Audiência Prévia

Projeto de decisão sobre segurança e integridade das redes e serviços de comunicações eletrónicas

27 de Janeiro de 2012

Resposta do Grupo Portugal Telecom ao Sentido Provável de Decisão sobre

"Projeto de decisão sobre segurança e integridade das redes e serviços de comunicações eletrónicas"

A. INTRODUÇÃO

O presente documento representa a pronúncia comum das empresas do Grupo Portugal Telecom seguidamente identificadas (doravante "Grupo PT"), em sede de audiência prévia, ao Sentido Provável de Decisão sobre o "*Projecto de decisão sobre segurança e integridade das redes e serviços de comunicações electrónicas*" aprovado pelo Conselho de Administração do ICP-ANACOM, de 22 de Dezembro de 2011, notificado por ofício circular com a referência ANACOM-S104581/2011, de 29 de Dezembro de 2011, constituindo, assim, a resposta conjunta das seguintes empresas:

a) Portugal Telecom, S.G.P.S., S.A.

b) PT Comunicações, S.A.

c) TMN – Telecomunicações Móveis Nacionais, S. A.

B. CONSIDERAÇÕES GERAIS SOBRE O PROJETO DE DECISÃO

Em primeiro lugar, e conforme reconhecido pelo ICP-ANACOM, cumpre salientar que o Projeto de Decisão em apreço vem regular, *ex novo*, uma matéria intrínseca ao próprio funcionamento do setor das comunicações eletrónicas.

Com efeito, e embora do ponto de vista legislativo, a matéria relativa à segurança e integridade das redes e serviços de comunicações eletrónicas assume um maior relevo no novo quadro regulatório nacional e europeu, importa referir que a mesma reveste-se de particular importância para os operadores, na medida em que, cada vez mais, o mercado exige redes e serviços dotados de robustez para suportarem os serviços cada vez mais complexos disponibilizados aos utilizadores finais, sendo que estes, por seu turno, exigem cada vez mais segurança e integridade das redes nas quais se suportam os serviços contratados, constituindo este aspeto um fator relevante no momento da contratação de redes e serviços de comunicações eletrónicas.

Por outro lado, num momento em que o desenvolvimento da sociedade de informação se carateriza pela introdução exponencial de novos serviços e de novas plataformas tecnológicas, cuja interoperação potencia incidentes de segurança e integridade, o Grupo PT entendeu que deveria reforçar o seu compromisso na defesa de valores essenciais, designadamente, em valores como os da segurança e privacidade e da proteção de dados pessoais, pela incontestável importância que têm vindo a assumir em todos os setores de atividade, em particular no domínio das comunicações eletrónicas.

É por esse motivo que Grupo PT tem vindo, nos últimos anos, a realizar investimentos consideráveis na área da segurança da informação, materializados nomeadamente na implementação, em 2010 de processos de gestão de segurança certificados (ISO20000) e na criação de um CSIRT – Computer Security Incident Response Team (csirtPT), reconhecido a nível nacional (Rede Nacional de CSIRTs) e a nível internacional (TI/TERENA). Tais medidas têm permitido, segundo o Processo de Gestão de Incidentes de Segurança, a prevenção, deteção, reação e dissuasão face a incidentes de segurança, entendidos segundo as definições incluídas na norma ISO27000 e do âmbito do csirtPT.

Efetivamente, o Grupo PT tem uma abordagem extremamente cuidadosa no que diz respeito a matérias relativas à segurança e integridade da rede, pelo que tem vindo a aumentar de forma

significativa o investimento em matéria de segurança lógica e física das infraestruturas, plataformas e sistemas de suporte às operações e serviços que presta aos Clientes e, na grande maioria das vezes, em antecipação às obrigações de conformidade com a regulamentação internacional.

As *best practices* apontam no sentido de existência de estruturas autónomas de *compliance*, dentro de cada organização, a quem compete definir, acompanhar e coordenar matérias de segurança e privacidade, bem como estabelecer meios adequados ao eficaz controlo do cumprimento do quadro legal estabelecido. Neste contexto e em linha com as melhores práticas internacionais, o Grupo PT criou um Comité de Segurança e um Comité de Privacidade e de Proteção de Dados Pessoais.

Não pode, pois, o Grupo PT deixar de realçar e reafirmar que reputa da máxima importância todas as questões relacionadas com a Segurança e Integridade de Redes e Serviços, tema esse objeto de especial atenção no processo de reforma do quadro regulatório das comunicações eletrónicas recentemente concluído com a transposição das Diretivas Europeias para o ordenamento jurídico nacional, através da Lei n.º 51/2011 de 13 de Setembro, que altera a Lei n.º 5/2004, de 10 de Fevereiro ("LCE").

Neste contexto, é com agrado que assistimos à consagração, ao nível legal e regulamentar, de medidas que, certamente, contribuirão para reforçar o enfoque dos operadores na adoção de medidas tendentes a assegurar um risco mínimo em termos de segurança e de integridade das respetivas redes. Adicionalmente, não devem ser relegados para segundo plano os claros benefícios que tal atuação terá para o setor, globalmente considerado, porquanto aportará claros benefícios para todos os *stakeholders*.

