

Ministério das Comunicações



Ministério das Comunicações

Comissão de Ciência e Tecnologia, Comunicação e Informática – CCTCI

Comissão de Defesa do Consumidor – CDC

Comissão de Fiscalização Financeira e Controle – CFFC

Comissão de Legislação Participativa – CLP

Comissão de Relações Exteriores e de Defesa Nacional – CREDN

Câmara dos Deputados

Brasília, 14 de agosto de 2013



Pauta

- ❖ Dimensões estratégicas da Internet e das telecomunicações
- ❖ Aspectos críticos nas comunicações globais
- ❖ Ações empreendidas pelo Governo

Dimensões estratégicas da Internet e das telecomunicações



Dimensões estratégicas da Internet e das telecomunicações



- Direito à privacidade e à intimidade dos cidadãos
- Liberdade de expressão e direito à informação
- Segurança e defesa cibernética
- Inovação, novos modelos de negócios e defesa da concorrência
- Comércio eletrônico, tributação e direitos do consumidor
- Inclusão digital e massificação dos serviços de telecomunicações
- Governança internacional da Internet e soberania nacional

Garantias à privacidade dos cidadãos brasileiros

- A **Constituição** e a legislação brasileira asseguram o direito à **inviolabilidade da intimidade** das pessoas, assim como a **inviolabilidade do sigilo das comunicações de dados e telefônicas**
 - **Única exceção:** ordem judicial, para fins de investigação criminal ou instrução processual penal
- É **crime** realizar **interceptação de comunicações telefônicas, de informática ou telemática**, ou quebrar segredo da Justiça, **sem autorização judicial** ou com objetivos não autorizados em lei.

Denúncias veiculadas pela imprensa

- Milhões de e-mails, ligações e tráfego da internet de brasileiros teriam sido monitorados por programas americanos de inteligência
- Existiria parceria operacional de empresas brasileiras de telecomunicações e Internet com empresas americanas
- O Brasil seria um dos alvos prioritários no monitoramento do tráfego de telefonia e dados
- Teria havido espionagem de comunicações diplomáticas durante a 5ª Cúpula das Américas, em 2009
- Teria ocorrido monitoramento não apenas de metadados, mas também vigilância em tempo real das atividades de internautas determinados

theguardian

The Washington Post

O GLOBO

**Aspectos críticos nas comunicações
globais**



Coleta de dados nas comunicações telefônicas internacionais

- Para que usuários possam realizar chamadas internacionais ou utilizar seus terminais em *roaming*, são necessários acordos de interconexão internacional entre empresas brasileiras de telecomunicações e empresas em outros países
- No momento da interconexão, há troca de informações de sinalização entre as operadoras (metadados), incluindo:
 - Número de origem, número de destino, duração e horário da chamada
 - Tais dados viabilizam a concretização da chamada e seu posterior faturamento ao usuário que a originou
- Os dados saem do país por meio de saídas internacionais, como cabos submarinos ou satélites

Ass. A	T	Ass. B	Id	Inicio	Duracao	Dia	ti	de	RE	JE	RS	JS	CC	RA	B	Rsv
1161234576	0	1932891234	01	164657	000101	0508	0	01	R13E	0005	----	----	10	0-0+	----	----
1161234599	0	1932891234	01	164731	000027	0508	0	01	----	----	R13O	0168	10	0-0+	----	----
1161234534	0	1932891234	01	164751	000008	0508	0	01	R13E	0023	----	----	10	0-0+	----	----
1161234532	0	1932891234	01	164748	000011	0508	0	01	R13E	0033	----	----	10	0-0+	----	----
1161234520	0	1932891234	01	164749	000010	0508	0	01	----	----	R13O	0163	10	0-0+	----	----
1161234546	0	1932891234	01	164758	000002	0508	0	01	R13E	0017	----	----	10	0-0+	----	----
1161234596	0	1932891234	01	164729	000031	0508	0	01	----	----	R13O	0195	10	0-0+	----	----
1161234592	0	1932891234	01	164721	000040	0508	0	01	----	----	R13O	0171	10	0-0+	----	----
1161234524	0	1932891234	01	164751	000011	0508	0	01	----	----	R13O	0190	10	0-0+	----	----
1161234521	0	1932891234	01	164747	000015	0508	0	01	----	----	R13O	0198	10	0-0+	----	----
1161234597	0	1932891234	01	164722	000040	0508	0	01	----	----	R13O	0178	10	0-0+	----	----
1161234533	0	1932891234	01	164742	000021	0508	0	01	R13E	0012	----	----	10	0-0+	----	----
1161234523	0	1932891234	01	164733	000030	0508	0	01	R13E	0004	----	----	10	0-0+	----	----
1161234545	0	1932891234	01	164802	000001	0508	0	01	----	----	R13O	0177	10	0-0+	----	----
1161234531	0	1932891234	01	164752	000011	0508	0	01	----	----	R13O	0161	10	0-0+	----	----
1161234518	0	1932891234	01	164731	000033	0508	0	01	R13E	0005	----	----	10	0-0+	----	----
1161234596	0	1932891234	01	164722	000042	0508	0	01	R13E	0039	----	----	10	0-0+	----	----
1161234522	0	1932891234	01	164743	000021	0508	0	01	----	----	R13O	0189	10	0-0+	----	----

