

compilações doutrinais

VERBOJURIDICO

MONITORIZAÇÃO DA INTERNET

ONDE FICA O DIREITO À PRIVACIDADE

DR. HUGO LANÇA SILVA
MESTRE EM DIREITO E DOCENTE



verbojuridico[®]

SETEMBRO 2006

Título: Monitorização da Internet – Onde fica o direito à privacidade ?

Autor: Dr. Hugo Lança Silva
Mestre em Direito pela Universidade Católica de Lisboa
Licenciado em Direito pela Universidade Moderna de Lisboa
Docente no ESTIG/IPB e Universidade Moderna de Beja

Data de Publicação: Setembro de 2006.

Classificação: Direito...

Edição: Verbo Jurídico © - www.verbojuridico.pt | .eu | .net | .org | .com.

Nota Legal: Respeite os direitos de autor. É permitida a reprodução exclusivamente para fins pessoais ou académicos. É proibida a reprodução ou difusão com efeitos comerciais, assim como a eliminação da formatação, das referências à autoria e publicação. Exceptua-se a transcrição de curtas passagens, desde que mencionado o título da obra, o nome do autor e da referência de publicação.



Ficheiro formatado para ser amigo do ambiente. Se precisar de imprimir este documento, sugerimos que o efective frente e verso, assim reduzindo a metade o número de folhas, com benefício para o ambiente. Imprima em primeiro as páginas pares invertendo a ordem de impressão (do fim para o princípio). Após, insira novamente as folhas impressas na impressora e imprima as páginas ímpares pela ordem normal (princípio para o fim).

MONITORIZAÇÃO DA INTERNET

Onde fica o direito à privacidade

WORKING PAPER ¹

Por Dr. Hugo Lança Silva

Mestre em Direito pela Universidade Católica de Lisboa
Licenciado em Direito pela Universidade Moderna de Lisboa
Docente no ESTIG/IPB e Universidade Moderna de Beja

1. Introdução 2. O problema 3. Definição de dados pessoais 4. Análise legislativa 5. Conclusões

Resumo:

O que procuramos com esta pequena apresentação é contribuir para uma discussão, que urge fazer-se sobre o direito à privacidade na utilização da Internet, contribuindo como uma argumentação crítica. Desde logo, que fique claro; não oferecemos respostas, apenas dúvidas; falta-nos tempo, inteligência e conhecimento para oferecer mais do que propostas sobre a forma de compatibilizar a necessidade de privacidade com a responsabilização pelas condutas praticadas neste “admirável mundo novo”.

Palavras-chave:

Monitorização; Internet; Privacidade

Abstract:

What we intend with this small presentation is to contribute for an argumentation critical and imperative about the right of privacy, when we use the Internet. Must be clear that we won't offer answers, but only more doubts, trying to contribute for a reflection; without time and knowledge, we only offer you more proposals, looking for making compatible the right to the privacy with the responsibility of the behaviours practised in this “Brave New World”.

Word-Key:

Monitoring; Internet; Privacy

¹ Este texto corresponde à versão em português da conferência que apresentamos no seminário Monitoring and Supervision Seminar 15 June 2006, Rotterdam, The Netherlands, organizado por The Centre for Computer Science and Law, Erasmus University Rotterdam.

1.

Tem sido prática comum enumerar o 11 de Setembro como um momento decisivo para o crescimento de uma tendência securitária, na sequência da ameaça terrorista. Com o devido respeito, não sufragamos esta visão. É nossa convicção que o 11 de Setembro apenas foi o perfeito pretexto para legitimar as tensões sempre existentes entre a defesa da privacidade e a propensão para a implementação de severas medidas de segurança; o acto terrorista, deu sustentação política para legitimar práticas já existentes, pela vulgarização na opinião pública de um sentimento de insegurança, criando um ambiente favorável ao surgimento de legislação castradora dos direitos individuais.

Quando em 1890 quando Samuel Warren e Louis Brandeis escreveram o artigo com o título “Right to privacy”, onde de forma inaudita estabeleceram os princípios gerais do direito à intimidade da vida privada, este tem sido um direito difícil de definir, com limites polémicos e objecto de constantes controversas; definir quais as prerrogativas que compõem este direito continua a ser uma árdua tarefa para a melhor doutrina.

