Breves notas sobre segurança da informação, acesso a dados e privacidade[1]

O escrupuloso respeito pela **privacidade**, a adequada salvaguarda da **intimidade da vida privada** e o princípio da **inviolabilidade das comunicações**[2], bem como a magna questão da legitimidade ou ilegitimidade do **acesso a dados** e, sobretudo, a *segurança*, a *obtenção*, a *transparência*, a *disponibilização*, a *divulgação*, a *comunicação* e a *publicitação* de **informação** não são preocupações exclusivas das **autoridades reguladoras, de controlo ou de supervisão**; e dos seus dirigentes, funcionários, ou colaboradores; são **direitos do homem**, por isso humanos, universais, básicos ou fundamentais, oponíveis a todas as pessoas.

Neste texto meramente informativo e sem pretensões, elaborado como suporte para uma **acção de formação interna** de vários quadros do **ICP-ANACOM**, procuraremos tocar cada uma destas realidades de modo informativo, prático, concreto, sintético e útil, mas sempre partindo de uma **perspectiva jurídica** própria e interessada, a fim de *compreender e reduzir* riscos e *vulnerabilidades* pessoais e organizacionais e, igualmente, para promover a *partilha* de legislação e de jurisprudência, a *divulgação* do saber e do *saber-fazer*[3].

Duas das áreas que irão ser particularmente abordadas são precisamente a da **segurança**[4]**,** numa das suas várias vertentes, e a do **sigilo das telecomunicações**[5] e, nessa medida, as **regras de protecção** e as *excepções*, bem como os especiais **deveres das autoridades no exercício dos poderes de conformação, de controlo e de disciplina da actividade dos regulados** e, por tabela, dos poderes e deveres de outras autoridades, designadamente judiciais, judiciárias, policiais e administrativas, nos procedimentos da sua competência.

---

[1] Texto disponibilizado por **Carlos Pinto de Abreu**, Advogado, para acção de formação do **ICP-ANACOM** sobre *Segurança da Informação* e realizada na Faculdade de Direito da Universidade de Lisboa, dia 28 de Junho de 2013, com a sua coordenação, a do Engº Manuel Barros (DSC) e a do Professor Doutor Eduardo Vera-Cruz Pinto (FDL).

[2] O Acórdão do Tribunal da Relação de Guimarães de 10 de Janeiro de 2005, proferido no Processo 2013/04-1, decidiu que: "*I - A distinção entre dados de tráfego das comunicações e o seu conteúdo é, hoje em dia irrelevante, já que* ***a Lei 41/2004, de 18 de Agosto, equipara os dados de tráfego aos dados de conteúdo para efeitos de garantia da inviolabilidade das comunicações"*** e que *"III- Na preservação do chamado "direito à intimidade da vida privada", prevê a lei - artº 17º, n. 2, da Lei nº 91/97, e artº 5º da Lei nº 69/98, - que nesta área das telecomunicações, o dever de sigilo, conexo com o referido direito, possa ser invocado. Aliás, constitui crime, p.p. nos termos do artº 198º do Cód. Penal, a violação do dever de sigilo."* Já a Lei do Cibercrime, no seu artigo 18.º, n.º 3, considera o acesso a dados de tráfego como um *minus* em relação aos de conteúdo.

[3] Esta **concreta preocupação com a segurança** tem já mais de uma década. Cfr. o teor da Comunicação da Comissão ao Conselho, ao parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões para *criar uma Sociedade de Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade* (Bruxelas, 26.01.2001 COM(2000) 890 final. Mas tem-se vindo a sentir a **crescente necessidade de promover a segurança informacional, física e digital** – v.g. na integridade das redes e na fiabilidade dos dados.

[4] A **prova digital tem especiais problemas de segurança** desde logo quanto à sua **autoria, fidedignidade ou genuinidade**, como foi desde logo reconhecido pela Directiva 1999/93/CE do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999. O Decreto-Lei n. 290-D/99, de 2 de Agosto, alterado que foi pelos Decretos-Leis n.º 62/2003, de 3 de Abril, 165/2004, de 7 de Junho, 116-A/2006, de 16 de Junho, e 88/2009, de 9 de Abril, regula a validade, a eficácia, o valor probatório dos documentos electrónicos e, em especial, a assinatura electrónica. São também importantes nesta matéria o Decreto Regulamentar n.º 25/2004, de 15 de Julho, que aprova as regras técnicas e de segurança exigíveis às entidades certificadoras que emitem certificados qualificados e a Portaria n.º 597/2009, de 4 de Junho, que rege os termos a que obedece o registo das entidades certificadoras que emitem certificados qualificados.

[5] A Lei n.º 41/2004, de 18 de Agosto, com as alterações da Lei n.º 46/2012, de 29 de Agosto, estatui no seu artigo 4.º, sob a epígrafe de **Inviolabilidade das comunicações electrónicas**, que "*1- As empresas que oferecem redes e ou serviços de comunicações electrónicas devem garantir inviolabilidade das comunicações e respectivos dados de tráfego realizados através de redes públicas de comunicações e de serviços de comunicações electrónicas acessíveis ao público. 2- É proibida escuta, instalação de dispositivos de escuta, o armazenamento ou outros meios de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com excepção dos casos previstos na lei. 3- O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respectivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transacção comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.4- São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza."*

A análise de alguns destes temas irá aqui ser feita à luz dos **normativos vigentes** que regulam **organização interna** e **regimes;** das leis e boas regras que presidem ao exercício das suas **atribuições** e da sua concreta **actividade,** actividade essa que tem vindo a ganhar uma crescente importância e, correspondentemente, a consolidar a **independência orgânica e funcional**, bem assim como a **autoridade** e o **prestígio** desta concreta instituição pública, a quem se deve a génese e organização deste evento, o ICP-ANACOM.

Os temas da segurança[6], dos segredos e do sigilo convocam as realidades práticas da **fidedignidade da informação** e, claro, do **acesso aos dados**[7]**,** que pode ser obrigatório, conforme ou não conforme à lei e, se desconforme, pode configurar mesmo, entre outros ilícitos, um **crime** e, como já foi dito (Snowden), até um **crime contra a humanidade**.

Elementos essenciais, pois, da fidedignidade ou da **segurança de informação** são sobretudo três - a **autoria**, a **genuinidade** e a **integridade**, tanto que, para além do **crime de falsificação**, no Código Penal, até a tutela nos novos domínios digitais foi reforçada com a previsão específica do **crime de falsidade informática**, na Lei do Cibercrime.[8]

---

[6] Existem já vários mecanismos tecnológicos, e estão a ser desenvolvidos outros, para melhorar a **segurança no ciberespaço**. Esta resposta tecnológica inclui medidas para: garantir a segurança de elementos críticos das infra-estruturas através da utilização de infra-estruturas essenciais públicas (PKI), do desenvolvimento de protocolos de segurança, etc; garantir a segurança de ambientes privados e públicos através do desenvolvimento de programas informáticos de qualidade, protecções (*firewalls*), programas antivírus, sistemas electrónicos de gestão de direitos, codificação, etc. [e] garantir a autenticação de utilizadores autorizados, a utilização de cartões inteligentes, a identificação biométrica, as assinaturas electrónicas, as tecnologias de acesso pela função, etc. – cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

[7] E é por isso que *«nos serviços de telecomunicações podem distinguir-se, fundamentalmente, **três espécies ou tipologias de dados** ou elementos: os dados relativos à conexão à rede, ditos **dados de base**; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), **dados de tráfego**; e os dados relativos ao conteúdo da comunicação ou da mensagem, **dados de conteúdo**. Sendo os vários serviços de telecomunicações utilizados para a transmissão de comunicações verbais ou de outro tipo (mensagens escritas, dados por pacotes), os elementos inerentes à comunicação podem, por outro lado, estruturar-se numa composição sequencial em quatro tempos: a **fase prévia à comunicação**, o **estabelecimento da comunicação**, a **fase da comunicação** propriamente dita e a **fase posterior à comunicação**. No primeiro tempo relevam essencialmente os dados de base, enquanto que nos restantes importa essencialmente a consideração dos dados de tráfego e de conteúdo. Os **dados de base** constituem, na perspectiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respectivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço. (...) Diversamente dos elementos de base (elementos necessários ao estabelecimento de uma base para comunicação), que estão aquém, antes, são prévios e instrumentos de qualquer comunicação, os chamados **elementos de tráfego** (elementos funcionais da comunicação), como os elementos ditos de conteúdo, têm já a ver directamente com a **comunicação**, quer sobre a respectiva **identificabilidade**, quer relativamente ao **conteúdo** propriamente dito da mensagem ou da comunicação. Os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, é operada ou transmitida, são a direcção, o destino **(adressage)** e a via, o trajecto **(routage)**. (...) Estes elementos funcionalmente necessários ao estabelecimento e à direcção da comunicação identificam, ou permitem identificar a comunicação: quando conservados, possibilitam a identificação das comunicações entre o eminente e o destinatário, a data, o tempo, e a frequência das ligações efectuadas. Constituem, pois, **elementos já inerentes à própria comunicação**, na medida em que permitem identificar, em tempo real ou a posteriori, os utilizadores, o relacionamento directo entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, **devem participar das garantias a que está submetida a utilização do serviço**, especialmente tudo quanto respeite ao **sigilo das comunicações**. Finalmente, os **elementos de conteúdo** - dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede».* (Cfr., por todos, o doutamente decidido no Acórdão do Tribunal da Relação de Guimarães de 12 de Abril de 2010, proferido no âmbito do Processo n.º 1341/08.4TAVCT - http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/045285606f260ef2802577180050fdf9?OpenDocument&Highlight=0,anacom [sublinhados nossos]

[8] Estabelece o artigo 3.º, n.º 1 da Lei n.º 109/2009 de 15 de Setembro, intitulada **Lei do Cibercrime**, que *"1 - Quem, com intenção de provocar engano nas relações jurídicas, **introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos**, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias."* [sublinhado nosso]

Por outro lado, a ilegitimidade de acesso aos dados armazenados num sistema informático pode constituir, entre outros, um crime de **acesso ilegítimo**[9] estatuído na Lei nº 109/2009, de 15 de Setembro, no seu artigo 6.º, ou um crime de **violação de correspondência ou de telecomunicações**[10] previsto no artigo 194.º do Código Penal, em particular no seu n.º 2, ou, ainda, um crime de **violação de segredo de correspondência ou de telecomunicações**[11] de acordo com o disposto na als. a) a c) do artigo 384.º do Código Penal, designadamente quando estejamos perante funcionário de serviços de telecomunicações, e, claro, consoante as circunstâncias e se estivermos a falar do direito interno.[12]

Em matéria de acesso a dados, é necessário destrinçar a natureza dos dados de que estamos a tratar, ou de que estejamos a falar, embora tal distinção seja hoje menos **importante do ponto de vista prático**, pois que agora todos "*os elementos de informação respeitantes aos utilizadores de serviços de telecomunicações, geralmente designados como dados de tráfego e dados de conteúdo, e bem assim os dados de base relativamente aos quais os utilizadores tenham requerido um regime de confidencialidade* (...) *estão sujeitos ao sigilo das comunicações*[13] (Parecer n° 21/2000 da PGR).

---

[9] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 6.º, sob a epígrafe de Acesso ilegítimo, que "*1- Quem, **sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele**, de qualquer modo **aceder a um sistema informático**, é punido com pena de prisão até um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2- Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3- A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. 4- A pena é de prisão de 1 a 5 anos quando: a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 5- A tentativa é punível, salvo nos casos previstos no n.º 2. 6 – Nos casos previstos nos n.ºs 1, 3 e 5 o procedimento penal depende de queixa."* [sublinhados nossos]

[10] O Código Penal, estatui no Livro II, Título I, Capítulo I, artigo 194.º, sob a epígrafe de violação de correspondência ou de telecomunicações, que "*1- Quem, **sem consentimento**, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou **tomar conhecimento**, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias. 2- Na mesma pena incorre quem, sem consentimento, se **intrometer no conteúdo** de telecomunicação ou dele tomar conhecimento. 3 – Quem, sem consentimento, **divulgar o conteúdo** de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias."* [sublinhados nossos]

[11] O Código Penal, estatui no Capítulo IV, Secção IV, artigo 384.º, sob a epígrafe de Violação de segredo de correspondência ou de telecomunicações, de acordo com o disposto nas alíneas a) a c), que "***O funcionário de serviços dos correios, telégrafos, telefones ou telecomunicações** que, sem estar devidamente autorizado: a) **Suprimir ou subtrair** carta, encomenda, telegrama ou outra comunicação confiada àqueles serviços e que lhe é acessível em razão das suas funções; b) Abrir carta, encomenda ou outra comunicação que lhe é acessível em razão das suas funções ou, sem a abrir, tomar conhecimento do seu conteúdo; c) **Revelar** a terceiros comunicações entre determinadas pessoas, feitas pelo correio, telégrafo, telefone ou outros meios de telecomunicação daqueles serviços, de que teve conhecimento em razão das suas funções."* [sublinhados nossos]

[12] "*A própria natureza das infracções informáticas coloca, quer a nível nacional quer internacional, o **problema dos procedimentos aplicáveis**, na medida em que afectam **soberanias, competências e legislações diferentes**. Mais do que em relação a qualquer outra forma de **criminalidade transnacional**, a rapidez, a mobilidade e a flexibilidade da criminalidade informática desafiam as regras existentes em matéria de direito penal processual*"– cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade. Ali se elencam "*quatro categorias de infracções penais: 1) **infracções contra a confidencialidade, a integridade e a disponibilidade dos dados e sistemas informáticos**; 2) **infracções informáticas**; 3) **infracções relativas aos conteúdos** e 4) **infracções associadas às violações da propriedade intelectual e dos direitos conexos***". [sublinhados nossos] Nestes direitos conexos estão a protecção da privacidade e da intimidade da vida privada.

