Aníbal Manuel da Costa Fernandes

A dimensão política da Segurança para o Ciberespaço na União Europeia:

A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE-OTAN

Universidade dos Açores

DEPARTAMENTO DE HISTÓRIA,
FILOSOFIA E CIÊNCIAS SOCIAIS

Ponta Delgada

2014

Aníbal Manuel da Costa Fernandes

A dimensão política da Segurança para o Ciberespaço na União Europeia:

A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE-OTAN

Dissertação Realizada para Obtenção do Grau de Mestre em Relações Internacionais pela Universidade dos Açores (6.º Edição 2012/2014)

Orientadores: **Carlos Eduardo Pacheco Amaral**, Professor Associado com Agregação do Departamento de História, Filosofia e Ciências Sociais da Universidade dos Açores;

António José Telo, Professor Catedrático da Academia Militar da República Portuguesa

Universidade dos Açores

DEPARTAMENTO DE HISTÓRIA,
FILOSOFIA E CIÊNCIAS SOCIAIS

Ponta Delgada

2014

Anexos

Conteúdo

A.i – Compilação não exaustiva da Legislação, Regulamentação e *Governance* (LRG) referenciada no texto

Código	**LRG0A**
Área(s)	**Data Protection**
Data	24/10/1995
Referência	Diretiva de Pretección de Datos 95/46 CEE
Descrição	*on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
URL	http://ec.europa.eu/justice/policies/privacy/docs/95-46-CE/dir1995-46-+art1-es.pdf ; Acedido em 27/12/2014

Código	**LRG01**
Área(s)	**CybCr**
Data	26/01/2001
Referência	Comission Communication COM(2000) 890 final
Descrição	*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2000:0890:FIN:EN:PDF; Acedido em 24/02/2014

Código	**LRG02**
Área(s)	**eSocEU[>2007-NIS]**
Data	06/06/2001
Referência	Comission Communication COM(2001) 298 final
Descrição	*Network and Information Security:Proposal for A European Policy Approach / Segurança das Redes e da Informação: Proposta de abordagem de uma política Europeia*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2001:0298:FIN:EN:PDF; http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2001:0298:FIN:PT:PDF; Acedido em 24/02/2014
Obs.	COMUNICAÇÃO DA COMISSÃO AO CONSELHO, PARLAMENTO EUROPEU, COMITÉ ECONÓMICO E SOCIAL E COMITÉ DAS REGIÕES

Código	**LRG02a**
Área(s)	**eSocEU[>2007-NIS**[Telecoms]**]**
Data	07/03/2002
Referência	Comission Communication 2002/21/EC
Descrição	*common regulatory framework for electronic communications networks and services*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:NOT;Acedido em 24/03/2014
Obs.	Virá a ser melhorada através da **Regulation (EC) No 717/2007** que entrou em vigor a 30.06.2007 e transposta até 30.8.2007, publicada no OJ L 171 de 29.06.2007 conjuntamente com a **Regulation (EC) No 544/2009** que entrou em vigor a 02.07.2009 sem data de transposição, publicada no OJ L 167 de 29.6.2009 e mais tarde consolidada pela **Directive 2009/140/EC** (LRG23a) que entrou em vigor a 19.12.2009 e transposta até 25.05.2011 e publicada no OJ L 337 de18.12.2009.

Código	**LRG03**
Área(s)	**eSocEU[CybCr]**
Data	28/05/2002
Referência	Comission Communication COM(2002) 263 final
Descrição	*eEurope 2005: An information society for all*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2002:0263:FIN:EN:PDF;

Código	**LRG04**
Área(s)	**eSocEU[>2007-NIS]**
Data	12/07/2002
Referência	Directiva 2002/58/CE
Descrição	*relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML; Acedido em 24/02/2014 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:PDF; Acedido em 24/02/2014

Código	**LRG05**
Área(s)	**eSocEU[CybCr]**
Data	18/02/2003
Referência	Council Resolution (2003/C 48/2)
Descrição	*On the implementation of the eEurope 2005 Action Plan*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:52003XG0228(01):EN:HTML;

Código	**LRG06**
Área(s)	**eSocEU[>2007-NIS]** - ***Text with EEA relevance***
Data	10/03/2004
Referência	Regulation of the European Parliament and the Council (EC) No 460/2004
Descrição	*Establishing the European Network and Information Security Agency*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:32004R0460:EN:HTML;

Código	**LRG06a**
Área(s)	**eSocEUCybCr]**
Data	20/10/2004
Referência	Comission Communication COM(2004) 702 final
Descrição	*Establishing the European Network and Information Security Agency*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:PT:PDF;

Obs.	Não foi publicado no Jornal Oficial

Código	**LRG07**
Área(s)	**eSocEU[>2007-NIS] – Revogado por COM(2010) 517 de 30/09/2010**
Data	24/02/2005
Referência	Decisão-Quadro 2005/222/JAI do Conselho
Descrição	***relativa a ataques contra os sistemas de informação***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:32005R0222:PT:PDF; Acedido em 24/02/2014 http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:32005F0222:PT:HTML;
Obs.	*Jornal Oficial nº L 069 de 16/03/2005 p. 0067 – 0071* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=32005F0222&model=guichett; (Em 30 de setembro de 2010 é apresentada, à CE, uma proposta, por parte do PE e do Conselho, de revogação da **Decisão-Quadro 2005/222/JAI**(LRG07) indexada **Commission Communication COM(2010) 517** Final(LRG29) [1])

Código	**LRG08**
Área(s)	**eSocEU**
Data	01/06/2005
Referência	Comission Communication COM(2005) 229 final
Descrição	*"i2010 – A European Information Society for growth and employment"*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2005:0229:FIN:EN:PDF;
Obs.	Desta iniciativa deriva, mais tarde (em 2007), conjuntamente com a L11 o conceito de NIS (conceito igual a Cibersegurança na UE)

Código	**LRG09**
Área(s)	**eSocEU[>2007-NIS]**
Data	17/11/2005
Referência	Comission Communication COM(2005) 576 final
Descrição	*LIVRO VERDE RELATIVO A UM PROGRAMA EUROPEU DE PROTECÇÃO DAS INFRAESTRUTURAS CRÍTICAS*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2005:0576:FIN:PT:PDF; Acedido em 22/02/2014

Código	**LRG09b**
Área(s)	**eSocEU[CybCr]**
Data	24/11/2005

[1] "In June 2011 it was reports that the European Council reached a general approach on the compromise text of the proposed Directive. All EU Member States, with the Exception of Denmark, agreed with this approach. The Directive also refers to 'tools' that can be used in order to commit the crimes listed in the Directive. Examples of such tools include malicious software types that might be used to create botnets. If the offences are against a 'significant' number of computers or affect critical infrastructure then the Directive establishes a minimum sentence of five years. (RAND Europe, 2012, p. 29)

Referência	EC 14781/1/05 REV1 JAI 452 ENFOPOL
Descrição	*The European Union Strategy for combating Radicalisation and Recruitment to Terrorism*
URL	http://register.consilium.eu.int/pdf/en/05/st14/st14781-re01.en05.pdf ;

Código	**LRG10**
Área(s)	**eSocEU**
Data	27/04/2006
Referência	Comission Communication COM(2006) 181 final
Descrição	*Para uma parceria mundial na sociedade da informação: Seguimento da fase de Túnis da Cimeira Mundial sobre a Sociedade da Informação (WSIS)*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2006:0181:FIN:PT:PDF; Acedido em 23/02/2014

Código	**LRG11**
Área(s)	**eSocEU[>2007-NIS]**
Data	31/05/2006
Referência	Comission Communication COM(2006) 251 final
Descrição	*Estratégia para uma sociedade da informação segura – "Diálogo, parcerias e maior poder de intervenção"*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2006:0251:FIN:PT:PDF; Acedido em 24/02/2014
Obs.	Desta iniciativa deriva conjuntamente com a L08 o conceito de NIS (conceito igual a Cibersegurança na UE)

Código	**LRG12**
Área(s)	**NIS – COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES**
Data	15/11/2006
Referência	Comission Communication COM(2006) 688 final
Descrição	**Combater o *spam*, o *spyware* e o *malware***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2006:0688:FIN:PT:PDF; Acedido em 24/02/2014

Código	**LRG13**
Área(s)	**NIS**
Data	31/05/2006
Referência	Comission Communication COM(2006) 786 final
Descrição	*relativa a um Programa Europeu de Protecção das Infra-Estruturas Críticas* - ***PEPIC***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2006:0786:FIN:PT:PDF; Acedido em 23/02/2014

Código	**LRG13a**
Área(s)	**CybCr**

Data	22/05/2007
Referência	Comission Communication COM(2007) 267 final
Descrição	*Towards a general policy on the fight against cyber crime*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2007:0267:FIN:EN:PDF; Acedido em 15/03/2014
Obs.	**that sought to improve operational law enforcement cooperation, political cooperation and coordination among MSs It also promoted political and legal cooperation with third countries as well awareness raising, training research and reinforced dialogue with industry for possible legislative action.**

Código	**LRG13b**
Área(s)	NIS[Telecoms]
Data	30/08/2007
Referência	Regulation (EC) No 717/2007
Descrição	*relativa à*
URL	http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009R0544; Acedido em 22/02/2014
Obs.	Consolida a **Comission Communication 2002/21/EC**[LRG02a] de 07/03/2002 e é publicada no OJ L 171 de 29.06.2007

Código	**LRG13c**
Área(s)	**eSocEUCybCr]**
Data	29/05/2007
Referência	EC 8457/3/07 REV3 ENFOPOL66
Descrição	*Council Conclusions on cooperation to combat terrorist use of the Internet ('Check the web')*
URL	http://register.consilium.eu.int/pdf/en/07/st08/st08457-re03.en07.pdf ;
Obs.	Check the Web foi uma iniciativa adotada durante a presidência alemã

Código	**LRG14**
Área(s)	**NIS -** DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO (Proposta)
Data	13/11/2007
Referência	Comission Communication COM(2007) 697 final
Descrição	*relativa à autorização de redes e serviços de comunicações electrónicas*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2007:0697:FIN:PT:PDF; Acedido em 22/02/2014
Obs..	**que altera a Directiva 2002/21/CE, relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas, a Directiva 2002/19/CE, relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos, e a Directiva 2002/20/CE -** apresentada pela CE

Código	**LRG15**
Área(s)	**NIS -** DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO (Proposta)
Data	13/11/2007
Referência	Comission Communication COM(2007) 698 final
Descrição	*relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004*

	relativo à cooperação no domínio da defesa do consumidor
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2007:0698:FIN:PT:PDF; Acedido em 22/02/2014
Obs.	**que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE20/CE -** apresentada pela CE

Código	**LRG16**
Área(s)	**NIS -** REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO (Proposta)
Data	13/11/2007
Referência	Comission Communication COM(2007) 699 final
Descrição	*que institui a Autoridade Europeia para o Mercado das Comunicações Electrónicas*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2007:0699:FIN:PT:PDF; Acedido em 24/02/2014
Obs.	apresentada pela CE

Código	**LRG17**
Área(s)	**eSocEU - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES**
Data	17/04/2008
Referência	Comission Communication COM(2008) 199 final
Descrição	*Preparar o futuro digital da Europa Avaliação intercalar da iniciativa i2010*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2008:0199:FIN:PT:PDF; Acedido em 23/02/2014
Obs.	Comission Communication COM(2005) 229 final, *"i2010 – A European Information Society for growth and employment"*

Código	**LRG18**
Área(s)	**NIS** - Text with EEA relevance
Data	24/09/2008
Referência	Regulation of the European Parliament and the Council (EC) No 1007/2008
Descrição	***establishing the European Network and Information Security Agency as regards its duration***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:32008R1007:EN:HTML;
Obs.	amending Regulation (EC) No 460/2004 - *Official Journal L 293 , 31/10/2008 P. 0001 - 0002*

