IV Fórum da Internet no Brasil
Pré IGF Brasileiro 2014

Relatório Completo

Trilha: Segurança e Privacidade

Data: 25/04/2014

1. INTRODUÇÃO

A **Trilha 2 – Segurança e Privacidade** do IV Fórum da Internet do Brasil e Pré IGF Brasileiro 2014 foi realizada no dia 25 de abril de 2014 no Grand Hyatt Hotel em São Paulo (SP). A coordenadora da trilha foi Nazaré Bretas, representante do setor governamental e conselheira do CGI.br. Os painelistas foram representados pelos quatro setores que compõem o CGI.br:

- Setor Academia: Ricardo Dahab, Universidade Estadual de Campinas (UNICAMP);
- Setor Empresarial: Edmundo Matarazzo, Instituto de Tecnologia de Software (ITS);
- Setor Governo: Coronel Camelo, Centro de Defesa Cibernético do Exército Brasileiro (CDCiber);
- Terceiro Setor: Sérgio Amadeu, conselheiro representante do Terceiro Setor do CGI.br e professor da Universidade Federal do ABC (UFABC).

Por fim, foi convidado para participar como comentarista internacional Jacob Appelbaum, do Projeto Tor.

Assim, o relatório divide-se em quatro partes:

1) Temas discutidos, consensos e dissensos na trilha;

2) Exposição dos Painelistas;

3) Exposição dos Participantes nos Grupos de Aprofundamento;

4) Anexos.

2. TEMAS DISCUTIDOS

Foi identificado como tema apontado pelos painelistas e participantes da trilha:

a. Políticas Públicas e Ambiente para Inovação

2.1. Políticas Públicas e Ambiente para Inovação

Tabela 1 - Posicionamentos sobre o tema Políticas Públicas e Ambiente para Inovação

Academia	**Setor Empresarial**
• O ambiente para inovação no país (política, legislação, cenário macroeconômico) é totalmente inadequado, inclusive considerando a baixa participação do setor TIC na economia e na sociedade. • No âmbito das políticas públicas, é mais adequado apoiar as empresas com potencial de crescimento do que apoiar as *startups*. • A indústria deve ser tratada como principal vetor de inovação. • É necessário abrir o mercado brasileiro à competição mundial para incentivar a inovação e o empreendedorismo. •	• A inovação não se restringe a grandes empresas, e tem nos pequenos negócios um terreno fértil, mas as políticas de fomento estão distantes da pequena empresa. • A capacitação é essencial para que os processos de inovação gerem resultados. • A capacitação das pequenas empresas é um pressuposto para que a inovação seja gerada em grande escala. • A legislação brasileira não está preparada para tratar/absorver/aprimorar a inovação. • É necessário aproximar os pequenos provedores de Internet das incubadoras e universidades. • É necessário criar um programa de capacitação para os provedores de Internet. • É necessário absorver as inovações por meio de premiações e editais de pesquisa. • É necessário criar o SIMPLES da inovação.

Governo	**Terceiro Setor**
• A capacitação dos empreendedores em negócios inovadores de alta tecnologia é insuficiente. • *Open Innovation* é o sistema que mais se adequa ao processo de inovação e evolução da Internet no mundo. • O principal gargalo da inovação está no desenvolvimento de produtos e negócios. • Existe incentivo e fomento governamental para a inovação de Tecnologias da Informação e Comunicação – TIC. • Existem recursos e políticas públicas disponíveis para inovação e empreendedorismo. • A inovação deve ser apropriada pela sociedade, seja pela forma de negócios ou inovação social. • O processo de inovação na Internet deve ser aberto; deve considerar tanto o aperfeiçoamento do funcionamento da Internet como o desenvolvimento de serviços e aplicações.	• Importância do conceito de *Permissionless Innovation* para manter o dinamismo da Internet. • Estimular *hackerspaces* como ambientes propícios para inovação.

Tabela 2 - Posicionamento dos Participantes sobre o tema Políticas Públicas e Ambiente para Inovação

- O governo precisa ter uma política pública de inovação mais agressiva.
- Toda a inovação está ligada ao desenvolvimento da indústria que está em um contexto de “desindustrialização”.
- Há um ambiente inóspito para inovação no Brasil.
- É preciso criar mecanismos de incentivo a inovação a partir de diferentes espaços e tipos de iniciativas.

Tabela 3 - Consenso sobre o tema Políticas Públicas e Ambiente para Inovação

- Para todos os setores, há necessidade de capacitação de pessoas para incentivar a inovação.
- Setores governamental e empresarial e terceiro setor concordam sobre a relevância dos pequenos negócios para a inovação.
- É necessário criar mecanismos para garantir que a inovação seja absorvida pela sociedade.
- É necessário aumentar os incentivos aos processos de inovação e empreendedorismo no cenário brasileiro.

Tabela 4 - Dissensos sobre o tema Políticas Públicas e Ambiente para Inovação

- Os setores empresarial e acadêmico entendem que o ambiente brasileiro é desfavorável para o fomento da inovação, ao contrário do entendimento do setor governamental.
- Ao contrário do setor governamental, o setor acadêmico e os participantes entendem que o país passa por uma "desindustrialização", o que é prejudicial aos processos de inovação.
- Há divergência quanto ao papel do setor acadêmico no processo de inovação.

Tabela 5 – Pontos a Aprofundar sobre o tema Políticas Públicas e Ambiente para Inovação

- Incentivo a startups versus empresas de alto rendimento.
- O papel do professor/pesquisador face à inovação.
- *Hackerspace como* instrumento de promoção de práticas inovadoras.
- Criação do SIMPLES para a inovação.
- Conceito de *Permissionless Innovation*.
- Planos de desenvolvimento para a inovação no Brasil.

3. EXPOSIÇÕES DOS PAINELISTAS

A **Trilha 2 – Segurança e Privacidade** teve a apresentação de quatro painelistas que representavam quatro diferentes setores, o Setor Empresarial, representado pelo ***Edmundo Matarazzo***, ***do Instituto de Tecnologia de Software (ITS)***, a Academia representada por ***Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP)***, o Terceiro Setor, que teve como painelista ***Sérgio Amadeu, conselheiro representante do Terceiro Setor do CGI.br e professor da Universidade Federal do ABC (UFABC)*** e o representante convidado para expor pelo Setor Governo foi ***Coronel Camelo, do Centro de Defesa Cibernético do Exército Brasileiro (CDCiber)***. Além dos painelistas, a trilha contou com um comentarista internacional, ***Jacob Appelbaum***, ***do Projeto Tor***.