[13] Convém esclarecer, mais uma vez, que «*numa classificação aglutinadora dos **dados pessoais** (...), podemos distinguir três tipos de dados: os dados de base, os dados de tráfego e os dados de conteúdo. **Os dados de base** consistem nos elementos fornecidos pelo utilizador à empresa que fornece o acesso à rede e ou ao serviço de comunicações electrónicas, v.g., nome, morada, e os dados que aquela empresa fornece, em sentido inverso, ao utilizador para efeito de interligação à rede e ou ao serviço de comunicações electrónicas, v.g., número de acesso, nome de utilizador,* password*. Os **dados de tráfego** dizem respeito aos elementos funcionais da comunicação e permitem o envio da comunicação através de uma rede de comunicações electrónicas, v.g., data e hora do início da*

Contudo não foi assim inicialmente pois "*em relação aos **dados de base**, ainda que cobertos pelo sistema de confidencialidade a solicitação do assinante, tendo em consideração que **o sigilo profissional em causa releva de um simples interesse pessoal do utilizador que não contende com a respectiva esfera privada íntima**, os correspondentes elementos de informação poderão ser comunicados, a pedido de qualquer autoridade judiciária, para fins de investigação criminal*" (Circular nº 8/2000, da PGR)[14] [sublinhados nossos].

A **Lei n.º 48/2007, de 29 de Agosto**, submeteu a obtenção de **dados de localização** celular **ou de registo de conversações ou de comunicações** às regras de catálogo de crimes e da indicação de alvos do regime das escutas telefónicas, sujeitando esta **obtenção de prova**, sem discriminação, à **reserva de juiz**[15].

Assim, numa formulação compreensiva tanto se pode ter, pessoal ou institucionalmente, inteira **legitimidade no acesso aos dados**, como, na medida em que a obtenção destes dados seja precedida do acesso ilegal ou não autorizado a um sistema informático, ficar incurso num crime de acesso ilegítimo ou, até, noutro tipo e natureza de responsabilidade.

Com efeito, se estivermos já no âmbito processual ou procedimental, tanto se pode lograr uma **obtenção de prova por meios legais e processualmente admitidos**[16], como por meio de desrespeito ou de violação das regras substantivas e processuais[17], podendo gerar-se deste modo vícios processuais de diferentes gravidade e efeitos, conforme o caso.

Ou seja, o desrespeito ou a violação das regras substantivas e processuais, no processo-crime, pode gerar **proibições de prova**, **nulidades insanáveis**, **nulidades dependentes de arguição** ou meras **irregularidades**, e, no processo contra-ordenacional, simplesmente nulidades, embora estas também possam ter diversa natureza e diferentes efeitos.

---

*sessão (*login*) e do fim (*logoff*) da ligação ao serviço de acesso à Internet, endereço de IP atribuído pelo operador, volume de dados transmitidos, entre outros. Os **dados de conteúdo** baseiam-se no conteúdo da comunicação transmitida pela rede de comunicações electrónicas*». Mas mais recentemente «*com a evolução das directivas comunitárias em matéria de comunicações electrónicas verificou-se uma metamorfose no paradigma da protecção jurídica dos dados pessoais em que, ao lado da mencionada trilogia de dados de tráfego, de base e de conteúdo, surge agora a definição de dados de localização*». [sublinhados nossos]

[14] E também a Lei n.°109/2009, de 15 de Setembro, a Lei do Cibercrime, estabelece, no seu art. 14°, n° 4, que «o disposto no presente artigo é aplicável a **fornecedores de serviço**, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.» [sublinhado nosso]

[15] "*Constitui uma **devassa intolerável da privacidade do cidadão** a localização celular se não está concretizado nenhum alvo, nem existe a probabilidade forte de os elementos pretendidos poderem vir a evidenciar um qualquer suspeito dos atos em investigação*" [sublinhado nosso]. Cfr. o teor do Acórdão do Tribunal da Relação de Évora, de 21 de Maio de 2013.

[16] *O Acórdão do Tribunal da Relação de Évora, de 13 de Junho de 2002, decidiu então que* "*Não nos deparamos com qualquer violação do segredo das telecomunicações ou profissional quando se fornece ao Tribunal a informação quanto à residência dum assinante*".

[17] O Acórdão do Tribunal da Relação de Évora, de 20 de Dezembro de 2012, decidiu que "*I – A defesa do entendimento que se considera adequado à **salvaguarda de sigilo** a que se está obrigado, com o propósito de o quebrar nas condições que se entendam isentas de responsabilidade, não pode considerar-se como **conduta que embaraça o regular andamento de um processo***" e que "*II – Em simultâneo, não pode julgar-se ilegítima a recusa na prestação de elementos solicitados e impor-se a sanção prevista no n.º 2 do artigo 521.º do Código de Processo Penal. Tal **sanção** apenas pode ser imposta se, tornando-se definitiva a decisão sobre ilegitimidade da recusa, quem está obrigado a prestar informações persistir em não as fornecer.*" [sublinhados nossos]

E assim há que evitar incorrer em actos ou omissões que possam implicar violação de deveres de função ou, até, no limite, **violação de segredos**, **devassa da vida privada** ou **violação da protecção de dados pessoais**, cumprindo e fazendo cumprir os pressupostos legais e os limites constitucionais à obtenção e utilização de informação, ou de prova digital, em instâncias informais, pessoais, ou judiciais, mas não só.

E isto sob pena de **violação de lei e perda da prova**, sem prejuízo da **responsabilidade criminal, civil e disciplinar** que possa ser invocada, por infracção dolosa ou negligente das normas procedimentais que ao caso couberem.

Em matéria de normas processuais neste domínio, existem **meios clássicos da obtenção de prova**, onde avultam, desde logo, a **apreensão de correspondência**[18] e as **intercepções nas comunicações**[19].

---

[18] O Código de Processo Penal, estatui no Livro III, Título III, Capítulo III, artigo 179.º, sob a epígrafe de **Apreensão de correspondência**, que "*1 - Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que: a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa; b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova. 2 - É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime. 3 - O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.*"

[19] O Código de Processo Penal, estatui no Livro III, Título III, Capítulo IV, nos artigos 187.º, 188.º, 189.º e 190.º, respectivamente, o seguinte sobre: **Admissibilidade** – *"1 - A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes: a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos; b) Relativos ao tráfico de estupefacientes; c) De detenção de arma proibida e de tráfico de armas; d) De contrabando; e) De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone; f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores. 2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efectivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes: a) Terrorismo, criminalidade violenta ou altamente organizada; b) Sequestro, rapto e tomada de reféns; c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário; d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal; e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262.º, 264.º, na parte em que remete para o artigo 262.º, e 267.º, na parte em que remete para os artigos 262.º e 264.º, do Código Penal; f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima. 3 - Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de setenta e duas horas, ao conhecimento do juiz do processo, a quem cabe praticar os actos jurisdicionais subsequentes. 4 - A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra: a) Suspeito ou arguido; b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido. 5 - É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime. 6 - A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade. 7 - Sem prejuízo do disposto no artigo 248.º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1. 8 - Nos casos previstos no número anterior, os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho do juiz, ao processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito.";* **Formalidades das operações** – *"1 - O órgão de polícia criminal que efectuar a intercepção e a gravação a que se refere o artigo anterior lavra o correspondente auto e elabora relatório no qual indica as passagens relevantes para a prova, descreve de modo sucinto o respectivo conteúdo e explica o seu alcance para a descoberta da verdade. 2 - O disposto no número anterior não impede que o órgão de polícia criminal que proceder à investigação tome previamente conhecimento do conteúdo da comunicação interceptada a fim de poder praticar os actos cautelares necessários e urgentes para assegurar os meios de prova. 3 - O órgão de polícia criminal referido no n.º 1 leva ao conhecimento do Ministério Público, de 15 em 15 dias a partir do início da primeira intercepção efectuada no processo, os correspondentes suportes técnicos, bem como os respectivos autos e relatórios. 4 - O Ministério Público leva ao conhecimento do juiz os elementos referidos no número anterior no prazo máximo de quarenta e oito horas. 5 - Para se*

E existem, ainda em processo penal especial, e não obstante a **regra geral da reserva de juiz**, algumas **medidas especiais de obtenção de prova digital** previstas na Lei n.º 109/2009, de 15 de Setembro, a saber, a **preservação expedita de dados**[20], a **revelação expedita de dados de tráfego**[21] e a **injunção para apresentação ou concessão de acesso a dados**[22].

---

inteirar do conteúdo das conversações ou comunicações, o juiz é coadjuvado, quando entender conveniente, por órgão de polícia criminal e nomeia, se necessário, intérprete. 6 - Sem prejuízo do disposto no n.º 7 do artigo anterior, o juiz determina a destruição imediata dos suportes técnicos e relatórios manifestamente estranhos ao processo: a) Que disserem respeito a conversações em que não intervenham pessoas referidas no n.º 4 do artigo anterior; b) Que abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado; ou c) Cuja divulgação possa afectar gravemente direitos, liberdades e garantias; ficando todos os intervenientes vinculados ao dever de segredo relativamente às conversações de que tenham tomado conhecimento. 7 - Durante o inquérito, o juiz determina, a requerimento do Ministério Público, a transcrição e junção aos autos das conversações e comunicações indispensáveis para fundamentar a aplicação de medidas de coacção ou de garantia patrimonial, à excepção do termo de identidade e residência. 8 - A partir do encerramento do inquérito, o assistente e o arguido podem examinar os suportes técnicos das conversações ou comunicações e obter, à sua custa, cópia das partes que pretendam transcrever para juntar ao processo, bem como dos relatórios previstos no n.º 1, até ao termo dos prazos previstos para requerer a abertura da instrução ou apresentar a contestação, respectivamente. 9 - Só podem valer como prova as conversações ou comunicações que: a) O Ministério Público mandar transcrever ao órgão de polícia criminal que tiver efectuado a intercepção e a gravação e indicar como meio de prova na acusação; b) O arguido transcrever a partir das cópias previstas no número anterior e juntar ao requerimento de abertura da instrução ou à contestação; ou *c) O assistente transcrever a partir das cópias previstas no número anterior e juntar ao processo no prazo previsto para requerer a abertura da instrução, ainda que não a requeira ou não tenha legitimidade para o efeito. 10 - O tribunal pode proceder à audição das gravações para determinar a correcção das transcrições já efectuadas ou a junção aos autos de novas transcrições, sempre que o entender necessário à descoberta da verdade e à boa decisão da causa. 11 - As pessoas cujas conversações ou comunicações tiverem sido escutadas e transcritas podem examinar os respectivos suportes técnicos até ao encerramento da audiência de julgamento. 12 - Os suportes técnicos referentes a conversações ou comunicações que não forem transcritas para servirem como meio de prova são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo. 13 - Após o trânsito em julgado previsto no número anterior, os suportes técnicos que não forem destruídos são guardados em envelope lacrado, junto ao processo, e só podem ser utilizados em caso de interposição de recurso extraordinário."*; **Extensão** – *"1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes. 2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo."*; **Nulidade** – *"Os requisitos e condições referidos nos artigos 187.º, 188.º e 189.º são estabelecidos sob pena de nulidade."*

[20] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 12.º, sob a epígrafe de **Preservação expedita de dados**, que "*1- Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecer de serviço, que preserve os dados em causa. 2- A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal. 3- A ordem de preservação discrimina, sob pena de nulidade: a) A natureza dos dados; b) A sua origem e destino, se forem conhecidos e; c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses. 4- Em cumprimentos de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual. 5- A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano*".

[21] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 13.º, sob a epígrafe de **Revelação expedita de dados de tráfego**, que, "*tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participam, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada*".