Contudo, importa que a abordagem legal e regulatória nesta sede não descure os princípios da proporcionalidade e da promoção do investimento eficiente em infraestruturas pelos operadores, devendo igualmente permitir-se aos mesmos operadores algum nível de flexibilidade na implementação das medidas destinadas a assegurar o cumprimento dos objetivos visados pelas normas relativas à segurança e integridade das redes.

A este propósito, não pode o Grupo PT deixar de expressar a sua apreensão quanto aos impactos, financeiros e operacionais que a adoção de algumas medidas de concretização de princípios

válidos e amplamente aceites pode ter nesta sede. Assim, e tendo procedido a uma análise dos possíveis impactos do projeto de Decisão que agora se comenta, entende a PT que o mesmo encerra alguns aspetos relativamente aos quais não pode dar seu acordo.

Desde logo, não se descortinam os motivos subjacentes à opção de o Regulador pretender estabelecer condições (*triggering thresholds*) mais exigentes que os estabelecidos, por exemplo, pelo OFCOM, quer no que respeita à duração do incidente a considerar para efeitos de notificação, quer quanto aos próprios prazos de notificação, e bem assim quanto ao número de notificações que poderão ocorrer e respetivo conteúdo, entre outros aspetos.

Como o ICP-ANACOM não poderá descurar, a implementação dos requisitos necessários a dar cumprimento a tais condições tem associados custos significativos, e que são claramente desproporcionais se ponderado o esforço dos operadores face aos objetivos (benefícios) visados por tais condições. Por outro lado, há igualmente que recorrer ao *benchmark* existente e à ratio inerente à obrigação de notificação – garantir que apenas os incidentes realmente significativos sejam notificados - para avaliar os reais benefícios que poderão advir das notificações, caso a Decisão final venha a ser adotada nos moldes do atual Projeto de Decisão.

Ante o exposto, e sem prejuízo dos comentários e sugestões de ordem mais específica que apresentaremos relativamente a cada um dos anexos do Projeto de Decisão, gostaríamos de começar por tecer os comentários de ordem geral que a seguir melhor descrevemos.

O Grupo PT não pode deixar de começar por expressar a sua apreensão quanto à forma como o ICP-ANACOM está abordar a regulação da segurança e integridade de redes e serviços, através do lançamento desta consulta e dos impactos que tal abordagem pode ter para os operadores, para os utilizadores dos serviços de comunicações eletrónicas e para o mercado em geral.

Neste contexto, o Grupo PT entende que, previamente à definição dos procedimentos de notificação de incidentes de segurança, deveriam ser concretizadas as medidas técnicas consideradas adequadas a que se refere o artigo 54-A da LCE a fim de aferir se elas se consideram adequadas a garantir a integridade das redes e prevenir a ocorrência de incidentes de segurança a que se faz referência na mencionada norma.

Com efeito, o objetivo fundamental subjacente à integração da matéria relativa à Segurança e Integridade de Redes e Serviços no quadro legal europeu (através da Diretiva 2009/136/CE e da

Diretiva 2009/140/CE, ambas de 25 de Novembro de 2009), transposto para o direito nacional, através da LCE, é o de contribuir para criar um ambiente de confiança em torno dos serviços de comunicações eletrónicas, possibilitando o crescimento de muitos serviços suportados nestes meios, como sejam o comércio eletrónico, o *e-government*, e-*health* e outros serviços da sociedade da informação.

Por outro lado, também a definição dos mecanismos de notificação dos incidentes tem, necessariamente, que ser concretizada em função do referido objetivo.

Na verdade, as consequências associadas a um incidente de segurança – sejam em termos de obrigação de notificação/divulgação ao público de um determinado incidente, sejam mesmo em termos de aplicação do regime sancionatório - deveriam ser avaliadas em função do cumprimento ou não, pelo operador, das obrigações definidas ao abrigo do artigo 54º-A da LCE.

Neste domínio, pensamos que deveria ser acolhida uma solução idêntica à que foi adotada na Diretiva ePrivacy, que nos parece muito mais adequada à luz dos objetivos que se pretendem alcançar com a divulgação ao público do incidente de segurança.

Com efeito, a ratio da Diretiva ePrivacy em matéria de notificação de incidentes com impacto na privacidade dos clientes é preventiva, isto é, visa permitir que os clientes adotem precauções para que o incidente não os afete negativamente.

Segundo o artigo 4.º desta Diretiva (ainda não transposta para o direito nacional) (i) a divulgação ao titular só é exigida se afetar negativamente os dados pessoais e a privacidade do assinante e (ii) em qualquer caso, a notificação de uma violação de dados pessoais a um assinante ou outra pessoa afetada não é exigida se a autoridade considerar que o operador tomou as medidas tecnológicas de proteção adequadas e que tais medidas foram aplicadas aos dados a que diz respeito a violação.

Este é, de facto, um regime que nos parece estar mais linha com os objetivos finais subjacentes à regulação das matérias de segurança de rede e que evita situações de alarmismo generalizado injustificado.

Importa, ainda, apontar um aspeto ao nível dos conceitos a LCE, na redação dada pela Lei n.º 51/2011, de 13 de Setembro, não é explícita no que se refere à definição de "violações de

segurança" e "perda de integridade". O texto do projeto de decisão também não contribui para uma clarificação destes conceitos.