Quando George Orwell escreveu a obra, aparentemente ficcionada, 1984, os mais cépticos estavam longe de acreditar que seria possível vivermos a era do Big Brother; mas a tecnologia ofereceu os meios que os Estados necessitavam para a criação de um mundo sem segredos...

Com efeito, através do telefone móvel é possível saber a todo o tempo onde cada um de nós está, através do cartão de crédito que compreender quais os produtos que adquirimos; através do telefone, quem quais as pessoas com quem contactamos; quando vamos a uma bomba de gasolina as câmaras de vigilância guardam a nossa imagem; se vamos ao médico, este elabora a ficha do paciente que fica gravada num computador, passível de ser acedida; ao utilizar a Internet, todas as nossas actuações na rede ficam registadas num *Internet Service Provider*.

O que fica escrito, torna-se ainda mais complexo, quando o relacionamos com o ambiente da Internet, onde historicamente assistimos a enorme relutância para com o primado do Direito, ao abrigo de um pretensível princípio da liberdade da rede.

A tentativa de criar um espaço à margem do Direito ou regulado por regras específicas alheias aos institutos jurídicos tradicionais, teve como consequência a criação de uma neblina de insegurança na Internet, ávida de uma maior segurança, que possa permitir um salutar desenvolvimento.

É insofismável que um dos principais propulsores do crescimento da ilegalidade na Internet é o anonimato da rede; sem dúvida que o facto de ser possível anonimamente criar páginas, fazer comentários, desenvolver blogues, enviar e-mails, é um impulsor da ilegalidade da rede, criando no

agente um espírito de impunidade, a sensação que tudo lhe é permitido, sem que lhe sejam exigidas responsabilidades pelas suas condutas.

O que procuramos neste pequena apresentação é contribuir para uma discussão que urge fazer-se sobre o direito à privacidade na utilização da Internet. Desde logo, que fique claro; não oferecemos respostas, apenas dúvidas; falta-nos tempo, inteligência e conhecimento para oferecer mais do que propostas sobre a forma de compatibilizar a necessidade de privacidade com a responsabilização pelas condutas praticadas neste “admirável mundo novo”.

2.

O século XXI poderá no futuro ser recordado como o século da informação. Com efeito, a informação é a mais potente arma da actualidade; controlar a informação na era digital é um passo decisivo para controlar a humanidade. Falar sobre o direito à privacidade é aquilatar qual a informação relativamente a cada um de nós que pode estar disponibilizado, quando, onde e por quem.

Se na actualidade o recurso às novas tecnologias permite a criação de uma “transparent society”, os próximos anos reservam-nos surpresas inimagináveis há bem pouco tempo.

Daqui a poucos anos vamos a caminhar na rua e recebemos uma *sms* no telemóvel a informar que os nossos produtos favoritos estão em saldo, numa loja a poucos metros, ou do restaurante da esquina a informar que o têm o nosso prato favorito ou que a nossa ex-namorada acabou de chegar à cidade. A rede vai saber mais sobre nós que os nossos melhores amigos, reunindo um impressionante conjunto de informação, sobre os nossos gostos e interesses, para, posteriormente, serem vendidos a qualquer interessado, que pague o devido preço.

Na próxima década, ao tirarmos uma fotografia com o nosso telemóvel, o aparelho envia a foto, conjuntamente com a nossa localização exacta, para uma organização que acrescenta esses dados ao nosso ficheiro pessoal, onde constam milhares de informações sobre cada um de nós. Essas informações irão ser vendidas no mercado.

As entidades a quem nos referimos, não é o Estado totalitário de Orweel, mas as multinacionais da comunicação, como a Google, Yahoo ou Microsoft: os conteúdos por estas empresas disponibilizados gratuitamente na rede, encontram aqui a sua justificação, encontramos aqui o seu preço.

Num mundo global, impregnado de perigosas ameaças para a vivência em sociedade, a necessidade de uma política de segurança é axiomática. Também é uma evidência que os meios de polícia não podem escamotear as inúmeras possibilidades oferecidas pela tecnologia, que apresentam soluções óptimas para auxiliar o desenvolvimento do seu trabalho.

Quando nos confrontam com o 11 de Setembro em Nova Iorque ou o 11 de Março de Madrid, é complexo, senão impossível, reconhecer o direito da família Warren de defender-se das notícias publicadas num jornais de Bóston, sobre o casamento da sua filha. Mas devemos abdicar da nossa individualidade em benefício de uma suposta maior segurança? Devemos renunciar à nossa intimidade na tentativa de construir uma sociedade mais segura?