[22] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 14.º, sob a epígrafe de **Injunção para apresentação ou concessão do acesso a dados**, "*1 – Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. 2 – A ordem referida no número anterior identifica os dados em causa. 3 – Em cumprimento da ordem descrita nos n.ºs 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade*

Bem como, e ainda, pode lançar-se mão da **pesquisa de dados informáticos**[23], da **apreensão de dados informáticos**[24] e da **apreensão de correio electrónico e registos de comunicações de natureza semelhante**[25].

---

judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados. 4 – O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços. 5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo. 6 - Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. 7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações".

[23] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 15.º, sob a epígrafe de **Pesquisa de dados informáticos**, que "*1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência. 2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade. 3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando: a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa. 4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior: a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação; b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal. 5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2. 6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista*".

[24] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 16.º, sob a epígrafe de **Apreensão de dados informáticos**, que "*1 - Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos. 2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora. 3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto. 4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas. 5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista. 6 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações. 7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes: a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) Eliminação não reversível ou bloqueio do acesso aos dados. 8 - No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital*".

[25] A Lei n.º 109/2009, de 15 de Setembro, estatui no seu artigo 17.º, sob a epígrafe de **Apreensão de correio electrónico e registos de comunicações de natureza semelhante**, que "*quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*".

Com excepção desta última medida - **apreensão de correio electrónico e de registos de comunicações de natureza semelhante**, todas as restantes **medidas especiais** supra elencadas podem ser determinadas imediatamente pela **autoridade judiciária competente**, isto é, pelo **Ministério Público**, desde logo na fase do inquérito - fase que tem como finalidade a investigação e recolha de prova, mas também, se necessário, posteriormente.

Como obstáculos, ainda assim removíveis, à recolha da prova, poderíamos discutir nesta acção os **sigilos** previstos em leis especiais, tais como o **sigilo das telecomunicações**[26], o **sigilo bancário**[27], o **sigilo comercial**[28] ou o **industrial**[29].

E poderíamos igualmente abordar a temática dos **segredos** impostos, pois que nem sempre é fácil distingui-los no caso concreto[30], desde logo o **segredo de Estado**[31], o **segredo profissional**[32], o **segredo de funcionário**[33] ou o **segredo de justiça**[34].

---

[26] O artigo 15.º n.º 2 da Lei n.º 88/89 de 11 de Setembro estatui "*Com os limites impostos pela sua natureza e pelo fim a que se destinam, **é garantida a inviolabilidade e o sigilo das telecomunicações de uso público**, nos termos da lei."* [sublinhado nosso].

[27] O artigo 78.º do DL n.º 298/92, de 31 de Dezembro prevê "*1.Os membros dos órgãos de administração ou de fiscalização das instituições de crédito, os seus empregados, mandatários, comitidos e outras pessoas que lhes prestem serviços a título permanente ou ocasional não podem revelar ou utilizar informações sobre factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços"*

[28] V. **Pareceres da Comissão de Acesso aos Dados Administrativos** acerca do acesso a dados sob sigilo comercial http://www.cada.pt/modules/cada/cada_pesquisa.php?assunto=assunto&artigos=artigos&resumo=resumo&corpo=corpo&sentidoparecer=sentidoparecer&requerente=requerente&queixade=queixade&descritores=descritores&entidaderequerida=entidaderequerida&checkall2=on&ligador=AND&txtPesquisa=segredo+comercial+clientes

[29] O DL n.º 16/95,de 24 de Janeiro, no seu artigo 318.º, sob a epígrafe de **Protecção de informações não divulgadas**, estatui que "Nos termos do artigo anterior, constitui acto ilícito, nomeadamente, a divulgação, a aquisição ou a utilização de **segredos de negócios** de um concorrente, sem o consentimento do mesmo, desde que essas informações: a) Sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exactas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; b) Tenham valor comercial pelo facto de serem secretas; c) Tenham sido objecto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas." [sublinhado nosso]

[30] Também o Acórdão do Tribunal da Relação de Évora, este de 7 de Dezembro de 2012, decidiu que "*A identidade de um cidadão que se liga a determinado blogue ou sítio da internet está coberta não pelo segredo das conversações ou comunicações regulado pelos art.º 187.º a 190.º do Código de Processo Penal, mas antes pelo segredo profissional a que se reporta o art.º 135.º do mesmo código e a ser tratado, quanto ao respectivo levantamento, nos termos indicados por esta disposição legal.*

[31] O Código de Processo Penal, estatui no Livro III, Título II, Capítulo I, artigo 137.º, sob a epígrafe **Segredo de Estado**, que *"1 - As testemunhas não podem ser inquiridas sobre factos que constituam segredo de Estado. 2 - O segredo de Estado a que se refere o presente artigo abrange, nomeadamente, os factos cuja revelação, ainda que não constitua crime, possa causar dano à segurança, interna ou externa, do Estado Português ou à defesa da ordem constitucional. 3 - Se a testemunha invocar segredo de Estado, deve este ser confirmado, no prazo de 30 dias, por intermédio do Ministro da Justiça. Decorrido este prazo sem a confirmação ter sido obtida, o testemunho deve ser prestado".*

[32] O artigo 14.º do Decreto-Lei n.º 309/2001, de 7 de Dezembro, nos seus números um e dois, respectivamente, estatui que "***os titulares dos órgãos do ICP – ANACOM, respectivos mandatários, pessoas ou entidades qualificadas devidamente credenciadas, bem como os seus trabalhadores eventuais ou permanentes, estão especialmente obrigados a guardar sigilo de factos cujo conhecimento lhes advenha exclusivamente pelo exercício das suas funções"*** e que ***"a violação do dever de segredo profissional previsto no número anterior é, para além da inerente responsabilidade disciplinar e civil, punível nos termos do Código Penal***".

[33] O Código de Processo Penal, estatui no Livro III, Título II, Capítulo I, artigo 136.º, sob a epígrafe de **Segredo de funcionário**, que *"1 - Os funcionários não podem ser inquiridos sobre factos que constituam segredo e de que tiverem tido conhecimento no exercício das suas funções. 2 - É correspondentemente aplicável o disposto nos n.os 2 e 3 do artigo anterior."*

[34] O Código de Processo Penal, estatui no Livro II, Título I, artigo 86.º, sob a epígrafe **Publicidade do processo e segredo de justiça**, que "*1 - O processo penal é, sob pena de nulidade, público, ressalvadas as excepções previstas na lei. 2 - O juiz de instrução pode, mediante requerimento do arguido, do assistente ou do ofendido e ouvido o Ministério Público, determinar, por despacho irrecorrível, a sujeição do processo, durante a fase de inquérito, a segredo de justiça, quando entenda que a publicidade prejudica os direitos daqueles sujeitos ou participantes processuais. 3 -*

Todos, sigilos e segredos, impedem ou de algum modo limitam ou delimitam a **publicidade**, **interna** ou **externa** e colocam uma especial exigência às autoridades administrativas, judiciais, judiciárias ou policiais no sentido de necessidade prévia de **despacho fundamentado da entidade competente**, de dispensa ou de quebra de sigilo por via dos procedimentos próprios e legitimadores do acesso a tal informação especialmente reservada, que podem até ser simples regras de bom senso em matérias procedimentais.

Em sede de **protecção ou de libertação de segredo e de sigilo na organização** é essencial, na prática, ter em atenção que na prossecução dos processos e na instrução de procedimentos estas matérias têm que ser salvaguardadas não só interna mas também externamente.

Na minha experiência na Ordem dos Advogados, quer em matéria de elaboração de pareceres em matérias profissionais, quer em matéria de decisão política ou de gestão, quer ainda, e em especial, na tramitação de processos disciplinares ou de dispensa de sigilo, verifiquei que é muito difícil[35] **manter, e manter a todo o tempo e a toda a prova, a reserva** que se exige.

Há, desde logo, que ter em conta que, por exemplo, um processo disciplinar ou sancionatório, enquanto se tramita internamente, na fase secreta e sem acesso público, senão, no limite, dos interessados directos que sejam autorizados a consultar os autos, não tem grandes riscos de ser publicitado ou, pelo menos, divulgado *urbi et orbi*.

Mas já assim não é se o mesmo processo findo ou pendente ou em fases já públicas nas instâncias internas da Ordem da dos Advogados – v.g. processo de dispensa ou de quebra de sigilo ou procedimento disciplinar após julgamento público - é objecto de impugnação

---

Sempre que o Ministério Público entender que os interesses da investigação ou os direitos dos sujeitos processuais o justifiquem, pode determinar a aplicação ao processo, durante a fase de inquérito, do segredo de justiça, ficando essa decisão sujeita a validação pelo juiz de instrução no prazo máximo de setenta e duas horas. 4 - No caso de o processo ter sido sujeito, nos termos do número anterior, a segredo de justiça, o Ministério Público, oficiosamente ou mediante requerimento do arguido, do assistente ou do ofendido, pode determinar o seu levantamento em qualquer momento do inquérito. 5 - No caso de o arguido, o assistente ou o ofendido requererem o levantamento do segredo de justiça, mas o Ministério Público não o determinar, os autos são remetidos ao juiz de instrução para decisão, por despacho irrecorrível. 6 - A publicidade do processo implica, nos termos definidos pela lei e, em especial, pelos artigos seguintes, os direitos de: a) Assistência, pelo público em geral, à realização do debate instrutório e dos actos processuais na fase de julgamento; b) Narração dos actos processuais, ou reprodução dos seus termos, pelos meios de comunicação social; c) Consulta do auto e obtenção de cópias, extractos e certidões de quaisquer partes dele. 7 - A publicidade não abrange os dados relativos à reserva da vida privada que não constituam meios de prova. A autoridade judiciária especifica, por despacho, oficiosamente ou a requerimento, os elementos relativamente aos quais se mantém o segredo de justiça, ordenando, se for caso disso, a sua destruição ou que sejam entregues à pessoa a quem disserem respeito. 8 - O segredo de justiça vincula todos os sujeitos e participantes processuais, bem como as pessoas que, por qualquer título, tiverem tomado contacto com o processo ou conhecimento de elementos a ele pertencentes, e implica as proibições de: a) Assistência à prática ou tomada de conhecimento do conteúdo de acto processual a que não tenham o direito ou o dever de assistir; b) Divulgação da ocorrência de acto processual ou dos seus termos, independentemente do motivo que presidir a tal divulgação. 9 - A autoridade judiciária pode, fundamentadamente, dar ou ordenar ou permitir que seja dado conhecimento a determinadas pessoas do conteúdo de acto ou de documento em segredo de justiça, se tal não puser em causa a investigação e se afigurar: a) Conveniente ao esclarecimento da verdade; ou b) Indispensável ao exercício de direitos pelos interessados. 10 - As pessoas referidas no número anterior são identificadas no processo, com indicação do acto ou documento de cujo conteúdo tomam conhecimento e ficam, em todo o caso, vinculadas pelo segredo de justiça. 11 - A autoridade judiciária pode autorizar a passagem de certidão em que seja dado conhecimento do conteúdo de acto ou de documento em segredo de justiça, desde que necessária a processo de natureza criminal ou à instrução de processo disciplinar de natureza pública, bem como à dedução do pedido de indemnização civil. 12 - Se o processo respeitar a acidente causado por veículo de circulação terrestre, a autoridade judiciária autoriza a passagem de certidão: a) Em que seja dado conhecimento de acto ou documento em segredo de justiça, para os fins previstos na última parte do número anterior e perante requerimento fundamentado no disposto na alínea a) do n.º 1 do artigo 72.º; b) Do auto de notícia do acidente levantado por entidade policial, para efeitos de composição extrajudicial de litígio em que seja interessada entidade seguradora para a qual esteja transferida a responsabilidade civil. 13 - O segredo de justiça não impede a prestação de esclarecimentos públicos pela autoridade judiciária, quando forem necessários ao restabelecimento da verdade e não prejudicarem a investigação: a) A pedido de pessoas publicamente postas em causa; ou b) Para garantir a segurança de pessoas e bens ou a tranquilidade pública."

[35] Difícil, mas possível.

administrativa ou até de outro tipo de reacção, até de recurso hierárquico e, ainda assim, há, total ou parcialmente, matéria sob sigilo em risco.[36]

Ou seja, **não é o simples facto de um processo ser público ou de poder vir a ser publicamente consultado que toda a informação que nele conste venha ou possa vir a ser livremente acedida**.

Se assim for, há, primeiro, que ter o **especial cuidado na tramitação interna** e, depois, quando e se for o caso[37], **na comunicação do processo instrutor** ao Tribunal a fim de só os directamente interessados ou visados no processo a ele terem acesso, não podendo ser cedidos a terceiros, não interessados, quer o acesso aos autos, quer quaisquer elementos cobertos por sigilo ou salvaguardados por um segredo específico, isto sob pena de responsabilidade disciplinar, civil ou, mesmo, penal.

