apdsi

associação para a
promoção e desenvolvimento
da Sociedade da Informação

Privacidade, CiberSegurança e Regulamentação Económica

15º Fórum da Arrábida

Repensar o Futuro
da Sociedade da Informação

7 de Outubro de 2016

ANACOM

AUTORIDADE
NACIONAL
DE COMUNICAÇÕES

O Fórum da Arrábida foi, pelo 15.º ano consecutivo, o local escolhido pela Direção da Associação para a Promoção e Desenvolvimento da Sociedade da Informação - APDSI - para receber um conjunto alargado de personalidades de diferentes formações e experiências profissionais, para debaterem as questões da atualidade relacionadas com Privacidade, Cibersegurança e Regulação Económica. O objetivo foi, uma vez mais, refletir e explorar novos caminhos a seguir no futuro da Sociedade da Informação e do Conhecimento em Portugal, num mundo onde, entende a Direção da APDSI, estas questões estão na ordem do dia.

Raul Mascarenhas, presidente da Direção da APDSI, abriu os trabalhos da 15.ª edição do Fórum salientando a importância deste encontro realizado desde 2002, a que chamou "um ponto alto de reflexão, este ano dedicado a uma troika" e apresentando aos participantes o livro que sumariza as conclusões obtidas nos 10 anos de Fórum da Arrábida. De recordar que a publicação foi aqui apresentada, pela primeira vez, em outubro de 2012.

A intervenção de Raul Mascarenhas também refletiu os tempos difíceis que a APDSI vive, agradecendo o patrocínio da ANACOM, considerado "um apoio importante para a Associação que tem de ir puxando a manta para chegar a todas as suas atividades, agora mais modestas, face aos meios que temos".

Para o arranque de trabalhos foi lançado o desafio de cada um dos três grupos identificar problemas e recomendações ao "estabelecer a relação entre temas para termos uma perspetiva mais geral". Para a sessão plenária ficaram prometidos os resumos dos trabalhos do dia.

João Confraria, administrador da ANACOM, está preocupado com o novo papel da autoridade.

A abertura da 15.ª edição do Fórum da Arrábida coube a João Confraria, administrador da ANACOM, que felicitou a Direção da Associação pela realização continuada do Fórum, "uma iniciativa que já faz parte do calendário das pessoas que se preocupam com a Sociedade da Informação", considerou, e também pelo tema porque "estamos numa altura de mudança da atividade da regulação das comunicações eletrónicas do futuro que vão estar penduradas nestes três grandes temas", acrescentou João Confraria.

Durante a apresentação introdutória, o responsável destacou a componente política de algumas atividades da regulação, naquilo a que chamou de "o concretizar de princípios que foram assumidos politicamente".

Um dos princípios políticos que os reguladores vão ter de concretizar, é o do serviço universal

de telecomunicações que, provavelmente, virá a ser "novamente objeto de uma decisão política em Portugal de uma forma operacional e racional. Esperemos que haja uma definição política até 2018". A defesa do consumidor foi outra área destacada pelo representante da Autoridade Nacional de Comunicações.

João Confraria apresentou como novidade o papel da ANACOM que, passando a fazer parte de um sistema, ao invés de ser apenas uma autoridade reguladora, "agora também está na segurança, que é uma área completamente diferente e que não resulta de uma atividade exclusivamente individual".

A ANACOM "agora também está na segurança, que é uma área completamente diferente e que não resulta de uma atividade exclusivamente individual" **João Confraria**

O administrador da ANACOM fala, agora, na conceptualização da atividade da Autoridade, que obriga a uma definição do domínio em que a ANACOM deve intervir, quer do ponto de vista das relações institucionais, e da forma como se constroem, quer com os outros pilares do sistema de cibersegurança.

Encontrar respostas para os fenómenos que estão a desenvolver-se à volta da cibersegurança é outra das missões da ANACOM que, reconhece o seu representante, ainda não tem uma opinião muito fundamentada sobre os novos tempos que aí vêm. Importa, nesta altura, perceber quem são "os grandes interessados e os grandes esquemas com que temos que lidar, dado que é uma área relativamente estranha para a ANACOM", disse.

Metadados que afinal são dados e "contam" mais do que é suposto

Nunca na História foi possível capturar, processar e relacionar rapidamente tantos dados de tantas pessoas e organizações como hoje e pode dizer-se que tudo começou com a Google e com o seu motor de busca.

Foi a partir daí e depois com outros serviços lançados pela gigante da internet como o Gmail, o Docs e o Google Drive que começámos a deixar os nossos dados e, mais importante ainda, os nossos metadados, informação sobre as pessoas que conhecemos, com quem interagimos, os locais por onde passamos. "O poder dos metadados é tão grande que nem dá para imaginar", alertou Paulo Veríssimo logo de início na sua intervenção durante a 15ª edição do Fórum da Arrábida promovido pela APDSI.

Por tudo isto o Professor da Universidade do Luxemburgo afirma veementemente que "hoje a Google conhece-vos melhor do que vocês próprios", lembrando que a tecnológica no ano passado controlou perto de 70% das pesquisas nos Estados Unidos e 90% na Europa. O enorme poderio da empresa norte-americana de reunir dados continuou a ser alimentado por outras propostas, nomeadamente com o sistema operativo móvel Android ou o assistente pessoal Google Now. "E agora é só pensarmos que a Google é dona de toda informação trocada nestas coisas todas juntas", sublinhou Paulo Veríssimo.

Entretanto redes sociais como o Facebook ou o Twitter tomaram a dimensão que tomaram, com tudo o que contamos nelas acerca de nós e, mais direta ou indiretamente, acerca dos outros – e aqui entra mais uma vez a questão dos metadados. Redes sociais à parte, também outras empresas, como a Samsung com as suas Smart TVs, quiseram a quota-parte dos dados dos seus utilizadores. "Porque é que isto aconteceu? Porque a Google mostrou o caminho e as outras empresas pensaram: se a Google pode porque é que nós não podemos?".

O acesso "facilitado" aos dados tomou toda uma nova e maior dimensão com o surgimento dos smartphones e do mercado das aplicações móveis. Se nos PCS o ecossistema continua a ser razoavelmente robusto, o ecossistema das apps está completamente quebrado e isso é gravíssimo, considera Paulo Veríssimo. "Neste *broken ecossystem*, que está mesmo quebrado, temos empresas com uma gula enorme por dados e isso

pode ter consequências que eram desconhecidas há 10 anos", alertou. Tiramos fotos para as redes sociais, mas com a informação da foto, vai informação adicional, nomeadamente "conhecimento transitivo". Para já não falar das técnicas de reconhecimento facial.

Neste capítulo, Paulo Veríssimo deixou ainda outro alerta relativamente aos estudos e análises e à anonimização dos participantes muitas vezes prometida e poucas vezes conseguida no momento que atravessamos, como já aconteceu com serviços como o Netflix ou mesmo com projetos na comunidade científica. "Estamos numa era em que temos de repensar os esquemas de anonimato" referiu, aludindo a todo o cruzamento de dados possível, muito graças a toda a informação que somos nós próprios a partilhar *online*. "'Vomitamos' informação cujo valor, até dada altura, ninguém percebia".

Uma infraestrutura gigante às vezes sem lei

O mundo está a tornar-se numa gigantesca infraestrutura. Temos cada vez mais capacidade de comunicação e poder computacional e, logo, armazenamento quase ilimitado e muito barato. "Antigamente recolhiam-se dados, mas não se podia guardar tudo, ia-se deitando fora. Hoje em dia quando dizemos que a Web não esquece é mesmo verdade", referiu Paulo Veríssimo. "Há uns anos era apenas um alerta para termos cuidado", mais relativamente àquilo que publicávamos a nível pessoal.

Além da capacidade, esta infraestrutura também é gigantesca porque tem tudo ligado: carros prestes a serem autónomos, casas, *utilities*, telefones com capacidade para entrar nas redes das empresas, drones, redes de tráfego, ou seja, toda uma infraestrutura com uma capacidade enorme de trocar informação em que as apps ajudam. A Google foi pioneira na criação de um modelo de negócio baseado na obtenção de dados em que toda a gente foi atrás. E hoje, de facto, os dados são muitos e conseguem ser processados e armazenados em tempo útil. E o que é que os Estados têm feito com isso?

O crescimento da capacidade de armazenamento e de processamento e a descida do seu custo tornaram possível a *blanket data colection* promovida pela NSA. No decorrer do escândalo Snowden, os Estados Unidos deram a volta à questão afirmando que estavam a espiar, mas era para o bem dos cidadãos, chegando mesmo a usar uma expressão do género "quem não deve não teme".

"Antigamente recolhiam-se dados, mas não se podia guardar tudo, ia-se deitando fora. Hoje em dia quando dizemos que a Web não esquece é mesmo verdade."
Paulo Veríssimo

"A possibilidade de guardar dados aumentou drasticamente tornando possíveis coisas que eram impossíveis há uns anos atrás e a ética e a moral das sociedades não está a acompanhar isso", considera Paulo Veríssimo.

Também é verdade que nos Estados Unidos pelo menos existem leis, "as tais leis chocantes, restritivas dos direitos fundamentais, mas estão escritas. É assustador, mas é legal". Por outro lado, há países que não têm leis.