Não se depreenda das nossas palavras que temos uma visão fatalista das novas tecnologias; é obvio que reconhecemos as suas inúmeras vantagens, permitindo tornar a vida mais fácil e mais cómoda; nenhum de nós estaria hoje preparado para sobreviver no mundo sem tecnologia. Apenas nos assusta que o mundo da tecnologia quebre todas as barreiras da nossa intimidade.

São precisamente as vantagens da era digital que tem impulsionado os cidadãos a abdicarem alegre e paulatinamente do seu *right to be let alone*; mas até onde estamos preparados para ceder?

É o momento óptimo para indagar sobre quais as ameaças específicas oferecidas pelas novas tecnologias, pela Internet em especial? Desde logo, sublinha-se o facto de a rede ter uma inesgotável capacidade para armazenar e tratar a informação; enormes “pedaços” das nossas vidas estavam dispersos por inúmeros registos, controlados por inúmeras entidades: a tecnologia, nomeadamente as bases de dados informatizadas, oferecem a possibilidade de agrupar toda essa informação num único registo global, susceptível de elaborar o perfil de cada um de nós, reunindo os nossos gostos, hábitos, locais que frequentamos, apetências, amigos, relações profissionais, consumos, ou seja, tudo o que nos caracteriza enquanto indivíduos, aquilo que é a nossa individualidade, aquilo que nos caracteriza e distingue de todos os outros.

Pelo recurso à vídeo vigilância, o controlo das chamadas telefónicas, as escutas telefónicas, através de chips de identificação, da análise dos cartões de crédito, podemos construir uma sociedade um pouco mais segura; mas queremos construir uma sociedade sem segredos, onde todos sabemos tudo sobre todos os outros? Estamos condenados a viver no mundo em que todas as nossas acções são monitorizadas, ou será possível descobrir equilíbrios?

Eis o momento de enfrentar a problemática; perguntamos: o que devemos entender por direito à privacidade? Qual o conteúdo e limite deste direito? O que é um dado pessoal?

São perguntas cuja resposta não é fácil. Numa primeira aproximação à resposta, podemos afirmar que se relaciona com a informação que cada um de nós está disposto a partilhar sobre a sua vida pessoal.

Procurando na lei a resposta, dado pessoal é “qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa

ser identificada 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”. (art. 3º da Lei n.º 67/98 – Lei da Protecção de Dados Pessoais).

No que concerne ao processamento de dados pessoais, entende-se “qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição” (ibidem).

Dada a amplitude da noção de dados pessoais, é importante distinguir no direito à privacidade a esfera pública, esfera privada e esfera íntima, recorrendo-se desta forma à tradicional distinção, esboçada pela jurisprudência alemã.

Na esfera pública encontramos as informações que o titular está disposto a fornecer voluntariamente; na esfera privada, a informação relacionada com as relações sociais de uma determinada pessoa, mas que ela não pretende disponibilizar.

Por fim, na esfera íntima encontramos as informações relacionadas com as convicções filosóficas ou políticas, religião, origem racial ou étnica, e os dados relativos à intimidade sexual, ao estado de saúde, incluído dados genéticos.

São sobretudo os dados constantes da esfera íntima que maiores preocupações devem causar aos intérpretes, uma vez que, são estas as informações que nos definem enquanto pessoas únicas e irrepetíveis e cujo conhecimento público mais constrangimentos nos podem causar.

3.

Numa muito breve análise ao “estado da arte”, ultrapassando as complexidades específicas da monitorização militar com pretextos de segurança interna dos Estados, – nomeadamente o sistema Echelon, que comporta cerca de 120 satélites espões, constituindo uma rede electrónica de vigilância susceptível de interceptar comunicações telefónicas, fax e correio electrónico à escala mundial, tornando-as disponíveis para os serviços secretos - com especificidades nebulosas, cobertas por uma mar de suspeitas e suposições, que impedem que o intérprete possa fazer conclusões objectivas, baseadas em verdadeiros factos, procuramos analisar três áreas em que existem enormes pressões sobre os legisladores e os tribunais para legalizar a monitorização da Internet.