RESUMO DA EXPOSIÇÃO DOS PAINELISTAS
O representante do terceiro setor, **Sérgio Amadeu**, comentou sobre o impasse vivido pelos Estados Unidos, que consegue proteger suas fronteiras físicas, mas o ciber espaço ainda é um problema. O resultado foi a criação de vigilância em massa para conter seus inimigos. Apontou também que Snowden parou uma lei americana que previa dar o acesso a todos os dados de empresas e clientes dessas empresas americanas ao governo, pois a economia da informação depende da interceptação de informação para ter alguma vantagem competitiva. Finalizou apontando que o artigo 15 do Marco Civil da Internet é a lei mais avançado do mundo pois defende privacidade e a neutralidade da rede. **Edmundo Matarazzo, Instituto de Tecnologia de Software (ITS)**, destacou a separação entre segurança, algo técnico e concreto, e privacidade, algo intangível e abstrato. Explicou cinco pontos de metodologia para segurança: disponibilidade, confidencialidade, integridade dos dados, controle e auditoria. Finalizou reiterando dificuldades da privacidade ser intangível e abstrata, sendo

que apenas a lei escrita não resolverá as problemáticas deste tema. **Coronel Camelo, do Centro de Defesa Cibernético do Exército Brasileiro (CDCiber)** declarou que os estudos na área cibernética existem há mais de duas décadas, contudo, é uma luta diferente da tradicional, pois não há como matar o byte do mal. Finalizou dizendo ter ficado satisfeito com a discussão do Tema do Marco Civil da Internet pela sociedade brasileira. **Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP)** tratou das temáticas de sua linha de pesquisa, segurança de informação e criptografia. Destacou três acontecimentos que modelaram os últimos anos, como as revelações de Snowden, o bug do OpenSSL que liberou várias chaves criptográficas e o Marco Civil da Internet no Brasil. Defendeu maior ação da Sociedade Brasileira de Computação (SBC) e que todos aprendessem noções básicas de computação para se defenderem. Para o professor, o governo precisa ouvir mais todos os setores da sociedade para criar boas políticas públicas de segurança e privacidade.

3.1. Apresentação do Terceiro Setor

O terceiro setor foi representado por ***Sérgio Amadeu, conselheiro do CGI.br e professor da Universidade Federal do ABC (UFABC),*** que expôs questões relativas à privacidade, deixando claro que não é possível tratar do tema sem falar também de segurança e economia. A apresentação foi baseada no livro "*In Athena's Camp: preparing for the conflict in the information age*", escrito por dois estrategistas norte-americanos que conta a história de uma revolução, cuja base é representada pela ideia que está havendo uma mudança na guerra que os Estados estão travando e irão travar: "Preparação para o conflito neste mundo exigirá a mudança para novas formas de organização... a informação e o conhecimento estão se tornando os elementos-chave do poder". O livro faz um paralelo interessante com a atual situação das fronteiras dos Estados Unidos. O país afirma ter pacificado suas fronteiras, com México e Canadá, a sul e norte, respectivamente, tem o domínio de seus limites marítimos, com os porta-aviões e seu poder militar, mas não tem o domínio das fronteiras interna e ciberespacial. De acordo com o conselheiro do CGI.br, por causa disso em conjunto com os acontecimentos de 11 de setembro, os Estados Unidos consideram qualquer pessoa como um potencial inimigo do Estado e a forma de vigiá-los se dá por meio da massiva espionagem de cidadãos comuns.

Isso acontece hoje em um cenário complicado, pois o tráfego de dados na Internet chegará a 1,4 zettabytes até 2017. É por conta disso que se monta aparatos de segurança e vigilância e se busca cada vez mais controlar o ciberespaço por meio de *data mining*, de *big data*, de coleta de informações dos cidadãos na rede: "A ciberguerra não tem fronteiras...não respeita cidadãos nem instituições...".

Definindo vigilância massiva, o painelista apresentou que esta se realiza a partir da entrega das nossas informações para um conjunto de corporações de tecnologia da informação (TI). Nesse contexto, é combinado o poder militar com o poder persuasivo que é feito a partir dos dados dessas empresas, a

quem as pessoas entregam os dados de maneira desavisada e despreocupada, ou seja, entregam prazerosamente seus dados para essas entidades. Citou como exemplo os termos de uso da Microsoft que permite inclusive que esta empresa entregue as comunicações das pessoas para cumprir a lei aos órgãos legítimos sem detalhar quais seriam estes tais órgãos.

Outro exemplo nessa mudança é visto na cada vez maior utilização de *drones*, sendo que nos últimos cinco anos o número de pessoas mortas por *drones* cresceu assustadoramente no governo Obama.

Em razão das denúncias de Edward Snowdem foi paralisado um projeto de lei nos Estados Unidos, cujo potencial é nefasto no entendimento do painelista: o *Cyber Inteligent Sharing and Protection Act of 2013* (CISPA). Este projeto de lei quer legalizar a articulação entre as empresas e o governo federal para compartilhar informações com a finalidade de prevenir ou organizar a defesa diante de ataques cibernéticos. Se aprovado, permitiria que as empresas entregassem os dados ao governo sem a necessidade de autorização judicial. O projeto encontra-se no Senado norte-americano desde abril de 2013 e contava com o apoio de empresas como Facebook; HP; Oracle; Intel; entre outras.

A economia da informação depende da interceptação, ou seja, depende do uso das tecnologias cibernéticas que são de comunicação e controle para poder analisar esses dados e lucrar sobre eles. Assim, a base da espionagem massiva, que é realizada por Estados, é feita sobre essa camada de violação de privacidade por motivos econômicos.

O representante do Terceiro Setor apontou que a solução dada pela comunidade hacker para evitar a violação da privacidade é a utilização da criptografia que não impede a captação desses metadados, mas dificultam o acesso aos mesmos. Deve-se buscar como saídas privadas, ou seja, individuais: usar criptografia no dia a dia; dificultar a captação de suas informações; e, atrapalhar, confundir e bloquear a formação do perfil e padrão de consumo. Como saídas públicas, o painelista sugeriu que deve haver uma legislação clara nos países de defesa de privacidade, declarando que todos os

dados guardados sobre o cidadão devem ter a sua concordância consciente e informada, diferentemente dos atuais termos de uso pouco claros providos pelas empresas. Não é possível proibir a coleta massiva de dados porque arrebentaria a estrutura da economia, mas esse tipo de ação pode ser regulada em prol da garantia da privacidade.

Concluiu a fala lendo o artigo 15 do Marco Civil da Internet, que, em sua opinião, é a lei mais avançada do planeta porque defende a privacidade e a neutralidade de rede. Entretanto, para ser aprovada teve uma grande dificuldade e acabou tendo artigos como o 15 que trata da guarda de logs. O problema do art. 15 é estender a guarda de logs a todo mundo, o que faz com que não haja condições de resguardar nada, dificultando a defesa da privacidade que é o maior problema de segurança do mundo. No ponto de vista do painelista, o Marco Civil da Internet (Lei nº 12.965/2014) deu um tiro no pé com esse artigo, aprovado, em grande parte, por conta da pressão de parte da Polícia Federal. Por fim, ressaltou que se deve cortar essa ideia de vigilantismo em massa, que promove a militarização da Internet, por meio da aprovação da proteção de lei de dados pessoais.

3.2. Apresentação do Setor Empresarial

O setor empresarial teve como painelista **Edmundo Matarazzo**, **Instituto de Tecnologia de Software (ITS)**. Em primeiro lugar, o painelista destacou que trabalhou em várias organizações da área das telecomunicações em âmbito nacional e internacional. Assim, propôs trazer várias visões sobre o tema que é complexo, pois mistura tecnologia e conceitos técnicos com direitos humanos, gerando uma confusão enorme, já que as pessoas não precisam conhecer tecnologia pra conhecer seus direitos e, às vezes, uma visão tenta sobrepor a outra.

