CONTRADITÓRIO
think tank

Diogo Duarte | A erosão da privacidade no combate ao terrorismo no contexto europeu

Policy Paper 16/37 | Junho 2016

A erosão da privacidade no combate ao terrorismo no contexto europeu

Diogo Duarte

Policy Paper 16/37

Junho 2016

Contraditório Think Tank

www.contraditorio.pt

e-mail: info@contraditorio.pt

Citação: Diogo Duarte, 2016, "A erosão da privacidade no combate ao terrorismo no contexto europeu", Policy Paper 16/37, Contraditório Think Tank, www.contraditorio.pt

RESUMO

A Era digital trouxe consigo profundas transformações sociais. O rápido acesso à informação e às comunicações dilataram a exposição virtual de todos aqueles que recorrem à tecnologia, e sobretudo à Internet. A privacidade do século XIX não tem reflexo no modo como esta é perspetivada no atual século. Há um fenómeno de erosão, por vezes autoinfligido, outras, imposto, que nos leva à incerteza de qual a dimensão real da privacidade e qual o sentido de a sustentar nos seus moldes clássicos.

O artigo proposto assenta num quase-paradoxo atualmente existente: como garantir a privacidade sem comprometer a segurança? Esta questão, assume maior relevância, depois de conhecidas as revelações de Edward Snowden sobre os programas de vigilância em larga escala, operacionalizados pelos serviços de inteligência de vários países, dos quais os Estados Unidos da América mais se destacam.

A matriz da estratégia internacional de combate ao terrorismo, parece impor, impreterivelmente, a sonegação de uma importante parte do direito à privacidade. A constante monitorização dos cidadãos, parece igualmente inverter a lógica jurídica, concretamente fundada no juízo de que a suspeita generalizada se impõe ao espaço de liberdade individual, numa asserção que se poderia firmar na expressão: "Suspeito, até prova em contrário".

A finalidade deste artigo é colocar em debate ambos os aspetos desta questão e responder à questão: Qual o liminar do interesse público e do interesse privado no que diz respeito à privacidade?

Palavras-chave: Internet; Privacidade; Direitos Fundamentais; Segurança; Digital

Autor: Diogo Duarte

A privacidade na Era Digital

O combate ao terrorismo internacional veio ocupar, nos últimos anos, um lugar cimeiro nas tarefas fundamentais dos Estados. Proteger as populações dos ataques terroristas é um imperativo absoluto, mas que, muitas das vezes, dificilmente se consegue assegurar. A imprevisibilidade e aleatoriedade, enquanto características do terrorismo, comprometem a capacidade de investigação das autoridades policiais, contribuindo assim para o clima geral de insegurança. O desenvolvimento tecnológico, por outro lado, relevou ser um instrumento essencial para os grupos terroristas, tendo em conta os propósitos que os animam. Através da rede digital global, estes grupos operam a longa distância; disseminam as suas ideias políticas e religiosas; recrutam novos membros; e propagandeiam as suas ações.

Face a esta nova ameaça global – apelidada "Guerra sem rosto" –, as autoridades policiais e os serviços de inteligência foram impelidos a adotar novos mecanismos de prevenção e investigação. Com o objetivo claro de proteger e garantir a segurança das populações, estes mecanismos pretendem atuar no âmbito da prevenção e investigação do terrorismo. Por mais uma década, as autoridades implementaram, longe do olhar público, várias estratégias e programas de inteligência, que se concentraram na vigilância maciça das comunicações pessoais.

Em junho de 2013, os documentos revelados por Edward Snowden surgiram perante alguns dos mais conhecidos jornais internacionais – The Guardian e The Washington Post –, neles se descrevendo detalhadamente vários dos programas que haviam sido implementados pela National Security Agency (NSA) e pelo United Kingdom's Government Communications Headquarters (GCHQ). Estas revelações evidenciaram a existência de extensos programas de vigilância global, através dos quais se monitorizavam as comunicações privadas de milhares de cidadãos, incluindo políticos e diplomatas. Assistia-se a uma mudança de paradigma. Os Estados, além de espiar outros Estados, espiavam agora os seus cidadãos.