Reportamo-nos ao Direito da Família, nomeadamente acções de divórcio, nas quais se pretende utilizar como meios de prova os dados obtidos de forma informática. Ninguém ignora que, pela

análise de um computador, é passível de se agrupar um conjunto de informação pessoal, um conjunto de provas de inegável interesse para uma acção de divórcio; os sites que frequentamos, os e-mails que trocamos, as conversas que temos através do Messenger, podem ser provas indesmentíveis da existência de uma infidelidade, sendo da óbvia utilidade a possibilidade de esses dados serem carrilados para o Tribunal.

No que concerne ao Direito do Trabalho, são infindáveis as possibilidades oferecidas pelas novas tecnologias. Limitando a nossa análise à monitorização do tráfego na Internet, para uma eventual acção de despedimento, importa traçar uma fronteira estável entre o admitido e proibido. As maiores tensões estão relacionadas com o correio electrónico: deve admitir-se que a entidade patronal possa investigar o conteúdo dos e-mail, utilizando os mesmos como motivação de um despedimento?

Refira-se, de forma clara e inequívoca, que plasmar na lei ou no contrato que o trabalhador não pode usar a Internet para fins pessoais e posteriormente impedir a Entidade Patronal de verificar o cumprimento da norma, significa retirar qualquer conteúdo prático à proibição: será justo onerar o empregador com os custos da utilização errónea da rede, impedi-lo de coibir o seu uso para finalidades exclusivamente profissionais?

Em outra perspectiva: deverão os interesses exclusivos da entidade patronal permitir que o vínculo laboral retire ao trabalhador qualquer expectativa de privacidade ao longo de toda a jornada laboral, permitindo ao empregador uma arbitrária investigação de toda a sua conduta nas instalações desta entidade?

Finalmente, o Direito Penal. É indesmentível que assistimos a uma enorme pressão dos meios criminais para uma massificação do recurso às novas tecnologias no combate ao crime. Ninguém acredita que a grande criminalidade pudesse ser combatida sem o recurso à vídeo vigilância, fotografia, escutas telefónicas e toda uma parafernália de novos meios, oferecidos pela nova ciência, para combater crimes antigos.

No caso específico da Internet, a sua monitorização é crucial, não apenas para punir os crimes realizados na rede, como os crimes realizados fora da rede, mas na qual esta é usada como um mero instrumento.

Preocupa-nos sobretudo o primeiro caso; defendemos que o crescimento da rede só é possível se a mesma for cada vez mais segura, se as condutas ilícitas praticadas na rede tenham a merecida punição. Se nos primórdios da Internet a primeira preocupação era o crescimento da rede, agora urge dota-a de credibilidade.

Este é o momento para deixar breves palavras sobre as motivações para a conflitualidade na rede. Abstraindo-nos da problemática sobre a sua dimensão global e o facto de os Estados terem

problemas de soberania na rede, a sua incapacidade para aplicar as decisões judiciais, cingimo-nos ao anonimato.

O pretensão total anonimato oferecido pela Internet é propulsor de cobardes e insidiosos comportamentos, impulsionando pessoas a actuar de forma totalmente inversa ao quadro de valores e referências que norteiam a sua conduta no mundo sensorial. Escondidos num pseudónimo, exortam frustrações e pecados privados, ficcionando uma pessoa que não são ou não têm coragem para ser. Mais do que isso; “o anonimato perfeito torna possível o crime perfeito”, pela impossibilidade de identificar o infractor; por outro lado os infractores agem sem plena consciência do desvalor dos seus actos, sem plena consciência da ilicitude da sua conduta, na ilusão de que tudo é possível e por nada devem ser responsabilizados juridicamente.

Voltamos, neste contexto, a uma preocupação recorrente no nosso pensamento; a necessidade de distinção entre as noções de privacidade e anonimato, que não pode ser um óbice para a responsabilização dos infractores. É nossa convicção que é possível compatibilizar a defesa da privacidade do utilizador da Internet, com a estatuição de uma profícua aplicação do Direito às ilicitudes *on line*; se sustentamos o supremo e inabalável direito de pesquisar livremente pela Internet, utilizando-a como instrumento de trabalho, como plataforma académica, para deleite pessoal, enquanto óbvia decorrência da privacidade individual, estes valores não podem ser incompatíveis com a responsabilização do internauta pelos conteúdos expostos na Internet. O anonimato, a defesa da privacidade não pode ser entendido como um valor sagrado, mas, como tudo na vida e no Direito, deve ser relativizado em cada caso concreto, de forma a arquitectar a consagração de soluções justas; existindo um acto ilícito, têm que ser consagrados mecanismos conducentes à identificação do prevaricador e a sua apresentação à justiça, de forma a que o Estado de Direito siga o seu rumo.