Código	**LRG19**
Área(s)	**eSocEU** - COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU
Data	24/09/2008
Referência	Comission Communication COM(2008) 588 final
Descrição	*UM QUADRO ESTRATÉGICO EUROPEU PARA A COOPERAÇÃO CIENTÍFICA E TECNOLÓGICA INTERNACIONAL*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2008:0588:FIN:PT:PDF; Acedido em 24/02/2014
Obs.	**Texto com relevância para o EEI**

Código	**LRG20**
Área(s)	**eSocEU** - Programa legislativo e de trabalho da CE para 2009
Data	05/11/2008
Referência	Comission Communication COM(2008) 712 final
Descrição	*Agir agora para uma Europa melhor- Volume I*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2008:0712:FIN:PT:PDF; Acedido em 22/02/2014
Obs.	**COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES – Outros Volumes?**

Código	**LRG21**
Área(s)	**NIS** - DECISÃO DO CONSELHO (Proposta)
Data	27/10/2008
Referência	Comission Communication COM(2008) 676 final
Descrição	*sobre uma Rede de Alerta para as Infra-estruturas Críticas (RAIC)*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2008:0676:FIN:PT:PDF; Acedido em 22/02/2014
Obs.	(apresentada pela CE)

Código	**LRG22**
Área(s)	**NIS** - *(Texto relevante para efeitos do EEE)*
Data	08/12/2008
Referência	Directiva 2008/114/CE do Conselho
Descrição	***relativa** à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PT:PDF; Acedido em 23/02/2014 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:PT:HTML; Acedido em 23 /02/2014
Obs.	*Jornal Oficial L 345de 23.12.2008, p. 75—82* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=308L0114&model=guichett;

Código	**LRG22a**
Área(s)	
Data	??/??/2009
Referência	Report on the implementation of the European Security Strategy (ESS)
Descrição	***relativa** à*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PT:PDF; Acedido em 23/02/2014 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:PT:HTML; Acedido em 23 /02/2014
Obs.	*Jornal Oficial L 345de 23.12.2008, p. 75—82* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=308L0114&model=guichett;

Código	**LRG23**
Área(s)	NIS
Data	30/03/2009
Referência	Comission Communication COM(2009) 149 final
Descrição	*relativa à protecção das infra-estruturas críticas da informação"Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2009:0149:FIN:PT:PDF; Acedido em 22/02/2014
Obs.	As part of the ***Action Plan*** agreed upon at the Tallinn Ministerial Conference on CIIP, the COM document, the EP3R, the EISAS and more the cyberexercises for Resilliense

Código	**LRG23a**
Área(s)	NIS[Telecoms]
Data	02/07/2009
Referência	Regulation (EC) No 544/2009
Descrição	*relativa à*
URL	http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009R0544; Acedido em 22/02/2014
Obs.	Consolida a **Comission Communication 2002/21/EC**(LRG02a) de 07/03/2002 e a **Regulation (EC) No 717/2007** que entrou em vigor a 30.06.2007 e transposta até 30.08.2007, publicada no OJ L 171 de 29.06.2007 e é publicada no OJ L 167 de 29.6.2009

Código	**LRG23b**
Área(s)	NIS[Telecoms]
Data	25/11/2009
Referência	European Parliament and Council 2009/140/EC 149
Descrição	*relativa à Telecommunication Framework Directive (TFD)*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=OJ:L:2009:337:0037:0069: EN:PDF; Acedido em 15/03/2014
Obs.	Assume the associated responsibilities as defined in Article 13A of the revised TFD Chapter III – For the ITC Sector http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:PT:PDF; Acedido em 18/03/2014 Consolida a **Comission Communication 2002/21/EC**(LRG02a) de 07/03/2002 e a **Regulation (EC) No 717/2007** que entrou em vigor a 30.06.2007 e transposta até 30.08.2007, publicada no OJ L 171 de 29.06.2007 conjuntamente com a **Regulation (EC) No 544/2009** que entrou em vigor a 02.07.2009 sem data de transposição, publicada no OJ L 167 de 29.6.2009

Código	**LRG23c**
Área(s)	NIS[Telecoms]
Data	02/12/2009
Referência	European Parliament and Council 17024/09
Descrição	*Relative to The Stockhom Programme – An open and secure Europe serving and protecting the citizens*
URL	http://register.consilium.eu.int/pdf/en/09/st17/st17024.en09.pdf ;Acedido em 15/03/2014
Obs.	CO EUR-PREP3 JAI 896 POL GEN 229

Código	**LRG23d**
Área(s)	NIS[Telecoms]
Data	18/12/2009
Referência	European Parliament and Council 2009/140/EC 149
Descrição	*Retificação relative* *à Telecommunication Framework Directive (TFD)*
URL	http://eur-lex.europa.eu/Result.do?RechType=RECH_celex&lang=en&ihmlang=en&code=32009L0140R%2801%29 Acedido em 15/03/2014
Obs.	Represents a decisive step towards a Community-wide regulation framework which should be transposed into the Legislation of all MSs **Retificação da Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, a Diretiva 2002/19/CE relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos e a Diretiva 2002/20/CE relativa à autorização de redes e serviços de comunicações eletrónicas** *«Jornal Oficial da União Europeia» L 337 de 18 de dezembro de 2009* http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=OJ:L:2009:337:0037:0069: EN:PDF;

Código	**LRG24**
Área(s)	**NIS -**
Data	18/12/2009
Referência	Resolução 2009/C 321/01 do Conselho
Descrição	***sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0075:01:PT:PDF; Acedido em 24 /02/2014
Obs	*Jornal Oficial L 345de 23.12.2008, p. 75—82 – Pub a 29/12/2009* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=308L0114&model=guichett;

Código	**LRG24a**
Área(s)	NIS[Telecoms]
Data	25/11/2009
Referência	European Parliament and Council 2009/140/EC 149
Descrição	*relativa à Regulatory framework for electronic communications in the European Union*
URL	http://ec.europa.eu/information-society/policy/ecomm/doc/Library/regframerec_dec2009.pdf; Acedido em 15/03/2014
Obs.	Assume the associated responsibilities as defined in Article 13A of the revised TFD Chapter III – For the ITC Sector http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:PT:PDF; Acedido em 18/03/2014

Código	**LRG25**
Área(s)	**eSocEU - COMMUNICATION FROM THE COMMISSION**
Data	03/03/2010
Referência	COM(2010) 2020

Descrição	***EUROPA 2020 Estratégia para um crescimento inteligente, sustentável e inclusivo***
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2010:2020:FIN:PT:PDF; Acedido em 06 /03/2014
Obs	http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20102020FIN.do;

Código	**LRG25a**
Área(s)	**eSocEU[CybrCr] - COMMUNICATION FROM THE COMMISSION**
Data	25/03/2013
Referência	COM(2010) 2020
Descrição	***Cyber Crime Action Plan***
URL	http://www.statewatch.org/news/2010/mar/eu-council-revised-cyber-crime-conclusions-5957-rev2-10.pdf; Acedido em 15 /03/2014 Não 404
Obs	Draft Council conclusions on na Action Plan to implemente the concerted strategy combat cybercrime > Europol > European Cyber Crime Platform ECCP

Código	**LRG26**
Área(s)	**eSocEU[CybCr]**
Data	20/04/2010
Referência	Comission Communication COM(2010) 171 Final
Descrição	**Realização de um espaço de liberdade, de segurança e de justiça para os cidadãos europeus - Plano de Acção de aplicação do Programa de Estocolmo**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:PT:PDF; Acedido em 08/03/2014
Obs	

Código	**LRG27**
Área(s)	**eSocEU - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES**
Data	26/08/2010
Referência	Comission Communication COM(2010) 245 Final/2
Descrição	**Uma Agenda Digital para a Europa /A Digital Agenda for Europe**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PT:PDF; Acedido em 08/03/2014
Obs	CORRIGENDUM: Annule et remplace le document COM(2010) 245 final du 19.5.2010 Concerne toutes les versions linguistiques http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF;

Código	**LRG28**
Área(s)	**eSocEU- COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, nos termos do artigo 294.º, n.º 6, do Tratado sobre o Funcionamento da União Europeia**
Data	18/05/2010
Referência	Comission Communication COM(2010) 251 Final

Descrição	**respeitante à Posição do Conselho em primeira leitura tendo em vista a adopção da proposta alterada de Directiva do Parlamento Europeu e do Conselho que estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0251:FIN:PT:PDF; Acedido em 23/03/2014
Obs	**(Texto relevante para efeitos do EEE)**

Código	**LRG29**
Área(s)	**NIS[eSocEU<2007] - DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO (Proposta)**
Data	30/09/2010
Referência	Comission Communication COM(2010) 517 Final
Descrição	**relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro 2005/222/JAI do Conselho**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PT:PDF; Acedido em 08/03/2014
Obs	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF; **revoga a Decisão-Quadro 2005/222/JAI do Conselho**

Código	**LRG30**
Área(s)	**NIS - REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO (Proposta) -** Text with EEA relevance ?
Data	30/09/2010
Referência	Comission Communication COM(2010) 521 Final
Descrição	**relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:PT:PDF; Acedido em 24/02/2014
Obs	Regulamento (CE) n.º 1007/20082 prolongou o mandato da ENISA até Março de 2012

Código	**LRG30a**
Área(s)	**eSocEU[CybCr]**
Data	??/??/????
Referência	Comission
Descrição	**EU Internal Security Strategy – Establishment of an EU Cybercrime Centre by 2013**
URL	**https://www.europol.europa.eu/category/publication-category/public-documents/european-cybercrime-center-ec3**; Acedido em 24/09/2014

Código	**LRG30b**
Área(s)	**NIS[ENISA]**
Data	??/??/????
Referência	n/a
Descrição	**The establishment of a network of Computer Emergency Response Teams (CERTs)**
URL	https://www.enisa.europa.eu/activities/cert/background/cert-factsheet ; Acedido em 24/09/2014

Obs	In all EU intitutions by 2012 (as well as the cooperation of these institutions with law enforcement)

Código	**LRG30c**
Área(s)	**NIS[ENISA]**
Data	??/??/????
Referência	Comission
Descrição	**The launching of a European Information Sharing & Alert System (EISAS) by 2013**
URL	; Acedido em ??/??/????
Obs	In all EU intitutions by 2012 (as well as the cooperation of these institutions with law enforcement)

Código	**LRG30d**
Área(s)	**eSocEU[NIS]**
Data	??/??/????
Referência	Comission COM (2012) 529
Descrição	**EU European Cloud Computing Strategy**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF; Acedido em ??/??/????

Código	**LRG31**
Área(s)	**NIS - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO**
Data	22/11/2010
Referência	Comission Communication COM(2010) 673 Final
Descrição	**Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:PT:PDF; Acedido em 25/02/2014

Código	**LRG32**
Área(s)	NIS
Data	31/03/2011
Referência	Comission Communication COM(2011) 163 final
Descrição	*Protecção das infra-estruturas críticas da informação«Realizações e próximas etapas: para uma cibersegurança mundial»*
URL	http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2011:0163:FIN:PT:PDF; Acedido em 22/02/2014
Obs	Consequência da Conferência de Tallinn

Código	**LRG33**
Área(s)	NIS**[eSocEU-CybCr] - COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU, AO CONSELHO AO COMITÉ ECONÓMICO E SOCIAL E AO COMITÉ DAS**

	REGIÕES
Data	07/02/2013
Referência	Join Communication COM(2013) 1 final
Descrição	*Estratégia da União Europeia para a cibersegurança: Um Ciberespaço aberto, seguro e protegido*
URL	http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_pt.pdf ; Acedido em 30/03/2014 ou http://webcache.googleusercontent.com/search?q=cache:L27YzDmyBa0J:www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join%282013%290001_/com_join%282013%290001_pt.pdf+&cd=1&hl=en&ct=clnk&gl=pt ;

Código	**LRG34**
Área(s)	**NIS -**
Data	??/??/????
Referência	Regulamento CE n.º 580/2011
Descrição	**Estratégia**
URL	http://europa.eu/legislation_summaries/information_society/internet/l24153_pt.htm ; Acedido em 24/09/2014
Obs	Amplió su vigência (ENISA) hasta septiembre de 2013).