Vários responsáveis políticos afirmaram que a recolha de dados, possibilitada por estes programas, incidia somente sobre metadados, isto é, sobre o conjunto de

informações relativas a outros dados, não abrangendo o seu conteúdo. Todavia, a questão veio a apresentar-se mais complexa. Os documentos que, continuamente vieram a ser divulgados, comprovaram que o conteúdo das comunicações estava a ser recolhido, juntamente com os metadados. Na prática, qualquer atividade que se realizasse através de um dispositivo eletrónico – telemóvel, computador, tablet, etc. – era passível de ser monitorizada, recolhida e armazenada.

Sob uma assimilação orwelliana, estes programas de vigilância e monitorização foram fortemente contestados, e abriu-se um debate em torno da legitimidade de que os Estados dispõem para vigiarem os seus próprios cidadãos. Com o pretexto da segurança, o debate que rapidamente se ergueu, rapidamente se apagou. A necessidade de assegurar a proteção das populações perante os atos de terrorismo permitiu que se formasse um largo consenso acerca da mitigação do direito à privacidade, encarado esta abnegação como um mal necessário para um fim legítimo.

Tendo presente o potencial antagonismo entre a privacidade e a segurança, na perspetiva de que existem direitos humanos potencialmente derrogáveis perante a existência de outros valores que se procuram tutelar, o debate sobre o qual incide o presente artigo, revela-se cada vez mais necessário e urgente. O pouco conhecimento da população geral acerca dos direitos humanos tem contribuído para a larga desinformação que esta questão conhece. A revogação da privacidade, operando de forma quase tácita, melindra a defesa efetiva destes direitos universais, abrindo portas à sua violação. Benjamin Franklin, cedo se apercebeu que a Segurança rivaliza muitas vezes com a Liberdade tornando celebre o seu pensamento: “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety”.

A ideia de que a defesa da privacidade mais não é que um subterfúgio para a defesa da criminalidade resulta num discurso perigoso, legitimador da arbitrariedade. Por outro lado, o desejo de viver numa sociedade mais segura reforça o pensamento comummente instituído de que há que optar entre ter privacidade ou viver em segurança, descartando quase por completo a sua convivência.

Nesse sentido, a presente análise discorre sobre o direito à privacidade e as suas exceções, tendo como contraponto o combate ao terrorismo e a manutenção da

segurança das populações. Através desse exame, pretende-se dar resposta à seguinte questão: como pode o direito à privacidade vingar na Era Digital, onde a segurança se apresenta como uma premissa basilar?

A privacidade na Filosofia e no Direito

Para responder à questão proposta, afigura-se necessário investigar a função social que a privacidade cumpre, para, posteriormente, analisar o seu regime jurídico à luz dos principais instrumentos de proteção dos direitos humanos.

Com fundamento nas teses aristotélicas, depois desenvolvidas por Thomas Hobbes, John Locke, Richard Price e John Stuart Mill, a essência social do Homem positiva-se enquanto prolongamento do ente intrínseco. Significa isto que o Homem, na qualidade de "animal social e político", revê a sua singularidade quando projetada na sociedade com que interage. A participação social é assim perspetivada como uma extensão dos indivíduos, a qual não inibe, nem surge como contrapartida, da sua individualidade.

Não obstante do elemento conceptual da privacidade se centrar na liberdade, e não no seu conceito – até então inexistente –, esta foi defendida por John Locke, na sua obra "Two Treatises of Government" de 1690. Nela, o autor defende a autonomia que os indivíduos têm para dispor, da forma que melhor entenderem, da sua pessoa, dos seus atos e de tudo quanto lhes pertença, submetendo-se a tudo o que a lei prescreve e à luz da qual se regula a sociedade. Esta autonomia, hoje assimilada como um autêntico direito à privacidade, era, na conceção de Locke, o primado para o desenvolvimento da sociedade e dos indivíduos que a compõem. Por outro lado, autores como John Stuart Mill equiparavam o indivíduo aos Governos. Na sua obra "On Liberty" de 1850, o autor descreve o indivíduo como soberano sobre si, o seu corpo, e sua

mente. Somente os atos do indivíduo que melindrassem os demais indivíduos estariam sujeitos a deveres de conduta e acarretavam a responsabilidade pessoal e individual. Os demais atos, *i.e.,* aqueles sobre os quais o indivíduo é soberano, estavam sujeitos à sua inteira vontade e liberdade. Nesta linha de pensamento, a autonomia e

soberania que o indivíduo dispunha em relação aos atos que, intrinsecamente, só a ele diziam respeito, levavam á exclusão da sua submissão perante o arbítrio dos demais.

