APRITEL

PROPOSTA DE LEI SOBRE O TRATAMENTO DE DADOS PESSOAIS E PROTEÇÃO DE PRIVACIDADE

COMENTÁRIO

Resposta da Associação dos Operadores de Telecomunicações à consulta da Secretaria de Estado das Obras Públicas Transportes e Comunicações sobre a proposta de lei que transpõe a Diretiva 2009/136/CE

31 de maio de 2012

Índice

Índice 1

I. Introdução 2

II. Considerações gerais 2

III. Comentários à Proposta de Lei 3

B. Definição de "dados de tráfego", "violação de dados pessoais" e obrigação de notificação 4

C. Adoção de medidas de segurança adequadas 8

D. Cookies 9

E Dados de Tráfego e de Localização 9

E. Comunicações não solicitadas 10

F. Dever de informação 12

G Competências do ICP-ANACOM e da CNPD 13

H. Incumprimento - em especial a imposição de sanções pecuniárias compulsórias 13

31 de maio de 2012

I. Introdução

O presente documento traduz a posição da APRITEL - Associação dos Operadores de Telecomunicações ("APRITEL"), relativamente ao texto da Proposta de Lei sobre o tratamento de dados pessoais e proteção de privacidade no setor das comunicações eletrónicas, que transpõe a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro ("Proposta de Lei").

No presente documento, apresentar-se-ão considerações gerais sobre o tema do tratamento de dados pessoais e proteção de privacidade no setor das comunicações eletrónicas e, de seguida, analisar-se-ão os temas/questões que, na Proposta de Lei, mais reservas colocam a esta Associação.

Anexo a este documento – e para facilitar a compreensão dos argumentos aqui apresentados – a APRITEL junta o texto da Proposta de Lei, desta forma alterado por forma a refletir os comentários aqui expostos.

II. Considerações gerais

Previamente à análise específica do texto da Proposta de Lei, a APRITEL gostaria de transmitir, desde logo, que as alterações introduzidas pela Diretiva ePrivacy (Diretiva 2002/58/CE), nomeadamente quanto à notificação de "data breaches", se revestem de especial importância e se assumem como um fator de desenvolvimento com um potencial de aumento do nível de segurança dos dados pessoais.

No entanto, e tal como a APRITEL teve a oportunidade de manifestar noutros fóruns, a introdução de um mecanismo de notificação de "data breaches" neste caso poderá acarretar uma imagem negativa do setor e, consequentemente, dos seus players.

Outras questões prévias se colocam, como sendo a necessidade de articulação entre este regime e a obrigação, que impende sobre os operadores, de manter confidenciais certos dados dos seus clientes.

De facto, a divulgação de informação acerca dos termos em que a violação ocorreu – nomeadamente o tipo de dados, os sujeitos envolvidos e o tipo de violação – poderá, no limite, comprometer novamente a confidencialidade dos dados pessoais em causa, disponibilizando publicamente informação coberta precisamente pela obrigação de confidencialidade.

A APRITEL não poderá ainda deixar de alertar para o risco de confusão entre os dois mecanismos de notificação que serão aplicáveis aos operadores decorrentes da presente lei e da Lei de Comunicações Eletrónicas (Artigo 54.º-B da Lei n.º 5/2004, de 10 de fevereiro, com a redação da Lei n.º 51/2011 de 13 de setembro). Deverá assim ser esclarecido se, em caso de incidente que, simultaneamente seja um incidente de segurança e uma violação de dados pessoais, os operadores deverão seguir os dois procedimentos de notificação – tal solução será manifestamente excessiva e desprovida de qualquer eficácia.

Deverá ainda ser esclarecido qual o mecanismo de notificação a adotar caso a violação de dados pessoais tenha dimensões transfronteiriças.

31 de maio de 2012

III. Comentários à Proposta de Lei

A. Resposta a pedidos de acesso a dados pessoais dos utilizadores que lhes sejam apresentados pelas autoridades nacionais competentes

Relativamente ao Artigo 1.º, a APRITEL gostaria de referir que, não obstante partilhar as preocupações do legislador em determinar a adoção, pelas empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público, de procedimentos internos que permitam responder aos pedidos de acesso a dados pessoais dos utilizadores que lhes sejam apresentados pelas autoridades nacionais competentes, tais procedimentos (ou pelo menos as diretrizes às quais devem obedecer) deveriam ser pré-determinados pelas autoridades competentes nesta matéria – neste caso, a Comissão Nacional de Proteção de Dados ("CNPD").