Em síntese, **nem tudo o que não é segredo ou sigilo pode ou deve ser livremente divulgado ou abertamente disponibilizado**, sem mais, pois não existe, nem pode ser defendida uma simples dicotomia entre o que é, e não é, público.[38]

Há diversos escalões de dados reservados, e não são reservados apenas os dados sujeitos a sigilo ou cobertos pelo segredo, estando precisamente neste âmbito os **dados íntimos, pessoais e privados**, mas não só.

E isto quer se trate da actividade de operadores ou do próprio regulador, sendo considerados **dados pessoais** quaisquer informações, de qualquer natureza e independentemente do respectivo suporte incluindo som e imagem relativas a uma pessoa singular identificada ou identificável[39].

Constataremos realidades, a jurídica concreta e a factual abstracta, e não curaremos da adequação ou inadequação do quadro legal ou das boas ou más práticas, ainda que saibamos que **nenhuma legislação é perfeita e nenhuma organização está isenta de erros**, pelo que não será preciso, aqui, recordar que "*as ideias da prevenção e da segurança assumem o papel de palavra-chave na "idade do homem global*" (Cristina Máximo dos Santos) e que, por

---

[36] E este é tema relevante ou tanto mais relevante quanto nele podem estar inclusos elementos cobertos até pelo segredo de Estado ou pelo sigilo profissional.

[37] Não é o caso quando o que está em causa é decisão final de indeferimento da dispensa de sigilo, pois que esta matéria não pode ser objecto de impugnação judicial.

[38] O Acórdão do Supremo Tribunal Administrativo, retirado no processo 0493/09 e proferido em 30 de Setembro de 2009 decidiu o seguinte: "*I - O art.º 268.º/2 da CRP impõe que a Administração paute a sua actividade pelos **princípios da transparência e da publicidade** de modo a que não só as suas decisões sejam públicas e acessíveis, mas também que o procedimento que as precede possa ser objecto de consulta e informação pois que só assim se permite que os interessados conheçam as razões que determinaram os seus actos. II - O **direito de acesso** aos arquivos e registos administrativos vem sendo considerado como um direito fundamental cujo sacrifício só se justifica quando confrontado com direitos e valores constitucionais de igual ou de maior valia, como são os relativos à segurança interna e externa, à investigação criminal e à reserva da intimidade das pessoas. IV - O regime geral que regula o acesso à documentação administrativa estipula que o interessado tem direito a esse acesso mas que ele pode ser restringido ou condicionado quando estiver em causa a consulta de documentos que revelem os seus segredos comerciais, industriais ou sobre a vida interna de uma empresa. V - O poder da Administração recusar o acesso à sua documentação é um **poder vinculado aos princípios e objectivos fixados por lei**, a ser exercido segundo os princípios da transparência e da proporcionalidade, que só deve ser invocado quando o mesmo for indispensável para evitar prejuízos que não poderiam ser evitados doutra forma. VI - O terceiro que queira aceder a documentos administrativos que contenham segredos comerciais, industriais ou sobre a vida interna da Administração e que não tenha a necessária autorização escrita para o efeito, só pode ver o respectivo direito reconhecido se demonstrar ter **interesse directo, pessoal e legítimo** nessa consulta e que este é suficientemente relevante de acordo com o princípio da proporcionalidade.*"

[39] É considerada **identificável** a pessoa que possa ser reconhecida directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

consequência, a reflexão e formação nestes temas é essencial à **melhoria da qualidade dos serviços**.

As matérias da **segurança da informação** e da **gestão da informação** são essenciais na relação de uma entidade pública com os cidadãos e empresas e, por maioria de razão, são-no também numa **relação entre supervisor e supervisionado**.

E tanto que para minimizar **riscos operacionais** ou **erros humanos**, a **autenticidade**, a **precisão**, a **actualidade** e a **integridade** dos dados – dados reservados, dados conservados[40], dados parcialmente disponíveis, dados notificados ou dados publicamente divulgados – são também características essenciais em qualquer actividade pública ou privada.

Questões de privacidade, de reserva ou de transparência ou a consideração e a colocação das **fronteiras** ou dos **limites** do segredo, do dado íntimo ou pessoal, da informação interna, da comunicação individual ou da divulgação externa colocam-se a qualquer **pessoa** ou no âmbito de qualquer **organização de poder ou de responsabilidade**, *maxime* do Estado, qualquer que seja a matéria a que pretende dar resposta[41].

E são questões que se colocam com especial acuidade se, como é o caso, estamos perante uma **autoridade administrativa com funções de controlo, de regulação e de supervisão prudencial e comportamental** desde logo pelos seus **particulares deveres de cuidado e de**

[40] A Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE estabelece, no seu artigo 7.º, sob a epígrafe de **Protecção de dados e segurança dos dados**, que "Sem prejuízo das disposições adoptadas nos termos da Directiva 95/46/CE e da Directiva 2002/58/CE, cada Estado-Membro deve assegurar que os fornecedores de serviço de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações respeitem, no mínimo, os seguintes princípios em matéria de segurança de dados no que se refere aos dados conservados em conformidade com a presente directiva: a) Os dados conservados devem ser da mesma qualidade e estar sujeitos à mesma protecção e segurança que os dados na rede; b) Os dados devem ser objecto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental, ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito; c) Os dados devem ser objecto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados; e de) Os dados devem ser destruídos no final do período de conservação, excepto os dados que tenham sido facultados e preservados.

[41] As maiores ameaças à privacidade dos cidadãos são mesmo as que provêem dos Estados e nestes dos seus serviços secretos ou de informações, sobretudo quando actuam sem lei ou fora da lei. Nos EUA, segundo notícias vindas a público, a NSA lança mão do PRISM – programa denunciado por Snowden que visa recolher e processar informação provinda de empresas como a Verizon, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype e YouTube, de cidadãos estrangeiros e americanos. Recolhe emails, arquivos enviados, conversas nos chats e também áudios, vídeos e fotografias. Antes deste foi denunciado o ECHELON – programa embrionário do PRISM, um projecto secreto de espionagem que surgiu nos anos 80, e que fazia a interacção mundial de comunicações através de palavras-chave. Era encabeçado pelos EUA (NSA) e tinha a colaboração do Reino Unido, Austrália, Canadá e Nova Zelândia, apelidada a rede dos cinco olhos. Segundo as constituições destes países, não era permitido espiar os próprios cidadãos, assim, cada país faria a vigilância dos cidadãos dos outros e partilhavam entre si a informação. Segundo denúncias, promovia-se também a espionagem industrial. O Parlamento Europeu apresentou um relatório completo sobre o programa Echelon, feito por uma comissão especial liderada pelo português Carlos Coelho em 2001, mas entretanto com o 11 de Setembro o assunto ficou convenientemente esquecido. No REINO UNIDO o GCHQ (GOVERNMENT COMMUNICATIONS HEADQUARTERS) desenvolve o Programa Tempora. Em FRANÇA a DGSE (DIRECCION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE) tem e desenvolve o programa de vigilância Frenchelon. Na ALEMANHA o BUNDESNACHRICHTENDIENST (BND) está limitado pelo Tribunal Constitucional Alemão que proibiu a recolha de dados a não ser em situações muito circunstanciais. Na RÚSSIA o FEDERAL SECURITY SERVICE OF THE RUSSIAN FEDERATION (FSB) tem o SORM (System for Operative Investigative Activities). Na ÍNDIA opera o RESEARCH AND ANALYSIS WING com o CMS (Centralized Monitoring System) DRDO NETRA. Na CHINA existe o STATE COUNCIL INFORMATION OFFICE e o mesmo lança mão da designada Grande Firewall da China. Em ISRAEL a MOSSAD beneficia de leis muito liberais de vigilância que permitem o acesso quase irrestrito a informação pessoal dos cidadãos para investigações de rotina e não apenas para prevenção do terrorismo, mesmo sem mandado judicial. Finalmente, em PORTUGAL não há quadro legal que permita escutas ou recolha de emails e correspondência por qualquer serviço de informação.

previsão de antecipação que se lhe exigem e pelo **padrão de exemplaridade** que deverá ser sempre assumido por uma entidade pública.[42]

Não se pode comparar uma **administração transparente e aberta**[43] com uma **administração intrusiva ou descontrolada**, nem sequer se deve confundir um **dever geral de reserva** com normas de **segredo** ou de **sigilo** específicas que reforçam a contenção de informação e a tutelam de forma mais severa.[44]

Por outro lado, e como mero exemplo, nesta sede, agora já não em investigações de natureza criminal, mas em matéria de **publicitação de dados pelo regulador**, ou de acesso a dados[45] disponíveis, muitos problemas concretos se podem colocar.

Mas o mais importante no domínio do ICP-ANACOM será estabelecer **regras específicas para divulgação de informação e documentação relevante para o sector** e, ainda, **regras gerais para divulgação de nomes de entidades operadoras sujeitas a processos de investigação**.[46]

Só numa **visão extremada e fundamentalista** (Julian Assange, Wikileaks), consequentemente perigosa, porque **intrusiva e desrespeitadora dos direitos individuais e colectivos**[47], "*o Estado não é proprietário de nada, as informações pertencem a toda a gente. Por isso mesmo qualquer documento do Estado deve ser um documento público*".

---

[42] É que se "*os progressos técnico-científicos tornaram possíveis* ***novas e diversificadas formas de intromissão e devassa***" (Tribunal Constitucional Federal Alemão, 3 de Março de 2004), os especiais poderes destas entidades, não temperados pelo cumprimento escrupuloso dos deveres, potenciam os riscos de abuso ou de mau uso que podem ocasionar situações geradoras de ilegalidade, injustiça ou responsabilidade.

[43] O artigo 65º do Código de Procedimento Administrativo, sob a epígrafe de **Princípio da administração aberta**, estabelece que "*1 - Todas as pessoas têm o direito de acesso aos arquivos e registos administrativos, mesmo que não se encontre em curso qualquer procedimento que lhes diga directamente respeito, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas*" e que "*2 - O acesso aos arquivos e registos administrativos é regulado em diploma próprio*"

[44] São conceitos e realidades distintas que se entrecruzam mas que se não confundem: uma coisa é a **salvaguarda da privacidade ou da intimidade da vida privada e a protecção da confidencialidade**; outra bem distinta é a **fidedignidade, a sobriedade e a contenção ou comunicação da informação** numa qualquer organização; outra ainda bem diversa é a **transparência e a universalidade de certos dados** ou, até, a **obrigatoriedade de publicitação e divulgação de determinados actos e normativos**.

[45] A Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE estabelece, no seu artigo 4.º, sob a epígrafe de **Acesso aos dados estabelece** que "*Os Estados-Membros devem tomar medidas para assegurar que os dados conservados em conformidade com a presente directiva só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. Os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado-Membro no respectivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem.*"

[46] Até porque nestes domínios há um conjunto de conceitos indeterminados que é necessário concretizar, ou seja, há que definir em ***guidelines*** o que é, ou pode ser, a ***matéria sensível para as entidades em causa*** e o que é, ou deve ser, objecto de sigilo interno ou de segredo externo, até para que estas matérias não sejam casuisticamente tratadas com subjectividade e a sempre possível mas indesejável arbitrariedade.

[47] E, assim, [sublinhados nossos] *"hoje* ***a protecção da vida privada encontra, precisamente, a sua área mais sensível no âmbito das novas tecnologias****. A vida do lar e a imagem continuam a fazer parte do núcleo de protecção da privacidade, mas a estes domínios acrescem as comunicações (por correspondência – em papel ou electrónica – e por telefone ou orais), independentemente de o conteúdo transmitido dizer respeito à vida privada"* (Rita Castanheira Neves). Deixemos, porém, as manifestações dessa constatação prática para a discussão que se seguirá à intervenção.

Aceitar este entendimento libertário e fundamentalista, sem fronteiras nem limites, é confundir liberdade com irresponsabilidade, transparência com *voyeurismo*; é defender a anarquia e promover a devassa.[48]

Por isso, um dos primeiros temas da discussão propostos para esta acção de formação é o da **segurança da informação**, sobretudo neste novo mundo digital[49] e, dentro desse, o das **estratégias de gestão e divulgação de informação por parte de uma autoridade reguladora, de supervisão ou de controlo**.

Permitam-me, pois, em matéria de **transparência** e de **reserva** no seio de uma organização, partilhar uma **experiência de governação** e uma outra de **gestão e divulgação de informação reservada**, mais concretamente na **adopção de regras para publicitação de actas do órgão de gestão e decisão** e na **adopção de procedimentos específicos de notificação de informação e de decisão proferida em processos de levantamento de sigilo profissional**[50].