Atentando no ponto II do Anexo A do Projeto de Decisão, tendo em atenção que o ICP-ANACOM considera todo o universo de 6 causas possíveis de incidentes, apenas é possível depreender um possível entendimento do conceito de "incidente de segurança" pelo ICP-ANACOM e que englobaria incidentes que podem ou não ser de segurança. Todavia, mesmo tal entendimento não se encontra explícito no documento.

Ora, a este respeito considera o Grupo PT que se afigura essencial o estabelecimento de uma definição concreta de "incidente de segurança", a qual deverá ser densificada consoante os vários serviços visados pela decisão final que venha a ser adotada tendo em conta a criticidade dos mesmos. Na verdade, acreditamos que sem se proceder a uma definição adequada deste conceito, não será possível a obtenção de previsibilidade e, bem assim, a garantia de certeza e segurança jurídicas que devem estar presentes no relacionamento do ICP-ANACOM com os operadores sujeitos às obrigações cujo cumprimento agora é agora concretizado no Projeto de Deliberação em apreço.

Assim, numa primeira sede, e sem prejuízo de podermos sugerir outras definições ao longo dos nossos comentários, o ICP-ANACOM poderia, na decisão final, adotar uma definição de incidente equivalente, no mínimo, à constante da norma ISSO/IEC 27035:2011[1].

Adicionalmente, o Grupo PT constatou que não está igualmente clara a definição dos serviços que se pretende sejam abrangidos pelo Projeto de Decisão e respetivos anexos.

Esta indefinição, consubstanciada numa abrangência demasiado lata do âmbito objetivo do Projeto de Decisão, não permite aos Operadores aferir da real dimensão e dos reais impactos do Projeto de Decisão, quer em termos de custos, quer em termos de período temporal de implementação. Por outro lado, e considerando o valor máximo das coimas que podem ser aplicadas em caso de violação das normas relevantes (€1.000.000), tal abrangência certamente conduzirá a um nível de litigância que não se deseja, sob pena de se colocar em risco a plena

[1] Ao abrigo da norma ISSO/IEC 27035:2011 um incidente de segurança da informação ("Information security incident") é definido nos seguintes termos: "An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security."

eficácia e efetividade dos normativos em questão.

Por outro lado, a aparente amplitude do âmbito objetivo do Projeto de Definição, a manter-se, poderá implicar que os operadores desenvolvam esforços e incorram em custos manifestamente desproporcionados face aos objetivos que pretendem atingir, o que não é de todo despiciendo para os operadores num contexto económico extremamente difícil e em que estes têm realizado investimentos avultados relacionados com a modernização e expansão das respetivas infraestruturas. A este propósito, não podemos deixar de mencionar que, por exemplo, o OFCOM não adotou uma postura tão exigente quanto a do ICP-ANACOM, nem a própria ENISA recomenda a adoção de medidas que impliquem um esforço desproporcionado aos operadores, o que não significa que estas entidades desconsiderem ou relativizem a importância do tema que aqui se aborda.

Nessa medida, e de forma a que na decisão final a adotar nesta sede esteja subjacente o necessário equilíbrio entre os objetivos visados neste âmbito, os interesses dos operadores e os benefícios para o mercado e para os clientes utilizadores de redes e serviços de comunicações eletrónicas, importa que o ICP-ANACOM balize os serviços abrangidos pelas medidas que pretende agora implementar, não podendo descurar igualmente, nesse âmbito, a criticidade dos mesmos. Assim, considera-se importante e necessária a inclusão de uma classificação dos serviços em termos de impacto, tal como o faz, por exemplo, a ENISA na sua proposta de *template* de comunicação, sendo que, na opinião da PT, apenas deveriam ser considerados os seguintes serviços para definição de esquemas de *reporting* de incidentes de segurança:

- Serviço Telefónico Fixo;
- Serviço Telefónico Móvel
- Short Message Services
- Serviço de Acesso à Internet
- Serviço de caixas de correio eletrónico

Ainda no que respeita ao âmbito do Projeto de Decisão, estranhamos a ausência de qualquer menção à delimitação das obrigações a cumprir em termos de comunicação de incidentes,

consoante o operador afetado por incidentes de segurança disponibiliza redes ou serviços de comunicações eletrónicas.

Com efeito, no caso das redes e serviços móveis, importa ter presente o facto de, em Portugal, existirem dois MVNOs, sendo necessário que a Decisão final do ICP-ANACOM claramente delimite o âmbito da responsabilidade de MNOs e MVNOs, relativamente ao cumprimento das obrigações de reporte, tendo em conta os tipos de MVNOs que existem e que podem vir a existir, como é o caso dos "full-MVNOs".

De uma forma geral, as circunstâncias (critérios para obrigatoriedade de notificação) são demasiado genéricas (deveriam ser específicas para cada serviço e ter um objetivo preciso), utilizam um critério geográfico de utilidade discutível e de custo de implementação elevado, fazendo ainda referência a uma série de casos particulares que representam custos adicionais de operacionalização. O facto de as circunstâncias serem idênticas para notificações de clientes e para notificações ao ICP-ANACOM, é revelador da falta de clareza em termos dos objetivos a atingir com a deliberação.

