2021

Entre o Vago e o Insuficiente: a Proteção de Dados em Portugal

CAROLINA PARDELHA GARCIA, FACULDADE DE DIREITO DA UNIVERSIDADE DE COIMBRA, ELSA COIMBRA

Índex

Conceito de dados pessoais 1
Entidades infratoras 3
Conflitos de direitos 4
Publicações consultadas 5

A questão da proteção de dados é daquelas questões que se provam em muitos aspetos território pouco calcado por juristas: mesmo com bases na legislação, há ainda da parte da lei, da jurisprudência e mesmo da doutrina um grande desconhecimento, até uma suspeita, em relação à matéria da proteção dos dados pessoais, particularmente nesta atual época de globalização e de informatização. Este contexto é indissociável desta discussão, remetendo sempre, de uma forma ou outra, para o mundo da tecnologia, um mundo que ainda é desconhecido para muitos de nós.

Prende-se aqui o primeiro dos muitos problemas desta temática, que vai muito para além da esfera do Direito: nem o leigo nem, verdade seja dita, o jurista, parecem ter noção precisa de tudo aquilo que é encapsulado dentro da noção de dados pessoais.

O conceito de dados pessoais parece estar ainda condenado a ter uma definição vaga. O artigo 35º/2 da Constituição conferiu ao legislador ordinário a competência para fixar uma definição, mas uma análise rápida dos primeiros artigos da Lei nº58/2019 mostra-nos que este age como se este fosse um conceito já estabelecido, privando-nos do que seria o nosso ponto de partida. Se não sabemos o âmbito de proteção torna-se difícil, talvez mesmo impossível, estabelecer mecanismos eficazes de proteção.

Assim sendo, se a ordem jurídica pretende estabelecer uma proteção eficaz dos dados pessoais dos cidadãos, tem de se deparar primeiro com algumas questões: que dados pessoais devem ser protegidos, contra quem e como irá resolver possíveis conflitos de direitos?

Qualquer facto relativo à nossa pessoa pode ser considerado um dado pessoal, mas este âmbito é demasiado vago e extenso para constar de uma lei. De um ponto de vista prático é impossível estabelecer um regime que nos garanta privacidade total de todos os aspetos da nossa pessoa. No máximo podemos estabelecer uma espécie de hierarquia, diferenciando a natureza e importância destes dados de modo a conferir dignidade superior a alguns deles.

O núcleo duro, essencial deste conceito pode ser apreendido facilmente com exemplos. O nosso nome, morada, dados financeiros, todos estes são dados que dizem diretamente respeito à nossa esfera particular e privada. Estes são dados que permitem a nossa identificação objetiva dentro de um vasto

universo de cidadãos. São as primeiras informações associadas ao conceito de dados pessoais, pelo que faz sentido que estejam sujeitos a um regime com mais regras e com sanções mais graves.

No nível mais básico desta discussão, o âmbito de proteção da lei terminaria aqui, mas a verdade é que experiências têm revelado que há outro tipo de dados que merecem proteção. Estes dados são um pouco mais sensíveis, dizem respeito a aspetos da nossa pessoa que permitimos serem conhecidos pela sociedade em geral, ou pelo menos pela nossa esfera social, mas que queremos proteger de determinadas entidades que possam usar esses dados contra os nossos interesses e até conta a nossa pessoa e o nosso bem-estar. Podemos chamar-lhes dados subjetivos.

Um texto sobre proteção de dados pessoais escrito em 2021 não pode ignorar o escândalo ainda este ano com CM de Lisboa, com o envio dos dados pessoais de organizadores e participantes de manifestações contra determinados regimes autoritários para as embaixadas desses precisos países.

A Constituição consagra certos direitos políticos, como o direito à manifestação, sendo esta uma liberdade pela qual se lutou arduamente. O exercício de todos estes direitos e liberdades revelam um dado fundamental quanto à nossa pessoa, a nossa orientação política. Este é um dado que a maior parte da população partilha com relativa facilidade, mas faz sentido que refugiados políticos ou outras pessoas que se procurem proteger contra regimes autoritários não queiram que estes dados possam ser conhecidos para além da extensão que consideram aceitável. Esta cautela, porém, não deve ser um impedimento ao livre exercício dos seus direitos.

Este nível de receio relativamente à proteção de dados pessoais pode não corresponder à experiência do cidadão comum de um Estado de Direito. Mas isto não significa que este não conte também com certas informações quanto à sua pessoa que se encontram no meio termo entre pessoal e de conhecimento mais ou menos generalizado e que mereçam tutela por parte da lei.