Esta necessidade resulta, sobretudo, do facto de os principais dispositivos legais que regulam esta matéria, e em que assentam os referidos procedimentos, nomeadamente a Lei nº 32/2008, de 17/07 (Lei de Retenção de Dados), a Lei nº 109/2009, de 15/09 (Lei do Cibercrime) e o Código do Processo Penal, concretamente o seu artigo189º, por conterem regimes que se sobrepõem e que, em alguns aspectos, poderão até ser entendidos como contraditórios, estarem a suscitar divergências de entendimento entre os operadores e as autoridades judiciais e a criar um clima de incerteza jurídica quanto à lei aplicável aos pedidos de acesso aos dados por parte destas entidades, trata-se não só de uma situação perigosa e intolerável atenta a sensibilidade da matéria em causa, como prejudica a célere e eficaz colaboração dos operadores na administração da justiça.

Com efeito, existem, nesta área, fruto do quadro legal em vigor, grandes divergências de entendimento entre os operadores e as autoridades judiciais quanto aos poderes para a obtenção de determinados dados (nomeadamente dados de tráfego) e quanto ao prazo e finalidades de armazenamento desses dados, sendo que muitas vezes os operadores são confrontados com ordens de obtenção de dados ilegítimas, e que no seu entender, se cumpridas, podem levar à prática de um crime de acesso indevido a dados, embora sejam depois ordenados a disponibilizar os referidos dados sob a ameaça de incorrerem em crime de desobediência.

Uma das principais fontes de divergência, prende-se com o regime previsto na Lei 32/2008, de 17/07, que veio determinar a conservação pelos operadores de todos os dados gerados e tratados no contexto da oferta de redes e serviços de comunicações electrónicas pelo prazo de 1 ano, em sistemas autónomos e com a finalidade exclusiva de transmissão dos referidos dados às autoridades para a investigação e repressão dos crimes previstos no artigo 2º, alínea g) do aludido diploma legal, designados de "crimes graves".

Ora, o regime em causa, ao restringir o acesso das autoridades competentes a estes dados apenas à investigação e repressão dos crimes previstos no *supra* referido normativo legal, está a impedir que estas entidades recorram a esta informação no âmbito da investigação e repressão de outros crimes, designadamente os previstos nas alíneas b) a g) do nº 1, do artigo 187º do Código do Processo Penal e os previstos na Lei do Cibercrime e relativamente aos quais é admitida a intercepção e gravação de comunicações.

Por maioria de razão, se em relação a esses crimes se permite a intercepção e gravações de comunicações (muito mais intrusiva da privacidade), faz todo o sentido que se permita, igualmente, no âmbito da investigação dos referidos crimes, o acesso às autoridades aos dados armazenados pelos operadores pelo prazo de 1 ano, posição que, aliás, muitos magistrados judiciais têm vindo a defender.

É pois absolutamente crucial aproveitar, desde já, a presente oportunidade para se proceder também à alteração da Lei n.º 32/2008, de 17 de Junho alargando o respectivo âmbito de aplicação, por forma a permitir aos operadores responder e colaborar com os tribunais no âmbito das investigações dos aludidos crimes com os dados que têm armazenados para fins de investigação criminal, em claro benefício da célere e boa administração da justiça.

Assim sendo, a APRITEL inseriu, no texto que se anexa da Proposta de Lei, um novo artigo aditado, que prevê essa mesma alteração, passando a definição de 'crimes graves' a corresponder aos "*crimes relativamente aos quais a lei admita a intercepção e a gravação de conversações ou comunicações*".

Ainda a este respeito, refira-se que os operadores já suportaram pesados investimentos na implementação de plataformas eletrónicas de disponibilização de informação às autoridades competentes (desde logo, aos tribunais), como é o caso da plataforma electrónica denominada de SAP DOC, referida pela Portaria n.º 694/2010, de 16/08, a qual , por entropias legislativas ou outras razões desconhecidas, não é utilizada pelos tribunais.

Com efeito, os associados da APRITEL recebem diariamente um número elevadíssimo de pedidos de informação de autoridades competentes, nomeadamente dos tribunais e dos órgãos de polícia criminal, para disponibilização de dados relativos à identificação dos titulares das linhas telefónicas, às chamadas efetuadas e recebidas (dados de tráfego), dados de localização, entre outros, assistindo-se, nos últimos anos, a um aumento exponencial do número de pedidos.

Isto dito, sublinhe-se que a colaboração prestada pelos associados da APRITEL acarreta elevados custos, nomeadamente com os recursos técnicos e os meios humanos necessários para receber, processar, gerir e enviar a informação pedida pelas autoridades.