Sobre segurança e privacidade, diferencia ambos apontando que segurança é algo que se consegue tocar e é principalmente técnica, enquanto

a privacidade é algo intangível, sendo esta última muito mais complexa de ser compreendida, entendida e protegida.

No contexto da tecnologia existem muito problemas para enfrentar, pois trata-se de um ambiente complexo formado por múltiplas tecnologias, múltiplos atores e múltiplas combinações. Portanto, pensar em como proteger a privacidade lida com esses diversos atores, sendo que as pessoas só têm controle sobre o terminal do usuário.

Quando se fala de segurança, existe uma tradição que envolve cinco objetivos para se garantir a segurança: disponibilidade, confidencialidade, integridade dos dados, controle e auditoria. O problema dessa metodologia para garantir a segurança é que esta varia conforme o ambiente. Portanto, o contexto de segurança varia muito conforme o ambiente e não está sob controle do usuário nas palavras do painelista.

A definição de privacidade faz parte de uma discussão longa sobre sua determinação, caracterização e como se consegue torná-la tangível. A relação entre privacidade e segurança possui uma distância enorme. Outra discussão importante para a sociedade é o balanceamento entre o direito de privacidade e o interesse público. O painelista comentou que essa discussão precisa ser feita.

Por fim, reiterou que a privacidade é algo mais intangível e difícil de ser resolvido porque não se pode usar um sistema qualquer, pois este tema já está enraizado em cada sociedade e a mesma revolucionará a discussão de direitos das pessoas pelo mundo e irá incomodar muitos governos. No entendimento do painelista isso será um desafio porque a tecnologia não define direitos ou a melhor forma de utilizar a Internet. Contudo, a tecnologia está transformando a sociedade e transformando-a em sociedade da informação. Já existe por volta de 8 gigabytes por habitante no planeta e a tendência é que aumente e as pessoas fiquem mais expostas. O painelista finalizou apontando que não acredita que simplesmente escrever a lei resolverá o problema desse tema até que o mesmo esteja enraizado na sociedade e vê no Fórum da Internet essa

importância, pois reúne diferentes pessoas e visões que ajudam a encontrar a melhor direção para a questão.

3.3. Apresentação do Setor Governo

A apresentação do setor governo foi feito por ***Coronel Camelo, do Centro de Defesa Cibernético do Exército Brasileiro (CDCiber)*** que teve como objetivo demonstrar como o Ministério da Defesa está vendo a questão da defesa cibernética. Os estudos sobre a área da cibernética já são feitos a mais de duas décadas. Mas os grupos puderam convergir esses resultados em 2008 quando a estratégia nacional de defesa foi publicizada. A partir daí as Forças Armadas começaram a se estruturar para lidar com a questão cibernética que é diferente de um combate tradicional que a área militar atua, pois não existe a possibilidade de se matar o "byte do mal". Em primeiro lugar, houve uma compatibilização das áreas de ciência e tecnologia. Também foram estruturadas as ilhas de segurança da Defesa. Houve um trabalho importante na busca de recursos humanos para essa área nas Forças Armadas.

O painelista detalhou que há interação com a área de cibernética de outros países, mas não há o propósito de absorver nenhuma cartilha desses outros. O CDCiber vem sendo procurado por diversos países devido a sua estrutura. Há uma expectativa em relação à defesa cibernética porque, enquanto em outros armamentos o país está há 30, 40, 50 anos defasados e é um conhecimento que nos será continuamente negado, a cibernética apresenta outras possibilidades.

Para Camelo, a sociedade está em um momento muito importante da história, pois se deve prestar atenção nas situações de ataques cibernéticos como o emprego na forma militar para desaparecer um país durante algumas horas. Também comentou que ficou satisfeito com a discussão desse tema com o Marco Civil, pois a sociedade está tomando mais consciência que deve pedir privacidade e proteção. Uma sociedade consciente é um instrumento

poderosíssimo tanto de dissuasão quanto de amadurecimento rápido do país para que possa chegar a resultados mais significativos. É importante a voz da sociedade para auxiliar na definição das regras e ampliar a discussão, impedindo erros.

3.4. Apresentação do Setor Academia

Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP) representou o setor academia e tratou especificamente da área de segurança de informação e criptografia que é sua linha de pesquisa.

Antes de iniciar a fala sobre o tema mencionou alguns acontecimentos: 1) as revelações do Edward Snowden causaram impacto pela ousadia porque se imaginava que existia espionagem, mas não o tamanho dessa trabalho e a falta de limites e respeito da *National Security Agency* (NSA) dos Estados Unidos; 2) foi espalhado um bug que também causou grande impacto, até na mídia e causou muito espanto porque em um pedaço de software que é usado pela maioria das instalações de servidores, web e de outros componentes que usassem o OpenSSL e liberou várias chaves criptográficas; e, 3) a aprovação do Marco Civil da Internet (Lei n. 12.965/2014) que carrega e desperta muitas discussões como as já tratadas nessa trilha.

O painelista defendeu que esses três acontecimentos tiveram efeitos interessantes e muito sérios, além de trazer a sensação de que a segurança da informação não é uma coisa que precisa ficar ou deve ficar restrita ao debate de especialistas, ajudando a trazer para mente das pessoas a importância de proteger dados, de entender quais são os problemas, mesmo que seja de forma rudimentar as pessoas precisam entender um pouquinho melhor o que significa apertar o botão de aceito dos termos de uso. Já existe na nossa sociedade a impressão digital das pessoas e esta pode ser usado como substituta da impressão tradicional das pessoas, caracterizando um problema muito sério na visão do representante da academia.

Para Ricardo há uma tensão evidente entre querer se expor na Internet e ao mesmo tempo preservar a privacidade em determinadas questões. Para resolver esse tipo de tensão é necessário prover meios para que essas questões possam ser materializadas e um esforço técnico grande para colocar ferramentas à disposição que possam ser usadas pela sociedade. O problema é que soluções não podem ser meramente técnicas, mas também devem ser bem embasadas. Do governo deve haver transparência e dos cidadãos é preciso prover privacidade. Essas coisas contribuem para que a solução seja muito complexa, não só no sentido técnico, mas no sentido do convencimento das comunidades pertinentes a esse problema.

Dahab comprometeu-se a falar da academia e o que este setor tem feito ou acha que deve ser feito e também dar um testemunho do quão pouco tem sido feito. Por mais que se tenha estabelecido uma comunidade e a comunidade esteja crescendo todo é questionado se ninguém vai falar nada dos aspectos de privacidade e se pronunciar em nome da academia no Fórum da Internet. Não tem uma voz organizada e isso é uma coisa que a academia precisa fazer: se organizar, aparecer, como um ente, uma entidade em que a sociedade vê. A maioria dos centros de pesquisa de ponta do Brasil são públicos e essas pessoas devem algum tipo respostas para essa sociedade que paga esses pesquisadores.