De momento é relevante apenas saber que é possível modelar vários aspetos da nossa vida online de acordo com aquilo que partilhamos, pesquisamos e publicamos. Um aspeto muito relevante que é afetado é o nosso consumo de informação: os algoritmos são capazes de detetar os nossos gostos e opiniões, dos mais inocentes aos mais fundamentais, de modo a condicionar o conteúdo que nos é apresentado, desde notícias, artigos ou até as publicações de terceiros, favorecendo aquilo que parecer mais compatível com o perfil que esse mesmo algoritmo cria de nós.

Num plano para nós mais relevante, tivemos já oportunidade de ver como esta manipulação de conteúdos é na verdade um entrave ao acesso a comunicação correta e fiável, significando, no limite, uma manipulação de eleições. Em Portugal tal ainda não se tornou um motivo de debate, mas já

tivemos oportunidade de ver a grande discussão durante as eleições americanas de 2016, com o escândalo da Cambridge Analytica.

Logicamente, somos capazes de entender que as nossas opiniões sociais e políticas são dados pessoais, e podemos entender porque merecem proteção, mas a ideia de uma privacidade legalmente exigida dos mesmos choca com os princípios mais liberais do nosso ordenamento jurídico. Já podemos encontrar aqui um problema de conflito de direitos e de interesses da pessoa.

Estes dados relativamente às nossas convicções pessoais, e também, como vamos ver depois, relativamente aos nossos hábitos, precisam de ser considerados se queremos elaborar uma lei que seja verdadeiramente capaz de oferecer a proteção prometida. Esta proteção, porém, tem de ser distinta, menos estrita, do que aquela que é oferecida ao já referido núcleo essencial dos dados pessoais, estabelecendo um regime com margem para a vontade da pessoa (considerando aqui o contexto concreto em que se daria a partilha dos seus dados) e o exercício dos seus direitos fundamentais.

É quando começamos a entrar no mundo das entidades infratoras que começamos a encontrar os maiores problemas, as maiores falhas da nossa lei atual. Sempre se soube que a privacidade é um bem jurídico digno de proteção, mas o direito apenas recentemente começou a entender que particulares poderiam ser agressores da privacidade, focando-se até muito recentemente apenas no Estado.

Atualmente, a Lei nº58/2019 faz uma referência no seu artigo 2º tanto a entidades públicas como a entidades privadas, estabelecendo elencos para ambas nos artigos 12º e 13º. Porém, ambas são tratadas quase da mesma forma, com os mesmos deveres a serem exercidos da mesma forma. Uma vez que se seguem as exigências básicas desta lei, como a designação de um encarregado de proteção de dados, estas entidades podem agir da forma que melhor entenderem.

Sendo a falta de controlo por órgãos externos um problema já bem conhecido (os relatórios de atividade da CNPD admitem a falta de recursos humanos e financeiros) há também o problema de estarmos a falar de duas esferas distintas, onde os interesses e mecanismos de intrusão são diferentes.

Na esfera pública não podemos impedir a recolha e partilha de informação. Pela sua própria natureza, as entidades públicas acabam por ter acesso aos nossos dados pessoais, sendo que o funcionamento da máquina administrativa implica também que estes sejam partilhados entre órgãos e pessoas coletivas de direito público (a atribuição de uma bolsa, por exemplo, poderá estar dependente de dados recolhidos na Segurança Social). Um regime jurídico de proteção de dados que vise estas entidades tem então de ter duas preocupações: a restrição destes dados recolhidos ao essencial e a garantia de que os mesmos nunca vão sair da esfera destas entidades.

Na esfera privada podemos ver contornos mais problemáticos. O interesse destas entidades é principalmente económico, em oposição ao interesse principalmente político das entidades públicas, e este interesse significa muitas vezes que não há aspeto da nossa vida pessoal que não possa ser apreendido, estudado e utilizado para incitar o nosso consumo.

