ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

Excelentíssimo Senhor
Deputado Paulo Mota Pinto
Presidente da Comissão de Assuntos Europeus

Ofício n.º 793/XII/1ª – CACDLG /2013 **Data: 12-06-2013**

ASSUNTO: Relatório – JOIN(2013)1.

Para os devidos efeitos, junto se envia relatório referente à *"Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido"* [**JOIN(2013)1**], que foi aprovado por unanimidade, registando-se a ausência do PEV, na reunião de 12 de junho de 2013 da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias.

Com os melhores cumprimentos,

O PRESIDENTE DA COMISSÃO

(Fernando Negrão)

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias
Assembleia da República – Palácio de São Bento
1249-068 Lisboa
Tel. 21 391 95 30/96 67 / Fax: 21 393 69 41 / E-mail: Comissao.1A-CACDLGXII@ar.parlamento.pt

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

RELATÓRIO

Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido – JOIN (2013) 1

I. Introdução

A Comissão de Assuntos Europeus, em cumprimento com o estabelecido na Lei n.º 43/2006, de 25 de Agosto, alterada pela Lei n.º 21/2012, de 17 de Maio, relativa ao "*Acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia*", e nos termos previstos no n.º 2 do artigo 7.º da citada Lei, remeteu à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, para a emissão de parecer fundamentado, a JOIN (2013) 1 - Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido.

II. Apreciação da iniciativa

1. Enquadramento

A Comunicação da Comissão insere-se na designada Agenda Digital para a Europa que, enquadrada na estratégia Europa 2020, afirma como objetivo o estímulo da economia digital e a resposta aos desafios sociais através das Tecnologias de Informação e Comunicação.

Reconhecendo a importância da Internet e do ciberespaço na vida dos cidadãos, das instituições e das empresas, bem como a necessidade de assegurar que o ciberespaço permaneça aberto e livre, a Comunicação identifica a necessidade de definição de uma

Estratégia da União Europeia para a cibersegurança, afirmando que *"os direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço"*, devendo aplicar-se *"no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico"*.

Afirma-se simultaneamente que se trata de uma realidade essencial ao crescimento económico, reconhecendo-se mesmo como *"a espinha dorsal do nosso crescimento económico"* e *"um recurso crítico de que todos os setores económicos dependem"*, com destaque para setores fundamentais como as finanças, saúde, energia ou transportes.

A concretização do mercado Único digital ou o aprofundamento da comunicação em nuvem são identificados como objetivos de particular relevância económica, afirmando-se a necessidade de proteção do ciberespaço contra *"ataques criminosos, politicamente motivados, terroristas ou patrocinados por Estados, assim como catástrofes naturais e erros involuntários"*.

Como fundamento da necessidade de intervenção neste domínio, são identificados elementos caracterizadores da evolução da realidade bem como alguns fatores de vulnerabilidade do ciberespaço:

a) O aumento a um ritmo alarmante dos incidentes de cibersegurança e a potencial perturbação da prestação de serviços essenciais como a água, a eletricidade ou os cuidados de saúde;

b) A repercussão económica da cibercriminalidade contra o setor privado, em crescente sofisticação e por vezes associada a fenómenos de espionagem económica ou até patrocinada por Estados;

c) A utilização abusiva do ciberespaço por governos de países que não pertencentes à UE para vigiar e controlar os seus próprios cidadãos, domínio em que se entende que a UE pode contrariar tal realidade promovendo a liberdade em linha e garantindo o respeito dos direitos fundamentais em linha.

A Comunicação reconhece a ação dos governos ao longo do tempo na adoção de medidas destinadas a garantir a necessária proteção e afirma a necessidade de projetar essas estratégias nacionais de cibersegurança numa dimensão internacional.

Nesse sentido, são apontados como princípios que devem orientar a política de cibersegurança na UE e a nível internacional:

1. Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade;
2. Assegurar a todos o acesso à internet e a um fluxo de informações livre;
3. Assegurar uma governação multilateral, democrática e eficiente;
4. Partilhar a responsabilidade para garantir a segurança.

2. Prioridades estratégicas e acões

A estratégia apresentada pela Comissão estrutura-se em cinco prioridades, visando a resposta aos desafios identificados:

1. Garantir a resiliência do ciberespaço

2. Reduzir drasticamente a cibercriminalidade

3. Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD)

4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança

5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

2.1. Garantir a resiliência do ciberespaço

A Comunicação sublinha a importância das medidas de desenvolvimento da política de segurança das redes e da informação (SRI), particularmente pelo seu impacto económico e na segurança interna.