Saliente-se ainda os pesados custos de implementação dos sistemas previstos na *supra* referida Lei nº32/2008, já realizados pelos operadores. Tais investimentos, que também passaram pela implementação de especiais medidas de segurança, ainda não se encontram totalmente amortizados, pelo que a necessidade de suportar custos adicionais constitui, no quadro atual da economia, uma preocupação dos operadores.

Como tal, as exigências de adoção de procedimentos internos deverá ter em consideração os pesados investimentos já realizados pelos operadores, não devendo ser impostas obrigações desproporcionais a este respeito.

B. Definição de "dados de tráfego", "violação de dados pessoais" e obrigação de notificação

Como a APRITEL já teve a oportunidade de manifestar anteriormente, a introdução de mecanismos de notificação de violações de dados pessoais constitui um desenvolvimento importante com um potencial de aumento do nível de segurança dos dados pessoais.

Cumpre, contudo, destacar e salientar um ponto prévio: a definição de dados de tráfego. Apesar de a presente Proposta não se pronunciar sobre este aspeto específico, a APRITEL gostaria de aproveitar o ensejo para refletir sobre esta questão.

De acordo com a redação atual do artigo 2º, n.º 1, al. d), dados de tráfego são "*quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da faturação da mesma*".

Ou seja, podem reconduzir-se à categoria de dados de tráfego todos os dados que sejam objeto de tratamento **(i)** no âmbito de uma determinada comunicação eletrónica ou **(ii)** para permitir a faturação dessa comunicação.

Esta noção de dados de tráfego é demasiado vaga e imprecisa uma vez que abrange todo o tipo de dados associados ou conexos à própria comunicação e à respetiva faturação, e não apenas, como seria desejável, os dados relativos à comunicação *de per se*.

Acresce que, nos termos da Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro), entende-se por dados de tráfego "*os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

Como se percebe, estamos perante duas concepções distintas e diversas o que tem como consequência imediata – altamente indesejável e perniciosa – a incerteza jurídica sobre um conceito muito relevante em matéria criminal e a existência de diferentes entendimentos sobre a competência para solicitar este tipo de dados.

É fundamental, por esta razão, que o conceito de dados de tráfego seja devidamente clarificado e uniformizado, com todos os benefícios daí decorrentes, nomeadamente a agilidade e aceleração processual.

A implementação da obrigação de notificação deverá ser efetuada com parcimónia, de forma a evitar a criação de um sentimento de desconfiança em relação aos operadores e à forma como estes tratam os dados pessoais dos seus clientes.

Assim sendo, não pode a APRITEL deixar de demonstrar a sua preocupação em relação à **definição de "violação de dados pessoais"** constante do Artigo 2.º da Proposta de Lei.

De facto, resulta da definição, ampla, genérica e não totalmente coincidente com a versão da Diretiva a transpor, que teoricamente qualquer violação que envolva dados pessoais poderá ser considerada uma violação para efeitos da determinação da obrigação de notificação dos denominados "*data breaches*".

Deverá também ser esclarecido quais os incidentes que são considerados como "violações de dados pessoais". De facto, os operadores prestam uma generalidade de serviços a diversas empresas que podem sofrer, por exemplo, ataques de *phishing.* Ora, estes incidentes, ainda que se verifiquem na rede de um operador, não deverão ser entendidos como "violações de dados pessoais" para estes efeitos. Apenas os incidentes que digam respeito a dados da responsabilidade do operador deverão cair no âmbito de aplicação da presente lei.

Ainda relativamente à definição de "violação de dados pessoais", salientamos que a introdução de um mecanismo de notificação de violações de dados pessoais não poderá

estar dissociada de uma análise de risco, casuística, tendo em consideração o tipo de dados em causa e a dimensão do incidente.

Ora, a definição tal como consta da Proposta de Lei abre portas para que qualquer incidente que envolva dados pessoais seja considerado como uma "violação de dados pessoais", com todas as consequências e danos, inclusive de imagens, para os operadores.

Quanto à **obrigação de notificação**, prevista no Artigo 3.º A, considera a APRITEL que o texto da Proposta de Lei coloca diversos problemas.

Em primeiro lugar, entende a APRITEL que a obrigação de notificação só deverá ter lugar nos casos em que a violação dos dados pessoais possa "afetar negativamente os dados pessoais do assinante ou utilizador" e não, como parece resultar do texto da Proposta, em qualquer situação.