Finalmente, em matéria de notificação ao ICP-ANACOM, o Grupo PT considera que o projeto submetido a consulta pelo ICP-ANACOM implica um esquema de reporte excessivamente burocrático, que deverá ser flexibilizado e aligeirado, de forma a permitir a implementação de um processo de notificação efetivamente eficiente.

No que respeita especificamente à divulgação dos incidentes nos casos em que o ICP-ANACOM considerar que há um interesse público na divulgação dos mesmos, também não pode o Grupo PT concordar com a opção defendida pelo Regulador.

Na verdade, a notificação de um incidente de segurança ao público deve ser vista com especial cuidado, pois a divulgação descontextualizada – muitas vezes as questões de natureza técnica/tecnológica não são adequadamente compreendidas pelos cidadãos - e sem um objetivo específico e legítimo, além de desproporcional, pode ser geradora de um sentimento de insegurança, tendo um efeito exatamente contrário ao pretendido. Pense-se a este respeito no aproveitamento que um incidente de segurança pode ter pelos *media*, sobretudo aqueles que têm uma linha editorial mais sensacionalista.

Ao exposto acresce que já hoje os operadores dispõem de mecanismos de divulgação de informação aos assinantes que sejam afetados por incidentes de segurança com impacto significativo.

Importa igualmente salientar que, de acordo com as disposições legais que regem esta matéria, a divulgação ao público de incidentes de segurança que revistam um especial interesse público é, originariamente, uma obrigação da autoridade reguladora nacional (cf. epígrafe do artigo 54.º-E da LCE). Só quando o Regulador, perante um caso concreto, considere ser do interesse público informar este do incidente, ou eventualmente determinar às empresas que o façam, é que poderá justificar-se impor aos operadores tal divulgação.

Tal é, de resto, confirmado pelo n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE, na redação dada pela Diretiva 2009/140/CE, nos termos do qual "a autoridade reguladora nacional em questão pode informar o público ou exigir que as empresas o façam, sempre que determine que a revelação da violação é do interesse público."

Consequentemente, entende o Grupo PT que a avaliação do interesse público na divulgação de incidentes de violação da segurança de redes e serviços de comunicações eletrónicas deverá ser feita numa base casuística, tendo em conta as caraterísticas, duração e especial gravidade da situação, sob pena de se prejudicar a necessária proporcionalidade da atuação regulatória.

Não pode, assim, a PT acolher a proposta do ICP-ANACOM de, por questões de interesse público, ser necessária a divulgação de todos os incidentes de segurança notificáveis ao abrigo do Anexo A do Projeto de Decisão.

Ainda relativamente à divulgação do incidente ao público, entendemos que é essencial definir um procedimento de comunicação e divulgação ao público articulado como o que se encontra previsto na Diretiva ePrivacy, por forma a que, caso o incidente tenha relevância em matéria de privacidade (o que poderá acontecer em grande parte dos casos), os operadores não sejam obrigados a seguir, em simultâneo, dois procedimentos de notificação distintos consoante a autoridades competentes, com diferentes formatos e conteúdos e sobretudo para garantir que existe uma abordagem integrada do incidente pelas duas autoridades.

Assim, é essencial que as autoridades se coordenem na definição dos procedimentos, de forma a que os recursos internos possam ser canalizados para a situação premente e que importa acautelar – solucionar o incidente.

Não podemos deixar de, nesta sede, manifestar igualmente a nossa discordância quanto ao prazo proposto pelo ICP-ANACOM para a implementação dos mecanismos de reporte e divulgação previstos nos Anexos A e B do Projeto de Decisão.

Na verdade, a implementação das propostas avançadas pelo ICP-ANACOM implica a definição de novos procedimentos internos e de alterações substanciais ao nível de sistemas de informação, para o que o prazo de 30 dias úteis proposto pelo ICP-ANACOM é manifesta e objetivamente inexequível.

Por último, refira-se que, no entendimento do Grupo PT, qualquer decisão adotada pelo Regulador relativamente à matéria ora em apreço deveria resultar dos esforços de coordenação entre o ICP-ANACOM e as empresas de redes e serviços de comunicações eletrónicas, para o que se sugere desde já a constituição de um Grupo de Trabalho integrando todos os interessados, para o que a PT desde já manifesta a sua disponibilidade, de forma a garantir quer a definição de incidentes de segurança a reportar, quer a definição de medidas proporcionais que sejam adequadas à realidade prática do setor e que tomem em consideração a criticidade dos serviços.

C. COMENTÁRIOS AO ANEXO A

"Circunstâncias, formato e procedimentos aplicáveis às exigências de comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público".

I. Circunstâncias

Nos termos do n.º 2 do artigo 54.º-C da LCE, os operadores estão obrigados a notificar ao ICP-ANACOM as violações de segurança ou as perdas de integridade com impacte significativo no

funcionamento das redes e serviços. Para o efeito, o ICP-ANACOM sugere um conjunto de incidentes que deverão ser objeto de notificação.

Em primeiro lugar, tal como sublinhado nos comentários gerais, é essencial que o ICP-ANACOM preveja na decisão final uma definição de "incidente", por forma a possibilitar a correta identificação, pelos operadores, dos eventos que são elegíveis para notificação ao Regulador.

Neste sentido e para este efeito, o Grupo PT propõe que incidente seja definido como "um evento que tem impacto num ou mais elementos de rede com a mesma causa raiz (root cause)".