Coleta de dados nas comunicações pela Internet (1/2)



- Tendo em vista que as principais empresas da Internet são dos EUA, identifica-se uma **concentração de tráfego e das receitas do setor** naquele país
- O **desequilíbrio do tráfego global da Internet** em direção aos EUA aumenta a vulnerabilidade das comunicações de brasileiros
- Custo para o Brasil, relativo a trânsito internacional IP, da ordem de **US\$ 650 milhões anuais**.

Coleta de dados nas comunicações pela Internet (2/2)



- As principais empresas da Internet são dos EUA, submetendo-se à sua **jurisdição**
- “**Termos de Uso**” extensos e de difícil compreensão, submetidos a foro e legislação de outros países
- Modelo de negócios baseado na **publicidade segmentada** é dependente do acesso e tratamento dos dados referentes aos hábitos de uso da Internet de cada usuário
- **Armazenamento** de dados de brasileiros **em data centers no exterior**
- **Transferência internacional** de dados de brasileiros **sem autorização específica** do usuário

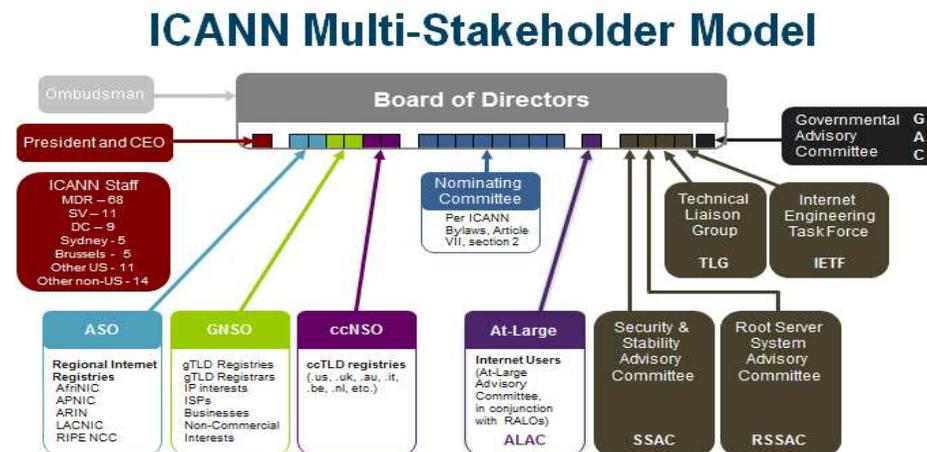
Exploração de vulnerabilidades de hardware e software

- Possíveis vulnerabilidades de **software e hardware** fabricado em outros países, que pode contar com recursos que permitem **monitoramento eletrônico remoto** do prestador de serviços sem seu conhecimento



Governança dos recursos da Internet

- A governança dos **recursos críticos da Internet** (números IP e nomes de domínio) é hoje realizada pela **ICANN**, empresa privada sediada na Califórnia vinculada ao Departamento de Comércio dos EUA
- Os governos participam da ICANN apenas a título consultivo, por meio do **Governmental Advisory Committee – GAC**
- As recomendações do GAC **não têm caráter vinculativo**, podendo ser desconsideradas pelo “Board” da ICANN mediante justificativa.
 - Caso .amazon e .patagonia



Controle sobre a raiz da Internet

- Os servidores-raiz da Internet hospedam e publicam o conteúdo do arquivo-raiz, arquivo de dados que está no ápice do sistema indexado de endereços.
- Há apenas **13 servidores-raiz no mundo**, supervisionados pela ICANN e pelo Departamento de Comércio dos EUA
 - **10 nos EUA**
 - 2 na Europa
 - 1 na Ásia
- Parte do conteúdo dos servidores-raiz é espelhado em outras regiões do mundo