Dou aqui a conhecer duas simples **regras de procedimento** que introduzi na Ordem dos Advogados, mais precisamente no Conselho Distrital de Lisboa da Ordem dos Advogados, enquanto a ele presidi.

Até ao triénio 2008-2010, e durante mais de oitenta anos de vida institucional, as **actas** do Conselho Distrital de Lisboa[51] eram elaboradas em suporte de papel e, por regra, **não eram publicamente divulgadas**, embora pudesse pedir certidão da acta qualquer advogado ou até qualquer cidadão que nisso mostrasse interesse directo e legítimo, sendo que frequentemente se levantavam **questões de legitimidade** (interesse em agir), existente ou não; ou de comunicação de dados (informação reservada), que pudesse ou não ser acedida.

A primeira **regra de procedimento** que instituí foi a de que nas **actas** se colocavam sempre, e só, todas as informações que se pudessem divulgar devendo a discussão e decisão de casos concretos ser feita e transcrita de tal modo que **não havia possibilidade de identificação do assunto, do caso concreto ou das pessoas visadas**, mas tão só a análise da situação em termos

---

[48] A informação publicitada tem sérias consequências na vida das pessoas e das empresas. **Mesmo sendo verdadeira, nem toda a informação é, ou deve ser, pública. Há designadamente princípios de reserva e de cuidado a preservar.** Basta pensar na existência de um processo sancionatório em curso e no princípio da presunção da inocência para equacionar logo um conflito possível na possibilidade de precipitação na divulgação de matéria sensível.

[49] Até porque "à medida que a Internet assume cada vez maior importância a nível comercial, começam a surgir **novos tipos de litígios** relativos ao registo abusivo de nomes de domínios relativos à ciberocupação (*cybersquatting*), ao açambarcamento (*warehousing*) e à apropriação abusiva (*reverse hijacking*)". E porque "a **protecção das vítimas da cibercriminalidade** inclui também as **questões relativas à responsabilidade, às vias de recurso e a indeminizações** que ocorrem quando se verifica um crime informático. A confiança depende não apenas da utilização de uma tecnologia adequada, mas também da **existência de garantias jurídicas e económicas** que a acompanhem", pelo que "existe manifestamente uma necessidade de **adopção de instrumentos eficazes de direito material e processual aproximados**, senão a nível mundial, pelo menos a nível europeu, de maneira a proteger as vítimas da criminalidade informática e perseguir os autores dessas infracções. Paralelamente, **as comunicações pessoais, a vida privada e a protecção dos dados, o acesso à informação e a respectiva divulgação constituem direitos fundamentais das democracias modernas**" [sublinhados nossos] – cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

[50] Cfr. o **Regulamento de dispensa de segredo profissional** - Regulamento n.º 94/2006 do Conselho Geral da Ordem dos Advogados.

[51] Artigos 49.º e 50.º do **Estatuto da Ordem dos Advogados**.

genéricos e o sentido da decisão em abstracto, mas de modo a que comunicada aos interessados contivesse todos os elementos da decisão.[52]

Já em matéria de **dados reservados**, isto é, sujeitos a sigilo profissional, também no triénio de 2008-2010 ocorreu um insólito e inesperado caso de **revelação abusiva de matéria sujeita a segredo profissional** e para evitar ocorrências posteriores similares foi alterado o modo de divulgação de decisões proferidas pelo Presidente do Conselho Distrital de Lisboa[53] em matéria de processos de dispensa de sigilo profissional.[54]

O facto de haver **decisões** sobre a concessão, ou não, de **dispensa de sigilo** levanta logo o problema de saber se essas decisões finais podem ser, ou como podem ser, dadas a conhecer fora do âmbito dos obrigados ao segredo[55] – o advogado requerente, o Presidente do Conselho Distrital e os serviços da própria Ordem.

Não se esqueça que os pedidos de dispensa de sigilo surgem sobretudo no âmbito de processos-crime, cíveis, administrativos ou arbitrais em que o advogado é chamado a depor ou a entregar um determinado documento ou a libertar uma específica informação.

Foi para isso adoptada a **obrigatoriedade de notificação** não apenas da decisão e da fundamentação (mas esta só acessível ao advogado requerente porque contém a totalidade da informação reservada que nem sempre é libertada) mas também de um **extracto autónomo de decisão** destinado, este último, e só este último, a ser dado a conhecer (pois que tem apenas a parte da decisão que pode ser divulgada publicamente), com expressa menção de **proibição de divulgação da decisão total** e de **permissão de entrega a terceiros apenas do extracto de decisão parcial**.

Por aqui se vê que **é possível conciliar transparência com reserva e direitos individuais com deveres institucionais** e talvez por isso, no programa desta acção, se parta da aparente dicotomia entre, por um lado, **deveres e responsabilidades institucionais e funcionais do regulador** e, por outro, **direitos, liberdades e garantias dos cidadãos, dos consumidores e das entidades reguladas**.

Coube-me, nele, no programa deste evento, a responsabilidade de abordar o subtema **direitos empresariais e garantias individuais**, pelo que poderia abordá-lo numa perspectiva que afirme

---

[52] Era um exercício difícil, desde logo no que toca à **decisão de casos individuais** e a **declarações de voto**, mas mostrou-se possível em três anos de exercício de funções e em mais de três dezenas de actas do Conselho, actas essas que eram **obrigatoriamente publicitadas** e constavam na sua plenitude no ***site* do Conselho**, nunca mais tendo ocorrido qualquer episódio de litígio sobre a possibilidade de acesso à informação. Ver o conteúdo das actas em: http://www.oa.pt/cd/Conteudos/Artigos/lista_artigos.aspx?sidc=31634&idc=490&idsc=107291

[53] Artigo 51.º do **Estatuto da Ordem dos Advogados**.

[54] Quer não se dispense ou quer até se dispense, determinado advogado, do **sigilo profissional** que sobre ele impende há dados que não podem, nunca, ser revelados publicamente.

[55] Artigo 87.º do **Estatuto da Ordem dos Advogados**.

a **absoluta necessidade de regulação específica da internet**[56], mas circunscrevi-o ao **direito à privacidade ou à intimidade da vida privada**.[57]

Adicionalmente, abordarei também a temática da **protecção da fidedignidade dos dados e registos** e, sobretudo, da **liberdade ou não de acesso à informação**, bem como dos procedimentos necessários para o efeito; não sendo, pois, das patologias criminosas ou dos ilícitos administrativos que nos ocuparemos, mas sim dos **riscos** e da **prevenção** da invasão da vida privada, o que não admira, pois que, segundo Castells, "*a Internet nasceu na encruzilhada insólita entre a Ciência, a investigação militar e a cultura libertária*".[58]

E é aqui que queremos chegar: à importância das autoridades no controlo, na regulação, na supervisão e, sobretudo, no profissionalismo, no exemplo, na excelência da sua actuação, pois **não há melhor pedagogia que a do rigor próprio e a do cumprimento escrupuloso dos deveres** e, permitam-me que o realce também, **não há autoridade que prevaleça quando a mesma não respeita nem se faz respeitar**.

E o primeiro sinal de respeito é o da **escrupulosa salvaguarda dos direitos fundamentais, dos direitos, liberdades e garantias do cidadão**.[59]

Ora, o **direito à privacidade,** como direito de personalidade, teve consagração como direito fundamental na Declaração Universal dos Direitos do Homem (1948)[60] e na Convenção Europeia dos Direitos do Homem (1950)[61].

---

[56] Em programa recente de outra acção de formação (Maria Eduarda Azevedo) escreveu-se que, *como rede global que tornou possível a comunicação e a difusão de informação em tempo real e sem perda de qualidade entre terminais situados em qualquer parte do mundo, a Internet representou indiscutivelmente uma revolução tecnológica. E que, nos planos social e político, a rede das redes gerou novas oportunidades de negócio, de actividades criativas, de acesso a informação de múltipla e variada natureza, de participação e activismo*, não deixando, contudo, de se alertar para a *outra face da moeda* que é a sua *utilização para fins ilícitos, engendrando formas de criminalidade de difícil controlo e prova; para os* ***riscos acrescidos de invasão da vida privada, de reprodução ilícita de obras protegidas****, de difamação*, entre outros. [sublinhado nosso]

[57] O Acórdão do Tribunal da Relação de Lisboa proferido no processo 1317/07-9 em 22 de Fevereiro de 2007 estabeleceu que "*III- Na preservação do chamado 'direito à intimidade da vida privada', prevê a lei - artº 17º, n. 2, da Lei nº 91/97, e artº 5º da Lei nº 69/98, - que nesta área das telecomunicações, o dever de sigilo, conexo com o referido direito, possa ser invocado. Aliás, constitui crime, p.p. nos termos do artº 198º do Cód. Penal, a violação do dever de sigilo.*"

[58] Efectivamente (Paulo Fernandes, Director da Microsoft Portugal), *"… **a defesa cibernética** passou a ter um protagonismo sem paralelo na estratégia global da defesa dos Estados e um impacto altamente relevante na presença online das instituições públicas na* ***protecção dos dados confidenciais e privados que lhes foram confiados****".* [sublinhados nossos]

[59] Até porque (Rita Castanheira Neves) "*numa época em que o crime pode ser todo ele executado a quilómetros de distância ou mesmo virtualmente, a dificuldade, quer de prevenir, quer de reprimir, sente-se particularmente (...) as ameaças deixam de ser espácio- temporalmente delimitadas*", sendo que "*…esta verdadeira revolução tecnológica, ao mesmo tempo que criou facilidades inimagináveis na área da comunicação, potenciou também os* ***riscos de violação da privacidade****."* [sublinhado nosso]

[60] O artigo 12.º da *Declaração Universal dos Direitos do Homem* estabelece 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****."*

[61] O artigo 8.º da *Convenção Europeia dos Direitos do Homem* consagra o **Direito ao respeito pela vida privada e familiar** *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. 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.* E o artigo 17.º do *Pacto Internacional relativo aos Direitos civis e políticos* estipula que "*1. Ninguém será objecto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.2. Toda e qualquer pessoa tem direito à protecção da lei contra tais intervenções ou tais atentados*".

Também o Conselho da Europa (Convenção n.º 108 de 28 de Janeiro de 1981)[62], a União Europeia (Directiva 95/46/CE de 24 de Outubro de 1995 e Decisão-quadro do Conselho 2008/977/JAI – Espaço de Liberdade, Segurança e Justiça) e a Carta dos Direitos Fundamentais da União Europeia (artigo 8º) elegeram o **respeito da vida privada** e a **protecção dos dados pessoais** como objectivos de relevo a salvaguardar.[63]

Igual exigência se impõe nos regimes e na abordagem dos **sistemas de informação**, tais como as bases de dados nacionais de informações, policiais, biométricas, biográficas e de ADN, como o SIS I (1990) e o SIS II (2013) – bases de dados das polícias (PJ, PSP, GNR e SEF), ou o sistema integrado de informação criminal, e das autoridades alfandegárias, como o Eurodac (2000) – registos de impressões digitais de requerentes de asilo, ou como o VIS (2008) – Visa Information System.

Tem consagração constitucional na nossa Lei Fundamental (1976) a **reserva da intimidade da vida privada e familiar** (artigo 26, n.º 1) e a **protecção de dados pessoais** (artigo 35º, n.ºs 1, 2, 3, 4, 6 e 7), acontecendo que, no entanto, o texto da Constituição da República Portuguesa (CRP) "*não estabelece o conteúdo e o alcance do direito à reserva da intimidade, nem define o que deva entender-se por intimidade*…" (Acórdão n.º 278/95 do Tribunal Constitucional)[64], obrigando os particulares e as pessoas colectivas, mormente as pessoas colectivas públicas, a conformar as suas actividades com um conceito geral e abstracto que devem interpretar e aplicar devidamente, sobretudo actualizando-o face aos crescentes desafios das inovações tecnológicas

E, por falar em inovações tecnológicas, o art. 35.º da Constituição da República Portuguesa salvaguarda também, designadamente, o **direito à autodeterminação informacional**, protegendo e salvaguardando o direito fundamental do cidadão de aceder, de forma livre, imediata e célere, aos seus dados informatizados, sem esquecer a qualidade, fiabilidade e actualização dos mesmos.

Ou seja, o texto da Lei Fundamental reconhece, entre outros, o direito de exigir a **rectificação, actualização** de todos os seus dados informatizados, quaisquer que eles sejam; o direito ao **conhecimento da finalidade** que presidiu ao seu tratamento e o direito a que esses dados não venham a ser usados para quaisquer outras finalidades, sem esquecer também, e finalmente, o direito a ver removida a informação desactualizada ou cancelados e obliterados os dados errados ou caducos.