Na Europa também há legislação, mas de início as coisas não correram bem, porque davam a qualquer pessoa, de uma qualquer empresa, a possibilidade de aceder à informação. Um pouco como o que se passou em Portugal, desde a história das Secretas à excessiva intromissão da Autoridade Tributária na vida dos contribuintes. "Há uma diferença entre o Estado e os funcionários, e as pessoas por vezes esquecem-se disso".

Paulo Veríssimo referia-se à situação em que mais de 10 mil funcionários de diferentes empresas, algumas privadas, tinham acesso aos ficheiros fiscais dos contribuintes. "Se a Administração Pública precisa de acesso aos dados dos contri-

buintes tem de se fazer um esquema de *lock* inviolável", aconselha. "Para que depois o cidadão tenha o direito de saber quem acedeu aos seus dados e quando".

Outro argumento usado quando os Governos querem fazer uma recolha exaustiva de dados é o enfraquecimento dos sistemas, e aí, internacionalmente, temos exemplos como a tentativa de controlo do Facebook ou do WhatsApp. "Estamos numa era complicada em que não podemos dar nada como garantido, nomeadamente a Democracia".

Paulo Veríssimo defende que é necessário que os EUA e a Europa percebam que não estão sozinhos nestas "coisas" de se espiarem uns aos outros. "Estão a dar o exemplo. Além de que os outros fazem melhor. E ainda por cima não são sociedades democráticas".

A situação deriva, na opinião do Professor, de uma falta de perceção cultural dos decisores, que promovem a militarização do ciberespaço, por confundirem cibersegurança com ciberpoder. Este status quo deu origem a uma regulamentação permissiva da exagerada recolha de dados pelas empresas. Está também a dar lugar a uma substituição da monitorização pela vigilância "e nem sempre dentro das fronteiras e em alguns casos com a ampla cooperação voluntária ou forçadas das empresas privadas".

Também não sem o contributo dos utilizadores finais. "Todos nós estamos a ajudar para a perda de privacidade. Temos comportamentos de risco. As atitudes têm de mudar". Do lado dos políticos justifica-se a recolha afirmando-se que são apenas metadados, "inofensivos" e que a vigilância massiva é necessária para a segurança da nação.

Mas há sinais de mudança, com legislação que tenta harmonizar as cibercapacidades com os princípios, como acontece no caso da nova diretiva do Parlamento Europeu.

"O poder dos metadados é tão grande que nem dá para imaginar".
Paulo Veríssimo

Segurança *versus* Privacidade

A privacidade, embora tecnicamente não seja equacionada assim, é segurança defende Paulo Veríssimo, do ponto de vista dos dados e dos metadados. Por isso, ao fazermos muita recolha de metadados, não podemos dizer que estamos apenas a recolher informação de um indivíduo: estamos a recolher informação sobre todos os indivíduos e negócios de uma nação, alerta.

"Temos de perguntar aos governos se querem mesmo sacrificar a segurança de todos os cidadãos e empresas para proteger a Nação. Se o fizerem o que sobra da Nação? É preciso refletir sobre isto", argumenta Paulo Veríssimo sublinhando que, ao fazerem vigilância massiva, os governos estão a sacrificar a segurança de todos os cidadãos.

O Professor defende, por isso, que as nações podem e devem fazer vigilância, mas dirigida. "Uma pessoa suspeita deve ser seguida. Não podemos é por norma arrasar com a vida das outras pessoas todas por causa dessa pessoa, senão destruímos todo o fundamento da razão de um Estado democrático se achar nesse direito".

"Estamos numa era complicada em que não podemos dar nada como garantido, nomeadamente a Democracia".
Paulo Veríssimo

Redefinir é obrigatório

Neste mundo de alta tecnologia as intenções até podem ser boas, mas a concretização tem de ser analisada em termos de exequibilidade e pela magnitude dos impactos negativos, considera Paulo Veríssimo.

É certo que as ameaças se tornaram globais e persistentes, promovidas por adversários muitas vezes poderosos, motivados, competentes e não regulamentados, "mas é impossível fazer recolha de dados maciça sem prejudicar severamente a sociedade e a democracia. É um tiro nos pés", garante.

"Na minha opinião estamos a viver uma ciberguerra de baixa intensidade num ambiente de difusão de ciberarmas, sem termos um tratado de 'ciber Geneve' e sem termos um tratado de anti proliferação de ciberarmas e isso é perigosíssimo".

Paulo Veríssimo argumenta que é imprescindível existirem definições claras daquilo que é cibersegurança e ciberpoder, assim como deixar de tentar militarizar o ciberespaço. "Temos de redefinir a privacidade como uma forma de segurança e regressar à vigilância dirigida, como os Estados sempre fizeram".

Regulação económica:
Digital mudou negócios e impõe novas regras

O mundo digital abriu novas oportunidades de negócio às empresas que aproveitam o potencial do comércio eletrónico e trouxe mais alternativas ao consumidor, mas renovou desafios, alterando papéis e equilíbrios, temas que centraram a apresentação de João Confraria no 15º Fórum da Arrábida.

O utilizador já não é apenas um cliente, é o produto. Os dados que gera têm valor e alimentam negócios. Isso mesmo fica patente no top das cinco maiores empresas a nível mundial, no que se refere à capitalização bolsista, totalmente dominado por tecnológicas americanas arrumadas nesta ordem: Apple, Google, Microsoft, Facebook e Amazon, destacou João Confraria, sublinhando que há hoje uma "troca desigual de acesso por privacidade" na relação que se estabelece entre quem utiliza e quem fornece serviços digitais, em larga medida "porque as pessoas têm estado dispostas a ceder essa informação gratuitamente".

"Há uma perceção errada dos riscos, ou uma intenção deliberada de arriscar porque os ganhos do comércio eletrónico são imediatos e certos, enquanto os prejuízos são incertos?" **João Confraria**

Em troca, recebem serviços que muitas vezes também são gratuitos, mas que são apenas a linha avançada de estratégias que vão monetizar essa informação com outros produtos, como a publicidade. Neste contexto, há todo um cenário de falhas de cibersegurança que vale a pena considerar e que para João Confraria podem resultar em dois tipos de consequências: ruturas nos serviços de comunicações eletrónicas e distorções nas relações económicas.

No primeiro grupo cabem os desastres naturais, roubos de materiais, atividades terroristas ou a concretização de ameaças externas. Já ameaças como o roubo de identidade, espionagem indus-

trial, *botnets* ou a violação de privacidade são falhas que podem provocar distorções nas relações económicas.

Constituem riscos que, apesar de estarem bem identificados, não impedem as pessoas de afluir aos meios *online*, legitimando a dúvida: há uma perceção errada dos riscos, ou uma intenção deliberada de arriscar porque os ganhos do comércio eletrónico são imediatos e certos, enquanto os prejuízos são incertos?

Num caso ou noutro, valerá e pena perguntar se não estamos perante uma desvalorização individual e social da privacidade? "E esta desvalorização progressiva da privacidade é mesmo uma desvalorização em euros", alerta João Confraria, que é ainda mais acentuada nas gerações mais novas.

"Há uma desvalorização progressiva da privacidade e é mesmo uma desvalorização em euros". **João Confraria**

Esperar que seja o mercado a resolver a equação e a encontrar formas de repor equilíbrios, para o professor, não é opção. E conduz a uma *balkanização* da internet, em função de condições de segurança. O fenómeno aliás já se verifica, defendeu, mas como solução não é viável, porque "o mercado não está preparado para dar às pessoas toda a segurança que estas precisam ou querem".

Para muitas das empresas que se movimentam no mercado digital, vender informação é uma parte importante do negócio. Proteger essa informação, que é do utilizador, não é a prioridade porque não gera receita. Este fator, associado a um conjunto de externalidades de rede, contribuirá para reduzir os incentivos ao investimento em cibersegurança, sobretudo numa fase inicial dos negócios onde o grande objetivo é acumular clientes e ganhar massa crítica.

Que papel para as políticas públicas?

As políticas públicas devem ajudar a regular este mercado e a restabelecer equilíbrios, mas a primeira questão que se coloca é saber que enquadramento e objetivos devem ter. Devem observar o princípio da eficiência económica? Se assim for é necessário redefinir o conceito e alargar o âmbito da sua utilização (no contexto europeu), destacou João Confraria. Ou fará mais sentido usar o princípio da precaução, adotando uma postura mais conservadora e levando a cabo apenas as medidas estritamente necessárias para fazer funcionar o mercado, correndo o menor número possível de riscos? O economista ainda colocou um terceiro cenário, onde o modelo de regulação assentasse numa norma de segurança.

Qualquer que seja a abordagem, o regulador terá de escolher entre uma postura mais ou menos interventiva. Ou adotando medidas restritivas que os atores dificilmente verão com bons olhos, ou esperando para ver como funciona o mercado e reagindo em função dos problemas que forem surgindo.

Nos dois modelos existirão falhas, admitiu João Confraria: "como sociedade teremos de decidir que tipo de erros queremos cometer". Olhando para outros mercados é fácil encontrar casos em que uma regulação ex-ante poderia ter prevenido problemas, mas é igualmente percetível que seguir outras vias não teria sido fácil. Confraria dá o exemplo do mercado financeiro e da crise de 2008, que acabou por abalar a zona euro. "O desfecho era previsível, mas qualquer banco central que tentasse impor medidas para o evitar teria contado com a oposição do sector financeiro", recorda.