7.

Este é o momento para enfrentarmos a problemática que nos propusemos dissecar: como pode a Internet violar o nosso *right to be alone*, como pode realizar-se a monitorização da nossa actuação *on line*.

Não vamos cuidar da monitorização pelos órgãos de polícia, nem sequer da monitorização no local de trabalho, realizada directa ou indirectamente no computador do visado. O que nos ocupa é a monitorização do cidadão comum, liberto de vínculos laborais ou indícios criminais.

Sem preocupações de exaustividade, que neste contexto seria sempre incompleta, devido às constantes inovações técnicas que oferecem a cada dia novos e melhores meios para conseguir controlar a nossa actividade na rede, deixamos escritas alguns dos mais comuns meios para monitorizar a nossa actuação na *world wide web*.

Basicamente existem poucos métodos para “roubar” informação de um computador, mas milhares de formas para o conseguir; se pretendemos tirar informação de um qualquer computador, temos de fazer, ou utilizar, um software concebido para essa finalidade. Estes programas são comumente conhecidos como *Trojan Horses*, *Spyware*, *Adware*, *Key-loggers*, entre outros e estão disponível na Internet.

Uma pergunta fica ainda sem resposta; como é que eu posso instalar esses programas no computador que pretendo monitorizar, sem o conhecimento desta pessoa. Analisemos as mais comuns modalidades para alcançar este desiderato.

Método Um: explorar as vulnerabilidades dos programas.

Uma das formas mais comuns para instalar um software no computador de um terceiro, sem que este dê autorização ou tenha conhecimento, é aproveitar as vulnerabilidades dos programas.

Para aceder à Internet utilizamos “ferramentas”, programas de computador que, podem ter incorrecções ou pequenos defeitos que afectem a sua integridade. É consabido que as maiores empresas de programação do mundo, como a Microsoft por exemplo, publicam milhares de “updates” por ano, com o intuito de corrigir as vulnerabilidades que vão sendo descobertas; no entanto, esta é uma tarefa ingrata, porquanto, novas falhas vão sendo conhecidas, sendo estas entidades impotentes para garantir a invulnerabilidade dos programas.

Método Dois: através do e-mail.

Um outro clássico; quando recebemos um e-mail, para além do texto, podemos receber conteúdos maliciosos, ou ser direccionadas para *sites* inseguros. Especialmente no que concerne aos anexos existe o real perigo de conterem programas que permitam a terceiros aceder ao nosso computador.

Método Três: Mensagens Instantâneas.

Os programas ordinariamente designados por *Messengers*, que permitem conversas em tempo real, por texto, áudio ou imagem, são verdadeiras ferramentas multimédia com uma heterogeneidade de funcionalidades. Não raramente, são usadas como meio para instalar programas indesejados que, posteriormente, vão permitir a monitorização do internauta.

Método Quatro: Peer2Peer.

Os programas Peer2Peer permitem trocar ficheiros através da Internet; concomitantemente são talvez a forma mais fácil para permitir a instalação de programas indesejados. Mais do que isso, o próprio conceito destas aplicações está umbilicalmente conexionado com ilícitos *on line*, mormente a pirataria informática e a violação dos direitos de autor, nomeadamente no caso das músicas.

A problemática adensa-se quando os utilizadores das aplicações Peer2Peer não têm suficientemente conhecimentos técnicos, ficando vulneráveis às mais vis práticas, entregues a poucos escrúpulos de infames utilizadores.

Método Cinco: os “*cookies*”.

Aparentemente para permitir que a nossa “navegação” seja mais agradável, os produtores de software, desenvolver uma ferramenta que permite ao Internet Service Provider reconhecer o utilizador, quando regressa a um qualquer site. Estes cuidadosamente alojam esta ferramenta, baptizada como “*cookie*”, no nosso computador, sobre o pretexto de as nossas experiências *on line* serem mais agradáveis e permitirem um tratamento mais personalizado.