No que respeita ao prazo para comunicação da ocorrência da violação:

- O legislador optou por não concretizar tal prazo, referindo que os operadores devem "de imediato" notificar o ICP-ANACOM da ocorrência de violação de dados pessoais.
- Desde logo refira-se que caindo na definição qualquer incidente que envolva dados pessoais, a APRITEL teme uma entropia processual, o que, manifestamente não será benéfico nem para os operadores nem para os reguladores.
- Quanto ao prazo em si mesmo, não se entende o conceito de "imediato" uma vez que **(i)** na Diretiva 2002/58 prevê-se que a notificação seja efetuada "*sem atraso injustificado"* e **(ii)** na Proposta de Regulamento do Parlamento Europeu e do Conselho, relativo à proteção de dados pessoais e à livre circulação desses dados, utiliza-se a expressão "*sem demora injustificada*".
- A APRITEL considera que este prazo deverá variar consoante o tipo e complexidade da violação, na medida em que não será possível antecipar quanto tempo levará a reunir a informação necessária para efetuar a notificação ao ICP-ANACOM.
- Deveria prever-se uma escala para avaliar a "severidade" da violação de dados pessoais e determinar, assim, o prazo para a notificação. A severidade deveria ser avaliada tendo em consideração diversos fatores, tais como o nível de vulnerabilidade e a categorização da possibilidade de exploração de tal vulnerabilidade.
- Tendo em consideração a escala e a avaliação efetuada, a notificação ao ICP-ANACOM deveria ocorrer tendo em consideração o nível de "severidade" do incidente.
- Ao determinar o prazo para notificar o ICP-ANACOM, dever-se-á ter em consideração que os recursos internos de cada operador deverão estar focados na resolução do incidente. Como tal, caso seja determinado um prazo diminuto, os recursos internos estarão focados em reunir a documentação e não em identificar e resolver o problema.
- Em qualquer caso, a notificação inicial ao ICP-ANACOM deverá ser efetuada através de um meio expedito (e-mail ou telefone), com a informação apenas de que ocorreu uma violação, sendo efetuado o follow-up de seguida, disponibilizando a informação necessária.

Quanto à notificação do assinante ou utilizador, quando a violação de dados pessoais possa afetar negativamente os seus dados pessoais, a APRITEL salienta os seguintes aspetos:

- A APRITEL considera que o *assessment* para determinar se uma violação afeta, ou não, negativamente os dados pessoais do assinante ou utilizador deve ser efetuado caso a caso, considerando diversos fatores, tais como: o tipo e natureza da violação, o tipo de dados (sensíveis ou não) e o volume de dados em causa. Refira-se, aliás, que é este o entendimento do Grupo de Trabalho do Artigo 29.
- Assim, deveria ser aprovada uma escala para determinar a "severidade" da violação, baseados nos critérios referidos anteriormente a propósito da notificação ao ICP-ANACOM.

O legislador propõe que fiquem excecionados da obrigação de notificação de violações de dados pessoais ao público, as situações em que os operadores comprovadamente demonstrem junto do ICP-ANACOM, e esta Autoridade assim o reconheça, que adotaram as medidas tecnológicas de proteção adequadas e que essas medidas foram aplicadas aos dados a que a violação diz respeito. Uma vez que, como anteriormente referido, tais medidas de segurança não estão definidas no diploma, importa defini-las sob pena do efeito útil desta exceção ser nulo.

Quanto aos meios e procedimentos de notificação, ainda que tais procedimentos não tenham naturalmente que constar da Proposta de Lei, a APRITEL aproveita a oportunidade para salientar a importância de prever meios e procedimentos comuns à União Europeia, tendo no entanto em consideração as realidades nacionais.

Desde logo, deveria ser admitida a notificação ao ICP-ANACOM através de e-mail, sendo enviada uma primeira notificação genérica e posteriormente disponibilizada a informação a que se referem os números 7 e 8 deste Artigo, no caso em que, no momento da deteção da violação, não seja possível reunir toda a informação.

Quanto aos clientes, dever-se-á prever diversas formas possíveis de notificação, consoante, desde logo, o tipo de violação e os dados em causa. Caso seja necessário que os clientes adotem medidas para minimizar os riscos, então a notificação deverá ser efetuada de forma eficaz e expedita. Pelo contrário, se a violação estiver controlada e não for solicitado ao cliente que implemente qualquer medida, então a notificação poderá ser efetuada através de uma publicação no site do operador ou através de informação na fatura a enviar a tal cliente.