---

[62] A **Convenção para a Protecção das Pessoas relativamente ao Tratamento Autorizado de Dados de Carácter Pessoal** visa *"garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito ("protecção dos dados")."*

[63] Ou seja, entende-se que *"os sistemas de tratamento de dados, estão ao serviço do homem, devem respeitar as liberdades e os direitos fundamentais das pessoas singulares, independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso social e económico, o desenvolvimento do comércio e o bem-estar dos indivíduos".*

[64] Referem tão só os art.ºs 26.º e 34.º, n.º 4, ambos da CRP que "*a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação" e, precisamente por isso, que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal*". Tudo isto, porém, sem que se esqueçam os princípios consagrados no art.º 18.º, n.º 2, também da CRP, mas não só (necessidade, legitimidade, especificidade, lealdade, adequação, idoneidade, proporcionalidade, determinabilidade, consentimento, acesso e fiscalização).

Até no particular modo como se exercem todos estes direitos, em domínios completamente novos[65], estamos, todos, nos juízos decisórios, perante ponderações de interesses[66] e, nas preocupações organizacionais e de civilização, perante questões de **segurança colectiva e individual**.

Mesmo sem ter em conta abusos típicos nas operações de *data mining* ou nas investigações de *individual risk assessment*, **sector onde a quebra de privacidade ou a violação da intimidade da vida privada comporta um maior risco é precisamente o das bases de dados e o das comunicações e, dentro deste último, o das comunicações pela internet**.[67]

Daí que, no confronto dos direitos fundamentais, até das normas convencionais internacionais[68], sobrevenha a **necessidade de definir e hierarquizar as fronteiras e os conteúdos de dois interesses antagónicos**, precisamente o **respeito pela vida privada** e **fomento da livre circulação da informação**, para o que é necessário compreender as três esferas na defesa da privacidade, ou seja, a esfera pública, a esfera privada, a esfera íntima.

A questão é (Garcia Marques) "*como compatibilizar o direito do individuo ao exercício das suas liberdades e ao gozo da sua intimidade com a necessidade do corpo social em que está integrado – e das entidades de direito público ou de direito privado com as quais vai estabelecendo relações jurídicas ao longo do tempo – de recolher informações acerca de si, do seu passado e do seu presente?*"

E a resposta não pode deixar de ser a seguinte: **se o cidadão abdica de um seu direito fundamental**[69]**, a *res publica* não pode deixar de assumir um conjunto de deveres especiais**; e por isso que se venha exigindo uma tríplice preocupação que passa, primeiro, pela **maior**

---

[65] No Acórdão do Tribunal da Relação do Porto proferido no processo 311/08.7JFLSB.P2 decidiu-se que "*II - Servindo, como servem, os "blogues" para difusão e troca de informação com destino ao público em geral, as comunicações neles realizadas não podem ser tidas como comunicações eletrónicas, no sentido de que estão abrangidas pela proteção de dados pessoais e da privacidade, configurando, antes, os crimes neles cometidos, uma situação relativamente à qual inexiste justificação para estender a proteção devida à intimidade da vida privada.*"

[66] O Acórdão do Tribunal da Relação de Coimbra proferido no processo 111/10.4JALRA-A.C1 em 6 de Abril de 2011 decidiu que "*2. Considerando a danosidade social que implica o acesso a dados de conteúdo e de tráfego das telecomunicações, o legislador foi muito rigoroso no estabelecimento de um **catálogo de crimes em relação aos quais é admissível a obtenção de prova através de telecomunicações***" e que "*3. Se o crime que se investiga não faz parte desse catálogo, e não é punível com **pena de prisão superior, no seu máximo, a 3 anos** (art.187.º, n.º1, al. a) do C.P.P.), a solução é indeferir o meio de obtenção de prova.*" [sublinhados nossos]

[67] E desde há muito que se reconhece [sublinhado nosso] que "*a implementação de projectos relacionados com as **questões da segurança na utilização da internet** para a realização de negócios, é considerada fundamental para combater receios de fraude, incerteza quanto à entidade do receptor, quebra de privacidade, vírus, falta de apoio legal na resolução de eventuais litígios*" (Plano de acção para a Sociedade da Informação, aprovado pela Resolução do Conselho de Ministros n.º 107/2002, de 20 de Novembro).

[68] O artigo 10º, nº 1, da Convenção Europeia dos Direitos do Homem salvaguarda expressamente no seu parágrafo inicial que "*qualquer pessoa tem direito à liberdade de expressão*", mas acrescenta logo no seu nº 2 que "*o exercício desta liberdade...implica **deveres e responsabilidades**, pode ser submetido a certas **formalidades, condições, restrições ou sanções**, previstas pela lei, que constituam **providências necessárias**, numa sociedade democrática, para a **segurança nacional**, a **integridade territorial** ou a **segurança pública**, a **defesa da ordem** e a p**revenção do crime**, a **protecção da saúde ou da moral**, a **protecção da honra ou dos direitos** de outrem, para impedir a divulgação de informações confidenciais*...". [sublinhados nossos]

[69] Pode porém um cidadão ser obrigado a abdicar de um seu direito fundamental, o direito à privacidade e à intimidade da vida privada, na vertente do **anonimato**? É que "*por um lado, a possibilidade de permanecer anónimo é essencial para salvaguardar os direitos fundamentais à privacidade e à liberdade de expressão no ciberespaço. Por outro lado, a capacidade de participar e de comunicar em linha, sem revelar a respectiva identidade, contraria o espírito das iniciativas desenvolvidas actualmente no intuito de apoiar outros aspectos fundamentais tais como o combate ao conteúdo ilegal e lesivo, à fraude financeira ou às violações dos direitos de autor*" – cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

aproximação ou mesmo harmonização de regimes na União Europeia, depois, pelo **aumento das obrigações de compiladores, controladores, processadores e emissores de informação** e também, finalmente, pelo **reforço dos mecanismos de supervisão, de fiscalização institucional e de controlo jurisdicional**.

É que só assim se poderão salvaguardar devidamente os **princípios da finalidade, da transparência, da qualidade dos dados, da adequação, da pertinência, da exactidão e da proporcionalidade, na vertente da proibição do excesso**.

Sendo uma das traves mestras em que assenta o Estado de Direito Democrático a **liberdade de informação**, a Constituição da República Portuguesa a todos reconhece, desde a sua redacção inicial, o *direito de se informar* (artigo 37º, n.º 1) – que na versão actual, introduzida na primeira revisão, em 1982, se decompôs em *direito de informar,* em *direito de se informar* e em *direito de se ser informado* – sem especiais reservas, sem quaisquer impedimentos de monta ou discriminações não justificadas.

Por isso, a **necessidade de tutela na protecção da fidedignidade dos registos e de regulação da liberdade de acesso à documentação** – ou seja, aos documentos[70] e aos documentos administrativos[71] - tem vindo a assumir uma crescente relevância nas preocupações quer do legislador e decisor (inclusive a nível constitucional[72], comunitário[73] e internacional[74]) quer da **administração pública**, a que cada vez mais se exige **profissionalismo, rigor, firmeza, abertura, transparência e sentido de missão ao serviço da comunidade**, quer dos cidadãos que, individualmente ou congregados em sociedades, associações e similares, vão tomando consciência dos seus **direitos de cidadania**.

Como direito fundamental, o **princípio do arquivo aberto**, isto é, o livre e geral acesso aos documentos administrativos pelo cidadão comum[75], independentemente da invocação (ou até da existência) de um interesse directo e pessoal, só foi consagrado na Revisão Constitucional de 1989, com o aditamento do parágrafo 2º ao artigo 268º, do teor seguinte: "*os cidadãos têm também o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto*

---

[70] ***Documentos*** são *quaisquer suportes de informação gráficos, sonoros, visuais, informáticos ou registos de outra natureza*, como *processos, relatórios, estudos, pareceres, actas, autos, circulares, ordens de serviço, despachos, instruções, orientações*, etc.

[71] ***Documentos administrativos*** são os *detidos por órgãos do Estado e das Regiões Autónomas que exerçam funções administrativas,* por *órgãos dos institutos públicos e das associações públicas, por órgãos das autarquias locais e das suas associações e federações,* por *outras entidades no exercício de poderes de autoridade, nos termos da lei.*

[72] A Lei Fundamental proclama, desde 1976, que "**os cidadãos têm o direito de ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam directamente interessados, bem como o de conhecer as resoluções definitivas que sobre eles forem tomadas**" (n.º 1 do actual artigo 268.º, que sucedeu em 1982, sem alteração do texto, ao n.º 1 do artigo 269.º da versão originária).

[73] V. Regulamento (CE) n.° 1049/2001; Livro Verde da Comissão, de 18 de Abril de 2007, intitulado «Acesso do público aos documentos na posse das instituições da Comunidade Europeia - Análise da situação» disponível em http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=pt&type_doc=COMfinal&an_doc=2007&nu_doc=185; e cfr., ainda, o teor da Proposta de Regulamento do Parlamento Europeu e do Conselho, de 30 de Abril de 2008, relativa ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão [COM(2008) 229 final – ao que saiba então não publicada no Jornal Oficial] mas disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008PC0229:PT:NOT

[74] O artigo 19.º da Declaração Universal dos Direitos do Homem estatui que "***todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão***".

[75] O n.º 1 do artigo 65º do CPA reproduz o conteúdo do n.º 2 do artigo 268º da CRP ao estabelecer que "*todas as pessoas têm o* ***direito de acesso aos arquivos e registos administrativos****, mesmo que não se encontre em curso qualquer procedimento que lhes diga directamente respeito, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas*".

na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas".

A densificação e regulamentação deste dispositivo foi obra da **Lei do Acesso aos Documentos Administrativos** (LADA)[76], tanto que nesta se estabeleceu que "*o acesso aos documentos administrativos é assegurado pela Administração pública de acordo com os princípios da publicidade, da transparência, da igualdade e da imparcialidade*" e que "*todos têm direito à informação mediante o acesso a documentos administrativos de carácter não nominativo*"[77], sendo que o acesso aos documentos referentes a **dados pessoais com tratamento automatizado** rege-se por legislação própria, que é actualmente a Lei n.º 67/98, de 26 de Outubro (Lei da Protecção de Dados Pessoais)[78].

Não se limita a lei a impor à Administração o dever de satisfazer pedidos de **acesso documental**, pois manda publicar, ao menos semestralmente, os documentos que comportem enquadramento da actividade administrativa, tais como despachos normativos internos e circulares, e o sumário (designadamente o seu título, matéria, data, origem e local onde se encontram acessíveis para consulta) de todos os que visem interpretar normas jurídicas ou descrever procedimentos administrativos.

Porém, o **princípio do livre acesso** aos documentos administrativos admite **excepções**, que o n.º 2 do artigo 268º da CRP arruma em três categorias: matérias relativas à **segurança interna e externa**[79]; matérias relativas à **investigação criminal**[80]; e matérias relativas à **intimidade das pessoas**[81].

Às três mencionadas categorias de **excepções** que o n.º 2 do artigo 268º da CRP expressamente ressalvou da regra do livre acesso aos documentos administrativos a LADA acrescentou outras, que passaremos a indicar.

O n.º 2 do artigo 10º da LADA (que já vem da primitiva redacção do diploma, embora então ocupasse o n.º 1 desse artigo) dispõe ser "*vedada a utilização de informações com desrespeito dos direitos de autor e dos direitos de propriedade industrial, assim como a reprodução, difusão e utilização destes documentos e respectivas informações que possam configurar práticas de concorrência desleal.*"

---

[76] Lei n.º 65/93, de 26 de Agosto, alterada pela Lei n.º 8/95, de 29 de Março, e pela Lei n.º 94/99, de 16 de Julho.

[77] O direito em análise compreende, além de informação sobre a existência e o conteúdo do documento, o seu acesso por via de consulta, que é gratuita, ou de reprodução, seja por certidão, seja por fotocópia ou por outros meios técnicos, incluindo os audiovisuais.

[78] Artigos 11.º a 15.º e 17.º.

[79] Que compreendem "os documentos que contenham informações cujo conhecimento seja avaliado como podendo pôr em risco ou causar dano à **segurança interna e externa do Estado** ficam sujeitos a interdição de acesso ou a acesso sob autorização, durante o tempo estritamente necessário, através de classificação nos termos de legislação específica". Esta legislação específica é, nuclearmente, a Lei n.º 6/94, de 7 de Abril (**Lei do Segredo de Estado**); mas nela se podem ainda incluir os diplomas relativos ao Sistema de Informações da República Portuguesa (entre outros, a Lei n.º 30/84, de 5 de Setembro, alterada pela Leis n.ºs 4/95, de 21 de Fevereiro, 15/96, de 30 de Abril, e 75-A/97, de 22 de Julho, e pela Lei Orgânica n.º 4/2004, de 6 de Novembro; o Decreto-Lei n.º 225/85, de 4 de Julho, alterado pelo Decreto-Lei n.º 369/91, de 7 de Outubro, e pelo Decreto-Lei n.º 245/95, de 14 de Setembro; e o Decreto-Lei n.º 254/95, de 30 de Setembro), a Lei n.º 20/87, de 12 de Junho (**Lei de Segurança Interna**), e a Resolução do Conselho de Ministros n.º 50/88, publicada no DR, n.º 279, I série, de 3 de Dezembro de1998.