Não há um instrumento de regulação perfeito

No que se refere aos instrumentos que de forma mais concreta podem levar a regulação da privacidade e cibersegurança ao terreno, João Confraria apontou vários e considerou que nenhum é perfeito. Aplicá-los de forma cumulativa será por isso a opção mais viável, na sua perspetiva.

A obrigação de divulgação de informação sobre incidentes de segurança, que hoje já existe, é um dos pontos destacados, sendo importante definir se essa comunicação deve manter numa esfera restrita ou chegar ao domínio público. A divulgação pública funcionaria como um incentivo às ações corretivas por parte das empresas; faria cumprir o direito de informação dos indivíduos e das comunidades; e permitiria criar uma base de dados com este tipo de registo.

A definição de regras ao nível do processo de fornecimento do serviço ao cliente, aplicadas a ISPs e a empresas de *software;* a imposição de testes no desenvolvimento do *software*; ou a criação de um regime de responsabilização civil (simples ou por negligência), foram outros instrumentos de regulação possíveis apontados pelo economista.

Sobre este último, Confraria deixou dúvidas em relação à viabilidade de a medida ser implementada com os Termos de Utilização que hoje sujeitam a generalidade dos serviços digitais.

São textos longos, complexos e exaustivos, que colocam nas mãos do prestador de serviço poder para manipular os dados que processam, sem que a maioria dos clientes o perceba porque nem chega a ler o documento. Confraria também refletiu sobre as consequências práticas de impor um regime que abrisse espaço à atribuição de responsabilidade civil por negligência, considerando que um dos desafios seria chegar à própria definição de negligência. O outro, seria integrar critérios de eficiência económica nos processos de decisão da justiça.

"O mercado não está preparado para dar às pessoas toda a segurança que estas precisam ou querem"
João Confraria

No campo dos instrumentos que podem efetivar políticas públicas de regulação nestas áreas da privacidade e da cibersegurança terão ainda espaço a tributação, para onerar as empresas em caso de falhas de segurança, ou o imposto, calculado em função dos custos impostos à sociedade em consequência de falhas de segurança.

Entre as duas opções, Confraria defende que a tributação pode ter melhores resultados em áreas onde o Estado tem pouca informação sobre o mercado em questão.

A ação certa pelas razões erradas pode ser eficaz?

João Confraria concluiu alertando para o risco, que historicamente se confirmou noutros mercados, de a regulação nestas áreas avançar efetivamente, mas pelos motivos errados. "Não seria algo novo na história, olhando para a regulação dos monopólios, que tem avançado mais por pressão de advogados e políticos que de economistas". O professor recorda que os receios de concentração do poder económico e a necessidade de abafar descontentamento social provocado por desigualdades económicas não são motivos novos para desencadear este tipo de processo e acredita que com empresas como a Google ou o Facebook pode vir a acontecer o mesmo. A regulação pode surgir mais como uma reação do mercado pelo muito dinheiro que entregam aos acionistas, do que por questões muito mais impactantes para o consumidor, como a forma de tratamento dos seus dados. E lança a questão: "se a regulação chegar pelas razões erradas, será possível fazer o certo?".

Confraria acredita que a Europa acabará por responder aos novos desafios que se colocam à privacidade e segurança dos dados no mundo digital com uma nova diretiva, mas também defende que esta resposta mais cabal só surgirá quando a tecnologia tiver condições para o permitir. E deixa o exemplo de um serviço que a Telefónica espanhola anunciou recentemente e que, a concretizar-se nos termos em que foi apresentado, pode contribuir decisivamente para alterar o equilíbrio de forças entre o utilizador que gera os dados e as empresas que os processam e manipulam.

O serviço em questão, com lançamento previsto para 2017, assenta numa plataforma que vai permitir aos clientes da operadora saber que dados seus estão a ser utilizados por empresas como o Facebook, o Google ou a Apple e atribuir-lhes um valor. Cada cliente poderá optar por ganhar dinheiro com a partilha dessa informação ou bloquear-lhe completamente o acesso.

O responsável também defende que qualquer intervenção pública nestas matérias tem ser feita com critérios claros e a interpretação de ambiguidades legais não pode ficar a cargo de entidades administrativas, como são os reguladores. Isso desencadeia litigância e prejudica o normal funcionamento do mercado.

"A Europa acabará por responder aos novos desafios que se colocam à privacidade e segurança dos dados no mundo digital com uma nova diretiva, que só deve surgir quando a tecnologia tiver condições para o permitir."
João Confraria

Grupo de Reflexão I

Privacidade e Cibersegurança

Moderador

Luis Borges Gouveia

Participantes

Alessandra Rodrigues
Álvaro Damas
Ana Neves
Carlos Lourenço
João Barbas
Joaquim Morgado
José Amaral Gomes
José Carlos Martins
José Dias Coelho
Luis Vidigal
Paulo Sousa

Conhecimento, privacidade, segurança, informação ou mesmo liberdade são temas que tomam toda uma nova dimensão entre as gerações mais novas. O território do desconhecido é hoje em dia o campo de aprendizagem das novas gerações, não sendo algo necessariamente relacionado com a falta de acompanhamento, ou com a falta de valores: é uma guerra de conhecimentos a vários níveis, começou por dizer Luís Borges Gouveia para lançar o debate no grupo de reflexão "Privacidade e Cibersegurança".

Tal relaciona-se com uma noção muito própria de privacidade, daquilo que é o seu comportamento na interação com os outros, dentro dos seus "círculos". Tudo isto dentro de uma espécie de lógica de utilidade: se não é útil, descarta-se. "As gerações mais jovens estão treinadas para descartar informação, no processo mencionado por Alvin Tofler de *'learn, unlearn and relearn'*, continuou o moderador.

São atitudes que fazem todo o sentido para os mais novos, mas que para as gerações mais velhas são incompreensíveis, pela lógica de criação de uma memória a que estamos habituados. "Eles [gerações mais novas] não percebem que um dia vão ter de ser confrontados com as suas ações e opiniões". Há um algoritmo que lhes vai dar isso quando chegar à altura? "Que vai dar ou tirar, que é o esquecimento".

Uma outra questão pertinente nas gerações mais novas é a dificuldade para filtrarem a informação. "Por um lado [as gerações mais novas] têm uma facilidade de capturar informação que nós nunca havemos de adquirir, não conseguimos. Por outro lado nem sempre conseguem distinguir entre conhecimento válido e não válido", referiu Álvaro Damas.

"O tempo acelerou de uma maneira com a qual não conseguimos lidar. Esse é um problema que vai registar-se em relação à legislação, em relação à segurança e privacidade".

Para José Emílio Gomes a geração analógica teve *"overtime, undersex e underinformation"*, enquanto na geração digital temos *"overinformation, oversex e undertime"* "São dois regimes completamente distintos que vão formatando as pessoas. Somos paleolíticos".

Na sequência de implicações da privacidade e da segurança surge uma outra questão: o direito ao esquecimento. "Hoje há uma memória instantânea e facilmente recuperável, eventualmente por todos. Já nós tivemos a sorte de os nossos 20

anos não terem deixado rasto digital", considera Luís Borges Gouveia. Esta espécie de "cicatrizes do rasto digital" liga-se inevitavelmente ao sentimento de liberdade.

A ideia da privacidade como *mind control* e como condicionante, porque efetivamente muda, até no espaço e tempo. "Hoje em dia se eu tenho liberdade para potencialmente fazer mais, paralelamente tenho menos liberdade para fazê-lo.

"O tempo acelerou de uma maneira com a qual não conseguimos lidar. Esse é um problema que vai registar-se em relação à legislação, em relação à segurança e privacidade" **Álvaro Damas**

A ideia do tempo como condicionante do conhecimento, como limitador do conhecimento é avançada. "O tempo desvaloriza o conhecimento", acrescenta Luís Vidigal.

Potencialmente pode fazer-se tudo com as ferramentas à nossa disposição, mas o fazer exige escolha, um processo no qual os mais jovens parecem ver um obstáculo, reforçou-se. "Conseguem descartar ou não lidar com a informação, mas têm uma grande dificuldade quando os colocamos perante uma opção", defende Luís Borges Gouveia.

Nos dias que correm a quantidade de informação que recolhem sobre nós também pode ser um elemento fortemente condicionador da nossa experiência em termos de navegação *online*. A ideia foi apontada por Ana Neves, que se referia à filtragem feita pelos motores de busca ou pelas redes sociais nos conteúdos apresentados quando as visitamos ou fazemos alguma pesquisa. "Os filtros são tão fortes que bloqueiam quaisquer outros argumentos". Embora de forma diferente ao que foi discutido até à altura, Ana Neves considera que esta situação também é um ataque à privacidade. "Ninguém vem buscar os meus dados para os usar no sentido que temos estado a falar, mas para condicionar a minha maneira de pensar", reforçou apresentando o caso Brexit, no Reino Unido, como exemplo.

"As empresas fazem isso como um sobreproduto da sua atividade, mas estão a 'cortar as pernas' à minha capacidade de argumentação, porque só vejo os argumentos de um lado, não me mostram os argumentos do outro lado. É dos piores ataques à nossa liberdade".

Alguém sublinhou que esta filtragem é feita pelos *media* desde sempre, mas o grupo foi consensual em considerar que nos meios de comunicação é algo assumido e nas redes sociais não.