Por outro lado, é igualmente relevante que seja claramente estabelecido o critério que determina a necessidade de notificação dos incidentes ao ICP-ANACOM. Assim, parece-nos que a decisão final deveria estabelecer que apenas serão objeto de notificação os incidentes que tenham um impacto significativo no funcionamento das redes ou na prestação de serviços ou que afetem a continuidade/disponibilidade das redes e dos serviços.

As definições acima apontadas afiguram-se-nos essenciais para prevenir que um somatório de incidentes não relacionados entre si possa estar abrangido pelos critérios de notificação avançados pelo ICP-ANACOM, para um incidente apenas (por exemplo, através do número de clientes afetados poderá estar-se em presença de mais do que um incidente que em bom rigor pode não ser um incidente de segurança).

Refira-se ainda que a obtenção da informação pretendida pelo ICP-ANACOM e constante do Anexo A implica a adoção de medidas ao nível dos SI's que se reveste de alguma complexidade e que, em certos aspetos, pode revelar-se inviável. Será, eventualmente, o caso da informação relativa à área geográfica afetada por incidente de segurança.

No que respeita especificamente às violações de segurança que o ICP-ANACOM propõe sejam objeto de notificação, temos os seguintes comentários:

1. Violações de segurança/perdas de integridade identificadas na alínea a) do Anexo A

A notificação das violações de segurança/perdas de integridade de acordo com a matriz proposta pelo ICP-ANACOM requer, à partida, um mapeamento nos SI's de nº de clientes e da

respetiva afetação geográfica. Se o primeiro poderá já estar acautelado em alguns OSS, o mesmo pode não suceder relativamente à identificação da área geográfica afetada, como acontece no Grupo PT. A este propósito, refira-se que o desenvolvimento dos SI's para acomodar tal requisito poderá representar um esforço significativo para os operadores, pelo que importa que o Regulador pondere adequadamente os interesses em causa, para decidir avançar com a respetiva implementação.

Ainda no que respeita aos patamares propostos no Projeto de Decisão, considera o Grupo PT que, se aplicados de forma indiscriminada a todos os serviços, os patamares propostos são inadequados. Os limiares devem ser aplicados por serviço, sendo claro o objetivo, e de acordo com a criticidade dos mesmos.

Conforme tivemos oportunidade de mencionar nas considerações gerais, apenas devem ser abrangidos pela decisão final, que o ICP-ANACOM vier a emitir, os serviços já identificados pela ENISA nesta sede[2] (Voz Fixa, Voz Móvel, SMS, Internet, E-mail).

Relativamente à definição dos patamares, e sem prejuízo de o mesmo ser "afinado" no âmbito do Grupo de Trabalho mencionado nas considerações gerais, o Grupo PT desde já propõe que, para os serviços suportados em redes fixas, seja adotado o conceito avançado pela ENISA[3], de combinação de limiares de percentagem de assinantes/acessos afetados e duração do incidente, e que reproduzimos na tabela *infra*:

Duração/ Assinantes/Acessos	**1h - 2h**	**2h - 4h**	**4h - 6h**	**6h - 8h**	**> 8h**
1% a 2% de assinantes/acessos					**X**
2% a 5% de assinantes/acessos				**X**	**X**
5% a 10% de assinantes/acessos			**X**	**X**	**X**
10% a 15% de assinantes/acessos		**X**	**X**	**X**	**X**
> 15% de assinantes/acessos	**X**	**X**	**X**	**X**	**X**

Note-se, no entanto, que podem existir situações fronteira cujas ocorrências podem ser consideradas como uma violação de dados pessoais, para efeitos da Diretiva ePrivacy, não

[2] *Technical Guideline on Reporting Incidents, Cap. 7.1.*
[3] *Technical Guideline on Reporting Incidents, Cap. 5.2.*

sendo claro se podem ser considerados incidentes de segurança para efeitos da Lei das Comunicações Eletrónicas (v.g., phishing).

Importa, igualmente, excluir do âmbito de aplicação da obrigação de notificação os serviços de suporte que sejam prestados sobre a rede de determinado operador, ou seja, na eventualidade de se verificar uma violação de segurança à plataforma de um cliente, prestada sobre a rede de um operador, julgamos que tal ataque não deverá ser considerado como um incidente se segurança que determine a obrigação de ser esse mesmo operador a reportar tal ocorrência.

2. Violações de segurança/perdas de integridade identificadas na alínea b) do Anexo A

O ICP-ANACOM propõe, ainda, que sejam objeto de notificação as violações que afetem a entrega de chamadas para o número único de emergência europeu 112, que direta ou indiretamente, seja dirigida a um ou mais PASP, com duração igual ou superior a 15 minutos.

Partindo do pressuposto de que a "entrega de chamadas" pode ser comprometida por falhas, tanto na origem, como no destino da chamada, de acordo com a proposta do ICP-ANACOM, a indisponibilidade de qualquer linha fixa telefónica ou serviço telefónico móvel por um período igual ou superior a 15 minutos terá de ser reportada.

Ora, uma vez que, tecnicamente, não é possível supervisionar a operacionalidade dos acessos, propomos que para o *reporting* dos incidentes relativos à entrega de chamadas para o número único de emergência europeu 112 se considerem os tempos a partir da data/hora de receção da participação de avaria realizada pelo MAI.