Refere-se igualmente a necessidade de reforço e modernização do mandato da Agência Europeia para a Segurança das Redes e da Informação, ENISA, criada em 2004, através de um novo regulamento que está a ser negociado pelo Conselho e pelo Parlamento. Registando-se as lacunas existentes em toda a UE, nomeadamente em termos de meios disponíveis a nível nacional, de coordenação em caso de incidentes que ultrapassem as fronteiras e de envolvimento e preparação do setor privado, a estratégia sob escrutínio é acompanhada por uma proposta legislativa visando:

a) Estabelecer requisitos mínimos comuns para a SRI (segurança das redes e da informação a nível nacional;

b) Criar mecanismos coordenados de prevenção, deteção, atenuação e resposta, que permitam a partilha de informações e a assistência mútua entre as autoridades nacionais competentes em matéria de SRI;

c) Melhorar o grau de preparação e a participação do setor privado.

É referido o papel do Mecanismo Interligar a Europa que concederá apoio financeiro a infraestruturas fundamentais, ligando as capacidades dos Estados-Membros em matéria de SRI e facilitando a cooperação em toda a UE.

Afirma-se a necessidade de realizar exercícios de simulação de incidentes informáticos ao nível da UE para treinar a cooperação entre os Estados-Membros e o setor privado.

Por fim, refere-se ainda a necessidade de reforço de ações de sensibilização dos utilizadores finais.

2.2. Reduzir drasticamente a cibercriminalidade

Neste âmbito sublinha-se a necessidade de a UE e os Estados-Membros se dotarem de uma legislação rigorosa e eficaz para combater a cibercriminalidade. A Convenção do Conselho da Europa sobre Cibercriminalidade – Convenção de Budapeste – é identificada como um tratado internacional que fornece um quadro adequado para a adoção da necessária legislação nacional.

São ainda sublinhadas medidas legislativas como a adoção que se prevê para breve de uma diretiva relativa a ataques contra os sistemas de informação, bem como a adoção de legislação relativa à cibercriminalidade, nomeadamente a diretiva relativa à luta contra a exploração sexual das crianças em linha e a pornografia infantil. A UE está também prestes a chegar a acordo sobre.

Por outro lado, é identificada a rápida aceleração da evolução das técnicas de cibercriminalidade, reconhecendo-se que as agências responsáveis não conseguem combater a cibercriminalidade com ferramentas operacionais ultrapassadas, pelo que se torna fundamental a disponibilização de meios operacionais acrescidos.

É ainda destacada a necessidade de reforçar a coordenação e cooperação a nível da EU entre autoridades judiciais e policiais e agentes públicos e privados com interesse direto nestas questões.

A Comissão afirma assim a intenção de:

a) Assegurar a transposição e a implementação rápidas das diretivas relativas à cibercriminalidade;

b) Instar os Estados-Membros que ainda não ratificaram a Convenção do Conselho da Europa sobre Cibercriminalidade a ratificarem e aplicarem as suas disposições o mais depressa possível;

c) Através dos seus programas de financiamento, apoiar os Estados-Membros na identificação das lacunas e no reforço da sua capacidade para investigar e combater a cibercriminalidade. Além disso, a Comissão irá apoiar os organismos que fazem a ligação entre a investigação/as universidades, os agentes policiais/judiciais e o setor privado, cujo trabalho tem afinidades com o atualmente realizado pelos centros de excelência para a cibercriminalidade já criados em alguns Estados-Membros e que são financiados pela Comissão;

d) Juntamente com os Estados-Membros, coordenar os esforços para identificar as melhores práticas e as melhores técnicas disponíveis, inclusivamente com o apoio do JRC, para combater a cibercriminalidade (por exemplo, no que diz respeito ao desenvolvimento e à utilização de ferramentas forenses ou à análise das ameaças);

e) Trabalhar em estreita cooperação com o recém-criado Centro Europeu da Cibercriminalidade (EC3), no quadro da Europol e com a Eurojust para harmonizar tais abordagens políticas com as melhores práticas na esfera operacional;

f) Apoiar o recém-criado Centro Europeu da Cibercriminalidade (EC3), enquanto ponto focal europeu no combate à cibercriminalidade. O EC3 fornecerá análises e informações (Intelligence), apoiará as investigações, garantirá investigação forense de elevado nível, facilitará a cooperação, criará canais para a partilha de informações entre as autoridades competentes dos Estados-Membros, o setor privado e outras partes interessadas e assumirá progressivamente o papel de porta-voz das forças policiais.

g) Apoiar os esforços para melhorar a prestação de contas dos agentes de registo de nomes de domínio e garantir a exatidão das informações sobre a propriedade dos sítios Web, nomeadamente com base nas recomendações *Law Enforcement Recommendations* à ICANN (Internet Corporation for Assigned Names and Numbers), em conformidade com o direito da União, incluindo as regras da proteção de dados.

h) Tirar partido da legislação recente para intensificar os esforços da UE no combate aos abusos sexuais de crianças em linha. A Comissão adotou uma estratégia europeia destinada a melhorar a Internet para as crianças e, juntamente com os países da União Europeia e outros, lançou uma aliança mundial contra os abusos sexuais de crianças em linha. A Aliança é um veículo para outras ações dos Estados-Membros apoiadas pela Comissão e pelo Centro Europeu da Cibercriminalidade.

