



Confidencialidade no uso de redes de telecomunicações no Brasil

Averiguações feitas pela Anatel

João Rezende

Presidente

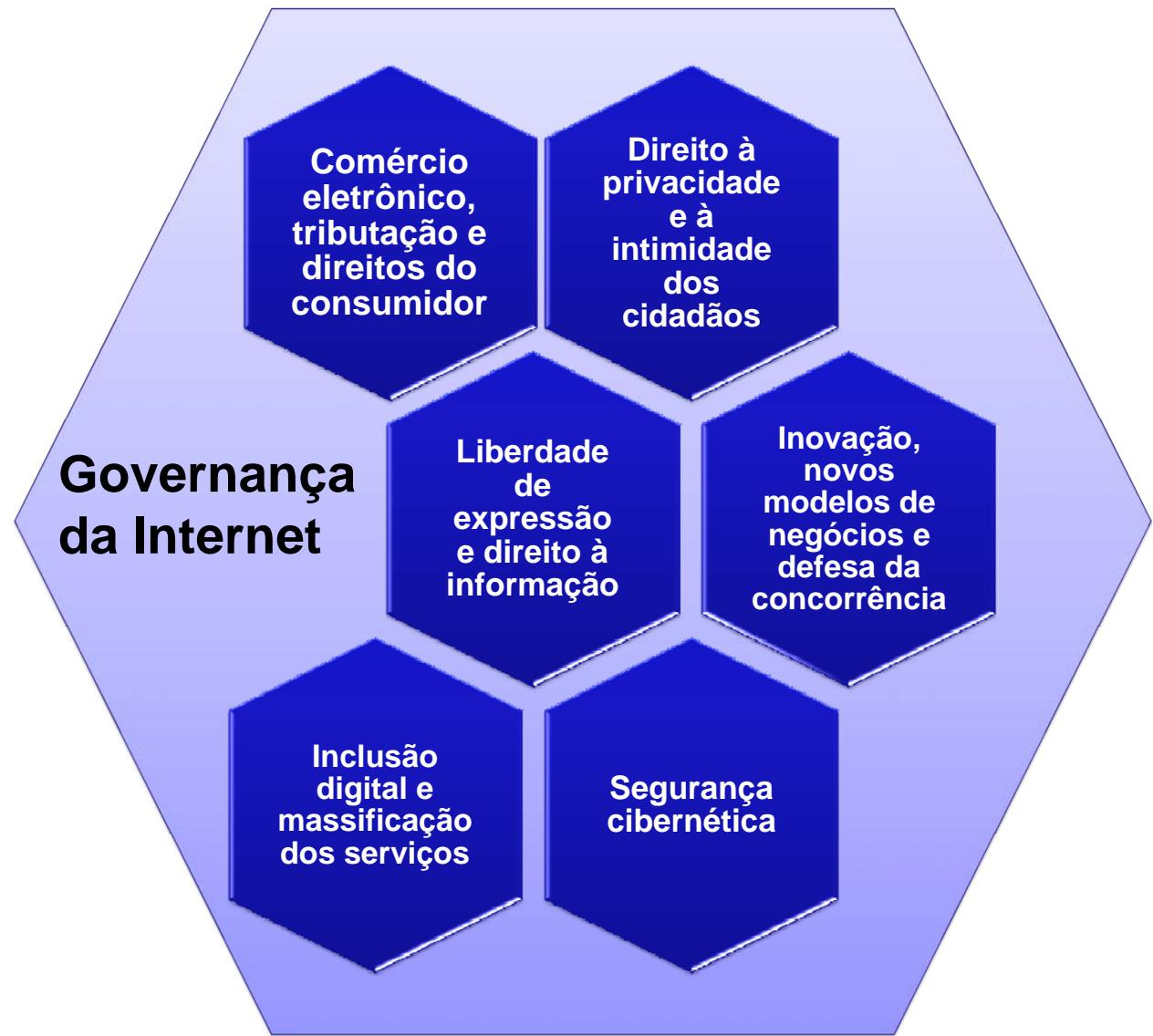
Brasília, 15 de outubro de 2013



Agência Nacional
de Telecomunicações

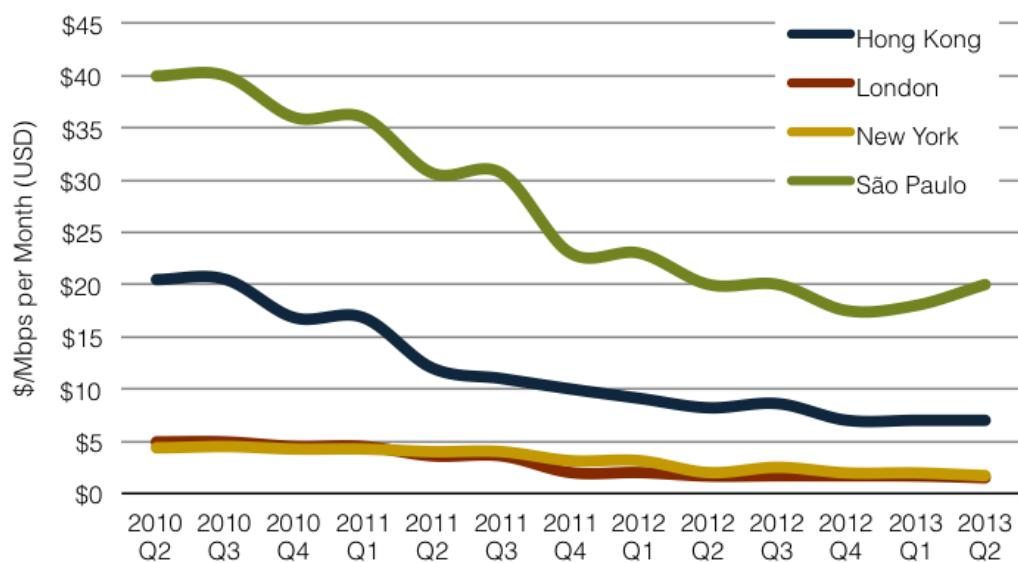
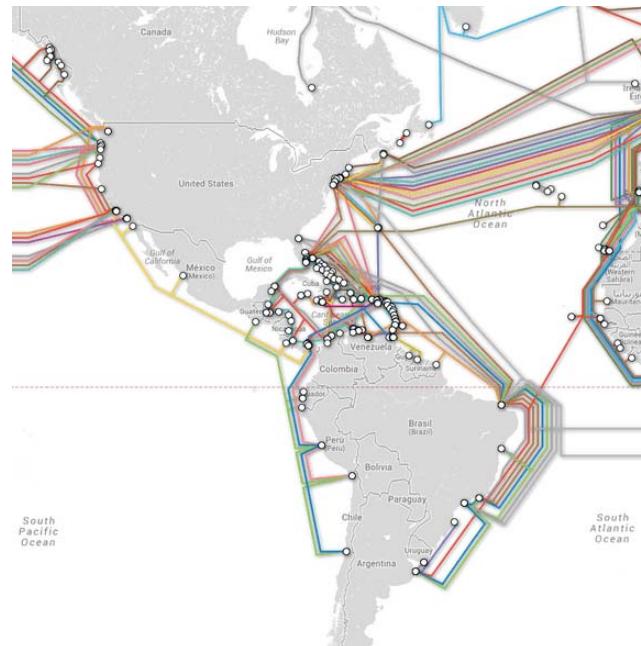
- Um ex-técnico da CIA (Edward Snowden) revelou segredos de segurança dos Estados Unidos.
- Segundo as informações divulgadas pela imprensa, alguns programas de vigilância do governo americano estariam utilizando dados de empresas de telecomunicações e outras como *Google*, *Apple* e *Facebook* para investigar a população em geral, inclusive diplomatas e governos.
- Há ainda documentos que mostram ações de espionagem em diversos países da América, incluindo o Brasil.

- 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.