Para ele, já tem alguns nichos da academia que há estudos de segurança de alta competência e de presença internacional. Alguns dos membros da academia já conseguiram produzir ciência a ponto de virar padrão internacional da indústria, especialmente na área de criptografia que é mais avançada. Também existe uma crescente colaboração internacional e um congresso regional na América Latina que vem angariando cada vez mais um número maior de pessoas e não é difícil trazer nomes aqui para o Brasil, pois já há uma reputação já estabelecida.

Na opinião do painelista a Sociedade Brasileira de Computação (SBC) poderia contribuir de formar mais decisiva, influenciando e incentivando a formulação de currículos específicos de segurança da informação nos

currículos universitários, pois se todo que fizessem primeiro o curso de programação, aprenderiam que toda vez que se lê uma variável, lê um dado, antes de você colocar isso na memória, a pessoa olha o que você tá trazendo para dentro do seu computador. Ter um papel mais evidente e participativo nas políticas de governo é uma coisa que a academia precisa fazer e não é fácil fazer essas coisas. Acha que A SBC tem esse papel, papel centro nisso, e poderia fazer esse trabalho melhor.

Apontou que vê a existência de um vazio no Brasil, pois ninguém tem uma presença predominante e não tem nenhuma voz que é ouvida com confiança sobre a questão da segurança da informação. A Europa, por exemplo, manteve uma rede de criptografia com vários países, e assim criaram uma enorme comunidade lá e foram coisas organizadas sem muito dinheiro. Simplesmente aproveitavam as potencialidades de cada grupo e replicavam isso com algum dinheiro para encontros etc. Mas foi uma estratégia organizada e pensada. Depois, como passo seguinte, foi criada uma agência europeia de segurança da informação e fundaram um órgão cuja única a fazer é pensar em soluções técnicas para garantir a cidadania. Que é disso que a gente esta falando aqui. Como recomendações mais gerais que esse trio de atores precisa fazer é: a) se preocupar com mais formação em segurança e tecnologia da informação; ter mais foco e organização por parte do governo com programas direcionados de financiamento, bem como mais diálogo para isso e mais cooperação com a indústria em fóruns claros e transparentes, e, c) criação de centros de pesquisas voltados exclusivamente para esse aspecto de cidadania e proteção.

O governo deve ser uma coisa mais do que, simplesmente, as Forças Armadas como representante único do governo nessas gestões de segurança da informação. O painelista entende que o governo como um todo precisa se organizar e ouvir mais as outras entidades sobre o tema.

3.5. Comentarista Internacional

O membro do Projeto Tor, ***Jacob Appelbaum***, iniciou sua fala agradecendo o convite para participar no Fórum e declarando que todas as pessoas deviam agradecer ao Edward Snowden e Sara (que salvou a vida de Snowden) porque é por causa deles que o diálogo proposto pela trilha pode ocorrer nos dias de hoje. Juntamente com o Wikileaks, sem essas situações este tipo de diálogo não teria acontecido e os discursos não incluiriam coisas como vigilância de massa e ações da comunidade de inteligência. De acordo com o comentarista, agências de inteligência estão se intrometendo na vida das pessoas e colocando sociedades inteiras em vigilância.

Na sua apresentação, traz como discussão inicial a existência de algumas vacas sagradas, especialmente algumas coisas que as pessoas tomam como garantidas nas discussões: 1) Vigilância traz segurança; 2) A sociedade precisa de serviços secretos e da comunidade de inteligência; 3) A forma correta de se agir nesse conflito não é uma guerra cibernética e deve-se fortalecer as Forças Armadas. O comentarista discorda totalmente dessas três alegações.

A discussão tratada na trilha, na opinião dele, não é apenas sobre segurança e privacidade, mas de agência, liberdade, dignidade, de autodeterminação e, claro, também de privacidade. A liberdade, a capacidade de escolher, a dignidade, a capacidade de determinar o que será feito da vida dele são impactadas pelo sistema que o Edward Snowden revelou. O cerne da discussão é se a sociedade quer democracias e se as que existem serão mantidas.

Tratar de privacidade é também tratar a questão da igualdade, liberdade e irmandade. Portanto, nesta trilha está se falando em algo muito mais ampla, mas que foi resumido em única palavra. Acredita que a pergunta seja: “Quando uso um computador, será que posso falar com outra pessoa pelo computador sem outra pessoa ouvir? Será que sou capaz de fazer isso?”.

As revelações do Snowden tiveram grande importância para responder essas questões, pois nos mostrou que existe uma grande batalha entre a segurança da informação e as agências de inteligência. Todo mundo está sob vigilância e de diferentes formas. Uma das formas são as pessoas que estão invadindo empresas e instalando coisas ou obrigam as empresas a se tornarem agente secreto do Estado. Para o painelista, se as pessoas quiserem estabelecer uma comunicação entre duas partes ou mais é necessária uma criptografia mais forte. Essa é a principal defesa para garantir quando alguém utiliza a violência de invadir a privacidade, pois se não encontrar a fonte da mensagem também não vai poder entender os sistemas que estão utilizados e só irá receber dados criptografados. É necessária uma fonte de números aleatórios que o atacante não possa prever e isso garantirá que uma mensagem possa ser devidamente criptografada. Ao sabotar padrões e conseguir compreender a mensagem isso permite, em primeiro lugar, a vulnerabilidade para outros explorarem a mensagem porque não é apenas a NSA que irá exploras esses dados. E muitas vezes, diferentemente do caso do Snowden, as pessoas vão pegar esses dados e ninguém vai saber que isso ocorreu. Esse ponto é extremamente perigoso no entendimento do comentarista. Além disso, isso mina as instituições fundamentais que são parte da sociedade e que as pessoas deviam confiar e é preciso instituições que digam o que pode ser feito em relação à isso.

Além disso, a forma como essas coisas estão acontecendo, fundamentalmente sugere que ainda existe um super poder no mundo. E não é assim. Simplesmente não é o caso. Porque a eletrônica que governa as pessoas é multipolar por natureza porque é projetada por um conjunto de pessoas, fabricada por outro conjunto de pessoas e programada por um terceiro conjunto de pessoas. Em cada camada cada conjunto desses de pessoa mantém um tipo de controle e seus controles não são exclusivos. O que isso significa é que cada dispositivo, em cada rede pode pertencer a uma entidade diferente. Pode ter lealdade nos chineses na parte do hardware e dos americanos na parte do software, e em termo de configuração, em quem tiver

invadido o sistema. O que isso most5ra é que no mundo multipolar, esses dispositivos provavelmente não são de confiança e não há forma, no momento, de garantir que estes sejam de confiança. Então, temos que aceitar que o mundo é multipolar. Isso significa que algumas decisões têm que ser diferentes. Uma delas, que é absolutamente crítica para o comentarista, é que se deve olhar as coisas em termos de igualdade. O maior problema é que ao invés de procurar igualdade, as pessoas estão procurando dominância. É o que as Forças Armadas querem e isso se reflete aqui na própria trilha. Então, é importante se perguntar se as pessoas querem militarizar a sociedade na Internet e se isso vai trazer a sociedade para mais perto da democracia. O comentarista rejeita totalmente a militarização da Internet porque acha que se deve lutar pela democracia. Para pensar nisso, se deve pensar em termos de construir a paz e não a guerra. E para isso, é necessário avançar as coisas, como a segurança da comunicação, por exemplo. Algumas pessoas sugeririam que o que deve ser feita é ter uma discussão honesta de como mundo é espiado e todo mundo é um espião. Em primeiro lugar, nem todo mundo esta espionando não; segundo lugar, pra aqueles que espionam, isso não é feito o de forma igualitária. Deve ter um sistema seguro, mas não se deve sacrificar a democracia e nem os veículos de comunicação aberta, que são o cerne de uma vida livre, para isso. As pessoas devem se proteger, mas isso deve ser feito de forma civil e não militar construída através da paz e para isso é necessário ter software livre para ter a liberdade.