Além disso, a Comissão entende ser necessário junto de outras entidades/instituições solicitar intervenção, nomeadamente:

A Comissão pede à Europol (EC3) que:

a) Inicialmente focalize a sua análise e o seu apoio operacional às investigações da cibercriminalidade efetuadas pelos Estados-Membros de modo a ajudar a desmantelar e a desorganizar as redes de cibercriminalidade principalmente nas áreas do abuso sexual de crianças, das fraudes nos pagamentos, dos «*botnets*» e da intrusão.

b) Elabore regularmente relatórios estratégicos e operacionais sobre as tendências e as novas ameaças, para identificar as prioridades e definir alvos para a atividade de investigação das equipas dos Estados-Membros especializadas em cibercriminalidade.

A Comissão pede à Academia Europeia de Polícia (CEPOL) que, em cooperação com a Europol:

a) Coordene a conceção e o planeamento de cursos de formação para dotar os órgãos policiais/judiciais dos conhecimentos e competências especializadas necessários para combater eficazmente a cibercriminalidade.

A Comissão pede à Eurojust que:

a) Identifique os principais obstáculos à cooperação judiciária em matéria de investigações da cibercriminalidade e à coordenação entre os Estados-Membros e com

os países terceiros e apoie a investigação e a repressão da cibercriminalidade, tanto ao nível estratégico como operacional, assim como as atividades de formação neste domínio.

A Comissão pede à Eurojust e à Europol (EC3) que:

Cooperem estreitamente, nomeadamente através do intercâmbio de informações, para aumentar a sua eficácia no combate à cibercriminalidade, de acordo com os respetivos mandatos e competência.

2.3. Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD)

A Comissão afirma que os esforços da UE no domínio da cibersegurança devem também envolver a dimensão da ciberdefesa, destacando a necessidade de o desenvolvimento de capacidades de ciberdefesa deve centrar-se na deteção de ameaças informáticas sofisticadas, na resposta a dar e na recuperação posterior.

Afirma ainda a necessidade de melhorar sinergias entre as abordagens civil e militar na proteção dos ativos informáticos críticos, num esforço apoiado pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da UE.

A Comissão afirma pretender explorar as possibilidades de a UE e a NATO complementarem os seus esforços para aumentar a resiliência das infraestruturas críticas das Administrações, da defesa e outras infraestruturas informáticas das quais dependem os membros de ambas as organizações.

2.4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança

A Comissão reconhece que muitos dos líderes mundiais em matéria de produtos e serviços TIC inovadores estão sedeados fora da UE, existindo o risco de a Europa se tornar excessivamente dependente não só de TIC produzidas noutros países mas também de soluções de segurança desenvolvidas fora das suas fronteiras.

A Comunicação sublinha a importância de garantir que os componentes de *hardware* e *software* produzidos na UE e em países terceiros que são utilizados em serviços e infraestruturas críticos, e também em dispositivos móveis, sejam de confiança, seguros e garantam a proteção dos dados pessoais.

A promoção de um mercado único dos produtos de cibersegurança é assim assumida pela Comissão como um passo necessário para atingir aquele objetivo, a par da promoção dos investimentos em I&D e em inovação.

2.5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

Afirmando que a preservação de um ciberespaço aberto, livre e seguro é um desafio de dimensão mundial a que a UE deve responder conjuntamente com os parceiros e organizações internacionais relevantes, com o setor privado e com a sociedade civil, a Comissão diz pretender:

a) promover a abertura e a liberdade da Internet;

b) encorajar os esforços tendentes a estabelecer normas de comportamento e aplicar as leis internacionais em vigor no ciberespaço;

c) tudo fazer para reduzir a clivagem digital e participar ativamente nos esforços internacionais para construir capacidade de cibersegurança.

d) que o envolvimento internacional da UE nas questões que dizem respeito ao ciberespaço pautar-se-á pelos valores fundamentais da UE, a saber, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos fundamentais.