Código	**LRG101**
Área(s)	**NIS -**
Data	??/??/????
Referência	JOIN (2013) 1 Final
Descrição	**E**
URL	http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do ; Acedido em 24/09/2014

Código	**LRG102**
Área(s)	**NIS -**
Data	20/12/2013
Referência	EUCO 217/13
Descrição	**E**
URL	http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf; Acedido em 24/09/2014

Código	**LRG103**
Área(s)	NIS**[eSocEU-CybCr]**
Data	??/??/????
Referência	T-CY
Descrição	**The Cybercrime and the European Union 2007**
URL	http://n/a; Acedido em

Código	**LRG104**
Área(s)	**NIS -**
Data	??/??/????
Referência	Council conclusions on the Commission and the HR EU FASP 2013
Descrição	**E**
URL	http://n/a; Acedido em

Código	**LRG105**
Área(s)	**NIS -**
Data	??/??/2013
Referência	Regulamento UE_526_2013
Descrição	**?**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:PT:PDF ; Acedido em 24/09/2014

Código	**LRG106**
Área(s)	**NIS -**
Data	??/06/2013
Referência	Regulamento 611/2013
Descrição	**(voluntário)**
URL	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:PT:PDF ; Acedido em 24/09/2014
Obs	Esta regulación va más allá que el obrigatório LRG107

Código	**LRG107**
Área(s)	**NIS -**
Data	10/06/2014
Referência	Commission COM (2013) 48 Proposta de la Directive sobre Seguridad de la Información y Redes (NIS)
Descrição	**Proposta de la Directive sobre Seguridad de la Información y Redes (NIS)**
URL	http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=202368 ; Acedido em 24/09/2014
Obs	Aprovada pelo PE em fev. de 2014. Pero que todavia necessita el consentimento del consejo <= 2014

Código	**LRG108**
Área(s)	NIS**[eSocEU-CybCr]**
Data	21/02/2014
Referência	A7-0139/2014
Descrição	**US NSA Surveillance programme, survailance bodies in various MSs and impact on EU citizens fundamental rights**

URL	http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN ; Acedido em 27/02/2014
Obs	p. 11

Código	**LRG108a**
Área(s)	NIS**[eSocEU-CybCr]**
Data	11/12/2008
Referência	S407/08
Descrição	implementação do relatório sobre a Estratégia Europeia de Segurança, adotado em 2008
URL	http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf ; Acedido em 30/05/2014

Código	**LRG109**
Área(s)	NIS**[eSocEU-CybCr]**
Data	10/03/2009
Referência	IESUE/SEM(09) 04
Descrição	**Cyber Security: what role for CFSP?**
URL	www.iss.europa.eu/uploads/media/Report_cyber_security_1_.pdf ; Acedido em 19/06/2014
Obs	P. 21 Consultado a partir de http://www.iss.europa.eu/activities/detail/article/cyber-security-what-role-for-cfsp/ a 19 de junho de 2014.)

Código	**LRG110**
Área(s)	**NIS -**
Data	27/01/2012
Referência	Commission COM (2012) 9 Final
Descrição	**Safeguarding Privacy a Connected World – A European Data Protection Framework for the 21th Century**
URL	http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009 ; Acedido em 24/09/2014
Obs	http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20120009.do

Código	**LRG111**
Área(s)	**NIS -**
Data	??/02/2012
Referência	HOME/2010/ISEC/FC/059-A2
Descrição	**Estratégia** RAND Europe
URL	http://www.rand.org/pubs/technical_reports/TR1218.html ; Acedido em 10/02/2014.

A.ii – Explicação não exaustiva de conceitos informáticos referenciados no texto e nas notas de rodapé

#	Conceito	Descrição	Observações
TD&T 01	**Stuxnet**	«The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals.» Acedido a 11/03/14 http://www.economist.com/node/17147862/print	«In July 2010, a computer security firm in Belarus announced that it had discovery the signature of a new piece of malware [**rootkit.tmphider**].» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 3) Symantec, W32.Stuxnet Dossier
TD&T 02	**Worm**	«A stand-alone program that replicates itself. It often hides by burrowing in and concealing itself amidst other program code, like a worm in dirt.» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 9)	
TD&T 03	**Virus**	«A piece of computer code that infects a program, much as a virus infects a person, and replicates itself» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 9)	
TD&T 04	**Malware**	«Short for "malicious software." A general term describing any software program intended to do harm.» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 9)	
TD&T 05	**SCADA**	«SCADA systems are used to control industrial processes, such as automobile manufacturing. They can be, but are not necessarily, controlled by other computer operating systems.» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 9)	
TD&T 06	**Botnets**	«Botnets work by infecting innocent computers with some piece of malware that then connect to a controller computer for instructions.» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 27)	
TD&T 07	**IDS**	Stands for "Intrusion Detection System." An IDS monitors network traffic for suspicious activity. It may be comprised of hardware, software, or a combination of the two. IDSes are similar to firewalls, but are designed to monitor traffic that has entered a network, rather than preventing access to a network entirely. This allows IDSes to detect attacks that originate from within a network. http://www.techterms.com/definition/ids	
TD&T 08	**Trojan ou Trojan horse**	«[…] is a computer program or message that, on the outside, looks like an innocent piece of code but contains a malicious piece of software» (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 27)	Related with **Spear Phishing**
TD&T 09	**Spear Phishing**	Usually, an attack begins with the simple communication, often an e-mail. This is called a **spear-phishing** e-mail, because it targets a specific individual or recipient, much like a spear used to catch a fish. These spear-phishing e-mails are designed to appear as though they have come from an innocent source [or a through source] but they have a malicious program hidden in either the e-mail itself [in a false hyperlink] or an attachment [in a false type of file, e.g. an Pdf, Xlsx, Docx, JPG, PNG, etc.]. » (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 28)	Can be initiated by **Social Engineering** process or mechanism

#	Conceito	Descrição	Observações
TD&T 10	**Logic Bombs**	«Sometimes, the object of an intrusion isn't monitoring for information at all. Sometimes, the attack is intended only to leave a package behind, a program that sits quietly in the computer doing nothing at all, waiting. When it finally get the signal to act – perhaps from the outside, or perhaps the program has a preset day and time – it will explode into action.» » (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 29)	
TD&T 11	**Keylogger**	«A program that captures all the keystrokes entered on a keyboard attached to a computer. They could. For example, capture the organization's bank account passwords.» » (ROSENZWEIG, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, 2013, p. 28)	
TD&T 12	**Zero-Day Vulnerability**	«[…] is one that the attacker is sure will work because it is never been used before. The vulnerability becomes known on the same day that the attacker uses it to take advantage of someone. In other words, there are zero days between when the vulnerability is discovered and when it is used» » (ROSENZWEIG, 2013, p. 29)	Also called a **Zero-day exploit**
TD&T 13	**SIEM**	Security Information Executive Management (SIEM) is an emerging technology solution that has been developed with the goal of introducing greater intelligence and automation into the collection, correlation and analysis of log and alert data, which, in turn, should allow security analysts to focus on what is most important. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/security-information-and-event-management-business-benefits-and-security-governance-and-assurance-perspective.aspx	
TD&T 14	**BigData**	The phrase "big data" is often used in enterprise settings to describe large amounts of data. It does not refer to a specific amount of data, but rather describes a dataset that cannot be stored or processed using traditional database software. http://www.techterms.com/definition/big_data What is big data? →	https://www.ibm.com/services/forms/signup.do?source=sw-infomgt&S_PKG=500016891&S_CMP=is_bdebook1_bdmicronav
TD&T 15	**APT**	Advanced persistent threat (APT) is a term that has been used frequently in the course of security threat discussions; however, confusion exists as to what an APT is and how to manage the risk associated with it. Although the study reveals that a large number of respondents feel that APTs are important and have the ability to impact national security and economic stability, the study also indicates that the controls being used to defend against APTs might not be sufficient to adequately protect enterprise networks. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/advanced-persistent-threats-awareness-study-results.aspx	APT1: Exposing One of China's Cyber Espionage Units This report is focused on the most prolific cyber espionage group Mandiant tracks: APT1. This single organization has conducted a cyber espionage campaign against a broad range of victims since at least 2006. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
TD&T 16	**Metadata**	Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document. Web pages often include metadata in the form of meta tags.	Description and keywords meta tags are commonly used to describe the Web page's content. Most search engines use this data when adding pages to their search index. http://www.techterms.com/definition/metadata

A.iii – Informação complementar não exaustiva sobre as seções do trabalho

- 20/06/2014 Europe's future security challenges

"The growing trend of Europeans fighting abroad in groups affiliated with terrorism, the diversification of international organised crime, and the increased risk of large-scale cyber-attacks. […]"

- 12/05/2014 EU guidelines on freedom of expression

"Freedom of opinion and expression are fundamental rights of every human being. Indispensable for individual dignity and fulfilment, they also constitute essential foundations for democracy, rule of law, peace, stability, sustainable inclusive development and participation in public affairs. States have an obligation to respect, protect and promote the rights to freedom of opinion and expression. [...]"

Fonte http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm, consultada a 01 de outubro de 2014.

Entrevista de Ana Gerschenfeld a Paulo Veríssimo -de 08 de setembro de 2014- no Jornal Público intitulada: "*Portugal ainda não concretizou a sua estratégia de cibersegurança*"

"Os ataques informáticos tornaram-se moeda corrente. Porém, não só os riscos de ciberterrorismo ou de ciberguerra parecem não preocupar muito a maioria das pessoas como, mesmo nos países tecnologicamente mais desenvolvidos, poucos são os políticos que estão a levar a sério este novo tipo de ameaça. Um dos maiores especialistas mundiais de cibersegurança é português – mas já não mora aqui."

Fonte http://www.publico.pt/ciencia/noticia/paulo-verissimo-portugal-ainda-nao-concretizou-a-sua-estrategia-de-ciberseguranca-1668772?page=-1 , consultada a 02 de outubro de 2014.

Reform of data protection legislation

In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data. The new proposals will strengthen individual rights and tackle the challenges of globalisation and new technologies. Read full details

- Factsheet on ECJ's ruling on the 'right to be forgotten'

On 13 May 2014, the Court of Justice of the European Union issued a landmark ruling on the 'right to be forgotten', in relation to online search engines. Read more (3 MB) details on the Court ruling, the facts of the case, and how it affects you.

Everyone has the right to the protection of personal data.

"[…] The EU's Data Protection Directive -**Directive 95/46/EC**[LRG0A]- also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad. […]"

Fonte: http://ec.europa.eu/justice/data-protection/ atualizada a 04 de setembro, consultada a 02 de outubro de 2014.

- 26/03/2014 EU-US cooperation on cyber security and cyberspace

"Cyberspace issues have acquired a growing importance in various international fora, with increasing focus on economic opportunities and threats, norms of behaviour and application of existing international law in cyberspace, as well as on protecting human rights online. The US and the EU share a commitment to support a universal, open, free, and secure Internet, based on an inclusive, effective, and transparent multi-stakeholder model of governance. […]"

Fonte http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm, consultada a 01 de outubro de 2014.

