet.com/news/law-enforcement-taps-googles-sensorvault-for-location-data-report-says/

Kilpatrick, H. (2018, 28 Dezembro). Become an online ninja: The ultimate guide to online anonymity. *NordVPN*. Disponível em: https://nordvpn.com/blog/how-to-be-anonymous-online/

Nouwt, J. (2008). Reasonable expectations of geo-privacy? *Script ED. 5*(2), 375-403. Disponível em: https://www.researchgate.net/publication/254799353_Reasonable_Expectations_of_Geo-Privacy

Nunez, M. (2016, 19 Agosto). All of the creepy things Facebook knows about you. *Gizmodo*. Disponível em: https://gizmodo.com/all-of-the-creepy-things-facebook-knows-about-you-1785510980

Oberhaus, D. (2019, 15 Maio). Space X is banking on Satellite Internet. Maybe it Shouldn't. *Wired*. Disponível em: https://www.wired.com/story/spacex-starlink-satellite-internet/

Olaye, M. (2017, 4 Novembro). Biometrics and facial recognition – a dangerous new frontier for data. *ITProPortal*. Disponível em: https://www.itproportal.com/features/biometrics-and-facial-recognition-a-dangerous-new-frontier-for-data/

Ohlheiser, A. (2017, 10 Fevereiro). Erasing yourself from the Internet is nearly impossible. But here's how you can try. *The Washington Post*: disponível em: https://www.washingtonpost.com/news/the-intersect/wp/2017/02/10/erasing-yourself-from-the-internet-is-nearly-impossible-but-heres-how-you-can-try/?noredirect=on&utm_term=.acf9dc91d11f

Oliveira, A. (2019, 4 Janeiro). Pegadas digitais e privacidade uma discussão urgente. *Público*. Disponível em: https://www.publico.pt/2019/01/04/tecnologia/opiniao/pegadas-digitais-privacidade-discussao-urgente-1856518

Oliveira, M. & Costa, R.M. (2018, 24 Maio). O que vai mudar nos dados pessoais. *Público*. Disponível em: https://www.publico.pt/2018/05/24/sociedade/perguntaserespostas/o-que-vao-mudar-nos-dados-pessoais-1830430

Paasche, T. & Klauser, F. (2015). Geography of surveillance and privacy. Disponível em: https://www.unine.ch/files/live/sites/inst_geographie/files/shared/Recherche/G%C3%A9ographies%20politiques/Espace%20et%20pouvoir/Publications/7.pdf

Palermo, E. (2013, 2 Maio). 5 places to look for your digital footprint. *TechNewsDaily, Mashable*. Disponível em: https://mashable.com/2013/05/02/your-digital-footprint/?europe=true

Palermo, E. (2014, 4 Junho). Google invests billions on satellites to expand internet access. *LiveScience*. Disponível em: https://www.livescience.com/46109-google-satellites-expand-internet-access.html

Patterson, D. (2019, 6 Abril). The dark web knows too much about me. *C-Net - Security*. Disponível em: https://www.cnet.com/news/the-dark-web-knows-too-much-about-me/

Pena, P. (2019, 20 Abril). Como o Facebook fez "chantagem" para não haver regulação europeia. *Diário de Notícias.* Disponível em: https://www.dn.pt/edicao-do-dia/20-abr-2019/interior/como-o-facebook-fez-chantagem-para-nao-haver-regulacao-europeia-10813242.html?targe%E2%80%A6

Pequenino, K. (2019a, 21 Janeiro). França multa Google em 50 milhões por infringir regras de privacidade. *Público*. Disponível em: https://www.publico.pt/2019/01/21/tecnologia/noticia/franca-multa-google-50-milhoes-euros-desrespeitar-regras-privacidade-europeias-1858779

Pequenino, K. (2019b, 25 Janeiro). Facebook vai fundir WhatsApp, Messenger e mensagens do Instagram. *Público*. Disponível em: https://www.publico.pt/2019/01/25/tecnologia/noticia/facebook-quer-fundir-whatsapp-messenger-mensagens-instagram-1859452