Assim, a Comissão pretende ver integradas as questões do ciberespaço nas relações externas e na política externa e de segurança comum (PESC) da EU, atribuindo uma importância renovada ao diálogo com países terceiros, procurando assegurar um nível elevado de proteção dos dados, nomeadamente em caso de transferência de dados pessoais para um país terceiro.

A UE procurará, nomeadamente, uma cooperação mais estreita com organizações como o Conselho da Europa, a OCDE, a ONU, a OSCE, a NATO, a UA, a ASEAN e OEA. A nível bilateral, a Comissão afirma que a cooperação com os Estados Unidos é particularmente importante e será mais desenvolvida, nomeadamente no contexto do Grupo de Trabalho UE-EUA para a Cibersegurança e a Cibercriminalidade.

Destacando a promoção do ciberespaço enquanto espaço de liberdade e de direitos fundamentais como um dos principais elementos da política internacional da UE no domínio do ciberespaço, a Comissão afirma que o aumento da conectividade mundial não deve ser acompanhado de censura ou de vigilância das populações, pelo que a UE deve promover a responsabilidade social das empresas e lançar iniciativas internacionais para melhorar a coordenação a nível mundial neste domínio.

Assim, a UE não apela à criação de novos instrumentos jurídicos internacionais para as questões do ciberespaço, sublinhando antes a necessidade de respeitar "em linha" as obrigações legais consagradas no Pacto Internacional sobre os Direitos Civis e Políticos, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais da União Europeia.

Destaca-se ainda a necessidade de reforço das capacidades em matéria de cibersegurança e desenvolvimento de infraestruturas informáticas resilientes nos países terceiros.

3 – Funções e responsabilidades

Por fim a Comissão destaca a importância de clarificar os papéis e as responsabilidades dos muitos atores envolvidos, afirmando a exigência de coordenação entre três planos de intervenção distintos mas complementares: o dos Estados, o da União e o da coordenação no plano internacional.

Reconhecendo aos governos nacionais melhor posição para organizar a prevenção e a resposta aos incidentes e ataques informáticos e para estabelecer contactos e redes com o setor privado e o grande público através dos canais estabelecidos e dos quadros legais, a Comissão afirma a necessidade de envolvimento da UE como fator de superação de obstáculos resultantes de diferentes quadros legais, devendo tais intervenções articular-se em torno de três pilares fundamentais: a SRI, a repressão e a defesa.

A Comissão desenvolve e caracteriza os diferentes níveis – nacional, da União e internacional – desta coordenação entre as autoridades competentes em matéria de SRI/CERT, as autoridades policiais e o setor da defesa.

Ao nível nacional afirma que os Estados-Membros devem dispor de estruturas preparadas para garantir a resiliência do ciberespaço, combater a cibercriminalidade e prover à defesa e devem atingir o nível de capacidade necessário para lidar com incidentes informáticos, sendo necessário otimizar a coordenação entre os diferentes ministérios. Os Estados-Membros devem definir, nas suas estratégias nacionais de cibersegurança, o papel e as responsabilidades das suas várias entidades nacionais.

A partilha de informações entre as entidades nacionais e com o setor privado deve ser encorajada, devendo prever-se nos planos nacionais de cooperação em matéria de SRI a ativar em caso de incidentes informáticos que os Estados-Membros possam atribuir claramente os papéis e as responsabilidades e otimizar as ações de resposta.

Ao nível da UE, sublinha-se a importância de encorajar a coordenação e a colaboração entre a ENISA, a Europol/EC3 e a AED numa série de domínios em que estão conjuntamente envolvidas, devendo estas agências, conjuntamente com a equipa CERT-UE, a Comissão e os Estados-Membros, apoiar o desenvolvimento de uma comunidade de confiança de peritos técnicos e políticos neste domínio.

Por fim, ao nível internacional a Comissão e a Alta Representante devem procurar garantir uma ação internacional coordenada no domínio da cibersegurança.

III. Opinião do Relator

A estratégia da União Europeia para a Cibersegurança, apontada na Comunicação da Comissão, assenta na consideração da utilização de dispositivos eletrónicos e sistemas de

comunicação digital como fator de crescimento económico, fonte de lucro, elemento de potencial desenvolvimento de "mercados únicos" ou espaço de disputas económicas entre grandes corporações ou mesmo Estados, desconsiderando o que deveria ser central: os perigos e vulnerabilidades a que os cidadãos são sujeitos em matéria de proteção da reserva e intimidade da vida privada, nomeadamente no que respeita à proteção de dados pessoais.