COM(2014) 72 final **COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES - A política e a governação da Internet: O papel da Europa na configuração da governação da Internet no futuro (Texto relevante para efeitos do EEE)**
"1. INTRODUÇÃO

Há mais de quinze anos que a UE tem vindo a contribuir para apoiar e desenvolver a Internet: enquanto elemento essencial das nossas vidas e pilar fundamental do Mercado Único Digital, a Internet tem promovido a inovação, o […]"

http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52014DC0072&from=EN Consultado a 02 de outubro de 2014

A.iv – Entrevistas, palestras e intervenções –transcritas- sobre os temas

Entrevistas

Estratégia Europeia de Cibersegurança (UE-ECS)

"I: Today we are talking about Cyber Security. Joining me to looking in the details of that is the Dutch MEP, Sophie in´t VELD. Q: Let's talk about Cyber Security. The Cyber Security has been a long time in the making, the announcement has been delayed and so forth, but you think quite vocal your criticism of the draft has been circulating? A: I am critical because that does not seem to be a very good definition of what Cyber Security really is. It seems to range from a, you know, secure payment systems, for paying on the Internet or the way down to the National Security and everything in the between, and I think, you know, the instruments they want to use for cyber security also are very wide ranging and I think we should distinguishes very clearly between law enforcement on one hand, and let's say, security and defence instruments on the other, and that of course you choose to have to do more with the Single Market or law enforcement at all, and it mixing that all up, and I think in a democracy that is wrong. In a democracy, law enforcements not security, is not a Single Market; Q: Well the Single Market was a big issue, that, we want free flow information and certainly want a more harmonized approach because the Internet does not respect boarders, so why they to put it all in a document that is all about defence all the boarders, if you like, of Europe? A: If, you know, we need, you say Cyber Security that sounds very interesting and everybody will agree readily that Cyber Security and security systems, but if you look more closely, you can see that this strategy is not a strategy, it's just a mishmash of different measures and I think we are on a slippery slope. Because if you look at, for example, illegally downloading or hacking, you know, certainly illegally downloading isn't a matter of National Security, cam 'on! So, I think we should define much better what it is about, than there is the term Cyber Crime, what set's apart cyber crime from other crimes. Why is a violation of copyright rules or child pornography or fraud, credit card fraud, why would be that different from on-line that it is off-line. It is still crime and should be punished, but we shouldn't invent a new crime, which is cyber crime; […]" Information systems can be affected by security incidents, such as human mistakes, natural events,

technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. In response, the European Commission releases its **Cyber Security Strategy** on Thursday 7 February. Leading ICT journalist, Jennifer BAKER, is joined by**Sophie in 't VELD MEP (ALDE)**, to discuss why she thinks the strategy is an incoherent hotchpotch. Consultado em http://www.vieuws.eu/ict/eu-cyber-security-mep-in-t-VELD-laments-lack-clear-strategy/ a 08/out./2013.

Reforma de Proteção de Dados [UE-(DPReg) e (DPR)]

"Today, we are talking about the Data Protection Reform. Joining me to look into the details of that is the Dutch MEP Sophie In't VELD. Thank you very much to be in here. Q: Commissioner Viviane REDING has separated the new data protection rules into a new regulation for general practices and that the Directive for Law enforcement. Do you think this is the right approach? A: No, I don't think so. We very much wanted a single instrument. I think it would have been Commissioner REDING personal preferences as well. A single standard for Data protection regards of the end users data, and of course, you can't always specifies for you know polices as different from companies or social networks, but we certainly recognize the Police Judiciary and Intelligence Services are no longer creating their own databases today, they using databases from companies. Data has been collected for commercial purposes. So if I gave my data to, you know, for a social network site or if I gave my credit card data for buying something on a site or I have joined a club or whatever, I gave those data for a specific purpose and I want to know if those data are than passed to the intelligence service or to the police. That I have the some right, that you know, my data are protected by the some standards and that is not he currently the case; […]" March 14, 2013 - Citizens & Consumers | ICT

In 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Commissioner Viviane REDING has separated the rules into a regulation, for general practice, and a directive, for law enforcement. Leading ICT journalist, Jennifer BAKER, is joined by Sophie in 't VELD MEP (ALDE), to discuss the details of data protection reform in the EU.

7th International Conference – 22, 23 and 24 January 2014, Brussels, Belgium

Computers, Privacy and Data Protection
Reforming Data Protection: The Global Perspective
CPDP 2014: EU Data Protection Reform: State Of Play.
Chair - Mr Christopher Docksey – director at EDPS

Christopher Docksey:"This is the so called 'Political Panel' to discuss the Data Protection reform. We hope to share lights today on the key actors, constellations and drivers affect for the progress. We have taken the questions around the website and put them, so if you can see them, and the idea is to have short interventions from the panelists and then driven by a moderator a nice discussion of each point.

I am the chair today. My name is Christopher Docksey. I am a director at EDPS. You remember that the Communication was launched in 2010, Package in 2012 and then often lot had happened since the last CDPD in January 2013, and over all this period, Nicolaj Nielsen (here on my left) has been write on these developments for the Euobserver website. Nicolaj was one of the oddest European journalists. In 2013, first we had a solteve freeding frazzle by consultancy which resulting by the famous 4000th order amendments by MEPs to the Data Protection Package. Many of these amendments were in watched down not new proposes, but even the existing legislation – my own personal favorite was 'sudonimization' as I can pronounce. The freeding frazzle slow down a little bit after the Summer and after the Snowden revelations has on june on wards.

Anna Fielder, on far my left, is the Chair of the Board at Privacy International was following on this and will provide some interesting insights. Anna is not just a privacy person but she is also a Consumer protection expert and that combination, I think, deserves us a great attention on from the privacy community.

In October 2013, the LIBE committee approved a substantial upgrade - I have to say (?), that in front my colleague from the Commission - to the Commission proposal. Indeed, this achieved by a standing majority vote, the committee was restored that been deleted and the final staged of the internal stage of Commission drafting process and proposed a lot of workable solutions to intractable problems such as thresholds and sanctions.

Now Wojciech Wiewiórowski (WW), who (here on my right) is the head of Polish Data Protection "the Giodo". Wojciech is one of the few privacy people, I think, which one, understand the tech side of it and as one has been the regulator as also an observer of the Council of Ministers the Working Party on Information Exchange and Data Protection (DAPIX) and so he will give us some insight of what was been inside the Council. I did suspected in 2013 when the lobby was in slow down, where the people with say gosh (used to express mild surprise or delight) we can watch if down, they will be showed down and it was exactly what it is happened 4 days after the LIBE vote. In the Council of Ministers there was a push to slowdown 'the all thing' to set a date to 2015 or even not set a dead line at all. But fortunately the people erode the conclusion of the European Council to call of they debut of the discussions and shifty the system to completely the Digital Single Market to 2015 and the Commission was interpreted that to mean that the Reform was to adopted by April. If we are going to contribute to the DSM in 2015, I like this interpretation and I hope the DAPIX working party of the Council equally convinced.

Philipous Meedwlton he was at my right. Is a senior lawyer at the Greek Data Protection A. & P. is on loan to the Council of Ministers as I understand it to advise the Greek Presidency (GP) on the Reform Process. And so P. will give you a read so good insight in the Presidency plans.

Lastly, in December last year we're threat to an excitedly and legal opinion by the Council Legal Service. The wonder to____ proposal to 'one-stop-shop', who was to complicated to the extensive to contribute to the right unaffected remedy. Commission was very unhappy, it his Legal Service produce as opinion say exactly the opposite. So before Christmas we was fall with a legal dead lock as a time when we shouldn't racing was agree mints between the Council and the Parliament. Now Paul Nemitz who is on my left is Director of Fundamental Rights and Data Protection in DG Justice in the Commission and I am sure he has strong views on this part of the process, particularly.

At this point, Î think I should pass the floor to Nikolaj and get the debate go.

06:06 Nikolaj NIELSEN, moderator :Right thanks. I think /twice, and this claim into word, Before we start on the questions we saw up there, if I ask to each panelist, what they thinking there was the most important issues for that part concerning the Data Protection Reform (DPR). We will start with Anne, please?

06:29 Anne Felder :Well, first of all, thank you very much to the organizers for inviting Civil Society (CS) here and forgiving me the honor for speaking first, I am sure that my colleagues learnt friends on my right they have much more important issues to say to us (to begin this important debate) just I make a little disclaimer. I spent yesterday and today asking colleagues from all CS organizations on they thoughts because I thought it was important me not transmit just Privacy International or my personal opinion, but the opinion of my colleagues of CS. We have working very closely with European Digital Rights on this agenda for the last 3 years. So I am not speaking by my self; If you asking me in essential essence what are the most important things to us CS, I would say to you, that a simple effective easy to understand piece of legislation that you can serve to ordinary people in the street and they all understand what is all about. This is, unfortunately, what not happening, but and , you know, we have a much approach at final LIBE, it was result in a more confusion than was before. I just give you an example: with the 'legitimate interest compromised close'; I gave that to two of our lawyers; one reputable international lawyer and other over a lawyer in PI and both they gave me a completed different interpretations on the close. So that create a very serious problem, maybe it can be rationalized, this must be simplified in the Council, but this one of the key demands of the CS are: 'get on with it, may an effective simple regulation' and make sure that the Data subject try are there and respected and make it so to the ordinary people what this regulation is about. So that is an introductory bit I lanced the next questions with more detail.

Paul Nemitz – DG Justice at European Commission at 08:04 : Yes thank you very much. I think the most important thing now is closer. If the EP can agreed with a very broad majority, across the most important parties – on a reasonable good text, then I would say the Council should also be able to do it. And to come back to a formulation of "Chris"[topher] Docksey on the interpretation of the European Council conclusions and how topics would interpret. Well, I think that is beyond the play greed of topics and this is part of the problem of this file. We now need Politicians, we need Ministers to take charge and we have to inject the normal legislative political wisdom (PWi) into the debate which is this: No law is perfect, no law solves all issues one can think about, and indeed that we have three lawyers and four opinions is also normal (relating to laws on the books). So let go beyond the perfectionism which some use to stall the process. Let it is recognize that we need a Regulation, which is better than the Directive we have (95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 - 0050), right now, just directly applicable on law which creates more legal certainty by been a Regulation rather then a Directive. Let it is get beyond beaconing and do what Industry and Europe need for growth, which is to create legal certainty. Let give Data Protection Authorities (DPA) more instruments to become real enforcement agencies, rather than, some say, you know - a club of gentlemen and gentle women who meet once in Warsaw and next year in Mauritius - to discuss important issues. Let equipped then to become really enforcement authorities. And let get this Law on the books which also increases the control of the individuals over his or her data. This file has a synergy between protection of individuals, the high level of protection of individuals and their Fundamental Rights and growth, because only if we install trust and reinstall trust of individuals that data will not be abused, the growth potential which we have in Europe, in all industries, not only in the digital industry, will be realized and so, if we have no a contradiction, we have synergy let is make now the use of it, let is take political charge and bring this to closer and the EU must be uploaded for the fact they have done the decider four step, now the move up to the Council. 11:04

Mr Melton 11:10 (not relevant)