As pessoas precisam ter as quatro liberdades. A primeira é aquela que permite examinar o código fonte, mudá-lo e compartilhar. Também é preciso um hardware livre. É necessário melhorar a capacidade de fabricação porque quando se controla os meios de produção isso permite controlar o resto das vidas das pessoas. Essas liberdades são pré-requisitos para uma sociedade livre e devem ser feitas em termos transnacionais e não apenas nacionais.

Para a sociedade ter chance, é preciso a total transparência. Transparência total não significa a destruição da liberdade individual, ao

contrário, significa que em todas as instituições as pessoas vão compreender como estas funcionam e trabalham.

Snowden revelou que há uma maciça conspiração de pessoas, organizações e estruturas que existem fora, e as vezes são estruturas estatais. Quando as comunidades de inteligência trabalham juntas para tratar as informações pessoais como moeda, como fluxo de informação e depois trocam essa informação entre si, além de qualquer supervisão e obrigação constitucional, que proteção de direitos as pessoas tem?

Acaba-se com um mercado não regulado e não irrestrito de troca de informações. E são assassinadas pessoas a partir do uso desses dados. O programa de *drones* é o exemplo exato disso. Dados de vigilância para servir a política de assassinato. Política que é alimentada por esses dados de vigilância. Então, vai contra tudo que a sociedade avançou no século XX para ter liberdade, justiça e transparência. A transparência total vai ajudar na próxima vez que alguém ter uma política de assassinato, pois é possível saber quem é essa pessoa, em que posição ela está, em que cargo essa pessoa está, e a sociedade poderá tirar essa pessoa desse cargo.

Acesso aberto à informação é pré-requisito também para muitas outras coisas. É importante garantir que as pessoas tenham acesso à informação, que as informações sejam abertas e disponibilizadas a todos para detonar as barreiras de classe social, de gênero e de nacionalidade. Deve se reconhecer que o Estado tem que tratar de forma igual e não com base no passaporte das pessoas. Na opinião do comentarista, o Brasil está liderando o caminho com o Marco Civil da Internet, embora ache que existe uma falha em relação à censura e retenção de dados.

Outro aspecto importante é o anonimato. Ter anonimato é importante, pois ajuda contra a perseguição de pessoas que mostram um erro de segurança. Muitas vezes as autoridades ao invés de se preocuparem com o erro de segurança, se preocupam com o mensageiro e o perseguem e o mata.

Hoje é falado sobre guerra cibernética em que muita gente irá morrer por conta disso. Isso deve ser evitado.

Os governos, em particular, possuem uma tensão porque não gostam que a liberdade cresça além do seu controle e é isso que é a vigilância. A vigilância trata não de segurança, mas de controle, de domínio, de uma forma assimétrica de controle que não é democrática, em quase todos os casos. Quando falamos de vigilância, a polícia age e é preciso remover isso. Não deveria ter uma câmera observando, vigiando todo mundo o tempo todo. Ninguém mais deveria fazer isso. As pessoas não estamos livres. Não estão acorrentados, mas não é liberdade. Claro que fica mais difícil um cara se levantar e me dar um tapa, principalmente quando nós consideramos que um dos opressores administram esses sistemas. E quando suas mãos estão acorrentadas, isso vai ajudá-los a cometer mais injustiças. Então, não é que a supervisão nos traz segurança, mas dão poder às pessoas que vão utilizar a vigilância de uma maneira não democrática. Não é preciso serviço secreto, às vezes é preciso atividade. Por exemplo, a importação de ferramentas atômicas é uma coisa que deve ser descoberta e achar as pessoas que proliferam essas armas, isso é importante e também pode ser feito civis e não precisa ser feito por agentes secretos ou pessoas que entram na casa alheia sem permissão. Isso não precisa acontecer do jeito que está acontecendo. É preciso negar a comunidade de inteligência e desmontar as partes que são absolutamente necessárias para nenhuma segurança, sem retorno positivo e pegar as outras coisas que são boas, positivas e assegurar que sejam de construção civil com supervisão, transparência, responsabilidade e objetivos específicos, com valores constitucionais de sustentar liberdade dos indivíduos e sociedade.

Não é preciso equilibrar liberdades fundamentais assim porque não é um trade-off, são liberdades fundamentais, são direitos fundamentais, não se pode equilibrar dessa maneira.

Por fim, apresentou sua proposta radical para a questão da vigilância e alertou que, no momento, ninguém concorda com ela. Sua proposta é que a vigilância deve ser sempre detectável. As vacas sagradas dizem que a vigilância deve ser sagrada, caso contrário as pessoas mudam seu comportamento. Isso é o reconhecimento tácito de que vigilância é controle e

ser observado leva a uma mudança de comportamento. Isso deve ser reconhecido e passar para frente. Quando uma autoridade não legal fizer a vigilância, pode ser notificada a sua autoridade plena que isto aconteceu; e desse jeito algum dia pode terminar essa questão.

É importante que atacar a narrativa do terrorista que diz que existe uma pessoa desumanizada e que não merece liberdades civis. É necessário erradicar isso. Ninguém no planeta deve ser desprovido de suas liberdades civis e ninguém deve ser terrorizado. Detectar a vigilância permite reganhar uma ideia de segurança, uma ideia de que se as autoridades mentem para a sociedade e que é uma temática, pode trazer, talvez, um pouco de verdade. Os "malvados" têm dinheiro e poder e podem evitar a vigilância. São os outros, no caso nós, que não tem dinheiro e poder e que necessitam dessa sensação, dessa segurança e de transparência, porque vai nos ajudar a trazer *accountability* para a sociedade que somos todos nós.

3.6. Debate dos Painelistas

A coordenadora da trilha convidou o conselheiro do CGI.br, Cássio, a dar sua opinião sobre o tema porque ele seria inicialmente o coordenador desta trilha, mas não pode por questões de saúde.

O conselheiro declarou que concorda com quase tudo que o Sérgio Amadeu falou. Ressaltou que o tema da trilha tem duas posições: a prevenção e a reação, sendo que se tem trabalhado muito mais no segundo do que no primeiro. Prevenção quer dizer conhecimento e saber do que se trata as condições e termos de uso para usar a Internet para o desenvolvimento e inovação. Considera o lado negro da Internet aquele que as pessoas utilizam a rede para proveito próprio, realizar crimes, entre outras coisas. E isso se relaciona com a guarda de logs e é importante acabar com a impunidade. Deve-se trabalhar para evitar a impunidade e garantir a privacidade.