[80] O artigo 6º da LADA estabelece que o acesso a documentos referentes a matérias em **segredo de justiça** é regulado por legislação própria – cfr. o disposto no artigo 86º do Código de Processo Penal.

[81] São **documentos nominativos** os que contenham dados pessoais, ou seja, informações sobre pessoa singular, identificada ou identificável, que versem sobre juízos apreciativos ou valorativos, ou que sejam abrangidas pela reserva da intimidade da vida privada.

E, segundo o n.º 1 do mesmo artigo 10º, aditado pela citada Lei n.º 8/95, "*a Administração pode recusar o acesso a documentos cuja comunicação ponha em causa segredos comerciais, industriais ou sobre a vida interna das empresas"*.

Trata-se de **restrições ou compressões do direito de acesso aos documentos administrativos** impostas pela necessidade de o conciliar com os direitos, também com assento constitucional, de propriedade (intelectual, comercial, industrial), de iniciativa económica (individual e empresarial) e de concorrência leal - cfr. artigos 42º[82], 61º[83], 62º[84], 78º[85], 80º, alínea c)[86], 81º, alínea e)[87], 82º, n.ºs 3 e 4[88], e 86º[89] da CRP.

Assim, para além das restrições decorrentes do **direito de autor**, contemplam-se aqui limitações justificadas pela **protecção da propriedade industrial, de segredos comerciais e industriais, de dados confidenciais sobre a vida interna das pessoas colectivas**.

---

[82] A Constituição da República Portuguesa, estatui na Parte I, Título II, Capítulo I, artigo 42.º, sob a epígrafe **Liberdade de criação cultural,** que *"1 - É livre a criação intelectual, artística e científica. 2 - Esta liberdade compreende o direito à invenção, produção e divulgação da obra científica, literária ou artística, incluindo a* ***protecção legal dos direitos de autor****."* [sublinhado nosso]

[83] A Constituição da República Portuguesa, estatui na Parte I, Título III, Capítulo I, artigo 61.º, sob a epígrafe **Iniciativa privada, cooperativa e autogestionária,** que *"1 - A iniciativa económica privada exerce-se livremente nos quadros definidos pela Constituição e pela lei e tendo em conta o interesse geral. 2 - A todos é reconhecido o direito à livre constituição de cooperativas, desde que observados os princípios cooperativos. 3 - As cooperativas desenvolvem livremente as suas actividades no quadro da lei e podem agrupar-se em uniões, federações e confederações e em outras formas de organização legalmente previstas. 4 - A lei estabelece as especificidades organizativas das cooperativas com participação pública. 5 - É reconhecido o direito de autogestão, nos termos da lei."*

[84] A Constituição da República Portuguesa, estatui na Parte I, Título III, Capítulo I, artigo 62.º, sob a epígrafe **Direito de propriedade privada**, que *"1 - A todos é* ***garantido o direito à propriedade privada*** *e à sua transmissão em vida ou por morte, nos termos da Constituição. 2 - A requisição e a expropriação por utilidade pública só podem ser efectuadas com base na lei e mediante o pagamento de justa indemnização."* [sublinhado nosso]

[85] A Constituição da República Portuguesa, estatui na Parte I, Título II, Capítulo III, artigo 78.º, sob a epígrafe **Fruição e criação cultural**, *que "1 - Todos têm* ***direito à fruição e criação cultural****, bem como o dever de preservar, defender e valorizar o património cultural. 2 - Incumbe ao Estado, em colaboração com todos os agentes culturais: a) Incentivar e assegurar o acesso de todos os cidadãos aos meios e instrumentos de acção cultural, bem como corrigir as assimetrias existentes no país em tal domínio; b) Apoiar as iniciativas que estimulem a criação individual e colectiva, nas suas múltiplas formas e expressões, e uma maior circulação das obras e dos bens culturais de qualidade; c) Promover a salvaguarda e a valorização do património cultural, tornando-o elemento vivificador da identidade cultural comum; d) Desenvolver as relações culturais com todos os povos, especialmente os de língua portuguesa, e assegurar a defesa e a promoção da cultura portuguesa no estrangeiro; e) Articular a política cultural e as demais políticas sectoriais."* [sublinhado nosso]

[86] A Constituição da República Portuguesa, estatui na Parte II, Título I, artigo 80.º, alínea c), sob a epígrafe **Princípios fundamentais**, que *"A organização económico-social assenta nos seguintes princípios: c)* ***Liberdade de iniciativa e de organização empresarial*** *no âmbito de uma economia mista."* [sublinhado nosso]

[87] A Constituição da República Portuguesa, estatui na Parte II, Título I, artigo 81.º, alínea e), sob a epígrafe **Incumbências prioritárias do Estado,** que *"Incumbe prioritariamente ao Estado no âmbito económico e social: e) Promover a correcção das desigualdades derivadas da insularidade das regiões autónomas e incentivar a sua progressiva integração em espaços económicos mais vastos, no âmbito nacional ou internacional."*

[88] A Constituição da República Portuguesa, estatui na Parte II, Título I, artigo 82.º, n.ºs 3 e 4, sob a epígrafe **Sectores de propriedades dos meios de produção,** que *"3 - O sector privado é constituído pelos meios de produção cuja propriedade ou gestão pertence a pessoas singulares ou colectivas privadas, sem prejuízo do disposto no número seguinte. 4 - O sector cooperativo e social compreende especificamente: a) Os meios de produção possuídos e geridos por cooperativas, em obediência aos princípios cooperativos, sem prejuízo das especificidades estabelecidas na lei para as cooperativas com participação pública, justificadas pela sua especial natureza; b) Os meios de produção comunitários, possuídos e geridos por comunidades locais; c) Os meios de produção objecto de exploração colectiva por trabalhadores; d) Os meios de produção possuídos e geridos por pessoas colectivas, sem carácter lucrativo, que tenham como principal objectivo a solidariedade social, designadamente entidades de natureza mutualista."*

[89] A Constituição da República Portuguesa, estatui na Parte II, Título I, artigo 86.º, sob a epígrafe **Empresas privadas,** que *"1 - O Estado incentiva a actividade empresarial, em particular das pequenas e médias empresas, e fiscaliza o cumprimento das respectivas obrigações legais, em especial por parte das empresas que prossigam actividades de interesse económico geral. 2 - O Estado só pode intervir na gestão de empresas privadas a título transitório, nos casos expressamente previstos na lei e, em regra, mediante prévia decisão judicial. 3 - A lei pode definir sectores básicos nos quais seja vedada a actividade às empresas privadas e a outras entidades da mesma natureza."*

Tudo com o objectivo de prevenir a violação dos princípios da sã concorrência, proteger a confidencialidade dos negócios privados e evitar a difusão de informações prejudiciais aos interesses comerciais e ao crédito ou, até, à reputação económica das empresas[90].

A lei impede assim que, através do **abuso do direito de acesso** aos documentos administrativos ou da **abusiva divulgação de informação**, alguém aproveite para conhecer ou difundir segredos de uma sociedade, eventualmente até sua concorrente (e, em prejuízo desta, tirar daí proveitos ilícitos), designadamente no domínio das estratégias ou operações comerciais ou de marketing, dados estatísticos confidenciais como os relativos a penetração no terreno, na clientela ou no mercado, processos técnicos de fabrico (know-how), inovações tecnológicas, ficheiros de clientes, de fornecedores, dados relativos a pesquisas e trabalhos de investigação e modelos ou patentes, etc.

A análise cuidada de todos estes temas, a discussão do que *é* e *deve ser* e a resposta a todas estas questões que se deixam elencadas mas não completamente respondidas, a fim de poder ser útil o diálogo nesta sessão de formação, também parte da **boa compreensão e interpretação das regras do sector**.

São **objectivos a prosseguir pelo ICP-ANACOM** a liberalização progressiva do sector das comunicações, especificamente das telecomunicações, o desenvolvimento de um mercado complexo e crescentemente concorrencial[91].

E nestes objectivos terão que se integrar também finalidades específicas, não menos relevantes, quer no que toca à **protecção dos direitos de cidadania e dos interesses dos consumidores**[92], quer ainda no incremento de um elevado nível de protecção dos dados pessoais e de privacidade, razão por que também estes objectivos constituem especial responsabilidade do regulador.[93]

Daí que seja de promover internamente a **formação específica** e a **investigação científica**, quer no âmbito da divulgação do quadro regulatório e dos direitos e obrigações das operadoras e dos consumidores de comunicações, quer na prestação de informações claras, quer ainda na regulação e nas áreas sancionatórias que devem ser caracterizadas pela **independência na acção e imparcialidade da decisão**. [94]

---

[90] O Acórdão do Tribunal Central Administrativo Sul proferido no processo 01877/06 em 26 de Outubro de 2006 estabeleceu que "*I - O **segredo comercial** visa impedir que sejam aproveitadas informações confidenciais, violando as regras da livre concorrência entre as empresas (art. 10º nº 1 da LADA* ", que "*II - Tais informações podem referir-se a técnicas de fabrico, patentes, informações e estratégias comerciais e de captação de clientes, cujo conhecimento por parte de concorrentes seria susceptível de afectar determinada empresa." E que* "*III - Deste modo, a Administração pode restringir o acesso a tal tipo de elementos, sem que com isso seja posto em causa o direito à informação constitucionalmente consagrado*." [sublinhado nosso]

[91] Ora tudo isto só é exequível procurando uma **real e efectiva igualdade de oportunidade dos operadores**, minimizando tanto quanto possível as barreiras à entrada ou à informação e promovendo o uso de tecnologias intensivas e a inovação permanente, a forte especialização técnica e a divulgação dos conhecimentos e das experiências acumuladas.

[92] Os principais problemas abordados nas legislações e regulamentações vigentes em relação ao domínio específico da criminalidade informática, tanto a nível da União Europeia como dos Estados-Membros, são os seguintes: **violações da vida privada; infracções ligadas aos conteúdos e violações da propriedade intelectual**. É preciso, pois, ver em concreto o que cada regulador deve prevenir ou reprimir nestes domínios.

[93] A criação de uma **cultura de exigência interna** e de **promoção de uma matriz humanista** que não prescinda da **qualidade técnica** e do **rigor procedimental** não podem estar arredadas da construção de uma convergência inteligente e harmoniosa das comunicações, dos meios de comunicação social e das tecnologias de informação que, sendo **instrumento**, devem estar ao serviço da comunidade e não ser obstáculo à liberdade económica ou ofensa de direitos individuais e colectivos.

[94] Para isso aqui fica um **desafio** para que o ICP-ANACOM realize, em breve, um **Encontro Nacional de Autoridades** para a discussão destas temáticas a nível nacional e transversal de modo a gerar um diálogo entre várias

O ICP-ANACOM como **Autoridade Reguladora Nacional** (ARN), inserida que está no Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE), tem como missão ser **entidade e autoridade de controlo, de regulação**[95] **e de supervisão** (prudencial[96] e comportamental[97]) com **funções de gestão, de arbitragem e de representação ao nível do sector das comunicações**.[98]

Em todas estas actividades, de modo geral, e em especial no exercício das funções de regulação, de controlo, de supervisão prudencial e comportamental, a entidade reguladora ou a autoridade de supervisão – o ICP-ANACOM – está sempre sujeita aos **princípios da legalidade, da necessidade, da subsidiariedade, da proporcionalidade, da imparcialidade, da clareza, da participação e da publicidade**, quando esta última não esteja afastada no caso concreto[99].

Questão que se pode colocar, quer no que toca a **recomendações concretas ou providências de reparação**, quer no que toca a **procedimentos sancionatórios ou decisões** neste proferidas, preparatórias, mas ainda não definitivas[100], é a de saber se é possível, como e quando, a divulgação da identidade das operadoras sujeitas a processo de investigação, ou a divulgação da matéria a investigar, assim como a divulgação das informações obtidas ou das decisões individuais ou sancionatórias interlocutórias entretanto adoptadas.

Convoca-se aqui a **necessidade da ponderação de interesses face aos especiais deveres de informação e prevenção, às necessidades de justiça e eficácia, face ao dever de reserva ou de sigilo, de respeito pelo princípio da presunção de inocência e de salvaguarda do bom-nome ou reputação do regulado**. Serão critérios de estrita **legalidade** ou, antes, juízos de **oportunidade** os critérios de resolução deste confronto aparentemente impossível de ultrapassar? Serão certamente **critérios jurídicos** e que determinarão, ou não, a legalidade, regularidade e bondade do acto, e que poderão, ou não, originar a responsabilidade da entidade e/ou dos seus autores.