Por outro lado, o Grupo PT considera que não devem estar abrangidos pela alínea b) os incidentes relativos a entrega de chamadas originadas em redes móveis, porquanto se a rede de um operador móvel estiver indisponível, as chamadas para o 112 serão encaminhadas pela rede de outro operador móvel, sendo esta funcionalidade disponibilizada automaticamente nas redes e equipamentos terminais utilizados para acesso ao serviço.

3. Violações de segurança/perdas de integridade identificadas na alínea c) do Anexo A

Relativamente às propostas do ICP-ANACOM plasmadas nas várias subalíneas da alínea c), somos da opinião que:

i. Caso o ICP-ANACOM opte por uma das definições de incidente propostas pelo Grupo PT, nada temos a referir quanto aos incidentes abrangidos por esta subalínea. Mantendo-se a atual redação do projeto de decisão e, em particular, os patamares identificados na tabela em *a)*, entende a PT que o critério avançado pelo Regulador se revela desajustado.

ii. Se afigura objetivamente inviável para os operadores aferirem o impacte acumulado de um incidente nas várias empresas, na medida em que não existem processos, nem sistemas aptos a registar e verificar os incidentes de forma a analisar as suas causas/efeitos e determinar se contribuíram para o mesmo tipo de incidente, nem efetuar a consolidação desses resultados para obter dados quanto ao impacte acumulado. Nesse sentido, propõe-se que este ponto seja eliminado da decisão final do ICP-ANACOM.

iii. Para que o reporte seja possível, as datas "relevantes" devem ser previamente definidas e divulgadas pelo ICP-ANACOM, com a necessária antecedência, em articulação com as entidades relevantes.

Considera-se, igualmente, que só deve haver reporte se os serviços e redes incluídos na tabela do ponto I *a)* forem afetados por um período superior a uma (1) hora.

iv. Propõe, ainda, o ICP-ANACOM que sejam reportados incidentes de segurança que face ao impacte geográfico, nomeadamente nas ilhas das Regiões Autónomas dos Açores e da Madeira, implicam corte no funcionamento das redes e serviços oferecidos por uma empresa numa ilha, com uma duração igual ou superior a 30 minutos, quer se inclua ou não, quanto ao impacte nos assinantes/acessos ou área, num dos patamares definidos na tabela constante da alínea a).

A este propósito, entende o Grupo PT que devem ser reportados os eventos com uma duração superior a uma (1) hora que afetem os serviços e redes incluídos na tabela do ponto I *a)*.

4. Violações de segurança/perdas de integridade identificadas na alínea d) do Anexo A

Deverão igualmente ser objeto de notificação, segundo o ICP-ANACOM, as violações de segurança ou as perdas de integridade reportadas por assinantes às empresas, ou pelas empresas aos seus assinantes, quando esses assinantes são organismos governamentais ou regionais, ou outras entidades relevantes em termos de serviços à sociedade e aos cidadãos (e.g. SIRESP), em termos nacionais ou regionais (Regiões Autónomas dos Açores e da Madeira), com uma duração igual ou superior a 30 minutos.

A este propósito, cumpre salientar que as empresas do Grupo PT, nos contratos celebrados com tais entidades, estão sujeitas a restritas obrigações de confidencialidade, que as impedem de partilhar informação, qualquer que ela seja. Como tal, consideramos que a informação requerida deverá ser recolhida diretamente pelo ICP-ANACOM junto dos Agentes, Organismos e Entidades por si consideradas relevantes em termos de serviços à sociedade e aos cidadãos.

II. Formato e procedimentos

Antes de mais, cumpre mencionar que, na opinião do Grupo PT, em termos globais e considerando sobretudo o número de notificações que podem estar envolvidas no reporte de um incidente, o processo proposto é excessivamente burocrático e mobilizador de esforços que os operadores podem, em alternativa, empregar para ultrapassar os incidentes e minimizar os seus efeitos.

Ao exposto acresce que, face às propostas do ICP-ANACOM nesta sede, se afigura essencial:

1. Definir a quem cabe a responsabilidade de coordenar os esforços de cooperação das empresas cujas redes ou serviços sejam impactados no seu funcionamento por um incidente de segurança;

2. De forma a possibilitar às empresas desenvolverem os esforços de modo a mitigar e a resolver o incidente de segurança, serem previamente compatibilizados os tempos de resposta e prazos para reporte. Sendo um processo algo burocratizado, é importante a salvaguarda de que deve ser dada prioridade à mitigação, podendo a compilação da informação e respetiva notificação ser realizada logo após a resolução do incidente. Aliás, a este propósito, refira-se que o facto de as comunicações serem realizadas por correio eletrónico tem impacto na realização das mesmas. Efetivamente, caso se verifique um incidente de segurança com impacto no funcionamento do serviço de acesso à Internet ou de correio eletrónico, então as notificações só poderão ser realizadas após o restabelecimento de tais serviços.

Relativamente ao meio de submissão das notificações, é nosso entendimento que a submissão por *e-mail* não garante os meios de segurança necessários, nomeadamente quanto ao remetente, integridade e confidencialidade da comunicação.