	Operador
1	Verisign Inc.
2	Universidade da Califórnia
3	Cogent Communications
4	Universidade de Maryland
5	NASA
6	Internet Systems Consortium
7	Defense Information Systems Agency
8	United States Army Research Laboratory
9	Netnod
10	Versign Inc.
11	RIPE NCC
12	ICANN
13	Projeto WIDE

Possível violação a normas de direito nacional e internacional

- **Direitos fundamentais consagrados pela Constituição** brasileira, em particular aqueles relacionados à inviolabilidade do sigilo das comunicações, da intimidade e da vida privada (art. 5º, incisos X e XII, CRFB).
- **Normas do direito internacional** sobre proteção à vida privada e à correspondência, liberdade de opinião e expressão e respeito ao Estado de Direito, aos direitos humanos e às liberdades fundamentais
- Iniciativas internacionais em prol da transparência governamental (**Parceria para Governo Aberto**)
- Preceitos internacionais relativos à **sociedade da informação** e à **governança da Internet** (em especial os artigos 39, 42, 44 e 46 da Agenda de Túnis)

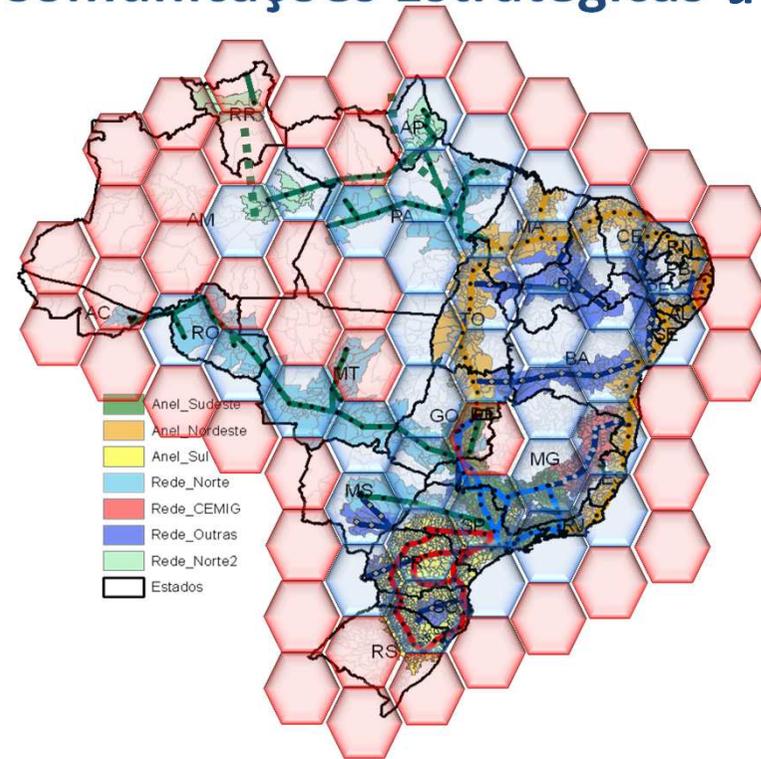
Ações empreendidas pelo Governo brasileiro



Satélite Geoestacionário de Defesa e Comunicações Estratégicas do Governo Federal (SGDC):



- Banda X (Defesa) e banda Ka (Comunicações)
- Lançamento: 2015
- Cobertura de **TODO** o território nacional
- Complementar à rede terrestre da Telebras
- A contratação dos serviços desse satélite pela Administração Pública **evitará que o tráfego das comunicações governamentais saia da esfera do governo.**



Telebrás – cabos submarinos

- Brasil-EUA
 - Brasil-Europa
 - Brasil-Angola
- A construção de cabos para a Europa e para a África **evita a necessidade de trocar tráfego nos EUA** para acessar conteúdos localizados nesses continentes.