Por tudo isto, Álvaro Damas considera que a liberdade e a privacidade são conceitos complexos que vão ter sempre de ser vistos com os vários condicionalismos que os rodeiam.

Também é verdade que o digital muda a procura da informação e ver só depois de decidir é algo que acontece muito, como se verificou com o caso Brexit.

Foi maioritariamente aceite no grupo que filtrar e condicionar a pesquisa de informação, potenciada pelo uso massivo dos mesmos pontos de entrada na Internet, é um ataque à privacidade porque, no campo individual, pode inclusive ser considerado uma espécie de "sobreposição do espaço informacional de uma pessoa".

Faces diferentes da mesma moeda ou indissociáveis?

Temos visto a privacidade e a cibersegurança como coisas antagónicas, "espaços aparentemente em conflito", sugeriu João Barbas, mas para haver interação entre as pessoas, pessoal e virtual, tem de existir um espaço favorável, que assegure graus de liberdade mínimos, de forma a que essa informação possa fluir entre as pessoas e dentro da organização. "Estou convencido que limitando as regras para a cibersegurança podemos dar

às pessoas mais liberdade e maior capacidade de conhecimento. Não vejo isso como capacidades antagónicas", defendeu.

"Nem é preciso ter acesso à informação toda para se dar mais segurança, nem é preciso prescindir da privacidade toda para se ganhar alguma ilusória segurança" **Carlos Lourenço**

A opinião vai ao encontro da ideia sugerida por Paulo Veríssimo, durante a sua intervenção, umas horas antes, de que "a privacidade é a segurança do ponto de vista do individuo". Para Luís Borges Gouveia, temos realmente visto sempre a segurança e a privacidade "como faces da mesma moeda". A solução está em arranjar um fator que permita resolver os dois problemas sem um significar o fim de outro.

Para Carlos Lourenço a frase quer dizer que se tratarmos o problema ao nível da segurança coletiva, da interação da rede e depois no nó do individuo, "resolvemos o problema de uma ser contra a outra".

A propósito, José Emílio Gomes sugeriu que "cidadania é o indivíduo que tem a capacidade de criar e coreografar os seus próprios dados". Aqui aplica-se a "metáfora do tubo" defendida por Luís Vidigal, relativa ao facto de se controlarem os dados "a partir de dentro", percebendo o uso que está a ser feito deles. Relativamente à frase de Paulo Veríssimo, Luís Borges Gouveia aponta questões importantes a reter, relacionadas com a defesa interna, através da sobrecarga da infraestrutura, comando e controlo e controlo de informação para deter conhecimento.

Paulo Sousa lembrou que no grupo estão "otimistas esclarecidos", mas isso não acontece com a maior parte da sociedade civil. "Todos nós somos atentos e somos conscientes, quer dos riscos para a privacidade, quer dos riscos para a segurança, mas mais de 90% das pessoas não estão preparadas para estas questões, não estão despertas para os riscos nem têm instrumentos para fazê-lo", defendeu catalogando o fenómeno como falta de awareness.

Se perguntarmos à grande maioria das pessoas se estão dispostas a abdicar da sua privacidade por um bocadinho de segurança elas dizem que sim, garante Carlos Lourenço, uma ideia que gerou consenso entre o grupo. "Neste momento o que está na moda é trocar a privacidade pela segurança, uma troca que não é ingénua", sublinhou. "Há um equilíbrio que não sei onde está. Do lado de quem tem de dar segurança é sempre difícil, mas será muito mais difícil não tendo acesso a esse manancial de informação sobre as pessoas". A ideia é a de que, para dar segurança, é necessário ter acesso aos dados e isso implica que o cidadão abdique da sua privacidade. "Estas duas coisas são simultaneamente verdadeiras e falsas", defendeu Carlos Lourenço. "Na minha opinião nem é preciso ter acesso à informação toda para se dar mais segurança, nem é preciso prescindir da privacidade toda para se ganhar alguma ilusória segurança", referiu. "É verdade que as forças que são a garantia da nossa segurança precisam de aceder aos nossos dados, mas por outro lado é um engano dizer às pessoas que lhes damos segurança, é ilusório".

"E o que é que se perde pelo facto de eu não dar os meus dados?", perguntou Luís Vidigal. "E quem define esse justo equilíbrio?" pergunta Dias Coelho. "Não me importo que os serviços de segurança acedam um pouco à minha informação para destacar que eu não sou um elemento de risco, mas já sou menos tolerante a uma empresa que quer tirar beneficio da minha informação".

Um dos problemas é que quando damos os nossos dados, desconhecemos quem acede aos mesmos e para que são utilizados, aponta Carlos Lourenço. "Damos para os bons motivos. Mas quais são os bons motivos?"

Entre estas intervenções, e a propósito, Luís Vidigal sugeriu a criação de uma espécie de "botão" ao género Facebook que quando carregado pelo cidadão lhe mostrasse os dados e metadados recolhidos sobre si, entre outros aspectos.

Legislação como garantia

A legislação é um ponto fulcral em todo este "conflito" que coloca privacidade e cibersegurança a par uma da outra e pode contribuir para a sua resolução. O Regulamento Geral de Proteção de Dados (RGPD) vem tentar responder isso, colocando a responsabilidade do lado das empresas, que vão ter de nos dar informação sobre o tipo de dados que recolhem, com que fins e onde são usados, afirmou Álvaro Damas.

Isto obriga a uma mudança comportamental significativa para todos, ao nível das empresas e organizações e dos cidadãos, mas também ao nível da regulação e penalização, que em Portugal vai estar a cargo da CNPD – e que também vai obrigar à mudança do funcionamento da própria comissão. Esta mudança também cria um mercado novo.

Manuel de Barros, da Anacom, contribuiu com a sua opinião para o grupo de reflexão, afirmando que olha para a privacidade e para a cibersegurança como dois primados fundamentais das sociedades atuais. "Há dois momentos de compreensão e perceção, porque são conceitos dinâmicos, não são conceitos que se mantêm no tempo, e têm lógicas geracionais e culturais subjacentes como aqui foi dito". Por sua vez, ambos os conceitos estão relacionados com a confidencialidade, com a noção de segredo. O que a nova legislação vem trazer é um aumento da transparência, das entidades para o exterior, defende Manuel de Barros. "A legislação repensa a confidencialidade. As entidades estão a ganhar uma noção de 'obrigação de divulgação de informação'".

O crucial é a existência prévia de arquitetura de informação, como supõe a RGPD, de "privacidade *by design*", sublinhou Luís Borges Gouveia. Neste capítulo é importante formar os gestores da informação, em especial o encarregado de proteção de dados.

É igualmente importante criar *awareness* na sociedade civil. "O cidadão tem de ser sensibilizado para os seus direitos e riscos, face à problemática da privacidade", reforçou-se. Os cidadãos devem ter acesso aos seus dados e aos mecanismos para poderem fazê-lo de forma expedita.

Um jogo de equilíbrios

Quando falamos em privacidade e segurança, falamos normalmente de uma transferência em que se tira de um lado para pôr no outro. Esta é uma visão clássica e não é propriamente uma visão de equilíbrio. No capítulo da liberdade, ficou demonstrado que as cicatrizes do rasto digital possuem uma memória instantânea e facilmente recuperada por todos nesta era. O tempo surge como uma condicionante: potencialmente, hoje faz-se tudo, mas esse tudo exige escolha, nem sempre fácil de fazer, que por sua vez leva a perdas, face a todas as solicitações em causa.

> "A nova legislação repensa a confidencialidade. As entidades estão a ganhar uma noção de 'obrigação de divulgação de informação'"
> **Manuel de Barros**

Ao longo da reflexão, a ideia da privacidade como *mind control* e o registo de condicionamento, que muda, foi outra das ideias patentes. Um dos pontos assentes logo de início foi que a geração analógica tinha *"overtime, undersex, underinformation"*, quando em relação à geração digital falamos de *"overinformation, oversex, undertime"*. A conclusão é que nenhuma se fica a rir: há coisas boas e más de um lado e do outro. Outro dos aspetos muito discutidos, principalmente relacionado com as redes sociais, tem a ver com o direito ao esquecimento. O que está em causa é se, de alguma forma, podemos descartar e eliminar informação. Gerimos a nossa pegada digital? Também há a discussão contrária: qual é o direito à lembrança?

Relativamente ao tema, há todo um conjunto de alternativas para se aprender e filtrar a

informação. Há que perceber que entender e lidar com o excesso de informação é um jogo que determina, em muito, aquilo que cada um faz.

A dimensão cognitiva de uma geração é diferente da outra e temos de atuar a partir daí, considera-se. Na forma de lidar com a informação, falou-se também da navegação, apontando-se o caso Brexit, como exemplo do "ver e depois decidir", já que houve muita confirmação da informação que ocorreu depois de toda a gente ganhar consciência da mudança que tinha ocorrido. Defendeu-se também que condicionar e filtrar a pesquisa da informação ou fazer sugestões, como fazem a Google ou o YouTube, é um ataque à privacidade. Não é algo novo, mas é diferente, por isso no individual pode ser considerado uma sobreposição ao espaço informacional de cada pessoa. A questão do valor também foi discutida, começando desde logo de correr atrás do prejuízo, desde o legislador que, e por princípio, também é reativo. Apontou-se a questão do baú de competências dos indivíduos e das organizações, que tem que evoluir e isso nem sempre é fácil. No contexto nacional é claramente um *handicap*.