A linha filosófica que oriunda do Renascimento e da Idade da Razão impulsionou igualmente o desenvolvimento da importância conceptual das realidades do indivíduo. As bases criadas por estes ramos de pensamento contribuíram para o desenvolvimento do direito à privacidade, sedimentado enquanto estandarte universal. As primeiras referências diretas à existência de um Direito à Privacidade surgiram com Samuel Warren e Louis Brandeis, num artigo científico denominado "Right to Privacy", publicado pela *Harvard Law Review* em 1890. A concretização conceptual do direito à privacidade surgiu em resposta à invasão da vida privada e familiar de Warren por parte dos jornais da época, os quais se lançavam rumores sobre a sua pessoa e situação conjugal. Após um exausto exame das normas jurídicas que pudessem tutelar a privacidade, os autores alcançaram uma fórmula que, ainda que imperfeita, constituiu a base técnico-jurídica da sua redação atual. Concebido como o "direito a estar só", os autores firmaram consequentemente os elementos que se englobavam neste direito, ainda que muitas das vezes recorressem a uma formulação pela negativa. Assim, o direito de privacidade, tal como foi definido, não proibia a publicação de qualquer matéria que se revestisse de interesse publico e geral; não vedava em absoluto a publicação de matérias privadas; previa o consentimento do lesado enquanto motivo de exclusão da culpa e da responsabilidade; não admitia a *exceptio veritatis* enquanto meio de defesa processual do arguido; e de igual forma, a ausência de dolo do arguido não era admitida em sua defesa. Do cômputo final resultava que o direito de privacidade abrangia somente as matérias concernentes à vida privada, aos hábitos, atos e relações privadas, cuja publicação, não sendo do interesse público e geral, não seria legítima.

A privacidade no Sistema Universal de proteção dos Direitos Humanos

O contributo de Samuel Warren e Louis Brandeis foi fortemente aceite pelos cultores do Direito e bastante disseminado nos ordenamentos jurídicos do *common law*. A formulação original conheceu uma progressiva evolução e, apesar de hoje o direito à

privacidade se redigir, em termos técnico-jurídicos, pela positiva, não se pode deixar de reconhecer a influência destes autores. Com efeito, tal influência estendeu-se mesmo aos principais instrumentos internacionais de proteção dos Direitos Humanos. Atualmente, ao prever que "*Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei*", a Declaração Universal dos Direitos do Homem (abreviadamente DUDH), no seu artigo 12.º, releva a proximidade conceptual com a formulação que anteriormente revestia o direito à privacidade. Mais, repare-se que, na redação atual, inexiste um regime claro quanto às suas exceções, sendo que Declaração apenas dispõe quanto às intromissões arbitrárias, sem mais nada acrescentar. Posteriormente, introduzindo pequenas nuances, o Pacto Internacional dos Direitos Civis e Políticos de 1966 veio adotar a fórmula vigente na Declaração Universal dos Direitos do Homem. A coerência entre ambos os instrumentos, de natureza universal, revela, com plena evidência, o acolhimento da tese de Samuel Warren e Louis Brandeis.

A privacidade no Sistema Regional Europeu de proteção dos Direitos Humanos

Contemporânea à Declaração Universal dos Direitos do Homem, a Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais (abreviadamente CEDH) impôs-se como instrumento regional de proteção dos Direitos Humanos por excelência. Elaborada no seio do Conselho da Europa, a Convenção Europeia veio somente a ser aprovada dois anos após a Declaração Universal dos Direitos do Homem, a 4 de novembro de 1950, nela se incluindo originalmente o direito à privacidade, formulado no artigo 8.º como o Direito ao respeito pela vida privada e familiar. Com uma fórmula juridicamente mais detalhada, o n.º 1 do artigo 8.º da CEDH, principia por afirmar que "*Qualquer pessoa tem* ***direito ao respeito da sua vida privada e familiar,*** *do* ***seu domicílio*** *e da* ***sua correspondência***". Esta fórmula surge redigida pela positiva, como um direito baseado na dignidade humana, inculcando a premissa ativa de que todos gozam do direito a ver protegida a sua privacidade.