Wojciech Wiewiórowski, GIODO (PL), Polish Data Protection Authority (DPA) 13':45" :"Thank you very much. I try to say the things from the position I have at the moment as a DPA in Poland, but also as person has taking part at the activities with the Reform also on the level DAPIX (representing the Polish DPA) is an expert body to the Government authorities in charge to taking the floor at the DAPIX meetings but we are generally presented the DAPIX meetings as we are observing what is going on there as well. If we meted a year ago (in January 2013) my introductory remarks would be the some as the Paul Nemitz. I would absolutely agree with what as Paul Nemitz said and what are the demands for the 2013. But after 2013 I actually have to change my mind, and I have to change my position on what as actually going on. We had at this point what the LIBE Committee has done really a great job. Preparing the result out of the 4000 amendments – we can, sometimes disagree with parts of things that was done there, but, I have to say that I admire the work that was done in the Parliament (EP), because, I never expected that they can go out of this 4000 amendments with the agreement of all the parties in the Parliament (EP). So once they where left alone, let is say, with all of this 4000 amendments and the text that was provided by the Commission they can do something out of that. Unfortunately this is not true with the Council, as you precisely know, and why a agree with Paul Nemitz that this political will (PWl) and the political decisions were expected in 2013, Commissioner Reding has done everything to achieve them, we did not achieve then. We did not because actually that was a big failure in explanation of what the really the Reform are all about. And I am saying that as a representative of DPA was always very supportive to the rules of the Regulation, also to support to as Directive – the Third Pillar Directive – and we managed to convinced the Government in Poland to be supportive as well. Those of you who heard what have Minister Bonnie at the International Conference in Olso, so that he really pushing to hard the new Regulation to be adopted as soon as possible. On his step down, for personal reasons in December, the new Minister responsible for that, is the MEP was taking part in this LIBE agreement (Mr. Rifak Trzaskowsky [Minister of Administration and Digitalization of Poland]). If we had MEP who is really involved in the Reform that was Minister Trzaskowsky and his right now the Minister responsible for that also in the Council. But unfortunately, I have to say, that after all this discussions we had in DAPIX to through 2013, we are losing the allies for the Regulations, and Poland is probably one of the last allies that is now, the Commission is now loosing, and that is defiantly the

failure of the Commission to explain to the Council, were is actually on practically level, not in the political level - not the level of the big words, but the level of real legal rules that are in the Regulation. What is really the things to be achieved and well I am sorry to say but, Paul (you are very open always to say what should be the role of the DPA, what should not be the role of DPA, what we should do and what we should not do; you did also yesterday during the meeting in the Permanent Representation of the Republic of Poland, but let me say what of the Commission should do: The Commission should support it is own project, it is own draft. And unfortunately, it was not able to do it. When we are coming back from the discussion on the Council, the main impression was, surprise and at least disappointment of what we had or what we did not in here. No answers, or the non precisely answers to the questions that was done by the Government sand unfortunately to said that the Political will who should be solved is defiantly not enough. So these are the things to be done in use to loops to burning these of the Council, not on Tweeter. That not is the way we should create the legal act. We should create them at the Council and that is the things that we not doing well, not by the Countries, but by those who actually support the draft. So, I have to say, that I am disappointed. In my opinion, we are facing the very difficulty of 2014 which what probably not finish with the good result. 18:52

Moderator - If we (not relevant)

19:16 Paul Nemitz :"Well I think, first of all the fact that the EP has been able to agree and of course it has agreed with a lot of explanations, on base of a lot of explanations the Commission gave and we have worked very closely with the Rapporteu and Shadow Rapporteurs shows, that on the Legislative body who would not share this analysis that we have just heard, that if you ask to the repporteurs, they are very content with the explanations we gave and of course, in the EP we have done what we have to do also between the institutions and also in the Council. We have made suggestions and brooked compromises were we sought middle lines. That is the job of the Commission in this case. And in the EP we was successful because wisdom (the ability to discern or judge), politically wisdom (PWi), politically guided and judgment, ruled. You know, turning to the Council, I can just say, you know, the commentary on Data Protection of 2000 pages which it was submitted in Germany that really appear to anyway. It does not matter how long the Council negotiate, that always will be questions when they will been open. The world that can not be end the technological progress, the business model progress can not be ended by Law and so, I think, what we are facing is a complex material, but as much as Legislation in the Parliament, in the Council which is complex and we are facing a clear political orientation by the European Council that 2015 as the target date for the function for the Internal Digital Market. And to this, we need to work together to this reason and not absolutely perfection standards which we can matter by reach in legislation to get to closer. And, so honestly we do, what we have done in European Parliament also in the Council, but regularly new issues, new problems are invented and I do not see any technical problem in this Regulation which can not be overcome if they are the political will. What is on the table now is progress, and it is not perfection, but that is no perfection in Legislation in democratic countries, because by the very nature of things one needs to make compromises therefore my wish is that Member States (MSs) rather in focus in some solution on this or on that, defined that corridors of acceptably/ twice. I think, that what we are needed to come, we need to come to compromises which we can carry by the necessary majorities.

Moderator - (not relevant)

22:21 Anna Felder :"So okay. So I do not disagree in principle that there is a political will and the will to progress it can not be achieved than we can have closer, but, the EP – I disagree with you on the point of that the EP having the political will. What they had, was two very speeding elements: one, was the elections coming up in the Spring – that can speed-up, you know, anybody; and the second, I thing, the very massive surveillance revelations had very big impact, both on the speed of the Parliament, but also on the sought of intensity of the lobbying they had the massive impact on the industry, because, they realize they suddenly read the big impact on the trust in the public relations issue and they had to do something about it.

So, the result we had in the EP having very much to do with all this externalities as well and it had any impact on the Commission, because in the first time in the next years, the Commission decided to investigate issues, like Safe-Harbor (SH) properly despite our calls to do so before, they did not do that until the last moment and it any confirm all the thing that the CS has been said for years. That it is not working, that it is a lot faults, and you know, it was a big impact on Data Transfer.

So, these other externalities as well. Who was the Council of course, has complete different motivations. They do not have elections, they have to work on the ground, they have sovereignty issues, they have the economic crisis issues, how much money this is going to cost them, you know! We know the United Kingdom (UK) ICO who is loosing founding as the new Regulation, so they has a big impact on how, for example, the UK has reacting. The motivations are different, you know, the Council has different expertise's coming to the light ---- you know, we heard from the Polish DPA. So, I think, if you are talking in terms of influences and the delaying situation is much more complex.

Moderator - (not relevant)

30'50" - Wojciech Wiewiórowski, GIODO (PL), Polish Data Protection Authority (DPA) : Several scenarios we can take in consideration. Let me say just about two of them. The most positive for me and the most negative for me. The most positive which I will be doughty, but I still try to believe in that, is the fact that, - well, sorry, first the information in the beginning; I do not believe the Package will done before the elections of the EP, okay! 'Full stop.' –They are no possibility of to do that. So this scenario not still exists. But the best scenario [has I said before], is that the Council which will not stop by the European elections will work on the Package will work on the Regulation at least and by the end of Summer they will reach the results, that will be the result of the Greek Presidency (GP) and that can be taken by the Italian Presidency in order to start the "trialogue' and the same at the end of Summer or early at Autumn, the new LIBE Committee or whatever committee will be, the Committee of the Parliament, will decide let is take all that is done in the last term and last follow with it. But, as I said it is very dough full. The worst scenario that I have, is that the Council will not reach an agreement, has not reach in the last few months and the dead lock will continue also until the end of the Summer, Which for the parliamentarians will mean, 'well we should rethink what we did in the previous time.' So it is mean, let is last open all the discussion again and have the 4000 amendments on the table and try to work on it again, which mean, we will not have the new prime work by 2020, probably. So these are the two scenarios I can draw and unfortunately, I have to say that once, we are not sigh the last allies of the Reform, the second scenario is more and more possible.

31:36 Paul Nemitz :"First of all, I think for the Trade negotiations with the US, the fact that the Regulation is not concluded, is a huge burden and uncertainty. Those, who want these negotiations with the United States (US) to be successful, I think have a strong interest to make sure that the Regulation is concluded this year. And, certainly on these subject is closer and trust is coming back, because alone with the Safe Harbor, for example, we will not be able to recreate the trust that the Digital Industry needs, in particular, the American digital Industry in Europe needs. Now of course, we are not claiming, nobody said this, but the Regulation solves all issues in relation to National Security Agency (NSA)? Obviously not! But the Regulation and the availability to agree on it between MSs is an important signal[ing] political (vice-versa) that in Europe we are able to hold Privacy high, it contains important rules which, let is say, may keeping alive of 'all saving, all looking, all grabbing' Secret Services (SS) more difficult, in particular that SS who relly on data transfers from private parties, which, of course, is the 'business model' of the United States NSA, that is the combination of Public Power combined with these private enterprises, which is uniqueness of the US-NSA model, and so I think has Vice-President Reding said: "The revelations where an wake-up call", also for those, many of those, actually, previous those who have problems with this Regulation. They have waked-up (is true the analysis which you [Ms Anne Felder] have made) and in the European Parliament, particularly, many people rethought previous positions and they have understood the 'wake-up call'. So, I think the most important sign to the US, is actually to the World, is whether in terms of businesses and in terms of individuals, that we have in European Union, able to continue taking the lead on defining what privacy is about and how it works. Are we able to equip our DPAs with better instruments or are we continue to fine Google 150,000.00€? You know, I can only say, this Regulation 'will not be perfect', but will provide more instruments to the DPAs, will provide more instruments to individuals, it will ensure a 'higher coherence of application Law'. Who will not be perfection, but a highest coherence application of Law true the fact that is a Regulation, not a Directive - the Directive is initiated now, who always leads to diversion already across States, because MSs implements Directives differently. So, the fact that we have a Regulation coherence mechanism and again even this coherence mechanism which is not perfect, combined with the Regulation will be better than the situation that we have now, [only] with the Directive [46/95/EC]. So what I am saying, is what is on the table now, in the EP and in the Council is a good basis for the two institutions to talk to each other and to come to a result which such is better than this status quo. And those who are asking for more, they take a high responsibility on then selves because, they may contribute to failure, and those like the Privacy Officer of Google, who go out and say 'this Regulation is dead', well, they have a policy agenda, they want it dead, that is not scientific analysis, that is political propaganda! 36:05

Moderator - Okay, okay I think Ms Felder wants to step on this as well.

36:12 Anne Felder : So I totally agree what Paul analysis this Regulation has to be past because of the externalities. The US has been an important delay influence on the Regulation - that is absolutely clear. And we have now the Transatlantic Trade Negotiations and we have being a sure debate? by a Trade Directive n/a and the Commission Data Protection will adopt be part of it, but perhaps some of you know, for example, two US Senators introduce a piece of Legislation in December in the Senate called 'The Digital Trade Act', which has some specific provisions to mandate to the US trade negotiators to make sure the trade negotiations to include provisions for free data flows including interoperability and I quote 'interoperability between different Data Protection Systems'. So this is clear a matter of divergence for this Regulation to be pass before any such Law is passed, before the Trade negotiations progress. On the matter of Safe Harbor, we believe that, it is not going to work. The thirteen demands the Commission made are probably not range be implemented simple because the Federal Trade Commission (FTD) does not have any sanction powers does not have remedy powers. I mean for example, yesterday ___ to? Announced and reveals 12 companies that do not have respected SH but they can not put sanctions on them, I think, because a matter of public consultation. And I think polish Safe Harbor put pressure on the US, for example, to implement the Obama Bill of rights, which was issued in 2012 with promises of a General Privacy Law in US as well, and this actually demanded by my colleagues in the US, as well (Marc is here, maybe he want to add during the public discussion something on this).

Moderator 38:25 : […] And this is interesting because here in Europe is a Fundamental Right and in the US is merely a Consumer Right, instead.

Public discussion

Question n.º 1 – Thobias Mor… (Germany) (not relevant)

Yes, Paul Nemitz you said the Regulation will bring trust. From my point of view at a moment is a point where I ask myself, more and more points are moved, safeguards are moved to the control of the EC and then I see SH under this condition. I see all our trade-off is happening, no safeguards are working and anyway in SH are not stopped or at least threatening to stop, then I ask myself what will be the other thing that are proposed in the new Regulation all such transfer is decided by the Commission.