Com efeito, tratando-se de uma temática de segurança, constitui uma falha grave a não inexistência de diretrizes de comunicação segura (troca de chaves, cifra, validação de autenticidade), que garanta a confidencialidade e integridade da informação transmitida acerca de incidentes de segurança dos operadores.

Neste contexto, o Grupo PT propõe que o ICP-ANACOM adote um meio de transmissão que garanta os meios de segurança necessários, seja pelo fornecimento de uma chave de encriptação para ser utilizada por cada um dos operadores, ou outro método de transmissão adequado. De facto, deverá ser assegurada a articulação da obrigação de notificação com as obrigações de confidencialidade que recaem sobre os operadores. A implementação de uma obrigação de notificação poderá ter efeitos adversos ao nível da confidencialidade, na medida em que a divulgação de informação acerca dos termos em que incidente ocorreu poderá, no limite, comprometer a confidencialidade dos dados pessoais em causa, disponibilizando publicamente informação coberta precisamente por tal obrigação de confidencialidade.

No Projeto de Decisão faz-se igualmente menção a "dados estatísticos disponibilizados trimestralmente ao ICP-ANACOM", não sendo, todavia, percetível o sentido e alcance da mesma. Assim, desde já se solicita ao ICP-ANACOM que clarifique este aspeto, uma vez que os dados fornecidos pelos operadores têm finalidades específicas e determinadas.

Adicionalmente, e de forma a garantir uma harmonização dos relatórios dos diversos operadores, sugerimos que seja disponibilizado um "template" único para as notificações, a ser utilizado por todas as entidades com obrigações de reporte, incluindo os MVNOs, à semelhança da sugestão realizada pela ENISA aos reguladores no seu documento "Technical Guideline on Reporting Incidents".

Conforme já referido nas Considerações Gerais do ponto B, o Grupo PT salienta ainda que é absolutamente essencial definir um procedimento de comunicação e divulgação ao público articulado como aquele que se encontra previsto na Diretiva ePrivacy, por forma a que caso o incidente tenha impacto ao nível da privacidade, os operadores não sejam obrigados a seguir, em simultâneo, dois procedimentos de notificação distintos às autoridades competentes, com diferentes formatos e conteúdos. Dever-se-á ter sempre presente que o objetivo primordial é garantir que existe uma abordagem integrada do incidente pelas duas autoridades.

Sublinhe-se, mais uma vez, que quando o incidente seja qualificado, para efeitos da Diretiva ePrivacy, como tendo um impacto ao nível da privacidade (cuja notificação às autoridades competentes será obrigatória), dever-se-ão criar mecanismos e procedimentos únicos.

No que respeita especificamente às várias notificações propostas pelo ICP-ANACOM, o Grupo PT considera que os prazos devem ser ajustados nos seguintes moldes:

- Notificação inicial – Consideramos que o prazo máximo de duas horas para a notificação deve ser alargado, pelo menos, para oito (8) horas úteis. De facto, o prazo de duas horas parece-nos bastante restritivo, pois, em muitos casos, poderá revelar-se impossível reunir os elementos que o ICP-ANACOM prevê e propõe, no prazo de duas horas, principalmente sendo estas as horas mais críticas no reconhecimento do incidente, dos seus impactos e das formas/meios de o resolver;

- Notificação intercalar de seguimento – Consideramos que o prazo para a notificação intercalar deve ser alterado para 8 horas úteis, após o fim do incidente, se o fim do incidente não tiver já sido comunicado na notificação inicial.

Relativamente à notificação final, é opinião do Grupo PT que a informação a disponibilizar neste âmbito e identificada no Projeto de Decisão deve revestir caráter facultativo, na medida em que, por exemplo, a área geográfica afetada é uma informação que nem sempre é possível precisar.

III. Entrada em vigor

Relativamente ao prazo proposto pelo ICP-ANACOM para implementação das medidas necessárias ao cumprimento do disposto na decisão final (30 dias úteis contados da data da notificação final), atendendo ao impacto que as medidas propostas têm, consideramos que o prazo mínimo para a sua implementação nunca poderá ser inferior a 180 dias contados a partir da data da notificação da decisão final.

Nesse sentido, desde já se apela ao ICP-ANACOM que considere um prazo de implementação de, no mínimo, 6 meses.

D. COMENTÁRIOS AO ANEXO B

"Condições em que o ICP-ANACOM considera existir um interesse público na divulgação ao público, por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações electrónicas acessíveis ao público, das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços, e conteúdo, meios e prazos relativos à referida divulgação".

I. Circunstâncias

Em termos gerais, o Grupo PT gostaria de salientar que a notificação aos utilizadores é, compreensivelmente, um ponto sensível para os operadores que têm como objetivo máximo ganhar e manter a confiança e preferência dos utilizadores nos seus serviços.

De facto, e sem prejuízo das considerações já tecidas no ponto B acima, salientamos que o objetivo da implementação de mecanismos de notificação de incidentes de segurança deverá ser

o de proteger os utilizadores quando tais incidentes possam provocar danos e permitir aos clientes a adoção de medidas para evitar/minimizar os danos decorrentes dos incidentes.

Assim sendo, e de forma a evitar um clima de desconfiança generalizada em relação aos operadores, a notificação aos clientes apenas deveria ser imposta quando, precisamente, exista um risco real do incidente provocar danos e quando tal notificação apresente vantagens reais para os clientes.