A grande diferença entre a redação pela positiva e pela negativa assenta no seu destinatário. Em ambos os casos se garante o direito à privacidade, todavia, quando formulada pela negativa, a norma tem como destinatário imediato os Estados e as demais pessoas – tanto singulares como coletivas –, e como destinatário mediato, o próprio indivíduo em nome do qual se inscreve este direito. Contrariamente, quando a redação jurídica se faz pela positiva, o seu destinatário imediato assenta no titular do direito, exigindo aos demais entes jurídicos – destinatários mediatos – o respeito pelo direito em causa.

Por essa mesma razão, a CEDH dirige-se aos demais entes jurídicos – Estados, pessoas coletivas, e pessoas singulares – no n.º 2 daquele artigo, fixando que "*Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver* ***prevista na lei*** *e constituir uma* ***providência*** *que, numa sociedade democrática,* ***seja necessária para a segurança nacional****, para a* ***segurança pública****, para o* ***bem-estar económico do país****, a* ***defesa da ordem*** *e a* ***prevenção das infracções penais****, a* ***protecção da saúde ou da moral****, ou a* ***protecção dos direitos e das liberdades de terceiros.***" Não valendo o direito à privacidade como um direito absoluto, ao contrário dos demais, os requisitos destacados constituem a sua exceção. Com assento em importantes princípios jurídicos, esta exceção traz à colação o princípio da legalidade, fundamento na exigência da ingerência se encontrar tipificada na lei; o Estado de Direito Democrático, enquanto expressão de respeito pela dignidade humana; e o princípio da adequação, subdividido nos princípios da necessidade e proporcionalidade, exigindo que a interferência na privacidade se realize nos moldes estritamente necessários para atingir os fins enunciados, contando que o faça com a menor lesão possível para o titular deste direito.

Por seu turno, no seio da União Europeia optou-se pelo tratamento diferenciado desta questão. Na Carta dos Direitos Fundamentais da União Europeia – a qual possui o mesmo valor jurídico que o Tratado de Lisboa – o direito à privacidade autonomiza-se no artigo 7.º, sob a epígrafe "Respeito pela vida privada e familiar", e no artigo 8.º, respeitante à "Protecção de dados pessoais". De forma simplificada, o primeiro artigo tutela a direito à privacidade como o direito que todas as pessoas têm ao respeito pela sua vida privada e familiar, pelo seu domicílio, e pelas suas comunicações. Já o segundo

artigo mencionado autonomiza a questão dos dados pessoais, garantido que "*Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito*". Tais dados, *"(...) devem ser objecto de um tratamento leal, para fins específicos, e com* ***o consentimento*** *da pessoa interessada ou com outro* ***fundamento legítimo previsto por lei***" sendo que "*Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação*".

Mais uma vez, tem-se presente – quanto ao primeiro artigo – a influência exercida pela Convenção Europeia dos Direitos do Homem, concretamente observável na redação jurídica positiva deste direito.

Contudo, maiores considerações são devidas ao artigo 8.º, o qual incide especificamente sobre a proteção dos dados pessoais. Como se sabe, o uso da Internet e das novas tecnologias gera um conjunto de dados referentes às atividades dos seus usuários, os quais muitas das vezes contêm informações de caracter privado. Nesse âmbito, ainda que o artigo tenha um alcance mais lato que o direito à privacidade, mantem-se com este intimamente ligado. Quanto ao seu regime de exceções, o n.º 2 do artigo 8.º da Carta da União Europeia exige que o tratamento dos dados, *i.e.*, o acesso, armazenamento, e utilização dos mesmos, deve prosseguir um fim específico, para o qual o seu titular tenha consentido, ou para o qual haja um fundamento previsto por lei.