Na determinação dos meios e procedimentos de notificação devem ser necessariamente conjugados os interesses em causa e os custos para os operadores na implementação de tal notificação.

Importa, de igual modo, esclarecer se as audições e pareceres da CNPD, referidos nos n.ºs 6 e 9, serão vinculativos.

Finalmente, refira-se, quanto ao registo de violações, que a APRITEL concorda com a sua existência, desde que seja centralizada pelo operador e de acesso restrito às autoridades competentes. De facto, contendo tal registo informação sensível e confidencial, deverá ser assegurado o acesso restrito pelas autoridades competentes. Deveria assim ser aprovado um *standard* comum de registo, contendo informação mínima sobre a violação (data, tipo de violação, dados em causa, medidas adotadas), bem como a indicação do período máximo de armazenamento dessas informações.

31 de maio de 2012

C. Adoção de medidas de segurança adequadas

A APRITEL reconhece a importância da adoção de medidas de segurança adequadas, tendo já implementado políticas rigorosas neste domínio.

Contudo, considera que tais medidas deverão ser claramente concretizadas pelas autoridades competentes, não só para que seja possível aos operadores assegurarem que as medidas que adotaram ou as que planeiam adotar no futuro são as que as autoridades competentes neste domínio consideram "adequadas", mas sobretudo na medida em que a adoção de tais medidas será determinante para aferir da necessidade de notificação, ao público, da ocorrência de violações de dados pessoais.

É certo que se avança com uma tentativa de indicação de medidas de segurança, reconhecendo-se, no entanto, que tais medidas são "medidas mínimas", devendo ser clarificado se tais medidas são as consideradas adequadas pelas autoridades competentes.

Acresce que as medidas de segurança a que se refere o Artigo 3.º da Proposta de Lei não poderão ser dissociadas das medidas de segurança que os operadores terão que implementar no âmbito da Lei das Comunicações Eletrónicas.

Estabelece-se ainda a possibilidade do ICP-ANACOM auditar, diretamente ou por entidade independente, as medidas de segurança adotadas e emitir recomendações práticas a este respeito.

Ora, a APRITEL considera que deverão ser clarificados os casos em que se recorre a uma entidade terceira para realizar as auditorias. Saliente-se por um lado que, numa lógica de garantia da confidencialidade dos dados pessoais dos clientes, será sempre desejável que a auditoria seja sempre levada a cabo pelo ICP-ANACOM e não por terceiros. Por outro lado, dever-se-á, numa lógica preventiva, determinar que medidas são consideradas como adequadas, tendo, naturalmente, em consideração os custos associados à implementação de tais medidas.

De igual forma, deverá ser clarificado em que termos podem acontecer as auditorias de segurança extraordinárias e com que antecedência mínima devem ser comunicadas.

Acresce que se prevê que "*em caso de risco especial de violação da segurança, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem gratuitamente informar os assinantes desse serviço da existência daquele risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis para o evitar e dos custos prováveis daí decorrentes*".

No entanto, não se define o que se entende, para estes efeitos, como um caso de "*risco especial de violação da segurança*", pelo que se desconhece o alcance e aplicação prática desta obrigação.

Esta obrigação pode, ainda, ter efeitos manifestamente contraproducentes: a comunicação da existência de um risco poderá levar a que os assinantes, de forma ilegítima e ilegal, tentem aproveitar esse risco – que lhes foi comunicado – para violarem os sistemas de segurança das empresas. Por outras palavras, tornar pública a ocorrência de uma situação de potencial risco poderá, em última análise, aumentar esse risco e colocar em perigo os mecanismos de segurança e os direitos dos assinantes e utilizadores.

Ainda relativamente ao Artigo 3.º, a APRITEL gostaria ainda de comentar a opção do legislador em impor ao fornecedor de rede pública de comunicações que sirva de suporte a serviços de comunicações eletrónicas acessíveis ao público prestados por outra empresa, a obrigação de "*satisfazer os pedidos que esta lhe apresente e que sejam necessários para o cumprimento do regime fixado no presente diploma*" quando, reitere-se tal regime não se encontra concretizado. Acresce que não pode o operador de rede ficar sujeito a pedidos por vezes incompatíveis, e com prazos reduzidos, devendo assim o regime ser uniformizado, sendo que os custos de implementação de tal obrigação não poderão naturalmente ser suportados pelo operador de rede.

Esta imposição poderá assim ser um "fardo" bastante pesado que se impõe ao fornecedor de rede pública de comunicações, que se vê obrigado a satisfazer os pedidos de adoção de medidas de segurança que não estão definidas.