Qualquer um que aceda a um site pela primeira vez será confrontado com um aviso relativamente a *website cookies*, seguido por um apelo do próprio website para as aceitar. Conhecidas no jargão técnico como *HTTP cookies*, falamos de ficheiros feitos de texto, partindo do servidor do website para o browser que o está a aceder. Uma vez aceite pelo browser, estas cookies começam a armazenar em si informação, criando quase que um perfil do usuário no site. Este perfil vai contar dados como passwords, mas também atividade prévia no website e, talvez o mais relevante, anúncios que o usuário já tenha visto e pesquisas frequentes. As *website cookies* em si são inócuas, sendo que se limitam a guardar uma série de observações sobre o nosso comportamento num website. Tornam-se perigosas apenas quando sujeitas a análise, criando, mais do que um perfil de usuário, um perfil de consumidor.

Se um usuário passar tempo suficiente num website, vai ser possível para as *cookies* distinguir o conteúdo que lhe é de maior ou menor interesse, elaborando daqui estratégias de *marketing*. Com a informação retida nas *cookies* é possível criar anúncios muito mais apelativos, vocacionando os mesmos para a nossa pessoa individual, os nossos gostos e, mais importante, necessidades.

Se a maior parte da nossa legislação em torno da privacidade se preocupa com prevenir e punir a partilha de informação privada, podemos ver que os principais infratores não estão a partilhar esta informação, mas sim a analisá-la. O que é partilhado já não são propriamente os nossos dados pessoais, é um tratamento dos mesmos. Para nós, portugueses, este é um problema: a lei que entre nós regula o tratamento de dados, a Lei nº42/2012, não conhece sequer do conceito de *cookie*.

Podemos ver por isso porque é que as entidades privadas precisam de ter a sua atividade acautelada de uma forma diferente. Se o controlo das entidades públicas pode ser feito muito com recurso ao Direito Administrativo, aqui vamos precipitar-nos já em questões do Direito do Consumo e de DUE, sendo que a *General Data Protection Policy* da UE já se debruçou sobre este problema.

Tudo isto nos leva ao nosso último problema, talvez o mais complexo: muitas estas entidades têm acesso aos nossos dados pessoais porque somos nós que os entregamos. O escrutínio da nossa vida privada parece tornar-se o preço que pagamos para ter acesso ao mundo que nos rodeia.

Sempre que acedemos a um novo website é-nos apresentada a sua *cookie policy*, essencialmente uma lista de todos os dados que serão recolhidos e para que fins. A tendência é aceitarmos estas *cookies*,

ou pelo menos aquelas tidas pelo website como "essenciais", caso contrário não temos acesso ao conteúdo que procuramos.

Daqui poderíamos retirar uma ideia de que o que está em causa é uma espécie de princípio do *caveat emptor*: sempre que acedemos a qualquer website são-nos mostradas todas as condições para o nosso acesso, pelo que o mínimo de diligência será ler essas mesmas condições. Se um usuário dá o seu consentimento sem ter o mais básico dos cuidados poderá a entidade por trás do website ser responsabilizada?

Neste aspeto, somos remetidos para matérias já conhecidas de Direito Civil: podemos mesmo considerar que temos liberdade para celebrar este acordo se estamos numa marcada situação de assimetria face à entidade que nos apresenta estes termos e condições? Até que ponto é que estas regras de conduta, apresentando-nos cláusulas gerais e pré-determinadas com que não podemos discutir, são diferentes de qualquer outro contrato de adesão? Se sim, não deveria existir um controlo mais efetivo, tendo muitas destas cláusulas, como já vimos, natureza abusiva?

Talvez esta seja a questão na qual não se pode apresentar uma solução simples. Toda a lei de proteção de dados, como já vimos, terá sempre de manter uma margem para permitir o livre exercício de outros direitos e liberdades da pessoa, mas, sendo esta uma matéria em muitos aspetos desconhecida para o comum cidadão, não podemos dizer que o mesmo exerça os seus direitos e liberdades de forma devidamente informada.

Podemos desenhar então dois percursos, que representam as duas soluções clássicas: aumentar (uma lei abrangente de todas as formas de proteção de dados aliada a um sistema de controlo mais ativo, correndo o risco de uma atitude paternalista) ou diminuir (uma proteção restrita aos dados objetivos e essenciais, deixando os restantes a cargo da responsabilidade individual de cada um, correndo o risco de deixar os cidadãos mais vulneráveis) a intervenção do Estado.

Publicações consultadas

CHEN, Angela. (2018). "Websites are (probably) making less money because of GDPR". MIT Technology Review.

H. Akin Unver. (2018). "Politics of Digital Surveillance, National Security and Privacy". Centre for Economics and Foreign Policy Studies.

Comissão Nacional de Proteção de Dados. (2021). "Relatório de Atividades 2019/2020."