Relativamente ao espaço de inovação e liberdade e sobre a diluição das fronteiras das nações, coloca-se a questão de qual é que é o espaço de decisão local, se esse não é transferido para cidades, se não é transferido para organizações de caráter regional. Colocam-se questões do ponto de vista geopolítico e a leitura que existe é a de que, claramente, as tensões se vão resolver de forma diversa e muito em função das relações de poder - não necessariamente económicas, mas quase de certeza energéticas. Acredita-se também que se é negócio, o mercado ajusta-se.

Nisto tudo, a legislação a aplicar a partir de 18 de Maio de 2017 é um fator muito importante, porque vai implicar uma mudança comportamental significativa para todos.

Surgiram também preocupações que ligam a questão da Cidadania à privacidade e à segurança, vistas, não necessariamente como conflituosas, em que tiramos porção de uma para dar à outra, numa visão mais comum, mas como a existência de um espaço favorável para considerar, não faces da mesma moeda, mas como dois elementos indissociáveis. A frase "a privacidade é a segurança do ponto de vista do individuo", de Paulo Veríssimo, coloca-nos perante uma abordagem diferente daquela que tradicionalmente temas de "ganho" ou "perda".

Conclui-se igualmente que a cidadania também é o individuo que tem a capacidade de coreografar os seus dados pessoais. Aqui entra a ideia da "metáfora do tubo", a ideia de que existem os dados visíveis, mas depois da sua transformação e processamento também pode haver interesse em aceder à informação resultante. Em princípio este conceito já está desenhado no CADA, mas precisa de ser materializado.

Relacionarmos diretamente privacidade e cibersegurança e cibersegurança e privacidade tem riscos com os quais o cidadão comum não está preparado para lidar. Normalmente o cidadão "dá" e não "recebe". Há uma falta de consciência do potencial de risco e não se ensina a questionar. Isto nota-se entre os mais jovens, que têm um grau de "tolerância" significativo: todos eles estão habituados a viver bem com um elevado grau de permissividade e partilha de dados. E nós? Estamos dispostos a abdicar da nossa privacidade? Provavelmente a resposta não será positiva, mas a "moda" é trocar a privacidade por segurança e

para ter segurança é preciso permitir o acesso aos dados - um argumento que serve como auxiliar de "convencimento". Terá que ser mesmo assim? Perde-se efetivamente se não fornecermos os nossos dados? Em muitos casos sim.

Há várias outras questões em aberto. Quem define o equilíbrio entre a privacidade e a segurança? A resposta poderá passar pela responsabilização de pessoas e empresas, através da nova lei Regulamento Geral de Proteção de Dados (RGPD), que, entre outras coisas, obriga à criação de um responsável da informação em qualquer organização, pública ou privada, que possua informação sensível. A CNPD vai ser a entidade responsável por regular este aumento da transparência das entidades para o exterior, para o cidadão, e de repensar o regime de confidencialidade do *"no need to know"* para *"open under request"*.

Os desafios que se colocam perante este cenário são de natureza dos sistemas de informação das instituições e da capacidade de resposta. Será que as organizações conhecem o seu *stock* de informação? Será que temos (ou devemos) recentrar a informação no cidadão? E que episódios existentes demonstram desintegração e processos/expedientes complexos?

Como ações e recomendações, o grupo de reflexão sugere sensibilizarem-se os agentes para as implicações práticas do RGPD; adequar os processos de negócio e a arquitetura de dados das instituições; e realizar um esforço para atribuir a guarda da informação aos reais donos dos processos. É igualmente crucial a existência prévia da arquitetura de informação, tal como é pressuposto da RGPD (de *privacy by design*) e apostar na formação das pessoas e dos gestores da informação, em especial, do encarregado de proteção de dados.

Recomenda-se além disso o acesso transparente do cidadão aos seus dados e aos mecanismos para poder fazê-lo de forma expedita, desejavelmente numa base digital e em regime de autosserviço. Sem dúvida que o cidadão deve ser sensibilizado acerca dos seus direitos e das suas obrigações face à problemática da privacidade e da cibersegurança.

Desafios

- Será que as organizações sabem o seu ***stock*** de informação?
- É relevante, o levantamento dos ativos de informação, dos sistemas e do seu propósito (existentes e a cuidar)?
- Será que temos (ou devemos) recentrar a informação no cidadão?
- Episódios existentes demonstram desintegração e processos/expedientes complexos

Revisitar os processos de negócio de forma a assegurar a privacidade.

Ação e recomendações

- Sensibilizar os agentes para as implicações práticas do Regulamento Geral de Proteção de Dados (RGPD);
- Adequar os processos de negócio e a arquitetura de dados das instituições;
- Realizar um esforço para atribuir a guarida da informação aos reais donos dos processos;
- É crucial a existência prévia da arquitetura de informação, tal como é pressuposto do RGPD (***privacy by design***);
- Formar as pessoas, os gestores da informação e, em especial, o encarregado de proteção de dados;
- O cidadão deve ter acesso transparente aos seus dados e aos mecanismos para o poder realizar de forma expedita;
- O cidadão deve ser sensibilizado dos seus direitos e obrigações face à problemática da privacidade e da cibersegurança.

Grupo de Reflexão II
Cibersegurança e Regulação Económica

A regulação económica e a cibersegurança podem vir a traduzir-se em valor? De forma simples, estas foram as questões de fundo durante toda a discussão do Grupo de Trabalho II, moderada por José Alegria, e que reuniu outros sete participantes com diversas origens e papéis na sociedade.

O grupo não foi dos maiores, o que facilitou uma boa sustentação dos diferentes pontos de vista que, ao longo de mais de duas horas, foram trocados no momento de discussão.

Exemplos de leis mais ou menos agressivas resultantes do ato político como reação a questões de segurança que possam ter sido extremas, na opinião de José Alegria trazem consequências demasiado agressivas para a economia que fazem com que o mercado sofra excessivamente devido a uma regulação europeia no terreno.

A história mostra que a lei pode ser injusta e mais ainda quando se estabelece o binómio segurança - impacto no desenvolvimento, que já está muito acelerado com a dinâmica da Internet of Things (IoT). "Quando criarmos regulação já a IoT está a funcionar. É preciso estabelecer o equilíbrio entre um e outro", desafiou José Alegria, que também citou resultados do mais recente World Economic Forum e das retrações que o mercado sofre em resultado de leis excessivamente penalizadoras na prevenção de violações de cibersegurança. Voltando à reação legislativa a incidentes de cibersegurança, José Alegria explicou que estes têm duas dimensões: será que existe dinheiro suficiente para se apostar numa resiliência digital com investimentos canalizados para o controlo ou será que isso pode provocar uma retração por parte de um mercado emergente? A resposta está no nível das ameaças que podem ter uma intensidade gradual (nada muito intensivo) ou o extremo em que existe uma intensidade dramática, como acontece com o terrorismo. Nestes casos as leis trazem segurança às populações mas provocam uma grande retração por parte de quem tem de investir. José Alegria lançou ainda para o debate a questão da relação que se estabelece entre a criação de legislação excessiva e a pressão excessiva que a mesma pode vir a criar, limitando as necessidades de modernizar operações. "Pelo meu lado, sou um liberal nesta área. Coloco-me mais no sentido de ser capaz de observar, enquanto cidadão, que tem uma atitude defensiva, apesar de estar do lado da 'polícia', disse José Alegria. A privacidade ao nível interno nas organizações também tem de ser tida em conta e os passos dos funcionários que lidam com informação considerada sensível, têm de ser conhecidos e controlados por parte de quem gere a empresa.

Moderador
José Alegria

Participantes
Pedro Carrilho Filipe
João Confraria
João Monteiro
Luís Moreira da Silva
Paulo Veríssimo
Joaquim Morgado
José Gomes Almeida

A privacidade ao nível interno nas organizações tem, obrigatoriamente, de ser tida em conta e os passos dos funcionários que lidam com informação considerada sensível, têm de ser conhecidos e controlados por parte de quem gere a empresa.

"O funcionário tem de estar controlado, senão, não se consegue dar garantia de privacidade aos clientes", assumiu.

Paulo Veríssimo ressalva que esse processo também tem de ser feito de forma a pensar na privacidade do colaborador, que "tem que ter margens de trabalho", mas também tem de ser auditado sempre que lide com informação sensível. Do ponto de vista económico, o valor da privacidade tem vindo a ser avaliado e as Privacy Technologies valem dinheiro desde que o mercado se aperceba disso. "No Brasil já está a ser estudado o valor económico da privacidade ao invés de se obstar ao desenvolvimento económico por questões de privacidade. Exemplos de constrangimentos da privacidade pelo seu valor económico não me parece ser o caminho", exemplificou Paulo Veríssimo, lembrando que o discurso em relação à cibersegurança é que vai ter um valor positivo e que tem de ser incentivado pelos regulamentos.

Luís Moreira da Silva acrescentou que "estamos num momento de mudança para a economia digital sujeita a inibidores que são próprios da cibersegurança". Voltando à noção de equilíbrio entre regulação e inibidores: face à dinâmica a que neste momento estamos a assistir, numa fase de arranque, José Alegria refere que o potencial económico pode ou não ser moderado através de uma inteligente regulação económica. Se não for inteligente, temos três cenários:

. **Digital Backlash**, em que os receios cria tanta legislação que o potencial das *startups* acaba por ser travado por questões de excessiva segurança;

. **Muddling**, em que há uma estagnação do mercado no momento atual;

. **Digital Resilience**, em que quem for capaz de se reintegrar de forma a ser resiliente no espaço digital sai vencedor.