41:28 Paul Nemitz: Yes, on the question of which institutions, in Europe, benefit from this Regulation. It is not the Commission. Is DPAs, because the DPAs sough this Regulation will get 'teeth´s'. we have a number apart from Poland DPA and we have a number of DPAs and Ex-DPAs in the room. Let it is do around questions here and which is higher fine those who have been imposed by them. What are other instruments really off been apply. I think, in terms of powers and the reality of DPA been able to make a difference in Law, this Regulation brings what they need to bring them up to speed and the power as national competent authorities. That is no reason why we should be protecting competition between enterprises in a more regular way than the individual freedom and personal data optional for the individuals. So I think not is a wrong analysis of this legislative process. It is powering the DPAs to make difference in the future and it is exactly what we need in this Digital World. On the second question of SH, here the draughts were the Commission will be able to work with US to implement what we have put out in terms of 13 recommendations for improvements. And I can take notes of this doubts – I am, myself, the chief negotiator with the US on this – and I would do my best. And, I am confident that we will be able to implement this recommendations, because my feelings as: the people in the US, they also believe in freedom, they believe in the protection of the individual life, or they identity. Americans do not want to be spied also on that they want to have Data Protection. They are a great country on Democracy with a free press and great individualism, and they have a vibrant CS and know working in Democracy. [And] I am confident then when we work together with them, they will be convinced conversion in the future of how we will be doing privacy and progress of the SH will be the some type of, not only the symbol, but relevant of this progress as the speech of the President Obama of Friday and the policy instructions, on protecting privacy also of people in another countries were a first step in create a sigh that this were the thing are going. This is the

only one way when privacy protection on both sides of the Atlantic. The digital future and that is more of it and I think more and more people in America, including in the Government understand and let it is make my confident that on the SH we will be able to make good progress and come back with the results against the doubts which are fair to have today. 43':57"

M – Can we see another up-hands are there? In the front of us, please.

44':07" Sure, my name is Marc Rotenberg of the Electronic Privacy Information Center (EPIC) organization in Washington DC. And all accepted Anne´s kind invitation to say a few words about the situation on the other side of Atlantic. One to say in the outset that the US Consumer organizations have stronger supporter the efforts to move the Regulation forward. Last year 22 of the leading consumer organizations sent a jointly letter to the European Parliament to express our support for the work of the Parliament and the Commission and been very direct we are our self interested we seen the strengthen of Privacy Protection and Data Protection in Europe as a way to improve global privacy standards, to improve privacy protections for the Internet users all around the World. So the fact that has been delayed appose US as you have just describe it is not good news for us as we know it also was not good news for you. And I think even quietly the US firms have pushed against the Regulation in light of the Snowden disclosures and that we have learn learnt? About NSA may I actually see fog? Private authorities as nothing issue all around networks so secure against the attacks that we have learnt has occurred. I want to say a word about the President Obama speech last Friday which I think is one significant area signal change in direction is positive. The first key point is that indicated at least the respect in the US that he would and the NSA telephone record collective program and for us in US that has absolutely critical, as we cannot imagine anything worst than an intelligence agency routinely collecting telephone records of all of this citizens. We will work to stop them as President has announced on Friday. The second think they had announce a committeeman to implement a majority the recommendation of the expert panel in review had put forward 46 very good proposes and real significance. I think for a global privacy standard for Internet security and openness and we support that as well. So I guess the question is to than what happens next and I think the firs observation which was Paul said just a moment ago, is we all have a common interest in moving privacy protection forward. We live in a global world, we operate on the Internet, you know, privacy protection is not just a concern of Europe, is a concern, really, of everyone and so any effort that moves this forward, I think it should be supported. So the SH issue, we know now that the protection is simply not working. Then, I think, the wise is to move in more closing to that and to say to want be done strengthen as Anne said not only to scrap? the outset but we have learnt want to recently confirms many of worst fears. So, we will continue to support the efforts to strength privacy safeguards in Europe as it is important for you, for us in the US and for everyone and I mean that at the end of the day we will really are in this together. We have a common cause and we will wish do the best.

M – Yes here in the corner, please.

48':11" - Allo. I am from the Danish consumer council NGO and then in Denmark is that could be a problem here concerning the discussion in the Regulation/Directive, because the Government in Denmark that even know they like privacy and sure when comes to the opinion that they think the early day light and they want to support this debate and the public authorities and they think that as much effort from them to do the privacy assessment that is too expensive to working with 'privacy by design', so even know that, consumer NGOs and the industry are together to support the Regulation, the Government and maybe other (and DPAs, I do not know), but the Government is against the Regulation. We are waiting still on the issue, but that is a new dead-line for the MSs to 'make-up the mind' concerning this debate on Regulation or Directive or it is sates as you say from Poland, that you just about to give-up, it seems like are there more MSs who are changing their opinion on this issue, because I was opening that we are going to have a Regulation even know that in Denmark is against this, but so I just want to know your state that issue?

50':00' - WW:I can star briefly, of course everything what I said is not the position of the Government, because, I am not representing the Government of the Republic of Poland (RoP). I am just representing the Poland DPA, which is an advisor or expert for the Government, but I have to say that all the doubts that where so far expressed in the countries are coming back on the table. I am very sorry to say, but we did not take any improvement in the Council for last few months. So it means, we are exactly at the same position that we were a few months ago and all the questions are discussed again and again/twice and we are facing the problem that the Governments will start to raise the question that not raised so far. I was admitting that the Polish representative enterprises they started to say precisely 'why not to keep the Data Protection Law who we have in the moment, in Poland. We are more used to that then that new solution'. So my term as a DPA is finishing in August and my successor could come in conclusion that we need to start to discuss again [his mandate was renewed for more 4 years in charge of DPA by the Senate of RoP in early August 2014]. And if they all the topics are still open in the council, then the discussion is start in a country like Poland, again. I am not going to say the name of the other countries that are so far supporting to the Regulation, but, I am just saying, we are losing the last countries, that are ready to supporting the Regulation in the Council.

51':47" Moderator : Mr. Nemitz, do you agree with this, that more and more MSs are more reluctant to push forward on this Regulation?

I think, we have just heard from Denmark is exactly the reason. Why? We in the Commission bleed? for Political level to take charge. Because, this is a question of political responsibility. If it is so that consumer associations and industry support the Regulation and in the Council Civil Servants working in other direction is a matter of political decision-making and one has to be responsibly political leadership if this happened. I think, yes. It is a complicated file. Yes, we have prostrated? discussions, but I am convinced that If politicians take charge, they will introduce the judgment, political judgment, which is necessary to overcome all the small problems of discussion here and there. Because, politicians know, nothing is perfectly in the world and legislation is the least perfect thing – as we know from [von] Bismark, who said 'two things people should not know: one – how our sausages are made; two – how our Laws are made!' So, on the question where we are, who conversions or where we are losing countries, I am alerted by what we heard here from the DPA of Poland, I am very much regarded at if political leadership of Poland change the direction on this, because, indeed, Poland was very supportive, so far, my view is, that we have moments that converse after all, and these movements can be substantial accelerated if politicians take responsibility, but I am not the only one who watching what is happening in the Council, Greek Presidency (GP) is also here, of course. 54':02"

54':08" - Represent from Greek Presidency Mr. Phillipous Medelton :Yes, thank you. I will have to agree with you Mr Nemitz and I would like to (I am show very sorry, I would like to correct about your last statement [Mr. WW], that the last discussions at

DAPIX working group [was], where a disaster.) I mean that was not a disaster, we did not, they are not succeed. Yesterday, for example, we had a very constructive and a very successful meeting there on the papers that the GP presented to DAPIX. We had a very large consensus this is a sign that we can go on if we try to find a common interest in view our common goal which is the protection of the Fundamental Rights of the Data Protection, and what our Danish colleague said, that, for example, the Danish government does not accept provisions – putting the obligations to adopt 'privacy by design' without impact assessments), because they cost money, for example. This is as example that this new provisions are provisions that protect individuals. I mean there are for the good of the people, of the individuals and also they will give, the opportunity to the Data Controllers to be able to proceed to processing Personal data in the more secure way and under legal certainty. So I think, that we all should try to give an effort for this constructive dialogue and I also would like to say to those who express doubts about the regulation, who ask: Okay we are in a such specific context and there are massive surveillance that they are Google or other companies do not process our data correctly and the Regulation does not give an essence to that? I mean may question would be: what would happen without the Regulation? We all know and we all agree that the actual, the existing data Protection regime is not enough to protect the individuals, so we need to work on that and go forward. If I am use just a personal touch in my intervention, I mean, when I, when somebody ask me; 'what I am doing in life, and I replay – Data Protection (DP)'. You know, what they say to me: 'DP? But there is no DP! Everybody monitoring our telecommunications, everybody …'. They do not trusting in DP, anymore.' And we need to give a response to that. People need that. People need to give back the lost confidence in order to go forward. That is my point of view and of course, I share the [worst?] best case scenario that you explained to us. And I would like to say that the intervention of the GP is to go on with this best case scenario because if not, if we go to the worst scenario, then I cannot imagine what the situation will be in 4 or 5 years, okay!

58':20"- Moderator : We talk a lot about the MSs and as not so much about the private sector but we have 15 minutes. So I see 2 more questions. If I can begin with this gentlemen first. Please.

58':32" – Martin Hastings. Privacy Consulting: Can I just thanks the Polish Regulator. I think is the first – I think- I believe you are the first international Regulator that are come out on the record has to declare that the Regulation would be not pass before the European Parliament Elections. But I find really interesting, was, why? And you talking about the failure of the Commission to support their own projects. And I am rough down when you said that the Commission should create support on Council and not on twitter. Now, this that mean there are something wrong institutional whit the Commission? Do you think that they will go to wait until Ms Reding or these elements? Left the stage, before that can be people within the Council who are able to engage more effectively with the MSs in DAPIX? Where can we go forward or came the Council changing their spots? So they can try to deliver something that we cannot to see?

59':10" – WW: Yes, everything which would be done about the political will in EU was been done. The statement from Vice-president Reding and from the members of the Cabinet of VP are showing the thing that Paul has just said a few minutes ago. It was not said precisely but, it did not reach on final on 6th December. On 6th December the answers which I heard from the Member countries was: 'well, we will not have a political will without having the legal text.' And I agree with Paul that the 'Political Will' (PW) is crucial. The problem is that the Commission did everything they could with the PW. What we have the problem with is, an explanation, what was exactly the Legal Text to be achieved. And that is something which, in my opinion, was not done correctly and which I am blame myself not been able correctly, because, I did not have enough support that what was rely did draw, because everything about the rules – the General Principles, I absolutely agree what is said the Commission, also about things about the DPAs not having enough possibilities to perform they wish of course I will say as well as a DPA, the problem is right now the problem is the Text, not the PW, the PW did not come without the Text.

01:01':01" - Moderator : Ladies and gentlemen's…(not relevant)

01:01':08" - Peter Schaar from the European Academy for Freedom Foundation and Data Protection in Berlin. Well, I completely agree with Paul Nemitz assessment that we have a political question, but if I agree on this, we have to ask; 'what is the political question'. This is not limited to the substance we discuss. It is also a question of powers. It is a question of competences. And from my perspective much of the criticism against the approach of the Commission that is coming from Mss is against giving a way – competences – the legal field has well on the practical field that is now space for legislation in the MSs. The competence goes to the EP, the Commission and the Council. And therefore the [influence] opportunities to influence these procedures are weaker from the national point of view, than today. This is one aspect. And the second, is: the role of the DPAs. The increase of the independence of the DPAs might seen as a threat by some Governments, because, if they are strong DPAs, - if they are real powers -, they are not dependent on the decisions of the Government and if they act in a different way, they might be the problem for the Governments. And I think, these are two crucial issues. On the first one, I think they could be a solution, at least if we focus on the main issues, in the Regulation, perhaps, they might be a third scenario, not only the both WW mentioned. Perhaps, the third scenario might be to focus on some main issues and to start again peharaps with these or to continue with these issues, not every single article or paragraph of the all Regulation – perhaps is necessary add the others. So we have to focus, but is not time to do this, today. I think, we try to support the EP and the Commission in been successful and we have try to convince our Governments, but if we fail, we have to avoid that will be a complete failure. So, but for the first scenario for me – scenario A – we need a Regulation and perhaps, we have to consider - a scenario B -, after the election of the EP and after the GP.

1:04':39" Moderator – Anybody come … on this?