Não questionamos que este objectivo seja alcançado; ao reentrarmos no site, este dá-nos os bons dias usando o nosso nome, oferece-nos informações relacionadas com o local de onde estamos conectados e até nos direccionada para o que podem ser os nossos interesses. Mas, importa sublinhar, que um *cookie*, é um sinal identificador único e específico alojado no computador do utilizador, que passará a identifica-lo sempre que aceda a um determinado *site*; assim, o *host computer* saberá que um determinado utilizador regressou ao site, quantas vezes, por quanto tempo, o que viu no site e de onde se está a conectar. Consegue-se desta forma estabelecer o perfil do utilizador, uma análise às suas preferências aos seus interesses.

Através dos Cookies não apenas é possível conhecer o padrão de utilização de um sítio, como é possível traçar toda a sua navegação na Internet.

Pelo que foi sendo escrito, é axiomático reconhecer que através da monitorização da Internet é possível saber o que uma pessoa procura, o que uma pessoa gosta, quais são os seus interesses, quais as suas necessidades.

E não se alegue que estes meios identificam computadores e não pessoas; na era do computador pessoal é um argumento falacioso, conjurado para criar uma névoa na visão do investigador. Estes meios permitem identificar em concreto a pessoa, monitorizando as suas condutas na rede.

E este é o cerne da problemática. A monitorização da utilização da Internet permite construir um perfil do utilizador, determinar os seus gostos, interesses e necessidades.

A técnica tradicional nos primórdios da rede de pedir ao utilizador o preenchimento de um formulário de registo, onde constavam várias questões sobre os seus gostos e apetências foi substituído por meios sub-reptícios, mas mais fiáveis, para conseguir essa informação, sem que o utilizador voluntária e conscientemente a forneça.

Mas para quê conhecer o padrão de utilização da Internet? A resposta, desde logo, está na publicidade.

A world wide web está a fornecer aos publicitários um mundo de sonho; a publicidade deixa de ser genérica e ambígua, para ser personalizada. A monitorização dos comportamentos na web permite criar uma “verdadeira base de dados de intenções”; tendo como exemplo a Google, esta empresa sabe o que a nossa cultura deseja, o que procura, e esta informação que está disponível para ser vendida.

Os milhares de *spam* que nos invadem a privacidade, não são fruto de listas cegas, mas cada vez mais elaboradas de forma específica, para responder às pretensas necessidades de cada utilizador, de acordo com os seus percursos pela rede; mas será que todos os problemas da violação da privacidade pela monitorização da Internet se resolvem através de um software anti-spam? Deixamos a nossa resposta para o delicado período das conclusões.

5.

Como o legislador aborda o tema, pode ser o título deste capítulo da nossa curta intervenção; iremos procurar respostas pela análise às normas legais cruciais para este estudo.

Não nos iremos deter na análise constitucional, nem nas convenções internacionais, para concluir o que neste momento é óbvio: O Direito Internacional e o Direito Constitucional Português reconhecem o direito à privacidade, com fundamento na protecção da dignidade da pessoa humana. Começamos por afirmar que as leis penais punem muitas das condutas descritas como crimes. Neste contexto, é interessante recordar a Convenção sobre o Cybercrime do Conselho da Europa, que íntima os Estados para a criação de legislação penal, de forma a puderem, com eficácia, combaterem os ilícitos na rede e através da rede.

No que se refere especificamente com a problemática em dissecação, sublinhamos dois diplomas fundamentais: a Directiva sobre a protecção dos dados pessoais e a Directiva relativa à privacidade e às comunicações electrónicas.

Numa análise não exaustiva à Directiva da protecção dos dados pessoais, porquanto a monitorização da Internet também se faz pela criação de uma base de dados com informações sobre os utilizadores da rede, enfatizamos a existência de vários direitos essenciais para a protecção dos cidadãos, tais como, o direito à informação, direito de acesso, direito de rectificação e eliminação e o direito de oposição.

No que respeito ao Direito de Informação, exige-se que o visado deva conhecer a finalidade do tratamento dos dados pessoais, quem o realiza e a quem irão ser comunicados.

Por direito ao acesso entende-se a possibilidade de qualquer pessoa aceder aos dados que sejam registados sobre si, sem restrições ou custos excessivos, bem como saber quaisquer informações disponíveis sobre a origem desses dados.

Deste acesso pode resultar o exercício do direito de rectificação e eliminação dos dados. Próxima é a possibilidade de exercer o direito de oposição, nomeadamente ao tratamento dos seus dados para fins de publicidade ou outros.