Na senda da Convenção Europeia dos Direitos do Homem, a Carta Europeia traz igualmente à colação os princípios *supra* referidos, nomeadamente, o princípio da legalidade e o da adequação, necessidade e proporcionalidade. Em primeiro lugar, refere que os dados devem ser objeto de um tratamento leal, ou seja, devem ser objeto do tratamento digno, com respeito aos direitos fundamentais dos utilizados e à sociedade de Direito Democrático. Em segundo plano, o tratamento dos dados deve realizar-se tendo em conta um fim específico, evitando desta forma a arbitrariedade e o uso abuso dos mesmos. Quando dispensado o consentimento, exige-se que haja um fundamento legítimo previsto em lei.

Sobre este aspeto, há que fazer três menções: primeiro, o fundamento exigido impõe-se à aleatoriedade, enquanto elemento jurídico fundamental que possibilita o tratamento dos dados pessoais; segundo, este fundamento tem de ser legítimo, e esta legitimidade somente pode ser encontrada nas razões que disciplinam uma sociedade democrática

baseada no primado do Direito; e em terceiro, tal fundamento, ainda que legítimo, tem de ter apoio na letra da lei, não apenas para conferir previsibilidade e segurança jurídica, mas igualmente para conferir uma proteção efetiva ao seu titular, podendo este salvaguardar a sua posição sempre que, ainda que fundamentado e legítimo, o tratamento dos seus dados pessoais não tenha base na lei.

A privacidade enquanto direito fundamental no contexto europeu

Uma vez conhecido o quadro normativo do direito à privacidade no contexto europeu, importa conhecer o escopo substantivo deste direito, ou seja, os elementos materiais o corporizam.

O direito à privacidade, enquanto Direito Humano, consubstancia-se numa garantia jurídica que protege os indivíduos e outros entes jurídicos contra as ações ou omissões dos Governos que atentem contra a dignidade humana. Este é assim um direito universal que compartilha das características dos demais direitos da mesma espécie, a saber, é inalienável, inviolável, efetivo, imprescritível, irrenunciável, e – em relação aos restantes – interdependente.

No plano europeu, nomeadamente no seio do Conselho da Europa, a violação do direito à privacidade faz parte do rol dos principais direitos invocados perante o Tribunal Europeu dos Direitos do Homem. Por diversas vezes, o Tribunal de Estrasburgo condenou os Estados-membros por violações cometidas contra a privacidade dos indivíduos. Reconhecendo que a privacidade é entendida em sentido *lato*, o Tribunal tem evitado limitar o seu alcance através de uma qualquer definição, estabelecendo, no entanto, que o termo engloba a capacidade de cada um para determinar os seus atos e condutas, bem como para realizar atividades se natureza individual, ainda que estas sejam perspetivadas como moral ou fisicamente prejudicais ao indivíduo – caso *Pretty v. The United Kingdom* (pedido n.º 2346/02 de 29 de abril de 2002).

Não obstante, considerando que a presente análise versa sobre privacidade na Era Digital, no contexto do combate ao terrorismo, é possível obter-se, através de uma breve

análise jurisprudencial, os principais elementos que compõem o escopo material deste direito.

Assim sendo, o Tribunal de Estrasburgo considerou, no caso *Roman Zakharov v. Russia* (pedido n.º 47143/06, de 4 de dezembro de 2015), que a recolha e armazenamento de dados pessoais constituem uma violação do direito de privacidade, valendo a mesma regra para a interceção e monitorização eletrotónica das comunicações dos indivíduos, quando para tal não é dado o consentimento do indivíduo, nem há fundamento legal que o justifique.

No mesmo sentido, as comunicações telefónicas corporizam o escopo do direito à privacidade. No caso *Halford v. United Kingdom* (pedido n.º 20605/92 de 25 de junho de 1997), conclui-se que a interceção das comunicações telefónicas sem qualquer base legal que a justifique, constitui uma potencial violação do direito à privacidade.

A recolha de informações pode constituir igualmente uma interferência a este direito. No caso *Rotaru v. Romania* (pedido n.º 28341/95 de 4 de maio de 2000), o Tribunal deixou firmado que a recolha e armazenamento de informação pública é passível de constituir uma violação à privacidade, quando a mesma é executada de forma sistemática pelas autoridades.

A impossibilidade de acesso aos dados pessoais, nomeadamente àqueles que respeitam à vida privada dos indivíduos, impeliu o Tribunal a considerar, no caso *Gaskin v. the United Kingdom* (pedido n.º 10454/83 de 7 de julho de 1989), que havia uma violação ao direito à privacidade por parte das autoridades. O acesso aos dados pessoais é igualmente pressuposto da privacidade.