4. EXPOSIÇÃO DOS PARTICIPANTES

- ***Hegle, advogada autônoma***: perguntou sobre uma dúvida em relação aos registros de conexão e registro de acesso, questionando quais registros de conexão podem ser guardados por um ano e os registros de acesso que são proibidos pelos artigos 13 e 14 da Lei do Marco Civil da Internet. E também questionou como isso se aplica na prática como na utilização da Internet, na consulta de website e no uso de redes sociais. Por exemplo, Skype que não é rede social talvez pudesse ser considerado como telefonia e nesse caso entraria a legislação ou não? O Whatsapp é outro caso que mistura telefonia e Internet. Por fim, perguntou qual seria a relação e se isso seria aplicado no Marco Civil;
- ***Sérgio Amadeu, conselheiro do CGI.br e professor da UFABC,*** respondeu a questão detalhando que o registro de conexão é obrigatório e o registro de acesso também por seis meses conforme disposto no artigo 15 do Marco Civil da Internet que obriga a registrar e guardar o log. Exemplificando, uma pessoa acessa um provedor de blog qualquer sem fins comerciais que esta hospedado no Brasil e deve-se guardar o registro por seis meses. Sugeriu que as pessoas baixem o Lightbeam[1] que mostrar para as pessoas todas as informações que são enviadas do site que está visitando outros sites naquele momento;
- ***Edmundo Matarazzo, ITS-SP***: auxiliou na resposta sobre a guarda de logs no Marco Civil. Elucidou que, na verdade, a guarda de logs é uma invenção oriunda de uma situação que acontece nas telecomunicações convencionais. Quando se fazia chamada telefônica desde os primeiros tempos, todas as chamadas eram registradas. É gerado um registro de chamada para poder cobrar por ela. Então, esses registros passaram a ser registros de chamadas que também eram utilizados nas investigações, apurações etc. Não tem gravação da conversa e são apenas os registros

[1] http://www.mozilla.org/en-US/lightbeam/

como o número que chamou, hora da ligação e duração da ligação. Para gravar uma chamada especificamente ou para poder ter o conteúdo da comunicação, existe muita discussão se isso é possível pela nossa Constituição e para fazer isso é necessária uma ordem judicial específica para colocar um grampo naquela chamada telefônica. Isso foi considerado muito importante e quando se discutiu Internet foi definido que deve ser feito a mesma coisa. A guarda de log é uma tentativa de se fazer a mesma coisa, que é o registro de suas conexões e registros de seus usos na Internet. O problema é que a tecnologia é diferente. Quando é feito isso na Internet se coleta muito mais informação do que quando é realizado o registro de uma chamada telefônica. Assim, o objetivo acabou um tanto quanto deturpado porque o exemplo que foi usado para criar essa ideia é diferente. Isso vale para qualquer uso da Internet. Sobre aplicativos como o Whatsapp, isso pode estar somente dentro da rede de dados da operadora local e não necessariamente estar usando a Internet. Com certeza a pessoa está usando a internet quando usa um browser. Apesar da tentativa, o que existe atualmente mesmo, no Marco Civil sobre esse assunto, é ainda muito pouco esclarecido para entender se funciona ou não. Independente do uso, qualquer que seja o aplicativo, este não é considerado um serviço de telecomunicações, ou seja, é um aplicativo de TI ou um aplicativo de Internet. Portanto, ficam fora da legislação e fora dessa regra;

- ***Edson Fontes, professor***: perguntou aos painelistas Coronel Camelo e Sérgio Amadeu, qual o modelo que eles sugerem para segurança cibernética brasileira.
- ***Coronel Camelo, CDCiber***: declarou que não tem uma resposta única para definir qual é o melhor modelo de segurança cibernética para o Brasil, considerando, contudo, o brasileiro como o melhor modelo. Para fazer o modelo brasileiro houve interação com os modelos de outros países também. Geralmente, se conhece pouco dos outros modelos porque estes são fechados e os acessos são negados. Um dos modelos utilizados pelo país é chamado de Doutrina Militar de Defesa Cibernética, mas este não é o

único utilizado. Em 2009, o primeiro modelo de defesa cibernética se dividia em sete áreas básicas como área científica, área de pesquisa e desenvolvimento, de capacitação. Já surgiram áreas complementares a essas, transformando-se em dez, baseando-se nos fundamentos do setor cibernético por projetos. São estabelecidos objetivos e produtos específicos em cada uma dessas áreas e esse projeto já está no terceiro ano de implementação. Logo depois começaram a surgir outros modelos complementares e ainda estão surgindo, que a própria evolução da área de segurança cibernética tem mostrado. Por exemplo, um dos laboratórios que está sendo usado para isso são os grandes eventos como Rio +20, Copa das Confederações, Copa do Mundo e Olimpíadas. Portanto, o modelo de defesa cibernética nacional ainda está sendo construído. Algumas coisas têm que ser inventadas, no bom sentido, a roda, porque isso é negado ao Brasil por outros países, enquanto em outras questões já se trabalha com tecnologias consagradas.

- ***Edmundo Matarazzo, ITS-SP***: também apresentou suas considerações sobre qual seria o melhor modelo de segurança cibernética para o país, apontando que existe outro problema muito sério de segurança e de arquitetura de segurança relacionado aos pequenos e médios empresários e às pessoas físicas. As pessoas não sabem se proteger e não sabem configurar uma proteção no seu terminal. As pessoas necessitam desse tipo de conhecimento e de mais informação disponível. Isso é tão importante quanto uma arquitetura de defesa cibernética;
- ***Claudia, Professora da PUC/SP***: apontou sua preocupação em relação à segurança das crianças e dos adolescentes na Internet e questionou como é possível, em termos tecnológicos e jurídicos, melhorar essa segurança na rede, garantindo os direitos das crianças e a criação de mecanismos por parte do governo que visam proteger as crianças na rede. Também pediu informações se o governo tem feito algo nesse sentido, já que esta tem sido uma recomendação importante;

