Relatório de Participação no Eurodig 2017 – European Dialogue on Internet
Realizado entre 5 e 7/6/2017 – Tallinn – Estônia
Conselheiro – Luiz Fernando Martins Castro

Resumo dos temas abordados, aspectos principais, e recomendações colhidos nas sessões assistidas.

Segunda-feira, dia 5/6/2017

Sessão 1 - Liberdade de imprensa na Ucrânia

Modelo soviético de comunicação, com controle estatal, passando para o modelo capitalista, controlado por oligarquias, com total falta de transparência e violência contra jornalistas.
Ressaltada a necessidade de jornalistas críticos - papel na informação - buscar fontes fidedignas.
Na Estônia – o jornalismo sofre influência dos países nórdicos – com liberdade de escolha e autonomia, onde a confiança é o maior capital. Transição do modelo estatal para o privado, juntamente com processo educacional - incluindo políticos.
Enquanto estatal, tinha que dizer o que o estado quer. Hoje existe guerra comercial.
Forte influência nas eleições, reproduzindo o problema geral, pan-europeu.

Ações do Conselho da Europa -
Apoio ao desenvolvimento do marco legal na Ucrânia.
Transparência da propriedade das mídias. Experts para dar consultoria, workshops, construção de marco legislativo. Compromisso do país com a EU.
Fortalecimento das capacidades dos grupos diretivos das empresas e apoio financeiro.
Questão da segurança dos jornalistas – Investigações efetivas das autoridades sobre ameaças a jornalistas, tratamento judicial adequado. Observatório de ocorrências de violações: Portal Media freedom
www.coe.int/en/web/media-freedom/ukraine
Efeito de colocar pressão nas autoridades.
Ainda que o CE esteja apto a apoiar, a implementação é do país.
Sugestão - enviar jovens para viver a experiência na Europa.

Sessão 2 - Willian Drake - Forced data localization

Internet global não existe mais – ela é basicamente local ou regional.
World Bank - os benefícios da informatização ainda não foram democratizados, os benefícios vão para os big players da indústria.
Problema de 'law enforcement' – ineficácia e complexidade do MLAT.
Os 'big palyers' utilizam as plataformas para ganhar dinheiro.
Desconfiança nos atores:
- Os principais atores têm dinheiro para fazer lobby.
- Existem camadas política, comercial e econômica.
- Necessidade de construção de confiança entre os stakeholders.

Os usuários suportam os custos das violações.
Como lidar com a diferença de ambientes legais e regimes?
Muitas incertezas - a discussão não é transparente.
As políticas internacionais - acordos comerciais bastarão para aplacar as questões derivadas do problema?
Recomendação: Uso de leis de direito humanos para tratar a questão.

Dia 1 - terça feira – 6/6/2017

1ª. Plenária - Como a Governança da Internet me afeta?

Importância de integrar os jovens para se garantir o futuro da internet.
Importância de considerar a China, que deve ser integrada.
Não se volta o relógio do tempo.
A única forma de sobreviver é lutar por igualdade e distribuição de possibilidades para todos.
Nos últimos 10 anos houve progresso, mas também retrocessos.
Cyberconflicts – da "Cold war" à "Code war".
No final dos tempos superou-se a guerra fria, agora temos que evitar a guerra dos códigos.
Multistakeholder é o modelo viável para a internet, a gerar Confiança, numa Internet para todos.
As políticas devem ser globais.
Especial atenção aos direitos dos menores de 18, sobretudo de acesso à educação.
Obra referida sobre o tema: 'Tallinn manual - how internal law apllies to internet' - Cambridge press, 600 pages - NATO Centre - Casos, hipóteses e soluções legais.
Ameaças à liberdade de expressão, notícia de bloqueio de acesso a domínios, por pretensas infrações a direitos de autor.
Necessidade de Accountability.