Importante no que respeita ao combate ao terrorismo, o caso *Gillan and Quinton v United Kingdom* (pedido n.º 4158/05 de12 de janeiro de 2010) deixou explicito que os poderes das autoridades britânicas revistar os cidadãos ainda que de forma aleatória, ainda que permitido à luz do Terrorism Act 2000, constituía uma violação do direito à privacidade.

Como se pode observar, a privacidade inviabiliza a recolha, armazenamento e tratamento de dados pessoais, quando para tal não haja base legal ou não tenha sido dado o consentimento do indivíduo em questão. Por outro lado, o respeito pelo direito à privacidade exige que seja transmitida informação sobre os dados recolhidos e que seja

facultado o acesso à consulta e alteração desses mesmos dados. Embora a questão não seja totalmente nova, verifica-se que o "direito a ser esquecido" inclui-se na consideração anterior, ou seja, aos indivíduos não assiste somente a possibilidade de acesso aos seus dados para alteração, mas também o direito de ver os seus dados retirados dos sistemas de dados existentes. Ainda que fosse possível alargar esta análise, os casos mencionados revelam, para o tema em questão, o núcleo fundamental do direito à privacidade.

Internet – questões sobre a privacidade

Em poucas décadas a Internet conquistou progressivamente a sociedade, deixando de ser exclusivamente uma plataforma militar. Consigo trouxe uma mudança de paradigma nas comunicações e relações humanas, alterando o quotidiano da sociedade. Esta rede digital possui atualmente milhares de utilizadores que a ela recorrem para comunicar entre si, para transacionarem bens e serviços, para gerirem os seus negócios e as suas empresas, para procurarem informação ou até encontrar entretinimento. Seja qual for o fim, resta uma certeza: a Internet representa um marco na História humana. Nem mesmo o Direito lhe ficou indiferente. Passando do mero plano da sua regulação, hoje os direitos tecnológicos afirmam-se enquanto direitos fundamentais de quarta geração. Igualmente, a consideração este é o "*último lugar da liberdade de expressão*" reflete a importância da Internet para o Direito.

Todavia é necessário relembrar que embora grande parte dos utilizadores recorra a Internet para fins legítimos, subsistem preocupações jurídicas e socais que devem ser devidamente acauteladas. A pirataria online, a fraude virtual, a economia paralela, o crime organizado, a disseminação do ódio, o *cyberbullying*, o acesso indevido a material impróprio por menores, e o roubo de identidade são alguns dos muitos exemplos que podem recortar de uma longa lista de crimes informáticos.

Por outro lado, se é justo afirmar que a Internet é um espaço de liberdade, é igualmente válido ajuizar pelas fragilidades que acarreta para a privacidade dos seus utilizadores. Desde logo, a ausência de um local físico-geográfico sobre o qual atue

determinada jurisdição revela o potencial conflito entre a Internet e o direito à privacidade, na medida em que não é possível garantir a existência de mecanismos legais que possuam força jurídica suficiente para punir os infratores. A existência de "paraísos informáticos" é assim uma realidade, na qual determinados crimes informáticos mantem-se praticamente impunes. O estímulo digital, a par da padronização de equipamentos e sistemas informáticos, contribui em larga medida para recolha e armazenamento de informações. O problema do armazenamento relaciona-se com a sua comercialização, existindo cada vez mais empresas que transacionam pacotes de dados relativos aos hábitos e interesses dos utilizadores.

Igualmente, a política de "*cookies*" é potencialmente lesiva do direito à privacidade do utilizador. O problema concreto quanto a este aspeto passa pelo armazenamento de informação que muitas das vezes é disposta de forma não voluntária. Embora os "*cookies*" obviem à capacidade de resposta dos servidores informáticos, os mesmos registam toda a informação do utilizador, nomeadamente aquela que contende aos seus padrões de comportamento. Ao fazê-lo, os "*cookies*" permitam o *tracking network*, ou seja, permitem detetar o rasto digital do utilizador, o que obviamente representa uma ameaça à privacidade, considerando sobretudo a comercialização destes dados.