Por fim, devemos ainda referir que o indivíduo tem o direito de exigir que os seus dados sejam recolhidos de forma lícita e leal, que não sejam comunicados a terceiros sem o seu conhecimento e consentimento ou utilizado para finalidade incompatível com aquela que determinou a recolha.

No que concerne à Directiva relativa à privacidade e às comunicações electrónicas, a Directiva “exige dos Estados-Membros que garantam os direitos e liberdades das pessoas singulares no que respeita ao tratamento de dados pessoais, nomeadamente o seu direito à privacidade, com o objectivo de assegurar a livre circulação de dados pessoais na Comunidade”.

Mais do que isso, a Directiva reconhece que estão a ser introduzidas nas redes de comunicações públicas da Comunidade novas tecnologias digitais avançadas, que suscitam requisitos específicos de protecção de dados pessoais e da privacidade do utilizador. O desenvolvimento da sociedade da informação caracteriza-se pela introdução de novos serviços de comunicações electrónicas. O acesso a redes móveis digitais está disponível a custos razoáveis para um vasto público. Essas redes digitais têm grandes capacidades e possibilidades de tratamento de dados pessoais. O desenvolvimento transfronteiriço bem sucedido desses serviços depende em parte da confiança dos utilizadores na garantia da sua privacidade”.

Por tudo, não estranha a recomendação para a estatuição de “disposições legislativas específicas para a protecção dos direitos e liberdades fundamentais das pessoas singulares e dos interesses legítimos das pessoas colectivas, em especial no que respeita à capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores”.

De extrema importância, e de encontro às nossas convicções, é a consagração de que “o equipamento terminal dos utilizadores de redes de comunicações electrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais. Os denominados "gráficos espíões", "programas-espíões", ("spyware"), "gráficos-espíões" ("web bugs") e "identificadores ocultos" ("hidden identifiers") e outros dispositivos análogos podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das actividades do utilizador e podem constituir uma grave intrusão na privacidade desses utilizadores. A utilização desses dispositivos deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa”.

Para alcançar estes desideratos, o art.º 4º *consagra que prestador de um serviço de comunicações electrónicas publicamente disponível adoptará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede.*

O mais importante princípio da Directiva é o primado da confidencialidade das comunicações; para alcançar os Estados-Membros garantirão, através da sua legislação nacional, a

confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceptação ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo...

Analisada a legislação existente, quer a portuguesa, quer a comunitária, concluímos, sem margem para dúvida, que existe excelentes diplomas legais, que procuram proteger de forma eficaz o direito à privacidade dos utilizadores.

Podemos dormir descansados? Infelizmente, penso que não. É insofismável que a legislação existente não está a ser cumprida.

7.

O Direito à privacidade, o direito a estar só, continuando previsto nos mais importantes diplomas internacionais e nacionais, corre o grave risco de se tornar num preceito desejável mas inoperante, subjugado aos mais diversos e heterogéneos fins, mera norma programática, uma homenagem a tempos idos.

A tecnologia quotidiana, “adoçando-nos” a boca com as suas vantagens, tais como software mais fiável e gratuito, enquanto se permite o privilégio de seguir e registar cada uma das nossas acções, cada um dos nossos movimentos, numa cega tentativa de descobrir todos os nossos pensamentos. É incontestável que vivemos uma era de voyeurismo governamental e empresarial absolutamente intolerável.

Por tudo, é tremendamente importante estabelecer que, quando eu utilizo a Internet, todas as informações que “deixo” na rede sobre os meus percursos, são privadas e confidenciais, pelo que, por ninguém, podem ser utilizados sem o meu consentimento.

Se existe meios técnicos passíveis de permitir aos *Internet Service Providers* monitorizar as nossas condutas *on line*, é igualmente verdadeiro que existe meios técnicos disponíveis para impedir essa actividade; software como anti-spam, - que filtram boa parte dos mails indesejados - , os *Privacy Enhancing Technologies*, - que permitem ao utilizador apagar os vestígios da sua navegação ou acções na Internet, possibilitando um *anonymous surfing* -, os programas de gestão de cookies – que permite rejeitar a instalação de *cookies* – ou a *Platform for Privacy Preferences Project*, que possibilita a criação de um perfil de privacidade que vai nortear toda a nossa actuação na rede. Por outro lado, o utilizador ciente da sua intimidade, pode sabotar os “perseguidores”, mentindo

quando preenchem os formulários, adulterando os dados nos cookies, pesquisando em sites que não correspondem aos seus interesses, enviando e-mails com linguagem codificada.