Cabe-nos a nós escolher entre o equilíbrio entre regulação económica inteligente ou assistir ao resultado de catástrofes que levam à criação de leis de emergência.

"Estamos num momento de mudança para a economia digital sujeita a inibidores que são próprios da cibersegurança".
Luís Moreira da Silva

João Confraria interveio para clarificar as diferenças entre privacidade e segurança e para defender o seu ponto de vista, no qual a empresa que garante privacidade ao cliente consegue recuperar o valor que o consumidor investe no seu processo de qualidade. "A segurança beneficia toda a gente. Se a empresa faz um investimento que beneficia toda a gente, o benefício é social porque mesmo os que não são clientes também vão beneficiar com isso. Criar-se um quadro regulatório que leve as empresas a investirem além daquilo que é o seu restrito interesse, é um desafio que os reguladores têm agora pela frente. Será que as entidades querem todas estar no espaço global?", desafia. João Confraria acredita que quando uma empresa investe ganha, ela própria, com isso, assim como todo o sistema.

Para inverter esta tendência, as empresas quando fazem investimentos privados, deveriam fazer uma análise também social e investir de acordo com a rentabilidade social e não apenas da em-

presa. "Os cidadãos também precisam de alguma autonomia para poderem circular em segurança", considerou João Confraria.

"Se o Governo conseguir que um número grande de empresas invista em cibersegurança, consegue obter-se o ótimo social", reforçou Paulo Veríssimo, igualmente sustentado por José Alegria que, mais uma vez, aposta na resiliência: "As empresas têm que se reinventar, não basta estarem sujeitas a mais controlos".

A existência de uma limitação clara e efetiva nas questões de segurança que podem vir a ser impostas, foi igualmente considerada um elemento fundamental no momento de se olhar para a segurança como elemento negociável. "Neste momento existe a necessidade de consumo imediato", reconhece Joaquim Morgado, sendo o primeiro a admitir que, facilmente, cede os seus dados pessoais e número de cartão de crédito em benefício do conforto de se fazer uma compra online. "Estamos todos a ficar habituados a comprar e depressa, ninguém neste momento questiona o facto de ter de dar os dados do seu cartão de crédito.

José Alegria refere que o potencial económico pode ou não ser moderado através de uma inteligente regulação económica. Se não for inteligente temos três cenários: Digital Backlash, Muddling ou Digital Resilience.

Nem sempre sabemos o que está por detrás disso porque não há entidades que certifiquem a empresa a quem estamos a comprar", alerta, enquanto se afirma que, apesar das pessoas terem uma crescente necessidade de consumo imediato, não têm consciência dos perigos desse consumo "porque os riscos ainda não aparecem no Correio da Manhã", brincou Joaquim Morgado. Se a regulação criar muitas barreiras vai contra a tendência atual de crescimento do setor. O valor potencial no caso de aparecer algum risco corresponde a um atraso de três anos nesse desenvolvimento.

Sobre o recente novo regulamento europeu da Proteção de Dados, José Alegria teme que possa tornar-se cego e vir a encriptar tudo, não resolvendo nada. Mais uma vez, fica a certeza de que a pressão dos factos anteriores pode levar a um controle excessivo e ao retrocesso da economia.

Luís Moreira da Silva entende que a vulnerabilidade da sociedade digital é um facto aceite mas a sua restrição pode levar a uma retração da economia e de novos mercados que possam beneficiar da adoção de novas tecnologias.

Sobre o novo regulamento europeu da Proteção de Dados, **José Alegria** teme que possa tornar-se cego e vir a encriptar tudo, não resolvendo nada.

A regulação pode espartilhar a inovação e restringir uma transição para a indústria 4.0, na qual "tudo comunica com tudo; é a quarta revolução industrial que advém da rede imensa da IoT e aqui o potencial de crescimento económico é avassalador. Como é que tudo isto pode ser regulado e seguro? Para nós é nova a questão da segurança que não é de coisas físicas". Moreira da Silva entende que se devem retirar lições aprendidas da segurança física (normas e regulamentos) para o ambiente digital.

Mais uma vez colocando-se do lado do consumidor, Joaquim Morgado acredita que a segurança descansa o cliente e pode vir a ser um excelente produto de marketing. Se o cliente tiver do seu operador essa garantia de segurança, ficará mais descansado. "Se o meu banco me der garantias de segurança, isso acaba por ser um argumento de venda. Se as empresas investirem nessas matérias e soluções, o cliente também vai ter vontade de se juntar a uma marca onde sabe que mais dificilmente será roubado.

"Os mercados devem procurar fazer a analogia entre a cibersegurança e a área ambiental." **José Alegria**

O cliente vai preferir as empresas que tenham esses mecanismos", prevê Joaquim Morgado.

Provou-se aqui, defende José Alegria, que os mercados devem procurar fazer a analogia entre a cibersegurança e a área ambiental. "Na Internet precisamos de convenções mas a regulação não pode ser binária, só no sentido de ou se pode ou não se pode. As organizações têm de criar uma arquitetura de espaços que são mais sensíveis que outros. O regulador tem de pensar *"out of the box"*, advoga José Alegria.

José Gomes Almeida acrescentou que os parâmetros da regulação devem ser globais, dando o exemplo do jogo *online* que "é um problema complicado pelo interesse que cada país tem sobre as leis e impostos que se lhes aplica. Há diferentes interesses estatais envolvidos".

"A IoT, neste momento, é como um bar aberto. A análise que é feita, é apenas em cenários", lembra José Alegria, que volta a focar a sua intervenção no quanto uma eventual catástrofe levaria à castração deste mercado emergente. A privacidade é importante, mas se a sociedade tiver receios há uma inércia e retração no segmento muito importante. As organizações têm de fazer uma transição segura, consoante a regulação. A metáfora do ambiente é "fabulosa" para Paulo Veríssimo que lembrou no seio da discussão do

grupo a resistência da indústria automóvel, por exemplo, e como a retirada de obstáculos nunca pode ser, ela própria, um obstáculo ao valor. "Se há infraestruturas críticas tem de haver regulação", concluiu. Também por comparação ao mercado automóvel, ficou a certeza de que quaisquer soluções que surjam nesta fase inicial, depois tenderão a embaratecer e a cibersegurança vai ser cada vez mais um bem tangível para os utilizadores: "Vamos ter a chamada *economics of security*. Quem tem capacidade de gestão terá de perceber o valor económico da segurança".

Joaquim Morgado adverte, no entanto, que essa transição para uma cibersegurança enquanto geradora de valor económico real, deve ser feita paulatinamente. "Devia haver uma classificação de maturidade que deveria ser atribuída em maior percentagem a quem melhor está a cumprir normas", lançou Joaquim Morgado, reforçado por João Monteiro que vai mais longe ao referir que quem obtivesse um valor mais alto de certificação, também deveria ter maiores benefícios fiscais. No debate, foi unânime a conclusão de que as empresas têm de se adaptar a uma nova realidade. "É fácil vender a ideia de que o produto foi certificado e é seguro", garante Joaquim Morgado.

Quanto às tão badaladas aplicações móveis, José Alegria defende que, também elas, deviam passar a estar certificadas porque "isso iria induzir uma permanente preocupação com o um nível de maturidade nos vários *stakeholders*. "Não há uma norma no ciberespaço". José Alegria resume que tem de ser criada uma entidade com vários níveis de certificação a atribuir.

Quem vai credenciar e quem credencia, é outra questão. Mas só o facto de existir certificação, já induz as pessoas a pensarem de forma resiliente no processo. "Na lógica da multa não se resolve. A ideia é perceber que não se avança se não estiverem cumpridos determinados parâmetros", acrescentou.

Paulo Veríssimo fez referências aos "perigos em que a Tesla está a sujeitar os seus condutores. A marca conseguiu pôr um carro autónomo a circular sem as devidas certificações. Como é que foi possível isto acontecer? Isso não acontecia se fosse na Europa". Operações críticas não deviam ter níveis baixos de segurança, refere Paulo Veríssimo.

João Confraria acredita que os clientes vão valorizar a cibersegurança a partir do momento em que ela possa ser mensurada. As *apps* para um banco português ou para a administração central deviam estar certificadas. Na opinião de João Confraria esse seria um bom e sólido passo rumo à regulação obrigatória.

Pedro Carrilho Filipe interveio para ressalvar a forma como a componente geográfica pode vir a ser aplicada ao nível da normativa "Como perceber a origem de uma *app*?", refere para questionar, ainda, o alcance da nova legislação europeia. O facto de os nossos dados valerem triliões de euros anuais e esse valor estar sempre a crescer, pode ser um bom incentivo à criação de regulamentação.

"Vamos ter a chamada *economics of security*. Quem tem capacidade de gestão terá de perceber o valor económico da segurança" **Paulo Veríssimo**

A educação digital para a cidadania foi, ainda, trazida à discussão por José Alegria que lembrou que os dados segregados podem, igualmente, funcionar como uma boa ferramenta de segurança: "Se alguém atacar a base de dados não os pode cruzar. Não devemos ter os ovos todos no mesmo cesto. A informação sensível não anda a passar". Recorrer a servidores com vários sistemas operativos foi outra solução apontada pelo grupo, como sendo um outro exemplo de resiliência.