Afirmando inúmeras preocupações com atividades designadas de "cibercriminosas" – cuja caracterização no entanto nunca é satisfatoriamente efetuada – a Estratégia aborda os problemas decorrentes das quebras ou ataques à segurança das comunicações eletrónicase dos sistemas informáticos primordialmente pelos perigos e riscos que daí decorrem para o funcionamento da economia e do Estado, para o desenvolvimento dos mercados e dos serviços.

A Estratégia foca-se em particular nos riscos e perigos a que estão expostas as grandes corporações e grupos transnacionais nas suas atividades por natureza potencialmente geradoras de maiores proveitos mas igualmente sujeitas a maiores vulnerabilidades.

Não é, assim, de estranhar que na caracterização da situação em matéria de cibersegurança e de evolução do designado cibercrime se "nivelem" as preocupações com as liberdades individuais e de expressão e a "espionagem industrial", ainda que só a final e de forma relativamente superficial se abordem aquelas primeiras preocupações.

Tratando-se os dispositivos eletrónicos e seus sistemas de comunicação digital de sistemas automáticos, passíveis portanto de ser vítimas de ataques massivos, as técnicas de ataque, por serem igualmente automáticas, são de fácil difusão, não carecendo praticamente de especial qualificação para serem aplicadas.

Por outro lado, a amplitude e densidade da informação e o seu valor económico tornam apetecível o mais dispendioso dos ataques, particularmente quando dirigido contra uma base de dados com alguns milhões de entradas uma vez que não só a probabilidade de sucesso do ataque se vê grandemente acrescida, como, e isso é o fundamental, o proveito do mesmo ataque bem sucedido é enormemente recompensado.

O problema é, pois, o de saber qual a eficácia que é possível (ou desejável?) garantir na proteção de direitos, liberdades e garantias dos cidadãos há muito existentes e consagrados, agora no âmbito destes meios digitais de tratamento de informação, sem que os curadores dessa informação sejam, por um lado, obrigados a defender esta informação tão eficazmente quanto o conhecimento e a técnica atuais permitem – impedindo práticas de desproteção para poupança de custos – e, por outro lado, responsabilizados sempre que um ataque é levado a cabo com sucesso e gerando danos por vezes permanentes aos cidadãos a quem a informação violada pertencia.

A realidade tem confirmado estes aspetos como centrais no debate em torno da designada cibersegurança, registando-se a insuficiência de organismos de observação e certificação –

como aliás a Comunicação refere – bem como de legislação e mecanismos preventivos e sancionatórios coerentes e adequados.

Neste quadro, o desafio de garantir aos cidadãos a proteção adequada de direitos que se reconhecem fundamentais é necessariamente contraditório com o desenvolvimento desregulado de novas áreas ou práticas económicas que, a coberto do combate ao cibercrime ou da cibersegurança, pretendem afinal garantir apenas a máxima proteção possível à exploração económica da utilização de dispositivos eletrónicos e sistemas de comunicação digital.

A par da superação de alguma vacuidade na identificação dos objetivos a atingir e meios a mobilizar que sobressaem na análise da referida Estratégia, importará – talvez até de forma prévia – assegurar que o quadro legal, os respetivos mecanismos de proteção dos cidadãos e os organismos de fiscalização não venham a ficar à mercê de quem beneficia com a sua ineficácia ou violação, nomeadamente dos interesses económicos que frequentemente motivam os descritos ciberataques com objetivos de violação da privacidade dos cidadãos ou venda de produtos de cibersegurança.

O que deve motivar o aprofundamento da reflexão em torno do caráter público dos referidos organismos, com a desejada participação das instituições e ensino e investigação mas assegurando também a ligação aos agentes económicos com atuação nesta área.

Tal abordagem permitiria recentrar a abordagem da cibersegurança naqueles que são os direitos fundamentais dos cidadãos, europeus ou não: o direito à privacidade e à reserva da intimidade da vida privada.

IV – Parecer

Princípio da subsidiariedade

A Comunicação incide sobre matéria que suscitará, certamente, no futuro intervenção legislativa da União Europeia, sobretudo considerando o conteúdo da estratégia apontada pela Comissão para a cibersegurança em termos de coordenação ao nível da UE e a nível internacional.

No entanto, não se tratando de iniciativa legislativa, não cabe proceder à apreciação do princípio da subsidiariedade.

Face ao exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias é de parecer:

a) Que a *Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a*

Cibersegurança: Um ciberespaço aberto, seguro e protegido – JOIN (2013) 1 não suscita apreciação do princípio da subsidiariedade;

b) Que o presente relatório deve ser remetido à Comissão de Assuntos Europeus.

Palácio de S. Bento, 12 de Junho de 2013

O Deputado Relator

(João Oliveira)

O Presidente da Comissão

(Fernando Negrão)