1:04':46" – Mr. Paul Nemitz – I think what WW has said, maybe the Commission has made before the argument that the Political Wisdom (PWd), the Political Judgment (PJg) has bo be inserted into this document, is right, but, you know, sometimes, one has to repeat the same argument over a sustainable time to convince, because, you know, things to have to mature and if at the technically level comes back once and say 'to huge technical problems, Minister!', and comes twice and three, four, five times, well, soon or later, the Political Level (PL) will se, you know, 'is this, just, technically argument, really what I want!' So, I think the lightly of politician take in charge creases over time on this file, and, so, I tink, it is right to again call on Politicians to take charge. We had a Council – informal Council – in Essex? (European Commission · The Commissioners (2010-2014) · President . ... Informal European Council, 30 January 2012. EU. It is not enough to focus on financial stability ... Parliament the conclusions of January's Informal European Council, http://ec.europa.eu/commission_2010-2014/president/news/speeches-

statements/2012/01/20120127_speeches_2_en.htm ?), this week, where Ministers have received good questions from the GP and I think this Council, informal Council, is an opportunity for Ministers to show that there are issues on which Mss can largely agree. Incidentally, is about International Transfers and the Application of the Regulation to companies that provides services from outside of Europe (EU). And I have some hope that the GP had a great skill and will be able, also, to turn a little bit of mood and attitude in the sense of Ministers will go home and see: 'Hei, they are things in which we can agree that also to ejects into the work of the very good knowledgeable experts. I think, it is an issue a little bit also attitude and willingness. We have many people, or some, who go around and say, 'quality before speed!', sounds great, a less it is instrumentalized to stall. So, I think we have to look at a little bit of attitude of people and call on, let it say, constructive readiness to work on 'corridors' of what is reasonable.

01:07':16" - Anne Felder: So I agree with the analysis of Peter Schaar and the Colleague from the GP. [time keeper - five minutes] Okay, one second, so balance, is better to have a Regulation speedily that not have it with probably consequences. One issue that was not been mentioned in noun of this PW, you know, one of the biggest countries that is currently delayed, is actually, Germany, if is far not mistaken. Perhaps, you know, It should be pointed out, to Germany that, you know, 82 million people that they data can easily keen out to a country where the DP Legislation is weaker, than it is in Germany, now, for example, Ireland. That could be a n incentive. So on balance, we would want the Regulation to pass speedily.

01:08':26" – Moderator: I think we have time to one quick question and then we need to readily rapped-up to have a conclusion. So I thought, I see a Lady back who is waiting …

01:08':35" – Hi. Julie Cohen from Georgetown Law Center: So, from the perspective of an American observer, there one aspect to this conversation that as just been bizarre. We have a very inadequate Data Protection Regulation, but we have a very robust practices surrounding transparency, particularly, regarding the accessing of lobbyists to the Government and I have not heard[ed] discuss at all, except in assertive masterly in direction, that. It is curious for me this to see severed months ago was a front page column of the New-York Times, that have all the major Us Government relations, all offers with lobbying in terms of opening offices in Brussels? and that they were no obligations to disclosure their client list and the amount of money being been dispended in the lobbying and particularly for someone who is doing Data Protection issues. I cannot accept that the Commission is a 'black-box' and you do not know what is go in it and you know what is coming from out of it, which that been discussed and I relay, and left been clear after listening to this panel whether it is delayed to discuss that in public which case come as such and been playing right now and my apologies or whether non been discussed that in the context of the process that we have been but really seems to me that is something near to be said and I to ask to some of you to see to respond. Thank you.

01:10':09" – Moderator : …(not relevant)

01:10':10" – Paul Nemitz : I think a lot of things we can learn from the US and Enforcement by FTC is one thing. Holding out fines, 20 millions, 30 millions on privacy, non compliance to Google and Facebook. You know. Something now thas is a thing that the DPA in European cannot do now. And Judie Brail the Commissioner of the FTC one said: 'the best for privacy would be, EU rules and US enforcement!' so I think on enforcement we can learn. What you say on transparency, it is also a very value point in Democracy for Europe as a whole as much younger than the Democracy of Washington, we only have an direct elected Parliament since 1979. I think there are a lot of things we can learn in the positive and in the negative from Washington. On the DP specifically, we may not have the good transparency rules (it is not my fill expertise, I cannot tell you what I am asking to my collaborators to take a good lock the time they make sure that has not uneven and I in person can be in favor of lobbying is much more, 'who see who is whom' in the EC, because I think, you know, that is an issue, but on DP, please go to lobbyplague.eu. It is a private initiative which in a fantastic way for creates transparency about the impact of lobbyists on creating amendments in EP. On this web site you can track from the letter of Amazon, Facebook, Google and the likes runt to the amendments presented in the Parliament. It is a fantastic thing of transparency and I am very proud that we have it, it shows that also Europe has good free speech and good activists and what is very useful contribution to the debate and to the preparation for the EU elections.

Moderator : Thank you and then to chis… to have some conclusions.

Christopher Docksey: "Thank you. I have made 3 comments, but, we handle the stuff about lobbying and a outside interests, so this make 2. First in keen out very strongly form this. Is the problem of understanding Legislation for normal people and the DPAs and also for the Lawyers and experts in the institutions? We forget these privacy experts how complicated this stuff is, what challenge it is. And an array these frauds in fact that the fraud of will be launching there a report legal to regress at this evening that apparently occur in the frontout. If you go to a lawyer, the lawyer do not know about DP and the Lawyer does not to get in to the Court-room and do not know otherwise?

So there is a real challenge the first conclusion to explain DP outside our community, both the legal professionals and to normal people. Then we the regard to the speed to this package is going to do through what we have learnt there were 3 conceivable opinions for the timing: before the European Parliament goes down; before the end of the year; or sine die.

I must say personally I am not understood why – if we have been working on this normally for times since January 2012, that is 2 full years, we have not made more progress and with respect, I think the true this is that in the Council some MSs are come to intensively very late and the deep-set reservation that others have the bad various aspects are only now standing come out in the underlines that was been mention today the use of Regulation which over right national Law converge the public sector giving real powers to the DPAs. So, my second conclusion is to argue with the speaker who said: 'that what we need to do now is focus on some critical issues that we cannot estimate progress.' For example, with regards of use of Regulation, which is absolutely critical, we have to provide the double real insure to the MSs, the countries like Germany, who will should pushing this forward not, it should be taking the lead. They have to be re should this will not readjust the standards and to other countries like the UK, that is worried about the economic aspects, they sometime they have to be ready persuaded that is better for business as we have heard in the panel this morning, to have one Law across 28 legal regimes than a myriad 28 national ones. Whit that lights I would like to thanks the CPDP for organizing this Panel. I would like to tanks to the panelists for their very frank views and I would like to thank to the moderator Nikola[s]j for running the debate. Thank you very much. [applauses]. 1:16':22"

Fonte https://www.youtube.com/watch?v=kl8an9Myrek, Consultada em 08/ago./2014.

Cyber Defence: global Responses to Emerging Threats

– in 15 Nov 2K13 at Conference Manrion House Dublin, organized by the Irish International External Affairs (IIEA1) http://www.iiea.com/cybersecurityconference

Heli Tiirmaa-Klaar, Cyber security Policy Advisor at European External Action Service (EEAS)

So, today, the topic is cyber defence, but if you allow me, then I would maybe start from a more philosophical notion of what actually is Cyberspace and how exactly it should treat this new domain. Cyberspace is something very new for all of us, for the Governments, specially for the Policy makers in the Governments, specially. If has been a very technical domain there is a good experience around and amount the technical communities and I see many practitioners in the room and I regale more and more practitioners also becoming Policy makers in this field. But as a public Policy maker for almost twenty-years, I seen quite interesting, similarities with other new fields in cyber, because we lack institutions domestically in cyber, as we lacked them possible in some of the areas before. We also so like the proper coordination of guide of domestically then in us we will try to put together our cyber projects nationally. And then we would like to skills the people. We would like to put programs and then we have awareness. So, I think we have to work hard and that will make in the end our cyber, let it say, in the future our cyber projects much more resilient. Because, we cannot really speak about the defence in traditional terms, when we speak about cyber issues. Cyber, is such, a very non-state concept, is IT technology in a way, innovation by the private sector and civil society enthusiasm, than asked to the Internet in last decades. So, this is a very anti-governmental concept. Governments are not easy to deal with this kind of asymmetric networking type of new entities because the Governments are more hierarchical, Governments rely on certain procedures and processes and Cyberspace is something new for the Governments. There for the Policy responses that we have choose tools that will be very different, that we are use to in more traditional areas, especially when we come to national security and defence . So, I would say what we need to do in Cyberspace in order to make it more resilient on defend our organisations on our computers or information systems, is to enhance the capacities at different levels. So, when we talk about National level, then we need a very strong bottom part of the pyramid in which is the civilian non-state strong cyber resilience capacities. It is 80% of the Private-sector that runs our businesses and we know that none of the Governments is powerful enough to tell a majority of the critical providers what exactly they should be done locally in order to protect the critical services running. So, this has to be done by private partnership and has test to be a project then involve all the private actors. Then, also cyberspace is not hierarchical, cyberspace is a network. In order to have a good resilient structure, a good crisis management structure, a good defence strategy, we have to start thinking as a network, is network against network, is not network against hierarchy, because, and I am very sorry, but the hierarchy will be loose, and this is something that we has been learned in 2007 in Estonia. That was a network of non-state actors, that helped to defende of the attacks, it was not a government agency, it was not only one organization in the coutry, it was a network of different organizations that coordinate and that how we could resist of three weeks of serious DDoS attacks.

So, when we come to a more policy response what we have seems so far, then I think the EU provides a very interesting example of different very resilient national governmental cyber models. Because see at least three or four different models now emerging inside of the EU by the different regions and the different countries there and in then every nation in the role test to find their own model to become more defended, more resilient in this space.

What we have in the EU right now, we can observe the Nordic strong voluntary Public-Private Partnership cooperation model, which also is possible in hands by the cultural institutional and organizational traditions of the Nordic nations, which I think Estonia belongs to, because we had a almost one thousand years of a certain culture of holding the society together, and that has help us to defend in ourselves also in cyber area.

Then we have a more intelligence lead gentlemen agreement model, which is the UK-model; where certain entities have good cooperation, coordination and agreements already that's back times it as already coordination takes back to the cold War times, were Critical Infrastructure is important and now this has been extended to cyber issues.

Then we have a third model which is more top-down, regulatory model. This more deregister model possibly is thus continental-European or central-European or that some people says – French model. But I do not think we should associate this to one country, so, they is good see there fill that we should regulate. That we should tell to da private sector what to do or how exact to do it. So, this kind of tendency is to see as well. So, as you know that EU proposal for a cyber directive still in the EO right now, and there policy makers are still deciding what kind of model and how, were and when this EU legislation will come out.

So, what this legislation possible should achieve is a little more unified cyber resilience across the EU because we have quite a bit differences about different regions and different countries in EU right now.

So, to ramp-up the national part of my presentation at before I will start at some comment at the international part I should say that when we came to the national defence & national security the successful national cyber defence model is already a multi-stakeholder model. It has to be a civilian and military cooperation that is based on it. It should have involvement by the private sector, it should have support of broad civilian base and possible the best advise would be to have good national exercises with all the different national agencies and organizations involved and star doing this often almost as possible in cyber and then a model comes together. So, if you are looking for an advise in this national part.

The second very important part to make cyberspace more stable, is to have a good international cyber policy. In Cyberspace what we have seen in the last decades is still a, it is a "baby policy", is what I called that! It is not comparable event to the traditional

international is very known what to do. We have some such agreements within the Governments, we have the clear understanding of the behavior of the biggest actors. In cyber we just are doing the first steps and so, it is good very clear news that yesterday night, actually, there was a very important set of cyber norms agreed at the OSCE, which stands for the Organisation for Security and Cooperation on Europe, on that is exactly the countries are supposed to be doing in Cyberspace. So, we have the first set of cyber norms now agred by almost fifty countries and participating states and stakeholders, so instead. So, I think this is very pretty achievement and I regale that this happen, this going to be a very good model globally, because the OSCE as, you know, as a large number of countries, that will be taken by other important security regional organizations, like ASEAN regional forum, where China also is part, so and this is a big with for the diplomatic community internationally that we have the first set for cyber norms now agreed.