D. Cookies

Relativamente aos "cookies" (Artigo 5.º), o legislador optou por estabelecer o regime de *opt-in*, prevendo que se considera como "consentimento" quando o assinante ou utilizador defina, no seu equipamento terminal, opções que permitam o armazenamento ou o acesso à informação armazenada nesse equipamento.

A este respeito a APRITEL gostaria de chamar a atenção para o facto de ser importante distinguir consoante o cookie contenha, ou não, dados pessoais.

Em bom rigor, a recolha deste tipo de informação é, na maioria dos casos, feita de forma anónima, revestindo-se de especial importância para os operadores adaptarem os serviços às necessidade e interesses dos seus clientes. Assim sendo, seria sempre preferível a adoção de um regime que não implicasse uma ação por parte do cliente, sendo-lhe, naturalmente, garantido o direito de oposição.

Acresce que o regime previsto poderá não ser de fácil e simples implementação pelo próprio utilizador, afastando-se assim da intenção do legislador comunitário que impôs que a forma de obtenção do consentimento do titular deveria ser o mais simples possível.

A APRITEL entende, também, que a alínea b) do n.º 3 – *Estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador* – carece de clarificação e concretização, na medida em que a redação proposta é demasiado genérica ("*serviço da sociedade de informação*").

Uma nota final para referir que este regime bastante restritivo limita (ou mesmo elimina) o negócio da publicidade online, que justamente utiliza este tipo de informações para adaptar os seus serviços aos interesses e preferências dos utilizadores.

E Dados de Tráfego e de Localização

No artigo 6º - Dados de Tráfego – prevê-se que as empresas passem a obter expressamente o consentimento prévio dos assinantes ou utilizadores para o tratamento destes dados, embora a Diretiva apenas venha exigir a obtenção prévia deste consentimento, sem que faça qualquer exigência quanto à forma de prestação do mesmo.

Por sua vez, no artigo 7º - Dados de Localização – prevê-se que o consentimento para o tratamento deste tipo de dados seja prévio e expresso. No entanto, na Diretiva agora transposta não se determina qualquer alteração a esta norma e, muito menos no sentido vertido na presente Proposta de Lei, ou seja, de passar a exigir o consentimento "expresso" dos assinantes ou dos utilizadores.

Uma vez que não se vislumbra a razão que leva o legislador nacional a ser mais exigente que o comunitário tendo em conta que com o consentimento prévio os direitos do utilizadores já estão devidamente acautelados, a APRITEL considera que as referidas alterações não devem ser introduzidas, sob pena de se perverterem os objectivos de harmonização destas matérias a nível comunitário

E. Comunicações não solicitadas

As alterações ao regime das comunicações não solicitadas são bastante significativas e levantam inúmeras objeções por parte da APRITEL.

Desde logo a alteração da moldura da coima prevista para a violação destas normas, a qual aumenta exponencialmente de € 2.500 a € 50.000, para de € 5.000 a € 5.000.000 €.

Esta alteração é absolutamente desproporcional e injustificável face à proteção dos bens jurídicos em causa.

Em segundo lugar, o texto do atual artigo 22º do Decreto-Lei n.º 7/2004, de 07 de Janeiro, utiliza de forma indistinta as expressões "marketing direto" e "publicidade" como sendo expressões de sentido equivalente, o que conduzia erradamente a que todo o tipo de mensagens não solicitadas fossem abrangidas pelo mesmo regime.

Na verdade, as mensagens de marketing direto são apenas as mensagens publicitárias dirigidas a alguém com o intuito específico de lhe propor a subscrição de um determinado serviço ou produto enquanto que a mera publicidade se destina a uma divulgação mais genérica, que não inclui necessariamente a aquisição de um produto ou serviço.

Transpondo isto para o plano jurídico, a mensagem de marketing direto aproximar-se-á mais de uma proposta contratual, enquanto que a mensagem publicitária será um convite a contratar.

Uma vez que o texto da Proposta de Lei – de uma forma mais coerente com o texto da Diretiva - passa a fazer exclusivamente referência ao "marketing direto", cremos que seria importante clarificar, eventualmente através de uma definição legal, o significado de "mensagens para fins de marketing direto", uma vez que, como resulta do ora exposto, todas as mensagens de marketing direto são publicidade, mas nem toda as mensagens publicitárias constituem marketing direto, e só a estas últimas é que a Diretiva e texto da Proposta de Lei se aplicam.