Conclusões

- A cibersegurança cria valor, nomeadamente através de quem é certificado.
- É preciso construir o caminho de forma mais estruturada, com o apoio do Governo
- As *startups* têm de pensar na cibersegurança desde a raiz
- Pode tirar-se partido dos incentivos às PMEs
- Segurança sem prescindir de flexibilidade.

Recomendações

- Por exemplo, IPQ e IPAQ podem certificar as empresas que cumpram com normas de qualidade em matéria de cibersegurança.
- Aproximação ao modelo ambiental com a atribuição de níveis de A a F, sendo que as mais certificadas teriam um valor de mercado mais competitivo.
- A exigência da certificação podia ser progressiva, já que uma empresa mais recente não teria os mesmos recursos de uma empresa sénior.
- A certificação não seria eterna e o seu incumprimento estaria sujeito a taxas/multas que estariam consignadas à estrutura certificadora.
- Sensibilização para a cidadania da segurança digital.
- Aumento da resiliência digital preventiva e reativa.

Grupo de Reflexão III
Regulação Económica e Privacidade

Dar critério económico à regulação da privacidade é um enorme desafio

Moderador
Manuel David Masseno

Participantes
Francisco Tomé
José Carlos Nascimento
José Maria Pedro
Mário de Almeida
Mário Rui Gomes

A falta de noção do valor económico dos dados gerados por qualquer utilizador de serviços digitais foi o ponto de partida da discussão no grupo III na 15ª edição do Fórum da Arrábida. Foi consensual no debate que a generalidade dos utilizadores não percebe que os seus dados pessoais têm valor económico e que quando aceitamos partilhá-los em troca de um serviço estamos, quase sempre, a fazê-lo em condições altamente desfavoráveis. E não perceber valor, significa não compreender riscos, admite-se.

"Se as pessoas não têm noção de que estão a lidar com informação com valor, como vão perceber que há riscos?", sublinhou Mário de Almeida, acrescentando que falta *awareness* para compreender o desequilíbrio que hoje sustenta a relação entre quem usa e quem fornece serviços digitais. Uma realidade que ganhará relevância sobretudo na faixa abaixo dos 35 anos, mas que não é exclusiva desse grupo etário.

Alterar a situação não é tarefa fácil, concorda o grupo, defendendo que as gerações mais novas "estão contaminadas". Estão rendidas aos novos serviços *cloud* e não estão preocupadas com as questões da privacidade, ao ponto de identificarem a necessidade de mudanças. Mesmo que o fizessem, esbarravam na maior de todas as questões para um consumidor informado: mas afinal quanto valem os meus dados?

Mário de Almeida acredita que "ninguém tem a perfeita noção do valor dos seus dados na internet". Na sua opinião isso reflete, por um lado, a abrangência exagerada e pouca clara de muitas das aplicações que hoje usamos: uma aplicação com uma lanterna pode pedir permissão para aceder à lista de contactos do utilizador. Para quê? Não sabemos. Por outro lado, demonstra que quando aceitamos dar acesso público aos nossos dados não sabemos quem os usa e com que finalidade (e como tal não conseguimos quantificar o seu valor). Mesmo assim cedemos, influenciados por um "certo fascínio" generalizado com todo o conhecimento e informação que os serviços digitais colocaram ao alcance de cada utilizador.

Não ter nada a esconder não significa ter de partilhar tudo

"Como não tenho opinião, abdico da minha liberdade de expressão" a provocação é de Edward Snowden, o analista da NSA que denunciou um sistema global de vigilância, mas Manuel David Masseno trouxe-a à mesa do debate para ilustrar aquilo que, na sua perspetiva, reflete a forma como boa parte dos que hoje navegam na internet e consomem serviços *online* olham para o tema.

A forma como hoje aceitamos usar serviços e aplicações digitais mostra que consentir nem sempre reflete uma escolha informada.

Promover uma regulação que proteja a privacidade, até de quem não sabe que precisa de ser protegido, é um desafio. Dar-lhe um enquadramento económico é um desafio ainda maior. São vários os exemplos que podem ilustrar como hoje há uma total desagregação entre questões económicas e questões da privacidade, sempre que as instâncias competentes são chamadas a intervir. Para Manuel Masseno essa é uma evidência clara da dificuldade que será combinar os dois elementos na mesma equação e aponta três decisões de tribunais europeus para concretizar: a anulação da diretiva de retenção de dados em 2014; o reconhecimento do direito ao esquecimento; ou a decisão adotar o Safe Harbour, o acordo que regula a troca de dados entre UE e EUA, entretanto substituído.

Na regulação económica hoje já cabem alguns aspetos relacionados com a segurança, mas cabe muito pouco no que se refere aos temas da privacidade, analisou Manuel Masseno. Falta perceber, no terreno, se o cenário se mantém ou se efetivamente se alterará com a nova legislação da proteção de dados (Regulamento Europeu Geral de Proteção de Dados), que estará no terreno até 2018. Um sinal menos positivo, destaca, pode ser o facto de o consentimento continuar a ser o conceito básico para definir a legitimidade do acesso a informação privada.

A forma como hoje aceitamos usar serviços e aplicações digitais mostra que consentir nem sempre reflete uma escolha informada. Na maior parte dos casos, em vez disso, significa dizer sim a um conjunto de condições que muitas vezes nem chegam a ser lidas.

Outra questão relevante, concordaram os participantes, tem a ver com a própria formulação dos termos de utilização dos serviços digitais, que deixam o utilizador desprotegido e à mercê da vontade de quem presta o serviço. É certo que há um conjunto de direitos consagrados na legislação que protegem os utilizadores de abusos neste domínio, mas a realidade mostra que é sobretudo em casos que chegam às últimas consequências, que a força destes princípios legais acaba por emergir. Dois exemplos citados no debate foram a guerra do regulador francês com a Google, por causa da aplicação do direito ao esquecimento em todo o universo de atuação do motor de busca (no Google.com e não apenas nas versões europeias do serviço) e a utilização pelo Facebook de metadados do Instagram. Há legislação que fundamenta a ilegitimidade da medida, mas a empresa avançou e só recuou na sequência de ações judiciais na Alemanha, em Itália e em Espanha.

"Ninguém tem a perfeita noção do valor dos seus dados na internet" **Mário de Almeida**

Os próprios Estados muitas vezes dão sinais contraditórios da interpretação das leis que já existem e dos seus esforços para manter tão resguardada quanto possível a privacidade dos seus cidadãos, alertam os participantes no debate.

José Carlos Nascimento dá o exemplo do Por-

tal da Saúde, onde o Estado usa ferramentas da Google (Google Analytics) para monitorizar o acesso dos cidadãos ao site, não obstante as muitas dúvidas que subsistem sobre a forma como a empresa gere as informações que passam pelos seus sistemas. E também comenta a forma como a impossibilidade legal de identificar o cidadão com um número único acabou por ser contornada para criar o Cartão de Cidadão, considerando que a "não existência de uma definição coletiva de regras para os dados geridos pelas instituições públicas é uma preocupação".

"A não existência de uma definição coletiva de regras para os dados geridos pelas instituições públicas é uma preocupação"
José Carlos Nascimento

As mesmas diretrizes seriam úteis para dar resposta a um fenómeno que, na perspetiva de José Maria Pedro, representa igualmente uma preocupação: a proliferação de centros de dados no universo da Administração Pública (AP) e de entidades públicas a tratar dessa informação.

"Na AP o excesso de privacidade tem custos muito elevados que pagamos e que nem sei se se justificam", defende o participante, perguntando se fará sentido manter tantas estruturas diversas, operadas de forma completamente autónoma, enquanto conclui que falta na AP uma visão mais integrada das questões tecnológicas e diálogo entre os grandes centros ministeriais e com organismos transversais.

Privacidade *by default*

De volta a uma perspetiva mais global, o debate seguiu com a convicção de que "chegou o momento de pôr alguma regra neste esforço [das empresas] para a obtenção de dados a todo o custo", como destacou Mário de Almeida. Uma das formas de lá chegar pode passar por adotar um princípio de privacidade *by default* ou *by design*, assumindo a existência de um nível de anonimato que não possa ser de todo violado, de patamares de informação inacessíveis, até como mecanismo de proteção de grupos mais vulneráveis, como os infoexcluídos ou os menores.

A aplicação, em termos práticos, do conceito intensificou o debate e desencadeou outra questão: "será que devia existir uma entidade a nível europeu para tutelar os direitos do cidadão?", atira José Maria Pedro. O grupo concorda que sim, mas defende que para regular de forma eficiente, é preciso conhecer bem todos os riscos.

Quando no mercado existem intervenientes que têm mais poder que um Estado, as intervenções têm de ir além dessa esfera.

Quando estiverem identificados, o enquadramento regulatório deve ser económico, porque o fator económico é a questão central - é o que gera o interesse nos dados. A grande questão, que permaneceu sem resposta, é como fazê-lo? Para Francisco Tomé a única forma é atribuindo um valor económico à privacidade e para tal é fundamental criar uma fórmula de cálculo desse valor.

Consensual foi a opinião de que, quer a definição de critérios, quer a monitorização do seu cumprimento terá de acontecer, pelo menos, a nível europeu, como destacou José Carlos Nascimento, ou não terá força. Quando no mercado existem intervenientes que têm mais poder que um Estado, as intervenções têm de ir além dessa esfera, defende o grupo.