Pequenino, K. (2019c, 7 Fevereiro). Alemanha obriga Facebook a recolher e combinar menos dados dos utilizadores. *Público*. Disponível em: https://www.publico.pt/2019/02/07/tecnologia/noticia/alemanha-obriga-facebook-recolher-combinar-menos-dados-utilizadores-1861068

Pequenino, K. (2019d, 8 Abril). Software da Microsoft investigado na UE por recolha de dados. *Público*. Disponível em: https://www.publico.pt/2019/04/08/tecnologia/noticia/regulador-dados-europeu-investiga-programas-microsoft-utilizados-uniao-europeia-1868445

Pequenino, K. (2019e, 21 Abril). Quando o telemóvel alimenta uma relação abusiva. *PÚBLICO*. Disponível em: https://www.publico.pt/2019/04/21/tecnologia/noticia/tecnologia-telemovel-violencia-domestica-1869696

Perry, P. (2016, 24 Agosto). Cognitive offloading: how the internet is changing the human brain. *Big Think*. Disponível em: https://bigthink.com/philip-perry/cognitive-offloading-how-the-internet-is-changing-the-human-brain

Pesyna, K.M, Heath, R.W & Humphreys, E. (2015, 2 Fevereiro). Accuracy in the palm of your hand. *GPS World*. Disponível em: https://www.gpsworld.com/accuracy-in-the-palm-of-your-hand/

Phillips, C. (2014, 20 Novembro). How smartphones revolutionized society in less than a decade. *Government Technology*. Disponível em: https://www.govtech.com/products/How-Smartphones-Revolutionized-Society-in-Less-than-a-Decade.html

Ponte, C. & Castro, T.S. (2019, 29 Abril). Contar o tempo ou fazer com que o tempo conte? *Público*. Disponível em: https://www.publico.pt/2019/04/29/tecnologia/analise/contar-tempo-tempo-conte-1870182

Poon, L. (2015, 10 Novembro). Maps made 'from the mind,' not from GPS. *City Lab*. Disponível em: https://www.citylab.com/design/2015/11/maps-made-from-the-mind-not-from-gps/415128/

Porter, J. (2019, 1 Maio). Google will soon let you auto-delete your location tracking data. *The Verge*. Disponível em: https://www.theverge.com/2019/5/1/18525384/google-location-tracking-data-auto-delete-history-app-and-activity-data-3-18-months

Porter, K. (2019). Biometrics and biometric data: what is it and is it secure? *Symantec*. Disponível em: https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Privacy Rights Clearinghouse (2017, 19 Dezembro). Smartphone privacy. *Consumer Guides*. Disponível em: https://www.privacyrights.org/consumer-guides/smartphone-privacy

Reilly, C. (2017, 29 Novembro). Dark Web 101: Your guide to the badlands of the internet. *C-Net – Security*. Disponível em: https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/

Richard (2017, 1 Julho). The value of stolen data on the dark web. *Darkweb News*. Disponível em: https://darkwebnews.com/dark-web/value-of-stolen-data-dark-web/

Ricker, B., Schuurman, N. & Kessler, F. (2014). Implications of smartphone usage on privacy and spatial cognition: academic literature and public perceptions. *GeoJournal. 80*(5). Disponível em: https://www.researchgate.net/publication/264457190_Implications_of_smartphone_usage_on_privacy_and_spatial_cognition_academic_literature_and_public_perceptions

Rodewig, C. (2012, 7 Março). Geotagging poses security risks. *U.S. Army*. Disponível em: https://www.army.mil/article/75165/Geotagging_poses_security_risks

Roe, D. (2018, 7 Fevereiro). 7 big problems with the Internet of Things. *CMS Wire*. Disponível em: https://www.cmswire.com/cms/internet-of-things/7-big-problems-with-the-internet-of-things-024571.php