What is this set of cyber norms? What is exactly the states had agreed? They now agreed to start talking on cyber business to each other officially, because so far is that happen is some of the partners sometimes read some success in some cases, but there is no good model or no good idea how exactly we should carry out this kind of cyber information exchanges or what we should do when in cyber crisis hits us; who should be called in another country, if we want to. So, everything that we have so far more sis basically very informally. Now, there is a first [formal], or a little more formalized norm agreed between the countries. So, then still politically and military field but hopefully that norms, the cyber norms some point also involve more stakeholder community.

So, the second step that we need to do internationally, is to make sure, is the «rule of law» and then the existing Laws, nor new Laws applying in Cyberspace. There are some calls for new treaties and new laws and sometimes in the biggest internationally organizations, and we «the cyber people» to think that new laws can fix Cyberspace. We have to apply the existing ones. We have the Budapest Convention for Cybercrime to address problems related to criminal activities in Cyberspace. We have the International Humanitarian Law, that has set very long time ago. The principles of kindling of behavior of the States during in conflicts. So, this is just has to applying now to Cyberspace, because that really, do not matter how do I hit you. I need to follow the some moral principles right! So, then we have other international Laws, like human Right Laws and other status that apply in Cyberspace. So has It was mention already before by our US colleague, we need to keep an Internet free and open. At this has been a big debate during last year. How exactly we will be doing it and we possible need a little better coordination between the lightly maid countries and not so also the lightly maid coutries to convince that the current model were the private sectors in the leads, exactly what we need for the future generations and economic growth. And this is our big goal for the next coming years and how we actually convince the countries that are just very poor or not very resourceful in technology field or fields that have different size of digitally divine. I think what we have to really concentrate on that capacity building and to find the right way to do it this also very important. Maybe, we should start to asking the countries that are stealing really at the beginning of these technologically development what exactly they should become, to help them and how to make them more resilient already from the outcome set, because they should not repeat our mistakes that we put all the system up than restart security with then maybe is possible for them have a little more resilient elements already in before they develop those systems. A Capacity building is one of the areas which is a possible that the biggest priority for the European External Action Service (EEAS), because the development aids are our traditional niche, we have here marked some funnies for the next 5 years for the project and we are going to find the model that works for us in the EU and of course we should coordinate that s globally, whit our partners. So how we can actually bring together in to the development countries, communities and cyber communities is still are? The second question is to actually to have a good understanding on the priorities in third countries what to be achieved there and also the question is: how to private sector would factoring to this project.

So, we try to organize this in the areas of workshops and events to answer these questions in the next year and it will be our absolute priority to make Cyberspace much more secure. Thank you.

Fonte http://www.youtube.com/watch?v=gyPsx1EyNfI, Consultada em 10/jun./2014.

Palestras e Intervenções (Seminários, Colóquios, Conferências, etc.)

Operações sobre Redes e Sistemas de Informação [CNO – (CND), (CNE) e (CNA)]

"I have one topic that I want to touch on here, which is 'CNE and CNA', and that is maybe a kind of bureaucratic for some folks listening, but if you had been working for the government, the idea on that, is cyber espionage and cyber attack are two different things and they belong to perhaps two different organizations, and I think one of the things is that probably behind that and on sometimes is hard to tell the difference between in cyber offence and cyber defence. I think the largest the skills set, sometimes the hacker can just be someone who knows your network better than you do and uses that information for nefarious purpose. The virtual skills on some way and one of the philosophical and practical debate in Washington DC, is the difference between – Computer Network Espionage or Computer Network Exploitation (CNE) and Computer Network Attack (CNA). […]" Seminário Web da autoria de Kenneth GEERS, Senior Global Threat Analist da empresa FireEye Inc., com a duração de 59':17" relacionado com (GEERS, 2013) - http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/new-fireeye-report-world-war-c.html que pode ser ouvida, após simples registo, em https://www.brightalk.com/webcast/7451/88921 entre 43´:14" e 46´:02". Consultado a 01/06/2014.

Vigilância Generalizada, Privacidade e Direitos Fundamentais

"First of all, a big tank you to the rapporteur Claude MORAES and their great job and the fellows shadow rapporteures on the match, The very proud that the only Parliament, the only Parliament and the only institution in Europe that has raced this issue, with very limited means, we conducted the inquiry, where the Councilor has been shame fully silent, they has not even them put

officially on the agenda of the Council. Massive violation of the rights of the European Citizens has been ignored by the Council. Shame on you! […]. Why not opposition politicians? They want to stop then. They even listening, not only, to the mobile phone of Mrs. Markel or Mr. Holland, even Mrs. Feinstein. How means far this will go? How can be sure that is not the very fabric of our democracy, the rule of law that we are talking about and a fined unbelievable that the European Popular Party (EPP) still hesitations here and ECR [*European Conservatives and Reformists Group* no *EP*] Is actually gone to vote against. This House was a standard for the right of European citizens, for democracy, for the rule of law. The way is late out our treaties. That is our job!" *Sophie in 't VELD 11 Mar 2014 plenary speech on Report: Claude MORAES (A7-0139/2014) – US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights* em http://www.vieuws.eu/alde/alde-sophie-in-t-VELD-on-us-nsa-surveillance-programme/;Consultado a 02/mar./2014.

A.v – Documentos e diagramas complementaress sobre os temas

Documentos

Conclusões da Cimeira de Cardiff (Gales) da OTAN sobre Ciberdefesa/Cibersegurança

"**72** As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."

"**73** We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies." De 4 e 5 de setembro de 2014.

Artigo -do autor- publicado na imprensa local – Jornal «Atlântico Expresso»

Iniciou-se a 1 de julho um período de seis meses de Presidência Italiana da União Europeia (UE). Este período segue-se a outro de igual duração da responsabilidade de outro Estado-membro: a Grécia. Este hiato de tempo, trás algumas expetativas devido à estreia no novo Primeiro-ministro de Itália que ganhou de forma algo inesperada as eleições naquele país. O Senhor Matteo Renzi, de trinta e nove anos, veio trazer «uma lufada de ar fresco» à desgastada e desacreditada forma de fazer política italiana. Este jovem político vem de funções desempenhadas na cidade toscana de Florença ao nível do poder municipal com razoável sucesso.

Foram colocadas na Agenda da Presidência Italiana vários e complexos assuntos que porão à prova a «arte» do Primeiro-ministro e da sua equipa dentro de portas – na(s) Itália(s) da «Lega Nord» e do Sul, incluindo o problema dos imigrantes clandestinos subsaarianos – e na Presidência do Conselho Europeu de Chefes de Estado e de Governo da UE até dezembro. Só para falar em alguns desses assuntos, lembramo-nos: da entrada em funcionamento da nova Comissão Europeia presidida pelo Senhor Jean Claude Juncker, após os votos contrários do Reino Unido do Senhor David Cameron e da Hungria do Senhor Viktor Orban; das escolhas do Colégio de Comissários e as almejadas paridades entre sexos, norte-sul, atlântica vs. «mitteleuropa», velhos e novos; das escolhas do futuro Presidente do Conselho da UE e do Vice-Presidente e Alto Representante da Ação Externa e Política de Segurança da União; das 6ª e 7ª rondas das negociações da futura parceria transatlântica ou TTIP; da redefinição de uma estratégia, até outubro, da UE para a Energia, após os graves problemas na península da Crimeia e consequentes pressões da Rússia à Ucrânia e de sansões à Federação Russa (FR); das implicações destas na redefinição da estratégia sobre o Clima; e de, pelo menos, sete prioridades relacionadas com as Tecnologias de Informação e Comunicação (TIC):

1. A ratificação pelo novo Parlamento Europeu (PE) e as consequentes negociações, supõe-se finais, com o Conselho da UE sobre o novo Regulamento de Proteção de Dados (DPR), posto na Agenda pela, até agora, Vice-Presidente e Comissária para a Justiça, Direitos Fundamentais e Cidadania, a luxemburguesa Senhora Viviane Reding. A DRP é cada vez mais pertinente, depois do «chumbo», do Tribunal Supremo de Justiça da UE (ECJ), da Lei de «Retenção de Dados» relativa às

telecomunicações no Espaço da União, consequência da rejeição do Tribunal Constitucional Alemão e de processos interpostos provenientes de outros Estados-membros;

2. A viabilidade do acordo com os EUA conhecido por «Safe Harbour» ou «Porto Seguro», após constatação de várias irregularidades quanto à proteção de dados de cidadãos europeus entrados nos EUA (o caso de vigilância generalizada efetuada pela Agência Nacional de Segurança/NSA) e de empresas europeias que «acusam» algumas americanas, que assinaram o acordo, de ter tido acesso a informação privilegiada e da consequente concorrência desleal, uma vez que, nos Estados Unidos não há Legislação de Proteção de Dados;
   https://www.huntonprivacyblog.com/2013/11/articles/eu-commission-recommends-changes-safe-harbor/
3. «O direito em ser esquecido» ou «Right to be forgotten» que opõe mais de 41000 queixas de cidadãos europeus (que pugnam pela alteração ou remoção de informação pessoal incorreta, desatualizada ou mesmo não autorizada) ao gigante americano Google e que está no ECJ. Este caso foi agudizado com as denúncias do ano passado relacionadas com o acordo «Safe Harbour» do ponto anterior;
4. O caso das Aplicações disruptivas (como a aplicação Uber que permite a partilha de serviços de táxi por mais do que um utilizador e que tem indisposto os taxistas de várias cidades europeias, nomeadamente em Londres.
5. O caso dos Direitos de Autor supostamente infringidos pela visualização de televisão nos dispositivos móveis telemóveis e «tablets», como por exemplo, utilizando a aplicação Aereo e que tem colocado os gigantes de televisão contra a UE pela obsoleta lei do Copyright e de Proteção da Propriedade Intelectual;
6. O caso do, suposto, monopólio da Google no mercado das Aplicações para Android e a queixa no ECJ interposto pela empresa europeia Apploid, sedeada em Barcelona;
7. Por fim, e de novo, a Google e o caso da discriminação de entidades não parceiras daquela nos resultados de pesquisa do seu «motor de busca» e a posição da «Net Neutrality» ou «Internet Neutra», defendidas pelos Comissários Nelie Kroes, Joaquin Almúnia e Michel Barnier e que corre no ECJ e para a qual se espera uma decisão, ainda, durante a vigência desta mesma Presidência.

Como se pode verificar, será uma Presidência de Conselho intensa, complexa e multifacetada. Logo se verá se a Itália e o Senhor Renzi poderão contribuir da melhor forma para o bem comum dos cidadãos e da UE.

Diagramas Complementares

Diagrama –do auto - expandido a (Ilustração11) de Cyberdefesa da OTAN

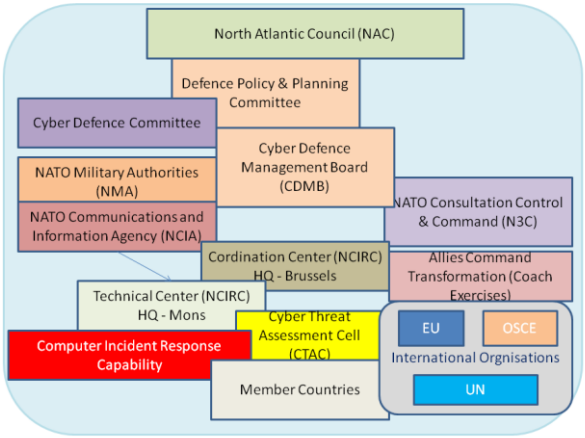

Diagrama –do autor- de capacidade de [Cyber] dissuasão da PESC da UE