---

sensibilidades, partindo de diferentes visões e missões e visando uma troca de experiências para estabelecimento de regras e boas-práticas em todos os sectores de actividade.

[95] Nessa medida, e em primeira linha, cumpre-lhe elaborar **regulamentos obrigatórios gerais**, **normas de eficácia externa**, **instruções para categorias de operadores e para categorias de prestadores de serviços**, mantendo a integridade e a segurança das redes de comunicação públicas e salvaguardando o regular funcionamento do mercado das comunicações.

[96] Depois, e em segunda linha, exerce **poderes de conformação da actividade dos operadores e prestadores de serviços** emitindo e impondo actos vinculativos individuais ou recomendações concretas, estas já no âmbito da fiscalização do cumprimento das normas legais e regulamentares, podendo ainda determinar providências necessárias à reparação das justas queixas dos utentes.

[97] Finalmente, como corolário da **fiscalização do cumprimento das normas legais e regulamentares**, bem assim como do dever de vigiar a actividade das entidades, para além de receber e registar queixas e reclamações, esta autoridade reguladora tem também como atribuição **instaurar, instruir e punir no âmbito dos processos sancionatórios**.

[98] Seria por isso também útil, e aqui fica mais um **desafio**, o de que pudesse ser iniciado, porventura até por iniciativa do próprio ICP – ANACOM, um THINK TANK a nível nacional e internacional para a **discussão alargada das temáticas de segurança da informação, da privacidade e do acesso a dados**.

[99] Já no seu múnus sancionatório está o ICP-ANACOM, por imposição constitucional, também obrigada a respeitar os **princípios da audiência e da defesa**, na sua vertente de audiência do interessado e de participação da decisão, de respeito pelo contraditório e pelos princípios do Código de Procedimento Administrativo, e, quando for caso disso, do Regime Geral das Contra-Ordenações.

[100] Isto é, o ICP-ANACOM tem a competência para iniciar, instruir e decidir todos os **procedimentos por contra-ordenações no sector das comunicações**. Por isso tem, para além **de funções de fiscalização e de investigação**, prerrogativas de **agentes de autoridade**, tanto que desde logo, pode proceder à **identificação** de pessoas que infrinjam normas legais ou regulamentares, pode realizar **averiguações e exames** com acesso livre a instalações, equipamentos e serviços das entidades sujeitas a inspecção e controlo, ou pode ainda formular a **requisição de documentação para análise, bem como de equipamentos e materiais** para a realização de testes.

Em suma, no âmbito do exercício concreto da sua **actividade** os titulares dos órgãos do ICP-ANACOM e os seus trabalhadores e agentes podem vir a ter que responder civil, criminal, disciplinar e financeiramente[101] pelos **actos e omissões** que pratiquem no exercício das suas funções, tudo nos termos da Constituição da República Portuguesa e da demais legislação e regulamentação aplicável, estando todos os seus actos, designadamente os lesivos de direitos, sujeitos a controlo judicial[102], que se exerce em diferentes tribunais consoante a matéria[103].

Não é, pois, demais pedir, exigir mesmo, rigor e prudência na conduta[104], bem como insistir na prioridade à prevenção[105], o que só se obtém apostando na qualidade e na excelência das pessoas, de cada pessoa, até para defesa própria e protecção da instituição, mas também da liberdade, da segurança, da legalidade e da cidadania.

[101] Com efeito, o artigo 52.º do Decreto-Lei nº 309/2001, de 7 de Dezembro, sob a epígrafe de ***Responsabilidade jurídica***, estabelece que "***os titulares dos órgãos do ICP – ANACOM e os seus trabalhadores e agentes respondem civil, criminal, disciplinar e financeiramente pelos actos e omissões que pratiquem no exercício das suas funções, nos termos da Constituição e demais legislação aplicável***".

[102] Os números 1 a 3 do artigo 53.º do Decreto-Lei nº 309/2001, de 7 de Dezembro, sob a epígrafe de *Controlo judicial*, estatuem que "*a actividade dos órgãos e agentes do ICP – ANACOM de natureza administrativa fica sujeita à jurisdição administrativa, nos termos da respectiva legislação*", que "*as sanções por infracções contra-ordenacionais são impugnáveis nos termos gerais, junto dos tribunais judiciais*" e que "*das decisões proferidas no âmbito da resolução de litígios cabe recurso para os tribunais judiciais ou arbitrais, nos termos previstos na lei*".

[103] Exemplificando, na **sindicância da actividade de natureza administrativa da entidade** tem competência a jurisdição administrativa, no eventual **julgamento da aplicação de coimas ou de sanções acessórias** aos regulados tem competência o Tribunal da Regulação e da Concorrência, no a**puramento da responsabilidade civil ou na resolução de litígios** tê-la-ão os tribunais judiciais ou os tribunais arbitrais e na **fiscalização de determinados actos e contratos públicos** tem-na o Tribunal de Contas.

[104] Ainda continua a ser essencial "...**aumentar a consciencialização pública para os riscos da criminalidade na Internet**, **promover as melhores práticas em matéria de segurança**, **definir instrumentos e procedimentos eficazes a fim de lutar contra a criminalidade informática**, bem como **incentivar a adopção de medidas tendo em vista mecanismos de alerta e de gestão das crises**" – cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

[105] Mas não basta formar pessoas e ter os melhores quadros; é necessário fazer um esforço continuado de investimento em recursos tecnológicos e de educação permanente, só possível com a formação contínua e uma cultura de responsabilidade e excelência. "De maneira a prevenir a criminalidade informática e a lutar eficazmente contra este fenómeno, é necessário a existência prévia de algumas condições [sublinhados nossos]: **disponibilidade de tecnologias em matéria de prevenção**; **sensibilização para os riscos potenciais associados à segurança e aos meios de os combater**; **disposições legislativas adequadas em matéria de direito material e processual**, no que diz respeito às actividades criminosas tanto nacionais como transaccionais; **disponibilização de pessoal dos serviços responsáveis pela aplicação da Lei, em número suficiente, com boa formação e correctamente equipado**; **reforço da cooperação** entre todos os intervenientes interessados: utilizadores e consumidores, empresas, serviços responsáveis pela aplicação da lei e autoridades responsáveis pela protecção de dados; **acções permanentes das empresas e do meio associativo**; **investigação e desenvolvimento** [etc.]" – cfr. o teor da Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

Bibliografia sumária

Costa, José de Faria.

Direito Penal e Globalização – reflexões não locais e pouco globais, Coimbra, Wolters Kluwer/Coimbra Editora, 2010.

Gonçalves, Pedro.

Direito das Telecomunicações, Coimbra, 1999.

"Criminalidade Informática – nova lei facilita investigação"; Boletim da Ordem dos Advogados, n.º 65, Abril 2010, p. 30-35.

Martins, Agostinho de Castro

Acesso aos documentos administrativos, edição de autor, 2005

Martins, A.G. Lourenço, Marques, J.A. Garcia, Dias, Pedro Simões.

Ciberlaw em Portugal – O direito das tecnologias da informação e comunicação, Lisboa, 2004.

Mesquita, Paulo Dá.

Prolegómeno sobre prova electrónica e intercepção de telecomunicações no direito processual penal português – o Código e a Lei do Cibercrime, in Processo Penal, Prova e Sistema Judiciário, Coimbra, Coimbra Editora, 2010, pp. 83-129,.

Neves, Rita Castanheira.

As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e Respectivo Regime Jurídico do Correio Electrónico enquanto Meio de Obtenção de Prova, Coimbra, Wolters Kluwer/Coimbra Editora, 2011.

Ramos, Vânia Costa.

Âmbito e extensão do segredo das telecomunicações: Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, de 2 de Março de 2006, *in* RMP 112/2007, pp. 141-162, 2007.

Santos, Cristina Máximo dos

As novas tecnologias da informação e o sigilo das comunicações, *in* RMP 99/2004, Lisboa, p. 89-116.

Venâncio, Pedro Dias

Lei do Cibercrime Anotada e Comentada, Coimbra, Wolters Kluwer/Coimbra Editora, 2011.

Verdelho, Pedro

"Apreensão de correio electrónico em processo penal", separata da RMP 100/2004, Lisboa, Editorial Minerva, 2004 pp. 153-164.

"Cibercrime e segurança informática", Polícia e Justiça, série 3, n.º 6, Julho-Dez. 2005, Coimbra Editora, 2005, pp.159 a 175.

"A obtenção de prova no ambiente digital", separata da RMP 99/2004, Lisboa, Editorial Minerva, 2004 pp. 117-136.

"A nova Lei do Cibercime", Separata da *Scientia Iuridica*, Outubro-Dezembro 2009, Tomo LVIII – 320, 2009

Tratado de Direito Administrativo Especial, volume V, Almedina, com coordenação de **Paulo Otero** e **Pedro Gonçalves**

- *Direito Administrativo das Telecomunicações* – **Nuno Peres Alves**, pp. 283 a 424

Sub judice – Internet, Direito e Tribunais, nº 35, Almedina, Setembro de 2006

- *Protecção de Dados Pessoais na Internet* – **Catarina Sarmento e Castro**, pp. 11 a 29

Revista de Direito da Sociedade da Informação:

- Direito da Sociedade da Informação – Vol. I, Coimbra Editora, 1999:
  - *Protecção de dados pessoais e direito à privacidade* - **Pedro Pais de Vasconcelos**, pp. 241 a 253.
  - *Tutela jurídica das bases de dados (A transposição da Directriz 96/9/CE)* **- Alberto de Sá e Mello**, pp. 111 a 161.

- Direito da Sociedade da Informação – Vol. II, Coimbra Editora, 2001:
  - *Criminalidade informática* – **José de Oliveira Ascensão**, pp. 203 a 228.
  - *Os multimédia, regime jurídico* – **Alberto de Sá e Mello**, pp.79 a 111.

- Direito da Sociedade da Informação – Vol. III, Coimbra Editora, 2002:
  - *Informação sobre direitos* – **Luiz Francisco Rebello**, pp. 193 a 210.
  - *Instrumentos de busca, direitos exclusivos e concorrência desleal* – **Alexandre Dias Pereira**, pp. 221 a 241.
  - *Bases de dados de órgãos públicos: o problema do acesso e exploração da informação do sector público na Sociedade da Informação* – **Alexandre Dias Pereira**, pp. 243 a 294.
  - *Os consumidores e a sociedade da informação* – **Luís Silveira Rodrigues**, pp. 295 a 312.

- Direito da Sociedade da Informação – Vol. IV, Coimbra Editora, 2003:
  - *Criminalidade informática* – **A. G. Lourenço Martins**, pp. 9 a 41.
  - *Cibercrime* **– Pedro Verdelho**, pp. 347 a 383.
  - *Publicidade ilícita e abusiva na internet* – **Celso António Serra**, pp. 455 a 573.
  - *Comércio electrónico e responsabilidade empresarial* – **Dário Moura Vicente**, pp. 241 a 288.

- Direito da Sociedade da Informação – Vol. V, Coimbra Editora, 2004:
  - *Internet e privacidade* – **José Augusto Sacadura Garcia Marques**, pp. 23 a 64.
  - *Tutela do consumidor na internet* – **Elsa Dias Oliveira**, pp. 335 a 358.

- Direito da Sociedade da Informação – Vol. VI, Coimbra Editora, 2006:
  - *A convenção sobre cibercrime do Conselho da Europa: repercussões na lei portuguesa* **– Pedro Verdelho**, pp. 257 a 276.
  - *A transposição para a ordem jurídica portuguesa da directiva sobre o Direito de Autor na sociedade da informação* – **Nuno Gonçalves**, pp. 249 a 256.
  - *Concorrência desleal na internet* – **Adelaide Menezes Leitão**, pp. 355 a 372.

- Direito da Sociedade da Informação – Vol. VII, Coimbra Editora, 2008:
  - *Sociedade da Informação e liberdade de expressão* – **José de Oliveira Ascensão**, pp. 51 a 81.
  - *Privacidade e protecção de dados pessoais em rede* – **Catarina Sarmento e Castro**, pp. 91 a 106.

PowerPoints vários de Seminários e /ou Intervenções

- *Políticas de segurança e protecção de dados pessoais na União Europeia* (23 de maio de 2012) - **Maria Eduarda Gonçalves** e **Inês Andrade Jesus**
- *A protecção da vida privada e dos dados pessoais na internet* (17 de maio de 2012) – Faculdade de Direito da Universidade de Lisboa
- *A Internet e o sistema de justiça – a questão da prova digital* – **Maria Eduarda Gonçalves**
- *A questão da regulação da internet*