Russon, M.A. (2014, 14 Maio). Right to be forgotten how do I delete myself from Google. *International Business Times*. Disponível em: https://www.ibtimes.co.uk/right-be-forgotten-how-do-i-delete-myself-internet-1448572

Ryan, Olivia (2018, 15 Janeiro). How Big Data influences geolocation trends. *TechBullion*. Disponível em: https://www.techbullion.com/how-big-data-influences-geolocation-trends/

Rzeszewski, M. & Luczys, P. (2018) Care, indifference and anxiety—attitudes toward location data in everyday life. *ISPRS Int. J. Geo-Inf. 7*, 383. Disponível em: https://www.preprints.org/manuscript/201807.0214/v1

Samsung (2017, 30 Março). [In-Depth Look] Samsung's biometric technologies bring added security and convenience to the Galaxy S8. *Samsung Newsroom*. Disponível em: https://news.samsung.com/global/in-depth-look-samsungs-biometric-technologies-bring-added-security-and-convenience-to-the-galaxy-s8

Samuels, D. (2019, 23 Janeiro). Is big tech merging with big brother? Kinda looks like it. *Wired – Opinion*. Disponível em: https://www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/

Schiffner, B. (2013, 22 Julho). Could you fall victim to crime simply by geotagging location info to your photos? *Digital Trends*. Disponível em: https://www.digitaltrends.com/photography/could-you-fall-victim-to-crime-simply-by-geotagging-location-info-to-your-photos/

Schofield, J. (2017, 26 Janeiro). What is the best way to track someone with dementia? *The Guardian*. Disponível em: https://www.theguardian.com/technology/askjack/2017/jan/26/what-is-the-best-way-to-track-someone-with-dementia

Schroeder, S. (2017, 25 Setembro). Top 11 worst location data privacy breaches. *Turtler*. Disponível em: https://turtler.io/news/top-11-worst-location-data-privacy-breaches

Schroeder, S. (2018, 24 Agosto). Google in hot water for their rampant location data tracking. *Turtler*. Disponível em: https://turtler.io/news/google-in-hot-water-for-their-rampant-location-data-tracking

Schroeder, S. (2019, 4 Abril). Samsung Galaxy S10+ can be tricked by a 3D-printed fingerprint. *Mashable*. Disponível em: https://mashable.com/article/samsung-fingerprint-scanner-fooled-3d-printing/?europe=true

Schwartz, M.J. (2012, 20 Agosto). 7 facts about geolocation privacy. *DARK Reading*. Disponível em: https://www.darkreading.com/risk-management/7-facts-about-geolocation-privacy/d/d-id/1105877

Seldin, J. (2018, 30 Janeiro). Concern fitness tracking app exposed us military bases just the start. *Voanews*. Disponível em: https://www.voanews.com/a/strava-heat-map-sparks-concerns-of-military-security/4230808.html

Shakila-Bu-Pasha, Alén-Savikko, A., Mäkinen, J., Guinness, R. &Korpisaari, P. (2016) EU law perspectives on location data privacy in smartphones and informed consent for transparency. EDPL, *Vol 2,* 312-323. Disponível em: https://edpl.lexxion.eu/article/EDPL/2016/3/7

Shaner, J. (2013, 15 Julho). Smartphones, tablets and GPS accuracy. *ESRI - ArcGIS Blog.* Disponível em: https://www.esri.com/arcgis-blog/products/field-mobility/field-mobility/smartphones-tablets-and-gps-accuracy/

Sheperd. C. (2018, 20 Novembro). Beijing pioneering citizens' 'points' system critics brand 'Orwellian'. *Reuters*. Disponível em: https://www.reuters.com/article/us-china-society-points/beijing-pioneering-citizens-points-system-critics-brand-orwellian-idUSKCN1NP0FT

Siciliano, R. (2019, 14 Março). Safety, security and GPS geolocation. *The Balance*. Disponível em: https://www.thebalance.com/safety-security-and-gps-geolocation-1947457