Todavia, se estas são as ameaças concretas à privacidade que os utilizadores conhecem, não se pode descurar aquelas outras que provêm dos programas estaduais de monitorização e vigilância informática.

Foi com base na necessidade de combater o terrorismo, que os serviços de inteligência de vários países se viram compelidos a adotar novos métodos de prevenção e de investigação criminal. Durante mais de uma década, estes programas operaram sob o completo desconhecimento do grande público, até que em junho de 2013, altura em que Edward Snowden revelou os documentos que deram a conhecer detalhadamente as atividades que os serviços de inteligência haviam colocado em prática, naquele que ficou conhecido como o maior *leak* informático da História.

O debate em torno da legitimidade destes programas conheceu um intenso debate nos fóruns civis e jurídicos, onde a privacidade e a segurança foram os temas centrais. A polémica em torno da atividade da *National Security Agency* levou a que se exigisse maior transparência e informação, apertando o cerco aos serviços de inteligência.

Contudo, o despoletar de novos ataques terroristas, nomeadamente aqueles que ocorreram em Paris e Bruxelas, e a vinda de refugiados para a Europa endureceu o discurso pró-segurança, legitimando – tacitamente – os programas de vigilância maciça.

A segurança como exceção à privacidade

O consenso em torno da ideia de segurança, reforçou a legitimidade das autoridades. O sacrifício da privacidade passou a ser encarado como necessário no combate ao terrorismo, ainda que se reconhecesse a abusiva ingerência na privacidade dos cidadãos.

A defesa da segurança, em detrimento da privacidade, assenta em quarto argumentos principais.

O primeiro relaciona-se com a ideia de que os programas de monitorização, ainda que violem o direito à privacidade, objetivam alcançar um bem maior: a segurança. Assim, ao intercetarem as comunicações privadas, as autoridades têm a capacidade de prevenir e antecipar a ocorrência de novos ataques terroristas.

O segundo argumento fundamenta-se no raciocínio de que somente os criminosos receiam a monitorização das suas comunicações. Pelo contrário, todos aqueles que utilizam a Internet com finalidades que são legítimas, nada tendo a recear, não necessitam de proteger a sua privacidade e anonimidade.

A dissuasão é outro dos argumentos utilizados, segundo o qual, a consciência de que as suas atividades e comunicações são monitorizadas e registadas, constrange os comportamentos dos potenciais criminosos, desincentivando os seus propósitos.

Por último, adita-se o argumento de que a vigilância maciça não acarreta qualquer malefício para o público geral, garantindo-lhe, ao invés, maior segurança.

Estes argumentos têm sido largamente acolhidos, de tal modo, que hoje veicula a perceção de que segurança e privacidade não são compatíveis, havendo que optar por uma em detrimento da outra.

Em defesa da privacidade

Embora os argumentos relativos à segurança possam colher em determinados aspetos, os mesmos não devem ser exacerbados, considerando as fragilidades que encerram.

Em primeiro lugar – e para grande espanto – não existe registo de que os programas de monitorização e vigilância maciça levados a cabo pela *NSA* tenham prevenido ou intercetado qualquer ataque terrorista. Embora o sucesso dos programas fizesse parte do discurso oficial, os documentos revelados por Edward Snowed contrariam-no. Mesmo quando confrontado com estes documentos, o diretor da *NSA*, Keith Brian Alexander, retrocedeu no seu discurso, limitando-se a afirmar que estes programas auxiliam as autoridades a compreender e a estudar o fenómeno do terrorismo. E a razão do fracasso deste tipo de programas é evidente. Como explica Bruce Schneier na sua obra "*Data and Goliath*" o insucesso baseia-se no facto deste programa operar com uma grande margem de erro, o que impossibilita as autoridades de atuarem com precisão, uma vez que ao monitorizarem milhares de pessoas ficam impedidas de acompanhar em detalhe a atividade individual de cada uma delas. Outra dificuldade prende-se com a caracterização dos ataques terroristas, que sendo um ato tipicamente isolado e aleatório, impossibilita que se observem previamente quaisquer padrões de comportamento considerados suspeitos.