Mas esta é uma falsa questão: iludir-nos com a possibilidade de nos defendermos de actuações ilícitas, não resolve o cerne da questão: a existência de actividades ilícitas.

Não devemos caminhar para um estágio em que, por existirem meios para nos tentarmos defender, todas as condutas ilícitas são admissíveis; não compete ao cidadão, a mais das vezes sem conhecimentos técnicos, proteger-se com software para defender o seu direito à privacidade.

Esta é uma obrigação dos Internet Service Providers; estes têm que respeitar a privacidade do utilizador, abstendo-se de condutas que a violem, obstruindo que outros o façam.

Se uma empresa tem como mote “*do not evil*”, não nos podemos satisfazer com uma declaração de intenções; é preciso não esquecer, que estas empresas têm os meios e a vontade para violar a nossa intimidade, expondo-nos a uma enorme heterogeneidade de nefastas consequências.

Os ficheiros com dados pessoais existem e são comercializados nos mercados; por enquanto, ao que se sabe, são sobretudo utilizados para finalidades publicitárias; mas é igualmente verdade que existem sérios receios para que esses dados possam ser utilizados para outras finalidades.

Em regra, estas bases de dados são ilegais; os utilizadores desconhecem que as mesmas existem, não conhecem o seu conteúdo, nada sabem sobre a razão de existirem, quem o realiza, quem as vende, quem as compra. Estas foram realizadas sem a devida autorização do utilizador ou através de um consentimento forjado ou dado de forma inconsciente, ao clicar no “I accept” no fim de um extenso formulário, elaborado com o firme propósito de ninguém ter paciência para o ler.

A acérrima defesa do Direito à Privacidade na Internet não é incompatível com a aplicação dos princípios do Estado de Direito; no que concerne a esta problemática entre a privacidade e anonimato, a nossa posição é clara: só aos meios judiciais, a uma decisão de um Tribunal, reconhecemos autoridade para quebrar esta complexa barreira. Explicamos. Entendemos que o consumidor de Internet tem direito pleno à privacidade que, em caso algum, deverá ser coarctada, excepto quando os Tribunais fundamentadamente decidirem o contrário; reconhecemos, assim, o direito a disponibilizar anonimamente todos conteúdos que lhe aprouverem; verificado que *in casu* os conteúdos são ilícitos, as autoridades judiciais (e apenas estas) podem demandar junto dos ISP para estes facultarem os meios conducentes à identificação dos alegados infractores. Sustentamos que só assim é possível conciliar o Direito à Intimidade da Vida Privada, com o respeito pelo Principio da Legalidade.

Mas não podemos conceber que o direito à privacidade como um direito menor, amovível por meros caprichos ou humores de *Internet Service Providers* ou subjugado a ímpetos de mercado, a pretensos legítimos interesses da economia.

O direito à intimidade da vida privada, é o direito à nossa individualidade, o direito a ser um verdadeiro e completo ser humano.

Se tudo o que escrevemos é certo, também há uma outra verdade que não queremos escamotear: o utilizador médio não está preocupado com a sua privacidade, desvalorizando as violações da sua intimidade, na cega ânsia de aceder a mais e melhores conteúdos na Internet, de usufruir até à exaustão as potencialidades fantásticas das novas tecnologias.

Muito do que fica escrito, não é novo; esta é uma querela que acompanha toda a história da humanidade; as novas tecnologias apenas aumentaram incrivelmente a capacidade de armazenar e pesquisar a informação. Por tudo, a questão exige-se com a força de uma evidência: quantas princesas, artistas, desportistas expuseram a sua intimidade, encheram revistas com a sua vida íntima, para beneficiarem de transitória fama ou dinheiro e, num determinado momento da sua vida, se arrependeram de ter seguido por esse caminho, quando já era demasiado tarde para regressar?

O Direito à Privacidade é uma das coisas na vida à qual apenas damos o merecido valor quando o perdemos. Importa nunca esquecer que a informação quando utilizada correctamente é algo de maravilhosa; a informação quando usado erradamente é uma poderosa e destrutiva arma.

HUGO LANÇA SILVA

Beja, 13 de Junho de 06