Sly, L. (2018, 29 Janeiro). U.S. soldiers are revealing sensitive and dangerous information by jogging. *The Washington Post*. Disponível em: https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

Smith, L.M (2019, 20 Janeiro). 5 ways to power up your digital footprint. *Black Enterprise*. Disponível em: https://www.blackenterprise.com/5-ways-to-power-up-your-digital-footprint/

Schmitz, P. & Cooper, A. (2019). Using mobile phone data records to determine criminal activity space. *IQPC International GIS Crime Mapping Conference*. Disponível em: https://www.researchgate.net/publication/30510050_Using_mobile_phone_data_records_to_determine_criminal_activity_space

Shifter (2019, 6 Fevereiro). Quando o controlo matrimonial saudita chega ao smartphone. *Shifter*. Disponível em: https://shifter.sapo.pt/2019/02/absher-app-arabia-saudita/

STH (2019, 22 Março). 18 most popular IoT devices in 2019. *Software Testing Help*. Disponível em: https://www.softwaretestinghelp.com/iot-devices/

Sommer, R. & Friedland, G. (2010, Agosto). Cybercasing the Joint: On the privacy implications of geo-tagging. *Proceedings of the 5th USENIX conference on Hot topics in security*. Disponível em: https://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf

Spangrud, D. (2019, 18 Fevereiro). Geo-privacy and personal location information. *GEO Awareness*. Disponível em: https://geoawesomeness.com/geo-privacy-and-personal-location-information/

SSD (2018, 30 Outubro). The problem with mobile phones. *Surveillance Self-Defense*. Disponível em: https://ssd.eff.org/en/module/problem-mobile-phones

Steele, C. & Cohen, J. (2018, 14 Agosto). How to get Google to quit tracking you. *PC Magazine*. Disponível em: https://www.pcmag.com/article/345340/how-to-get-google-to-quit-tracking-you

Symantec. (2019). How to clean up your online digital footprint. Security Centre – *Privacy*. Disponível em: https://uk.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html

Taylor, S. (2019, 18 Março). 5 eyes, 9 eyes, 14 eyes – explained. *Restore Privacy*. Disponível em: https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/

Thompson, N. & Vogelstein, F. (2019, 16 Abril). 15 months of fresh hell inside Facebook. *Wired*. Disponivel em: https://www.wired.com/story/facebook-mark-zuckerberg-15-months-of-fresh-hell/

Tomé S. (2019, 6 Abril). Google e Facebook comem 86% do bolo da publicidade mundial. Qual o impacto? *DN Insider*. Disponível em: https://insider.dn.pt/featured/google-e-facebook-bolo-publicidade/

Tomlinson, A. (2017, 5 Janeiro). We're paying with our data: Why privacy can be a problem with apps. *CBC – Science and Technology*. Disponível em: https://www.cbc.ca/news/technology/marketplace-apps-privacy-smartphone-1.3919832

Toor, A. (2017, 29 Agosto). Uber will no longer track your location after your ride is over. *The Verge*. Disponível em: https://www.theverge.com/2017/8/29/16219542/uber-location-tracking-app-ios-android-privacy

TOR Project (2019). Tor: overview. *TOR Project*. Disponível em: https://2019.www.torproject.org/about/overview.html.en

Trend Micro (2019, 30 Janeiro). Managing digital footprints and data privacy. *Cybercrime & Digital Threats*. Disponível em: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/managing-digital-footprints-and-data-privacy

Truscot, L.K. (2019, 4 Maio). Using GPS instead of maps is the most consequential exchange of technologies in history. *Salon*. Disponível em: https://www.salon.com/2019/05/04/using-gps-instead-of-maps-is-the-most-consequential-exchange-of-technologies-in-history/

Twenge, J.M. (2017, Setembro). Have smartphones destroyed a generation? Disponível em: https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/

Unidad Editorial (2019) Geolocation democratises maps. *The Daily Prosper*. Disponível em: https://thedailyprosper.com/innovation/technology/geolocation-democratises-maps/?lang=en