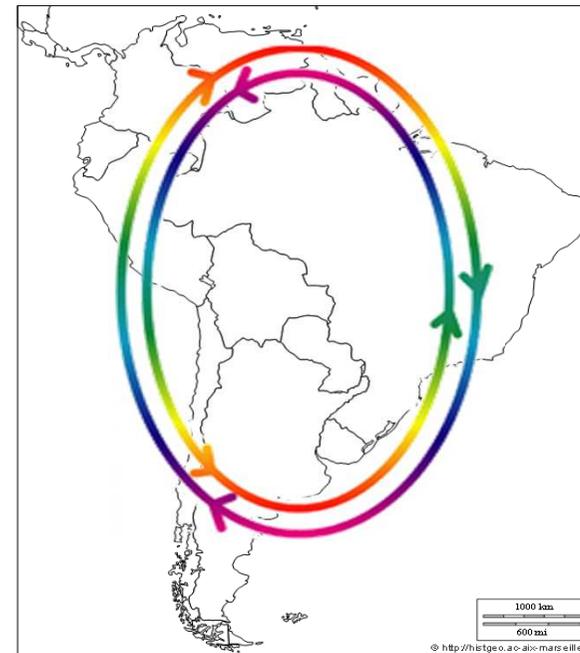
Anel ótico continental: UNASUL / COSIPLAN

Redução do custo com a comunicação entre os países sul-americanos

Redução dos custos com o tráfego intercontinental

- Ubiquidade das saídas internacionais
- Redução da demanda pelas saídas transoceânicas

Diminuição da necessidade de trocar tráfego nos EUA para acessar conteúdos localizados na América Latina



Estímulo à construção de data centers locais e à troca de tráfego no país

- Garantia de **observância da legislação brasileira** quanto a privacidade, defesa do consumidor, padrões da indústria, etc.
- Redução dos **custos de interconexão internacional**
- Melhoria da qualidade percebida pelo usuário na navegação
- Desenvolvimento de **novos serviços/negócios** vinculados à análise e coleta de dados

Estímulo a P&D e ao desenvolvimento de tecnologia nacional

- Estímulo ao uso de **tecnologia nacional** (portaria 950) nas redes de telecomunicações brasileiras;
- Possibilidade de estabelecimento de requisitos de **certificação** via Anatel;
- Possibilidade de criação de regras via **Processo Produtivo Básico – PPB**.

Na esfera legislativa

Marco Civil da Internet

- As empresas que exercem atividades comerciais no Brasil **devem se sujeitar à legislação brasileira**, que assegura a inviolabilidade do sigilo das comunicações, salvo por ordem judicial
- Dados de brasileiros devem, em regra, ser **armazenados no território nacional**
- A **garantia do direito à privacidade e à liberdade de expressão** nas comunicações é condição para o pleno exercício do direito de acesso à Internet

Projeto de Lei sobre Proteção de Dados Pessoais

- A coleta, armazenamento e uso de dados pessoais de brasileiros somente é permitido após o **consentimento livre, expresso, específico e informado do titular ou com base em legislação**

Investigação na esfera doméstica

Anatel

- Solicitada a investigação, na esfera administrativa, sobre as denúncias de **envolvimento de empresas brasileiras**
- Possibilidade de investigação sobre **vulnerabilidades de equipamentos** de redes de telecomunicações

Ministério da Justiça

- Abertura de inquérito para investigar as denúncias com **repercussão na esfera criminal**

Ações na esfera internacional

- Necessidade de concentrar esforços na criação e fortalecimento de **espaços de diálogo multilateral sobre a governança da Internet**, de modo a garantir a preservação dos **interesses soberanos de cada país e os direitos fundamentais de seus cidadãos**
- Estimular iniciativas para proibir abusos e impedir a **invasão da privacidade** dos usuários de telecomunicações e da Internet
- Promover o aperfeiçoamento de regras multilaterais sobre **segurança das telecomunicações e segurança cibernética**, assegurando a proteção dos cidadãos e a soberania de todos os países

Busca por esclarecimentos junto ao governo dos EUA

- Reunião entre o **Embaixador dos EUA Thomas Shannon** e o Ministro das Comunicações (08 de julho de 2013)
- Telefonema do **vice-Presidente dos EUA, Joe Biden**, à Presidenta Dilma Rousseff (19 de julho de 2013)
- Formação de **delegação de especialistas** governamentais para reunião, em Washington, com órgãos de inteligência estadunidenses (05 a 09 de agosto de 2013)
- Vinda do **Secretário de Estado John Kerry** a Brasília (13 de agosto de 2013)

Publicação de “White Paper” da NSA (09 de agosto de 2013)