Por outro lado, a redação do novo artigo 13-A, n.º 1 estabelece que a receção de comunicações não solicitadas carece do consentimento prévio e por escrito - requisito inovador e que levanta dúvidas quando à forma - independentemente da utilização de sistemas de chamada e de comunicação automatizados que não dependam da intervenção humana.

Isto é, as comunicações não solicitadas para fins de marketing direto, passam a ser proibidas sem o consentimento prévio, quer se usem ou não aqueles sistemas, e não apenas, como se estabelece na Diretiva, "quando" se usem esses sistemas.

Parece-nos preferível, por isso, manter a redação do atual artigo 22º n.º 1 do Decreto-Lei n.º 7/2004, de 07 de Janeiro, que já cumpria os requisitos de transposição do artigo 13 n.º 1 da Diretiva 2000/31/CE, de 08 de Junho, o qual, aliás, na Diretiva 2009/136/CE mantém praticamente a mesma redação, acrescentando-se eventualmente as referências aos envios por SMS ou MMS, referências essas que constavam já dos considerandos da Diretiva 2000/31/CE, de 08 de Junho.

A manutenção da redação do artigo 22º é, também, mais favorável no que diz respeito à ausência da obrigatoriedade do consentimento ser obtido por escrito, requisito este, aliás, que a Diretiva não impõe.

Além disso, este requisito levanta dúvidas quanto à forma (o mesmo poderia ser dado por SMS ou email), e afasta formas alternativas igualmente eficazes de obter esse consentimento, por exemplo, através de uma chamada de IVR ou de uma página na intermeta APRITEL considera, por isso, excessiva a obrigação de recolha de consentimento escrito para este efeito, até porque o mesmo poderá não ser adequado às práticas comerciais atuais que, muitas vezes, se desenvolvem por outras formas.

Refira-se ainda que este regime vai mais além do que a própria Lei de Proteção de Dados Pessoais estabelece para o consentimento para o tratamento de dados pessoais (inclusive dados sensíveis).

Assim, deveria ser eliminada a necessidade de obtenção de consentimento escrito.

O regime das comunicações não solicitadas previa uma importante exceção ao regime geral do *opt in*, quando o cliente tivesse fornecido os seus dados aquando da contratação de um serviço ou compra de um produto.

Nesses casos, o envio de publicidade relacionada com o produto ou serviço contratado, através da utilização de qualquer dado que o cliente tivesse fornecido, não carecia do consentimento prévio do mesmo.

A alteração desta exceção, restringindo-a apenas à utilização do dado de endereço eletrónico é extremamente limitativa, tanto para os remetentes da publicidade, como para os próprios destinatários, que se verão privados de receber, por outros meios, informações bastante úteis, relacionadas com o produto ou serviço que contrataram.

Por outro lado, nem em todas as transações comerciais os consumidores têm oportunidade de fornecer o seu endereço de *email*.

No caso do sector das comunicações, esta alteração é especialmente crítica, dado que a publicidade relacionada com os serviços contratados ou com serviços análogos é quase exclusivamente realizada através do envio de SMS.

Aliás, este é um meio cada vez mais usado pelas empresas para contactar os clientes adquirentes dos seus serviços ou produtos, pelo que a referida alteração se revela altamente prejudicial, tanto para as empresas como para os consumidores, que se verão privados de aceder a informações que são naturalmente do seu interesse.

O n.º 1 do artigo 13º - B vem inverter o sentido da regra atual: a obrigação de ter uma lista de pessoas que tivessem manifestado o desejo de não receber comunicações não solicitadas, passando agora a lista a ser de pessoas que tenham manifestado expressamente o desejo de as receber.

Ora, conforme já indicado, esta alteração traduz-se num impacto significativo para os operadores, os quais implementaram as medidas e realizaram os desenvolvimentos necessários ao cumprimento do regime anterior e agora se veem obrigados a implementar um regime com uma regra precisamente inversa, cujo impacto económico e requisitos de implementação não estão ainda calculados.

No que diz respeito às listas mantidas pela DGC relativas às comunicações não solicitadas, cremos que o regime se torna mais claro, agora que a lista da DGC se destina apenas às pessoas colectivas.

De qualquer forma, isso levanta algumas dúvidas, nomeadamente, quanto ao destino a dar à lista até à data mantida pela DGC de pessoas singulares que não queriam receber comunicações não solicitadas. Ou o que sucede se um cliente deu o seu consentimento posterior nos termos do Artigo 13.º A n.º 1 e o seu nome consta da lista mantida pela DGC.