- ***Sérgio Amadeu, conselheiro do CGI.br:*** respondeu ao questionamento de ***Claudia***, ***Professora da PUC/SP,*** ressaltando que não é com medidas de quebra de direitos dos outros que será garantido a segurança das crianças. A melhor garantia para a criança é a educação. A criança tem que ter um olhar claro. Outra proteção passa por uma legislação dura do governo, principalmente para essas coisas que não respeitam a faixa etária da criança e a formação psicológica dela. Mas isso não deve ser feito quebrando o direito das pessoas, guardando log e tornando tudo um festival do vigilantismo, pois não é assim que se garante a segurança das crianças. É um equívoco achar que a Polícia Federal não consegue pegar uma rede de pedófilo ou de pornografias. A suspeita deve levar a uma ordem judicial que permita agir. Esse é o padrão da democracia. Tem que haver suspeita e a ordem judicial. Ou seja, tem que haver uma ação pontual e não massiva;
- ***Edmundo Matarazzo, ITS-SP***: tratou da proteção das crianças, em contraponto à fala de ***Sérgio Amadeu, conselheiro do CGI.br***, dispondo que esta não pode estar sozinha na Internet como não pode estar sozinha na rua. Mas a tecnologia permite uma série de coisas. Existem exemplos em outros serviços que são interessantes como a televisão em que a maioria dos aparelhos tem uma função chamada controle dos pais. Fora do Brasil existem leis específicas, como nos Estados Unidos, que determinados conteúdos vem com informação que permite o seu bloqueio. A imagem não vai ser exibida e o canal não vai ser acessado. Isso é equipamento instalado lá no terminal, no aparelho de tv e é uma informação para quem tem o domínio daquele conteúdo. A consequência disso é que aquele vídeo que vai ser carregado por alguém na Internet precisa ser classificado para que você possa ou não barrar o acesso a esse material. Existe um grande equívoco de que levar a Internet para as escolas resolverá o problema do aluno. A criança não tem capacidade ou discernimento para utilizar a Internet. Então, é preciso ter professores preparados e ter uma estrutura de acesso à informação bem definida para

que a criança acesse primeiro aquilo que é importante para a sua formação e depois aprenda a utilizar a informação que está aberta e livre na Internet, garantindo que a criança saiba o que é um site confiável e o que não é um site confiável;

- ***Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP)***: complementou a discussão sobre a segurança da criança na Internet, apontando que as pessoas podem instruir o seu browser a não entrar em alguns sites e podem ser criadas listas que evitam o acesso de certos sites por crianças. Mas, para isso, é necessário se caminhar para desenvolver algum tipo de confiança quando a pessoa está navegando. Porque as pessoas terão as listas de sites onde seu browser não entra. Existem pesquisas que estão olhando para novos modelos da Internet e como organizar as novas gerações da Internet. Algumas delas falam, por exemplo, que não é necessário mais ter endereço fixo na Internet. As pessoas vão buscar dados na Internet e não mais coisas que estão em um lugar fixo. Esse modelo apresenta menos ameaças à privacidade porque não se tem a localização e endereço na Internet que não são mais fixos. A Internet desenvolveu até hoje e ninguém se preocupou com segurança. Então, essas coisas precisam entrar nessas discussões dos novos modelos, por exemplo, tem gente propondo que a Internet seja totalmente criptografada. Por trás disso tudo é importante conscientização das pessoas, tornando isso um pouco mais simples e conseguindo deixar as pessoas conscientes dos problemas que está sendo enfrentado em relação à privacidade e segurança. Em parte, esse evento e os últimos acontecimentos trazem isso à tona. Não se trata, também, de ficar vendendo pânico, mas as pessoas têm que estar conscientes dos perigos da rede;
- ***Diego***: perguntou para o professor ***Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP)*** se ele acredita mesmo que os universitários e que a academia possa fazer uma contribuição para o tema

de segurança e Internet pro Brasil e pro mundo e se o professor acha uma utopia pensar que as universidades trabalhem em rede algum dia;

- ***Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP)***: respondeu ao Diego declarando que não acho que seja utópica a ideia de cooperação na comunidade acadêmica, deixando claro que só depende da comunidade querer. No tema de segurança são várias áreas interagindo que envolvem aspectos técnicos, jurídicos, sócio-culturais. Então, ter uma comunidade variada e que consiga conversar e que se reúna frequentemente é muito importante. Isso ocorre no país por meio de simpósios a cada ano em algum local diferente. Entretanto, apontou que ainda tem certa barreira da universidade com as pessoas que mexem com segurança como hackers do bem, mas que não estão na universidade. Alguns professores já fazem algumas competições de segurança que a pessoa pode se inscrever mesmo que você não seja universitário. Não considera que o problema da academia seja a falta de motivação e é bastante otimista a respeito disso;
- ***Nazaré Bretas, representante do setor governamental e conselheira do CGI.br***: fez perguntas para professor ***Ricardo Dahab, da Universidade Estadual de Campinas (UNICAMP), Edmundo Matarazzo, ITS-SP*** e o ***Coronel Camelo, CDCiber***. Questionou ao professor se algum momento foi pensando em estratégias ou se ele acha que cabem estratégias para que o patrimônio que existe em pesquisa genética seja levado para outros grupos de pesquisas em outras áreas do conhecimento. Da mesma forma, gostaria de saber do representante do setor empresarial como esse setor coopera nesse segmento. Do mesmo modo pediu essa mesma reflexão ao Coronel sobre as Forças Armadas;
- ***Edmundo Matarazzo, ITS-SPL***: respondeu ao questionamento de ***Nazaré Bretas, representante do setor governamental e conselheira do CGI.br*** tratando da cooperação no setor privado em assuntos de segurança. A segurança no setor privado é algo bastante difícil, porque, primeiro, custa caro e existe desconhecimento do que isso pode trazer de benefícios e

como isso deve ser implementado na empresa. O problema é ainda mais delicado no grupo de empresas de pequeno e médio porte que dependem do uso de tecnologia de informação, mas não possuem nenhum apoio e condição de trabalhar as questões de segurança. O que tem se tentado fazer nesse segmento é usar as associações e os institutos para tentar reunir esses pequenos empresários, em torno dessas entidades e a partir daí, conseguir gerar uma ferramenta e algum apoio para que estes possam desenvolver um pouco mais essas questões de segurança. Também apontou que não é só o empresariado que carece dessa informação, mas as pessoas físicas precisam de mais informação sobre o tema, necessitando entender um pouquinho melhor o que é estar em risco e o que pode acontecer quando usam a Internet. Ressaltou também que a linguagem é muito importante, pois quem vai usar um sistema de segurança necessita entender o que está fazendo;

- ***Coronel Camelo, CDCiber***: Com relação de governo e de nível de maturidade ao que diz respeito ao tratamento de aplicação do processo de segurança, o CDCiber não tem um mostrador que tenha precisamente esse acompanhamento porque não trata exatamente o foco da entidade que trabalha em parceria com outras entidades, mas não realiza avaliação dos parceiros. Com sua experiência em segurança afirmou que a diferença é brutal em parceria de segurança no governo, mas está longe do que gostaria porque a própria estrutura do governo cresceu muito, as ameaças, também, mudaram e se multiplicaram. A cooperação não funciona mais como deveria porque são muitas organizações com finalidades, priorizações e conscientizações diferentes em relação ao tema. A máquina do governo é muito grande e muito complexa. Então, os resultados em termos de grupo, são lentos, mas sem dúvida melhoraram muito nos últimos anos. Claro que, se houvesse uma aceleração em termos de legislação, em termos de conscientização mais ampla do que já acontece, talvez isso pudesse ter resultados mais imediatos. Por exemplo, apesar de existir uma Política

Cibernética de Defesa, não há uma política nacional que aponte para todos os setores da nação.