2a. Plenária - Cybersecurity

Cooperação Internacional necessária - o desafio é a regulamentação e criação de marco legal comum.
Cooperação entre service providers – dados estão for a das fronteiras.
Não temos os multistakeholders tratando da questão da segurança.
A governança do cyberspace não protege o cyberspace.
As pessoas esperam segurança do governo, que deve liderar os esforços multissetoriais.
Cybersecurity é parte disso.
Ex.: As pessoas estão satisfeitas com a votação *on line* e anônima.
Necessidade de padrões internacionais para a IoT para assegurar maior segurança.
A Sociedade de Informação precisa de confiança, prevenindo incidentes e não apenas lidando com eles.
Segurança é direito básico dos consumidores, que devem ser empoderados em termos de segurança.
Cyberspace não é uma selva, porém problemas não resolvidos no mundo real não o serão na Internet ...

A sociedade civil pode ser poderosa. A responsabilidade deve ser doméstica, local, com normas internacionais de segurança comuns.
Os Shutdowns e monitoramento sob argumento de segurança pode colocar em risco direitos humanos e outros.
Excesso de regulação pode impactar a liberdade.
Proposta: códigos abertos, para possibilitar as soluções antes dos problemas surgirem
Não há uma 'bala de prata', mas a segurança deve ser buscada, globalmente, envolvendo a indústria, stakeholders, com educação, respeito aos direitos humanos e confiança dos usuários

Conferência - Key note - Erna Solberg - Primeira-ministra da Noruega

Nenhum país é capaz de lidar sozinho com as ameaças na internet.
Limites tênues entre o que pode ser regulado ou não.
Na Noruega, entendimento que a internet é global, aberta, responsável, transparente e representativa.
As escolhas políticas farão a internet mais desenvolvida e inclusiva.
Deve haver previsibilidade.
Uma maior digitalização, se mal conduzida, pode gerar alienação digital.
Prioridades: trabalho conjunto para remover barreiras, criar empregos, uso de dados para apoiar serviços públicos.
Preocupação especial com Cybersecurity e dados pessoais sensíveis.
"Nordic Baltic Cooperation" – objeto: Smart cities, segurança pública, remediação de desastres.
Para fortalecer o digital market temos que ser realistas. É pressuposto a existência de alto nível de competência e educação digital.
Trocas de experiência com a Estônica, que é digital by default e inspira.

Painel - Internet in the post-truth era.

Termo 'fake-news' está na moda.
Sobreposição – entre pós-verdade e fake news
Viés ideológico não pode ser chamado de 'fake news'.
Percebeu-se que a Internet pode minar a sociedade.
Quantidade imensa de informações – novo ambiente – incapacidade de administrá-la ou fazer uso crítico.
Era da pós-verdade – polarização da sociedade.
Não se trata de novidade, mas como avaliar a informação?
A verdade está sendo desconstruída, para se capturar o público.
Não há mais preocupação com a objetividade: como se avalia a informação?
Informação é movida por dados.
Propaganda x 'fake news'. Esta é produzida por interesses econômicos.
Isso seria por si só ilegal?
Quais os limites da liberdade de expressão?

Relato de caso da jornalista finlandesa – Jessikka Aro - atacada por 'fake news' lançadas por russos, que estava pesquisando para reportagem.
Levantamento de seu dossiê judicial, caso de uso de drogas.
Nem tudo que é disruptivo é bom!
"From fake to hate"

Para conter fake news, devemos:
Fortalecer a aptidão de análise da informação - "literacy".
Fortalecer a força de jornalistas, que devem ser educados.
Reescrever algoritmos.
Fortalecer checadores de notícias – 'Fact finders'
Monitoramento. Não cobrir notícias falsas, chacar a origem, endereços web.
Auto e co-regulação.