University of Otago (2018, 31 Agosto). *Otago-led research set to make smartphones even smarter.* Disponível em: https://www.otago.ac.nz/news/news/otago694439.html

U.S. Army (n.d.) Geotags and location-based social networking, applications, OPSEC and protecting unit safety. *Social Media Roundup*. Disponível em: https://dmna.ny.gov/members/geotagging.pdf

Valentino-DeVries, J. & Singer, N. (2018, 10 Dezembro). How to stop apps from tracking your location. *The New York Times*. Disponível em: https://www.nytimes.com/2018/12/10/technology/prevent-location-data-sharing.html

Valentino-DeVries, J., Singer, N., Keller, M.H. & Krolik, A. (2018, 10 Dezembro) Your aps know where you were last night. *The New York Times*. Disponível em: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Valentino-DeVries, J. (2019, 13 Abril). Tracking phones Google is a dragnet for the police. *The New York Times*. Disponível em: https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Vallina-Rodríguez, N. & Sundaresan, S. (2017, 30 Maio). 7 in 10 smartphone apps share your data with third-party services. *The Conversation*. Disponível em: https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404

Vincent, J. (2019, 17 Abril). Microsoft denied police facial recognition tech over human rights concerns. *The* Verge. Disponível em: https://www.theverge.com/2019/4/17/18411757/microsoft-facial-recognition-sales-refused-police-access

Vogelstein, F. (2019, 24 Abril). Facebook will finally pay – billions – for its privacy missteps. *Wired*. Disponível em: https://www.wired.com/story/facebook-will-finally-pay-billions-privacy-missteps/

Waite, E. (2019), 7 Maio). The CIA sets up shop on TOR, the anonymous Internet. *Wired*. Disponível em: https://www.wired.com/story/cia-sets-up-shop-on-tor/

Warburton, Nigel (2019, 30 Abril). Existence precedes likes: how online behaviour defines us. *Aeon*. Disponível em: https://aeon.co/ideas/existence-precedes-likes-how-online-behaviour-defines-us

Ward, D. (2018, 9 Março). Fit to be spied fitness: trackers and OPSEC Risks. *NCO Journal, Army University Press*. Disponível em: https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2018/March/Fitbit/

Watson, Libby (2017, 28 Março). Congress just gave internet providers the green light to sell your browsing history without consent. *Gizmodo*. Disponível em: https://gizmodo.com/congress-just-gave-internet-providers-the-green-light-t-1793698939

Webster, T. (2018, 4 Março). Smartphone apps are tracking and selling your location data, often without you realizing it. *The Blaze*. Disponível em: https://www.theblaze.com/news/2018/03/04/smartphone-apps-are-tracking-and-selling-your-location-data-often-without-you-realizing-it

Whittaker, Z. (2016, 2 Junho). Stop Facebook tracking you across the web, change these settings. *ZD Net*. Disponível em: https://www.zdnet.com/article/to-stop-facebook-tracking-you-across-the-web-change-these-settings/

Whittaker, Z. (2019, Janeiro). 3D-printed heads let hackers – and cops – unlock your phone. *TechCrunch*. Disponível em: https://techcrunch.com/2018/12/16/3d-printed-heads-unlock-cops-hackers/

WikiHow (2019). How to delete yourself from the internet. *WikiHow*. Disponível em: https://www.wikihow.com/Delete-Yourself-from-the-Internet

Wilde, C. (2018, 4 Outubro). Your digital footprint: analyze and maximize for better results. *Social SEO*. Disponível em: https://www.socialseo.com/your-digital-footprint-analyze-and-maximize-for-better-results

WWW Foundation (2018, Julho). Online privacy: will they care? Teenagers use of social media and their understanding of privacy issues in developing countries. Disponível em: https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf

Zetter, K. (2016, 3 Março). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. Disponível em: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. Londres, R.U.: Profile Books.