5. DEBATES DE APROFUNDAMENTO

Na Trilha 2 – Segurança e Privacidade os participantes foram divididos em cinco grupos que debateram sobre os seguintes temas:

- Educação em segurança e privacidade
- Privacidade e Espionagem
- Princípios e Direitos Fundamentais
- Inimputabilidade da Rede e Remoção de Conteúdo na Internet

5.1. Tema: Educação em Segurança e Privacidade

5.1.1. Grupo 1

Consensos

O grupo apresentou os seguintes consensos sobre o tema:

- Elaborar, estimular e disseminar materiais educativos, campanhas e estratégias de formação que facilitem a compreensão, apropriação do Marco Civil e da Governança da Internet entre crianças, adolescentes e jovens para conscientização em torno da cidadania digital e direitos humanos (e não do pânico moral), com linguagens adequadas às diferentes faixas etárias;
- Potencializar as campanhas sobre uso seguro e responsável da Internet para os operadores do sistema de garantia dos direitos das crianças e adolescentes com vista à efetivação da prioridade absoluta prevista no artigo 227 da Constituição Federal e no Estatuto da Criança e do Adolescente, em sintonia com o artigo 26 do Marco Civil da Internet;
- Obrigatoriedade da inclusão do tema segurança e privacidade no currículo escolar ligadas às iniciativas de inclusão digital, em programas como Banda Larga nas Escolas e letramento digital;
- Incentivo a pesquisas não apenas nas universidades, mas incluindo escolas de ensino médio e organizações da sociedade civil para pesquisa e desenvolvimento para ampliar os recursos à SL, criptografia

e demais ferramentas que contribuam na promoção da segurança na Internet;

- Estimular com que os termos de uso e termos de privacidade nos sites de redes sociais e aplicações sejam compreensíveis e legíveis de forma mais didática, facilitando a compreensão sobre os mecanismos de configuração dos serviços através de centrais de segurança e ajuda dos serviços com mais destaque.

Dissensos

- Usar os mecanismos de anúncios em redes sociais e aplicativos para disseminar orientações sobre uso seguro e responsável da Internet, com atenção às questões de privacidade, liberdade de expressão e legislações relativas aos direitos humanos na Internet.

Pontos a serem aprofundados

- Qualificar os debates em torno das concepções sobre terrorismo para que este tema não sobreponha os direitos humanos e temas relacionados como privacidade, liberdade de expressão, liberdade de associação e possibilidade de manifestações de movimentos sociais na Internet;
- Programas de garantia da segurança de CA não sejam violadores dos demais direitos como liberdade de expressão, privacidade e respeito à dignidade;
- Estimular pesquisas e debates para que possamos criar novos formatos de termos de privacidade e formas de uso de dados pessoais para que os usuários possam ter maior controle sobre os dados compartilhados não apenas na lógica do contrato de adesão “tudo ou nada”;

Participantes do Grupo

1	Rodrigo Nejm - SaferNet
2	Vânia Correa
3	Rafael Silva
4	Sebastian Roa
5	Gutierrez Silva
6	Izabela Silva
7	Olívia Lopes
8	Letícia Cardoso
9	Monique Costa
10	Luiz Felipe Bessa
11	Saulo Mota
12	Evelin Haslinger
13	Jefferson Leme
14	Anderson Jorge
15	Daniela Rueda
16	Diego Henrrique

5.1.2. Grupo 2

Consensos

O grupo apresentou os seguintes consensos sobre o tema

- Importância da alfabetização digital/currículo com segurança na educação;
- Pais precisam ser educados quanto aos riscos e segurança;
- Importância de um profissional da área de tecnologia nas escolas;
- Simplificar o uso das tecnologias de segurança – configurações iniciais com padrão de segurança instalado;
- Educar/responsabilizar empresas e desenvolvedores visando a entender/analisar o impacto de seu negócio na sociedade.

Dissensos

Não foram apresentados dissensos pelo grupo.

Pontos a serem aprofundados

- Custos de segurança para o usuário final;
- Como educar o usuário para entender o modelo de negócio dos "serviços gratuitos";
- Desafio de criar espírito critico/análise de conteúdo.

Participantes do Grupo

1	Cristine Hoepers – CERT.br/NIC.br
2	Klaus Jessen – CERT.br/NIC.br
3	Thiago Everton Vieira – Universidade Estadual do Ceará
4	Claudia Prioste

5.2. Tema: Privacidade e Espionagem

5.2.1 Grupo 3

Consensos

O grupo apresentou os seguintes consensos sobre o tema:

- Espionagem cibernética como ferramenta de ganhos políticos e econômico;
- Existe uma demanda para maior educação das novas gerações: compreensão de que a privacidade é um ativo econômico, e como lidar com a utilização desse meio em geral.

Dissensos

- Conceitos de Monitoramento e Vigilância;
- Limites da Intervenção Estatal;
- Utilização ou não de Softwares e Hardwares livres.

Pontos a serem aprofundados

- Desenvolvimento de programas que ajudem o usuário comum a criptografar seus dados, caso decida fazê-lo.

Participantes do Grupo

1	Caroline Zurakowski Nogueira - Relatora
2	Susana Jenifer Leone
3	Luana Aparecida dos Santos Rosa

5.3. Tema: Princípios e Direitos Fundamentais

5.3.1 Grupo 4

Consensos

O grupo apresentou os seguintes consensos sobre o tema

- Ampliar a participação direta de crianças, adolescentes e jovens (com representatividade das cinco regiões do país, de gênero étnica e pessoas com deficiência) nos debates e espaços de decisão sobre governança da Internet com mecanismos de apoio formal para participação em eventos como o CGI, Fórum da Internet no Brasil, IGF (Youth Panel), comitês do Banda Larga Nacional, Banda Larga nas escolas e audiências públicas relacionadas à segurança privacidade na Internet.

Dissensos

Não foram apresentados dissensos pelo grupo.

Pontos a serem aprofundados

- Estruturar espaços, formatos e metodologias de formação e preparação para participação direta de crianças, adolescentes e jovens nos fóruns de governança e consolidação do *Youth Panel Brasil*.

Participantes do Grupo

1	Rodrigo Nejm - SaferNet
2	Vânia Correa
3	Rafael Silva
4	Sebastian Roa
5	Gutierrez Silva
6	Izabela Silva
7	Olívia Lopes
8	Letícia Cardoso
9	Monique Costa
10	Luiz Felipe Bessa
11	Saulo Mota
12	Evelin Haslinger
13	Jefferson Leme
14	Anderson Jorge
15	Daniela Rueda
16	Diego Henrrique

5.4. Tema: Inimputabilidade da Rede e Remoção de Conteúdo na Internet

5.4.1 Grupo 5

Consensos

- Deve haver responsabilização da rede na medida em que: não retira conteúdo ofensivo após respectiva solicitação; demora demasiadamente na resposta de solicitações; não estabelece uma forma segura de identificação de perfis reais dos usuários, dificultando os perfis “fakes“;
- Cookies deveriam ser proibidos (propaganda abusiva fere os direitos do consumidor).

Dissensos

Não foram apresentados dissensos pelo grupo.

Pontos a serem aprofundados

- O que é ofensivo?
- Se algo publicado para um grupo de pessoas é encaminhado para pessoas não pertencentes ao grupo, há que se falar em violação de privacidade?

Participantes do Grupo

1	Ana Frank – Pedagoga (Terceiro setor)
2	Hegle M. Zalewska – Advogada