A internet e o universo de serviços digitais que acolhe tornaram-se vitais. Atingiram o mesmo nível que um conjunto de serviços hoje considerados *comodities*, como a água ou a luz, onde a regulação se tornou algo natural e indispensável, nota Mário de Almeida. Seguindo a mesma lógica, gigantes como uma Google ou Facebook têm de ficar sujeitos ao mesmo tipo de regras e é neles que os primeiros esforços de regulação devem focar-se, continua.

Mas a nível nacional também há um caminho a percorrer. Um aspeto relevante será promover uma melhor articulação e diálogo entre reguladores, neste caso Anacom, ERC – Entidade Reguladora para a Comunicação Social, Autoridade da Concorrência e Comissão Nacional de Proteção de Dados.

Também faz sentido para o grupo que os reguladores – no plano nacional e europeu - tenham um papel mais ativo na capacidade de influenciar o mercado, através de medidas de incentivo/desincentivo. Em relação às primeiras, o exemplo apontado é a certificação. Em relação às segundas, destacam-se as multas pesadas.

Os Estados podem desempenhar um papel importante ainda a outro nível, acredita Mário Rui Gomes, que defende a possibilidade de estes chamarem a si a negociação coletiva dos dados dos seus cidadãos, tirando partido do efeito de escala para balizar limites e obter benefícios.

Gigantes como a Google e o Facebook têm de ficar sujeitos ao mesmo tipo de regras que as empresas responsáveis por outros serviços que se tornaram *comodities*.

Síntese das Conclusões

1. O grupo começou por identificar quais as abordagens mais comuns para uma articulação entre a Regulação Económica e a Privacidade, designadamente:

a) A ausência de relações possíveis. A Privacidade, incluindo nesta a Proteção de Dados Pessoais enquanto Direito Fundamental a ser garantido e apenas suscetível de limitação por outros Direitos de idêntica natureza, não releva quaisquer considerações de natureza económica. Isto é, a Regulação da Privacidade sobrepor-se-ia a todas as Regulações com conteúdo económico. Neste sentido, foram apontadas as Jurisprudências do Tribunal Europeu dos Direitos do Homem e do Tribunal de Justiça da União Europeia.

b) A possibilidade de a Regulação da Privacidade ser reforçada, na respetiva eficácia, através de uma atuação concertada, ainda que subsidiária, dos Reguladores Setoriais, como os correspondentes às comunicações eletrónicas e da Concorrência.

c) A utilização de incentivos económicos, ou oriundos da Regulação Económica, como as certificações ou as avaliações de impacto, para a limitação dos riscos de pagamentos de indemnizações por danos causados aos titulares dos dados pessoais, ou de coimas a serem aplicadas pelos Reguladores da Privacidade. Nesta linha, temos o Novo Regulamento Geral para a Proteção de Dados da União Europeia.

d) A viabilidade, até demonstrável empiricamente, de determinar níveis mais elevados de rigor no tratamento de dados, acrescidos de uma compliance efetiva e reconhecida, sob controlo do Regulador da Privacidade, poderem constituir um factor de diferenciação positiva no Mercado Global, reforçando a posição competitiva das empresas. Também neste sentido, temos o Novo Regulamento Geral para a Proteção de Dados da União Europeia.

2. Mas, o grupo ainda se ocupou de outras questões, à partida, menos consensuais, todas elas resultantes da constatação do valor económico dos dados pessoais, vista a evolução geométrica das capitalizações bolsistas das empresas de internet e da tentativa de rendibilizar os dados que outras empresas, sobretudo de utilities, dispõem:

a) A necessidade de serem desenvolvidos métodos de determinação valor dos dados pessoais, por forma a estabelecer critérios de compensação efetiva dos respetivos titulares, assim como das Sociedades em que estes se inserem.

b) A identificação de uma esfera de Privacidade, a ser colocada absolutamente fora do comércio, em especial no que se refere aos grupos mais vulneráveis, como os menores e os infoexcluídos por razões económicas ou territoriais, assim criando níveis de Anonymity by Default.

c) A implementação de ferramentas, também tecnológicas, que possibilitem uma negociação transparente e equilibrada entre os titulares dos dados e os responsáveis pelo tratamento, possibilitando aos primeiros um retorno equitativo da monetização dos seus dados.

d) Do mesmo modo, fará sentido a avaliação da viabilidade de estabelecer vias de negociação coletiva dos dados, desde que cumpridos dos critérios legais de obtenção dum consentimento informado e explícito por parte de cada um dos titulares dos dados.

e) Prever ainda a possibilidade de o Estado negociar com terceiros os dados de que dispõe, com transparência, desde que obtenha o necessário consentimento dos respetivos titulares ou os mesmos sejam objeto de técnicas de anonimização robustas, só muito dificilmente reversíveis.

f) Estabelecer instrumentos de concertação obrigatória entre os Reguladores da Privacidade e os Reguladores Económicos, no nível nacional, mas sobretudo no nível da União Europeia, por forma a obter um controle efetivo e múltiplo nas Empresas da Internet, quase todas elas extraeuropeias e com aspirações "majestáticas".

Abrir novos horizontes e proteger os infoexcluídos

Reduzido a apenas um dia de reflexão, o tempo do Fórum da Arrábida terá sido pouco para condensar devidamente todos os contributos ali deixados pelos três grupos de trabalho que apresentaram as suas conclusões num debate final moderado por Raul Mascarenhas.

Gerindo os trabalhos com disciplina nos tempos atribuídos a cada um, Raul Mascarenhas, reservou espaço para a apresentação dos moderadores de cada grupo e para os comentários da plateia, que sempre enriquecem o debate.

João Confraria, administrador da ANACOM, considera que as várias conclusões foram "equilibradas no sentido de favorecer processos de acreditação". As notas finais apresentadas por João Confraria destacaram os pontos mais focados nos processos de acreditação, com ênfase na necessidade de definir quem irá liderar esses processos de acreditação. "Também apreciei bastante a ginástica que foi feita pelo primeiro grupo, em torno da definição de privacidade, que foi sofrendo mutações ao longo da apresentação", sublinhou.

O administrador da ANACOM não se mostrou otimista quanto ao novo regulamento de proteção de dados porque, afirmou, "nalguns casos parece-me que implica mudanças organizacionais que talvez sejam pacíficas mas noutros não". Fazendo eco de alguma tradição cultural portuguesa, João Confraria prevê que venham a aparecer Data Protection Officers: "Algumas organizações vão fazê-lo como deve ser feito mas outras vão abastardar o conceito só para dar a ideia que cumprem e não vão cumprir. Vai ser para inglês ver".

O administrador da ANACOM não se mostrou otimista quanto ao novo regulamento de proteção de dados.

O responsável acrescentou à apresentação das suas conclusões a ideia do impacto do regulamento na evolução da proteção dos dados efetiva que ainda virá a ser acompanhada no futuro pelo regulador.

"A liberalidade com que os Governos podem dispor dos dados" foi apontada pelo docente e investigador José Alegria como nota preocupante porque "o Governo da Islândia pode dispor dos dados dos islandeses e acho que a população não foi ouvida. Eles podem ter uma lei à parte só que, para mim, não faz sentido que isso aconteça sem que as pessoas queiram".

A convergência de ideias conseguida no fim do dia de trabalhos deu mote ao reforço por parte do professor aos incentivos que são dados às PMEs, no sentido de que as previsões da Proteção de Dados conferem amplas isenções e proteções

"A liberalidade com que os Governos podem dispor dos dados" foi apontada pelo docente e investigador **José Alegria** como nota preocupante.

para as pequenas e médias empresas, dizendo que "Portugal só tem a ganhar". Neste aspecto foi secundado pelo presidente da Direção da APDSI que alertou, contudo, para o facto de algumas PMEs poderem não ser economicamente fortes. Raul Mascarenhas subscreveu a opinião deixada por vários intervenientes que reconhecem o não antagonismo entre privacidade e cibersegurança. O ponto seguinte teve a ver com o valor económico dos nossos dados pessoais, "o que implica a possibilidade de serem transacionados". A opinião comum é que, mesmo que exista essa possibilidade de os dados serem transacionados, existem limites e direitos inalienáveis "que deverão ter uma proteção".

Ainda em jeito de conclusão dos trabalhos, coube a Raul Mascarenhas deixar umas palavras para "a proteção daqueles que não são capazes de ter controlo na sua decisão, como os infoexcluídos e os menores; alguém tem que os defender". Outro aspecto falado teve a ver com os mecanismos regulatórios, em analogia ao que se verificou no âmbito ambiental nos últimos anos, com várias intervenientes a apontarem o caminho para a certificação.

O problema pode passar pelo facto de muitas das *apps* serem gratuitas e de a certificação só abranger aquilo que é vendido.

Raul Mascarenhas deixou umas palavras para "a proteção daqueles que não são capazes de ter controlo na sua decisão, como os infoexcluídos e os menores; alguém tem que os defender".

A questão da atribuição de incentivos aos reguladores, para fazerem os operadores chegar a um bom caminho, também recebeu a concordância do plenário que considera que ainda há um *gap* entre estes pensamentos e a população a quem se destinam, mas a APDSI "contribuiu para a sua sensibilização neste Fórum da Arrábida", sumarizou.