Dia 2 – quarta-feira - 7/6/2017

IoT and human rights

Ambiente onde eficiência é privilegiada à segurança.
Guia do Conselho da Europa sobre proteção de dados tornou-se obsoleto ante o Big Data.
Direito de controle e de Live escolha. Uso ético dos dados. Políticas de uso claras e transparentes.
'Privacy by design'.
Como assegurar a conexão estável e ininterrupta para dados na nuvem?
Soluções técnicas para diferentes soluções. 'Edge computing'.
O usuário está ciente que seus dados estão indo para a nuvem? Onde está baseada? Qual a legislação aplicável? Regras contratuais.
O sistema daria retorno ao usuário, para que ele, por exemplo, pudesse economizar energia?
No caso de monitoramento de crianças e idosos, é seguro ter dados na nuvem?
Brinquedos – qualquer dado envolvendo crianças deve ser protegido.
A questão não é apenas saber onde estão os dados, mas quem pode ter/terá acesso a eles?
Você, empresas, governos? Por quanto tempo?
As pessoas devem ser conscientizadas – direitos humanos em risco.
Ética – como fazer uso que reverta aos indivíduos?
Riscos de Espionagem Industrial. Esforços de Segurança.
Necessidade de se trabalhar numa base ampla de IPv6.
Efeito na quantidade de dados, que aumenta incrivelmente, independentemente de nossa percepção e alerta. Conscientização obrigatória. Consentimento é necessário.
Nova Identidade - a quantidade de dados sobre mim cria um perfil do qual eu não posso me afastar.
Risco de apropriação do espectro pelos entes privados.
You have a company to run, you need the things under control
Organização do espectro é necessária para lidar com tamanha quantidade de dados.
Na maioria dos casos uma tecnologia 'low power' pode bastar além da adequação da tecnologia, mais compacta.
Ética se torna cada vez mais importantes, como o papel dos Comitês de Ética de Organizações Nacionais e Internacionais.
'DHBio committees'.
Anonimização não é mais efetiva.
Temos que ter a visão do ciclo completo dos dados.
Mercados globais – atores globais. Dados financeiros e de localização.
Regulação pelo lugar de estocagem e ou da coleta?
Propriedade dos dados – tema crucial, por ex.: na agricultura.
A segurança dos dados depende do quanto você ganha com eles?
'Natural risks management' – tsunamis – necessidade de espelhamento, e planos de contingência.
Importância da discussão para nos manter informados e atentos ao problema
Finalidade última da IA é a proteção do ser humano e não a sua ameaça - Asimov

Painel - Multistakeholder model and cybersecurity

A Internet não é regulamentada por governos.
Diferentes atores na internet, cada um tem que assumir a responsabilidade na sua parte.
Perspectiva contratual – definição de responsabilidades.
Legislação – deve considerar a habilidade do poder legal atuar e o setor privado não fazer,
Governos têm que fazer a parte dele. Aspecto colaborativo, o que reforça a importância do modelo multissetorial.
Proteção de redes e de dispositivos.
Necessidade de se ter um CERT.
Governos são responsáveis pela segurança da população e da infraestrutura crítica - criar resiliência.
Os fabricantes devem assegurar que os dispositivos que colocam no mercado não se tornarão 'bots'.
Cada player tem que saber o que fazer: cias. de energia, telcos, transporte, saúde, públicas ou provadas – igualmente.
'Wannacry' – a solução não veio de governos, mas de distintas partes atuando junto.
Distintos stakeholders possuem distintos interesses.
Modelo do CGI.br - pór nós relembrado - foi apreciado como foro de discussão que congrega diferentes pontos de vista e interesses.
Ressaltei a questão da independência, estabilidade política e financeira do CGI.br.
Importância da criptografia, sem a qual não haveria internet nem comércio eletrônico.
A matéria da legalidade da criptografia deveria ser fruto de uma decisão multissetorial e não apenas da polícia e Ministério Público.
Todos os argumentos são individualmente válidos. A abordagem colaborativa é fundamental. Distintas lógicas. Importante troca de informações e experiências.
Ainda que os governos tomem a frente da discussão, considerados os Direitos Humanos e enfrentamento legal, o fenômeno é global.
Necessidade da acordos globais de comércio e governança da Internet.

Encerramento – Próxima Eurodig 2018 – prevista para ser realizada na Geórgia.