- **Executive Order 12.333** – fundamento para a coleta, armazenamento, análise e disseminação, pela NSA, de informações de inteligência sobre estrangeiros
- **Foreign Intelligence Surveillance Act – FISA** – Procedimentos para a vigilância física e eletrônica e coleta de informações de estrangeiros

*“Os EUA são um dos principais hubs no sistema mundial de telecomunicações e o FISA foi projetado para permitir ao governo dos EUA coletar inteligência **estrangeira**, enquanto protege as liberdades civis e a privacidade dos **americanos**”.*

- É exigida a **colaboração de provedores** para a coleta de informação de inteligência. Ex: programas FAIRVIEW, BLARNEY, OAKSTAR, LITHIUM.
- Finalidade alegada: combate ao **terrorismo**
- Existem **mecanismos de supervisão** pelo Diretor de Inteligência nacional, pelo Chefe do Departamento de Justiça (*Attorney General*), pelo Congresso e pela Corte de Supervisão de Inteligência Estrangeira (*Foreign Intelligence Surveillance Court*).

Anúncio de medidas de transparência pelo Presidente dos EUA (09 de agosto de 2013)

- Reforma da **Seção 215 do Patriot Act**, que atualmente permite ao governo coletar registros telefônicos
- Aumento da confiança na **supervisão conduzida pela Corte de Supervisão de Inteligência Estrangeira** (*Foreign Intelligence Surveillance Court - FISC*).
- Aumento da **transparência** sobre os programas de inteligência, divulgando a motivação para as atividades de coleta de dados do governo sob a égide da Seção 215 do *Patriot Act*
- Criação de um **grupo de especialistas** de alto nível para, em 60 dias, apresentar relatório revisando as tecnologias de inteligência e de comunicação, considerando também a política externa do país, a segurança e a privacidade

Declaração dos Ministros de Comunicações da UNASUR (Lima, 09 de agosto de 2013)

- 8. Rechaçam qualquer ação de interceptação das comunicações sem autorização das autoridades competentes através do devido processo dos países membros, já que constitui uma **violação da soberania das nações**, do **princípio da não intervenção em assuntos internos dos Estados** estabelecida na Carta as Nações Unidas, dos **tratados e convenções internacionais**, dos **direitos humanos e fundamentais** e do **direito à privacidade dos cidadãos**.
- 9. Instam ao Grupo de Trabalho sobre Telecomunicações da COSIPLAN que siga explorando ações e trocando experiências para **fortalecer a segurança das comunicações dos países sulamericanos e reduzir a dependência tecnológica de outras regiões**, em coordenação com o Conselho de Defesa Sulamericano e as demais instâncias regionais pertinentes.

Obrigado!

Paulo Bernardo Silva

Ministro de Estado das Comunicações

www.mc.gov.br



twitter.com/Minicombrasil



conexaominicom.mc.gov.br



[flickr.com/photos/conexaominicom](https://www.flickr.com/photos/conexaominicom)



[youtube.com/minicombrasil](https://www.youtube.com/minicombrasil)

Anexos



Garantias à privacidade dos cidadãos brasileiros (1/3)

Art. 5º, inciso XII, Constituição Federal:

- X - são **invioláveis a intimidade**, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
- XII - é **inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas**, salvo, no último caso, **por ordem judicial**, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Garantias à privacidade dos cidadãos brasileiros(2/3)

Lei 9.296/96 (Lei de Interceptação)

- Art. 10. Constitui crime realizar **interceptação de comunicações telefônicas, de informática ou telemática**, ou quebrar segredo da Justiça, **sem autorização judicial** ou com objetivos não autorizados em lei.
- Pena: reclusão, de dois a quatro anos, e multa.

Lei n.º 9.472/97 (Lei Geral de Telecomunicações)

- Art. 3º O usuário de **serviços de telecomunicações** tem direito:
- V - à **inviolabilidade e ao segredo de sua comunicação**, salvo nas hipóteses e condições constitucional e legalmente previstas;

Garantias à privacidade dos cidadãos brasileiros(3/3)

Lei 12.737/12 (Lei de tipificação criminal de delitos informático)

- Art. 154-A. **Invasão de dispositivo informático alheio**, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e **com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo** ou instalar vulnerabilidades para obter vantagem ilícita:
 - Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
 - (...)
 - § 3º Se da invasão resultar a **obtenção de conteúdo de comunicações eletrônicas privadas**, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
 - Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
 - § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços **se houver divulgação, comercialização ou transmissão a terceiro**, a qualquer título, dos dados ou informações obtidos.
 - (...)