Como tal, ao invés de uma abordagem "cega" de determinação da obrigação de notificação ao público baseada em números, dever-se-ia prever um mecanismo de notificação ao público apenas quando tal notificação possa impedir ou prevenir eventuais danos.

Por outro lado, a aplicação dos mesmos critérios/patamares utilizados para comunicar à ARN parece-nos inapropriado. Como referido nos comentários ao Anexo A, o tipo de serviço deve ser um fator a considerar nas comunicações à ARN, sendo que para cada tipo de serviço devem, igualmente, ser definidos patamares específicos.

Acresce que, à semelhança do mecanismo de notificação de incidentes com impacto ao nível da privacidade previsto na Diretiva ePrivacy, a adoção preventiva de medidas técnicas deveria ser tida em consideração pelo ICP-ANACOM no momento de determinação da obrigação de notificação do incidente aos clientes.

Como já referido, a Diretiva ePrivacy estabelece que a notificação ao público de um incidente com impacto ao nível da privacidade não é exigida se a autoridade considerar que o operador provou cabalmente ter tomado as medidas tecnológicas de proteção adequadas e que tais medidas foram aplicadas aos dados a que diz respeito a violação.

Por outro lado, a abordagem proposta pelo ICP-ANACOM neste âmbito afigura-se demasiado restritiva e onerosa, pelo que desde já se propõe que seja ponderada a adoção de uma abordagem semelhante à do OFCOM, que parece ter deixado aos operadores alguma margem de liberdade de atuação, ou que seja claramente estabelecido que apenas estão sujeitos a esta divulgação incidentes graves que afetem o acesso ao 112.

Acresce que o "interesse público" depende dos horários em questão. A título de exemplo, o "interesse público" na divulgação a clientes de um "incidente de segurança" com afetação de

serviço entre as 6h00 e as 6h15 poderá ser negligenciável. Mas poderá não o ser, caso ocorra entre as 20h00 e as 20h15.

Por último, uma análise por serviço e respetiva criticidade deve ter ajustada aos meios de divulgação. Assim, a utilização de IVR, de sms, site na internet, etc. devem ser tidos em consideração consoante o serviço envolvido e a criticidade da situação.

II. Conteúdo, meios e prazos para a divulgação

Relativamente ao conteúdo, meios e prazos, temos os seguintes comentários:

- Conteúdo - A informação a disponibilizar deve ser esclarecedora para o público e tão precisa quanto possível, contendo nomeadamente o prazo expectável de resolução, que deve ser posteriormente atualizado para um novo prazo, se aplicável, e, após a resolução, para o prazo que efetivamente se vier a verificar.

  A este respeito, reiteramos o já referido no ponto A *supra*.

- Meios - Relativamente aos meios, não é clara a obrigatoriedade de "contacto telefónico específico". Importa, assim, que o ICP-ANACOM clarifique se está em causa, designadamente, munir os call centers com a informação a disponibilizar aos clientes, se os operadores estão obrigados a contactar telefonicamente os clientes afetados ou se poderão proceder ao envio de SMS para clientes.

  O Grupo PT entende que os meios de divulgação/notificação aos clientes deverão ser determinados, caso a caso, tendo em consideração o tipo de incidente e o nível de criticidade do mesmo.

- Prazos - Consideramos que a divulgação telefónica e na web, no prazo máximo de 1 hora após a deteção do incidente. é um requisito excessivo e que, na maioria dos casos, será inexequível.

Por outro lado, a divulgação a clientes no prazo máximo de 1 hora após a deteção do incidente constitui um prazo bastante exigente para uma divulgação com elevado risco para a imagem dos operadores.

Acresce que a manutenção do aviso do incidente na página web do operador pelo prazo de 6 meses afigura-se absolutamente excessiva. A ratio da notificação ao cliente será a de avisar este que o incidente, com impacto, ocorreu e deverá, antes de mais, permitir ao cliente adotar as medidas necessárias para minimizar e/ou eliminar os impactos negativos do incidente. No prazo de 6 meses, certamente, que tal objetivo terá sido alcançado. A manutenção de tal aviso por prazo excessivo poderá ter um impacto negativo acentuado no negócio do operador e, em particular, no nível de confiança dos atuais e potenciais clientes do operador, não se vislumbrando qualquer benefício que possa advir da manutenção dessa informação por tempo tão alargado.

III. Entrada em vigor e disposição transitória

Relativamente ao prazo proposto pelo ICP-ANACOM para implementação das medidas necessárias ao cumprimento do disposto na decisão final (30 dias úteis contados da data da notificação final), atendendo ao impacto que as medidas propostas têm, designadamente ao nível da necessidade de criação de procedimentos e de desenvolvimentos de sistemas de informação, consideramos que o prazo mínimo para a sua implementação nunca poderá ser inferior a 180 dias contados a partir da data da notificação da decisão final.

Nesse sentido, desde já se apela ao ICP-ANACOM que considere um prazo de implementação de, no mínimo, 6 meses, a contar da data de notificação.

O prazo de 6 meses deverá ser, igualmente, aplicável à comunicação dos contactos telefónicos e respetivo endereço web das empresas, na medida em que estes elementos serão definidos no âmbito da implementação das medidas que o ICP-ANACOM venha a determinar na decisão final sobre a presente matéria.