Nesta situação, entende a APRITEL que deverá valer a ação do titular que, num momento posterior à inclusão na lista da DGC, vem consentir no tratamento de dados para efeitos de comunicações não solicitadas.

Por outro, lado, apesar das cautelas implementadas na organização destas listas, também se levantam dúvidas se estas listas não estarão a servir para empresas menos escrupulosas, obterem precisamente os dados que necessitam para o envio de *spam*.

F. Dever de informação

A Proposta de Lei consagra, nos seus artigos 13.º C e 13.º F, a obrigação de prestação de informações, respetivamente aos assinantes/ utilizadores e às autoridades competentes.

A APRITEL reconhece a importância da disponibilização de informação aos assinantes/ utilizadores.

No entanto, deveria ser concretizado, pelas autoridades competentes, a forma como a informação deve ser prestada, bem como, em particular, consagrar-se a possibilidade desta constar da Política de Privacidade do operador disponível no seu site.

A APRITEL considera que a inclusão desta informação num documento que descreve os termos do tratamento de dados pessoais fará sentido, seguindo-se assim aquelas que são as boas práticas internacionais.

Quanto à informação às autoridades competentes, e impondo a presente Proposta de Lei, pesadas obrigações (também de informação) aos operadores, esta obrigação genérica de prestação de informações deverá ser aplicada com parcimónia, na medida em que poderá, novamente, fazer deslocalizar esforços internos para a resposta aos pedidos de informação, afastando-se assim do propósito principal de qualquer operador – a prestação de serviços de comunicações eletrónicas.

31 de maio de 2012

G Competências do ICP-ANACOM e da CNPD

A Proposta prevê que o ICP-ANACOM e a CNPD tenham competência em diferentes matérias, podendo as duas entidades exercer funções de fiscalização e aplicar sanções.

A APRITEL entende que, em face da sensibilidade das matérias em causa, não deveria existir uma divisão de competências, sugerindo-se, ao invés, que as atribuições e poderes previstos na Proposta sejam da responsabilidade exclusiva de uma das entidades.

Na realidade, e como se sabe, a existência de uma divisão de competências entre diferentes entidades conduz, não raras vezes, a decisões contraditórias e que têm origem, precisamente, em entendimentos diversos.

Como se compreende, este tipo de situações é suscetível de causar atrasos, incerteza jurídica e, inclusivamente, danos nos destinatários das normas, o que, cremos, não é, nem poderá ser, o objetivo do legislador.

A atribuição de competências exclusivas a uma entidade é, do ponto de vista da APRITEL, a solução que melhor se adequa e satisfaz os objetivos e obrigações decorrentes da Diretiva que se transpõe.

H. Incumprimento - em especial a imposição de sanções pecuniárias compulsórias

No que se refere às sanções aplicáveis em caso de incumprimento, a APRITEL gostaria de referir que é fundamental esclarecer o sentido e alcance das alíneas l) e m) do n.º 1 do artigo 14.º, uma vez que as duas normas (idênticas) são demasiado amplas e não indicam qualquer outra disposição normativa onde esteja prevista a obrigação que gera o incumprimento. Acresce que, não se compreende a expressão "legítimos" e que parece ser manifestamente redundante (uma vez que todas as ordens e mandatos deverão ser, por natureza, legítimos).

O regime estabelecido no Artigo 13.º G é manifestamente diferente e mais pesado do estabelecido na Lei de Proteção de Dados Pessoais, constituindo, à semelhança do que sucede com a obrigação de notificação de violações de dados pessoais, um tratamento diferenciado deste setor – o que poderá ser entendido como o reconhecimento (errado) de que este setor é o mais violador da privacidade dos seus clientes.

A imposição de um regime absolutamente penalizante – prevendo desde logo sanções pecuniárias compulsórias – deverá ser precedido da adoção de medidas e diretrizes claras quanto àquelas que são as boas práticas nesta matéria.

Note-se, aliás, que os critérios estabelecidos para fixação da sanção pecuniária compulsória são abstratos, de difícil concretização e existe uma desproporcionalidade manifesta entre o montante mínimo e máximo (excessivo).

31 de maio de 2012

A APRITEL não pode deixar de manifestar a sua preocupação relativamente a este regime de incumprimento quando, como já referido anteriormente, existem inúmeras obrigações que não se encontram claramente concretizadas e detalhadas. Ora, será manifestamente difícil evitar o incumprimento e aferir o cumprimento de uma obrigação, quando tal obrigação não é clara, precisa e determinada.

Lisboa, 31 de maio de 2012