O segundo argumento apresentando falha na sua essência, pois parte do princípio de que somente os criminosos pretendem beneficiar do direito à privacidade. Este, como qualquer outro direito fundamental, inscreve-se a favor dos indivíduos exatamente para evitar o abuso por parte dos Estados. Como primeiramente foi analisado, a privacidade é intrínseca ao ser humano, e afastá-la em nome da segurança leva a que assista à sua uma "revogação" tácita, além de que permite aos Estados uma atuação arbitrária, contrária às sociedades democráticas baseadas no primado do Direito. Nesta lógica, a violação de direitos fundamentais revela-se como um problema ainda maior. Perante cada novo ataque terrorista não é apenas a segurança diminui, mas também a efetividade dos direitos fundamentais.

O argumento da dissuasão é igualmente contrariado à luz da realidade. Se a monitorização das comunicações se mostrasse como fator dissuasor, grupos como o Daesh não recorriam às redes sociais, e à Internet em geral, para disseminarem o seu ódio político e religioso, para recrutarem novos apoiantes, para estratificarem novos ataques e divulgarem os seus atos, dando-lhes caracter publicitário. De facto, a deteção das suas comunicações é uma das grandes preocupações destes grupos. Por esse motivo, o uso de programas de encriptação de dados ou mesmo o recurso à *deep web* e à *dark web* é bastante recorrente, dificultando a possibilidade de se efetuar um rastreio informático. Por oposição, a maioria do tráfego informático dá-se ao nível da *surface web*, onde as comunicações entre grupos terroristas ocorrem com pouca probabilidade.

O último dos argumentos mencionados também é passível de ser contrariado. De facto, a vigilância e a monitorização informática têm impacto na sociedade, por três ordens de razão. Em primeiro lugar, a abusiva ingerência do direito à privacidade, apresenta-se contrária a uma sociedade democrática baseada no Direito. Em segundo lugar, a existência de programas informáticos de inteligência como o PRISM – programa de vigilância que interceta comunicações de forma secreta – e o CAPPS – *Computer Assisted Passenger Prescreening System* – contrariam a lógica das garantias jurídicas inscritas a favor dos indivíduos. Através das comunicações intercetadas por estes programas, os indivíduos são catalogados como suspeitos consoante o seu grau de perigosidade, ficando a sua identidade e respetivos dados registados numa base digital. Ora, sendo tal facto alheio ao conhecimento dos indivíduos, coarta-se a possibilidade de estes afastarem as suspeitas que sobre si residem. Desta forma, o conteúdo essencial das garantias jurídicas é gravemente afetado. Por outro lado, o financiamento destes programas representa um custo efetivo que recai sobre todos os contribuintes. Países como os Estados Unidos da América concentram avultadas quantias na manutenção e desenvolvimento destes programas, não obstante do seu insucesso. Tais gastos refletem-se ainda na contração dos métodos tradicionais de investigação criminal, os quais tutelam a privacidade de forma equilibrada.

Desta presente exposição resulta, portanto, que a argumentação a favor da segurança não pode colher sem que a privacidade seja equacionada. Ambas as realidades devem suster-se num todo coerente, sem presidirem extremismos a favor de uma ou de outra.

Conclusão

Da súmula desta análise poder-se-á retirar a conclusão de que o direito à privacidade, enquanto direito humano, não pode, nem deve ser suprimido em razão a maior segurança das populações. Como se observou, a manutenção da segurança, não obstante de ser um fim legítimo aos Estados, não pode acarretar um prejuízo avultado para a privacidade.

Por outro lado, o enquadramento jurídico do direito à privacidade favorece sua a defesa nos seus moldes atuais. Não sendo este um direito absoluto, as suas exceções não deixam de conferir aos indivíduos importantes garantias jurídicas. Baseadas em princípios que presidem às sociedades democráticas baseadas no primado do Direito, estas exceções permitem igualmente às autoridades diligenciar pela segurança, concentrado a sua atuação em fatores relevantes e evitando a dispersão dos meios técnicos de investigação e prevenção do terrorismo.

Por último, dir-se-á necessário encontrar o equilíbrio entre a segurança e a privacidade, a fim de evitar o consentimento tácito perante as abusivas ingerências das autoridades policiais. Assim, se é verdade que o terrorismo afeta a segurança das populações, cabe aos Estados prevenir que este afete o direito à privacidade dos indivíduos. Caso contrário, o terrorismo vencerá.