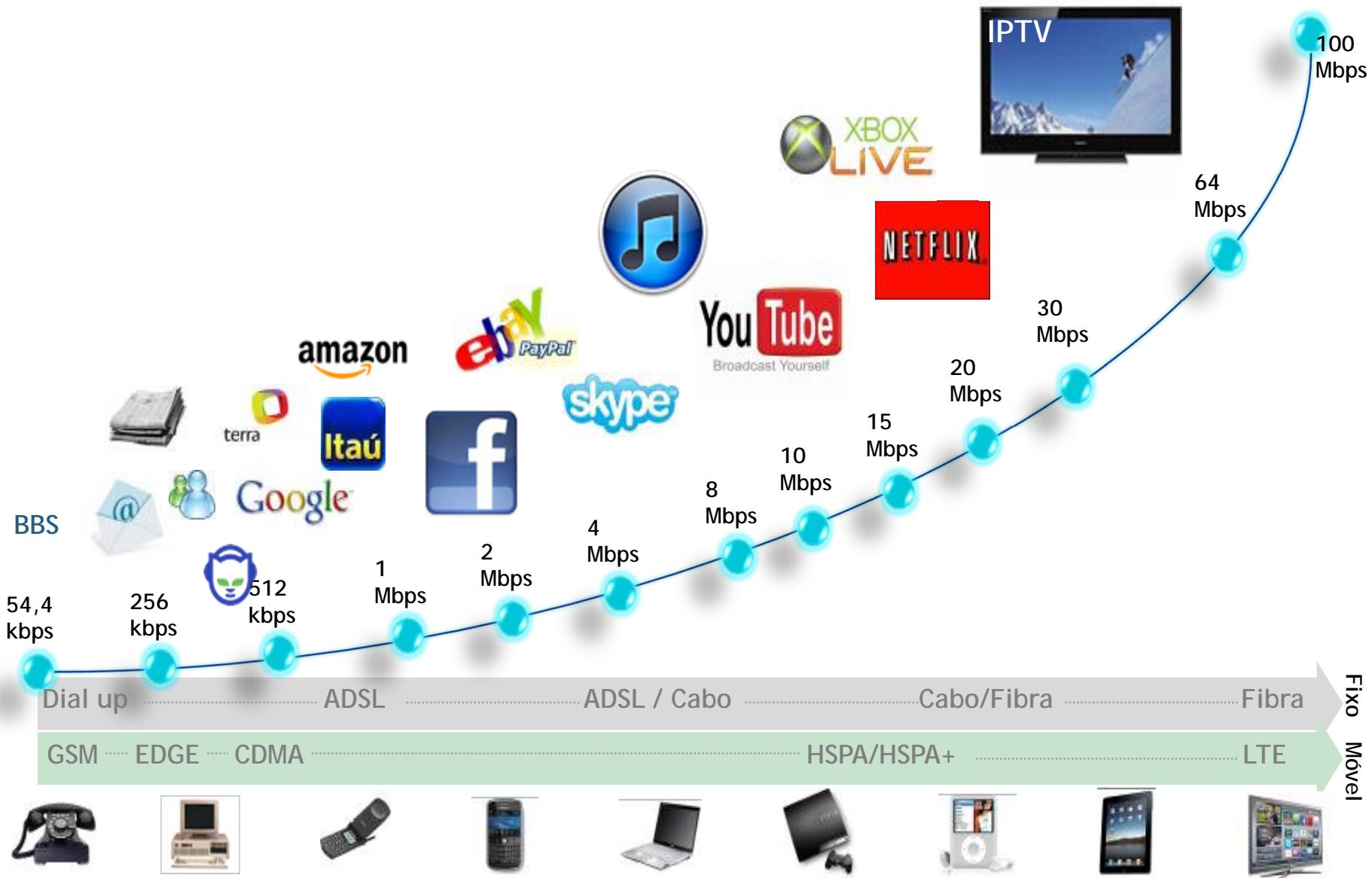


- Para que usuários possam realizar chamadas internacionais ou utilizar seus terminais em roaming, são necessários **acordos de interconexão** internacional entre empresas brasileiras de telecomunicações e empresas em outros países.
- No momento da interconexão, há troca de informações de sinalização 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

- 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 São Paulo, relativo a trânsito internacional IP, da ordem de US\$ 20 Mbps/mês.



Crescimento do tráfego de dados



- As prestadoras são responsáveis pela inviolabilidade do sigilo das comunicações em toda a sua rede, pela confidencialidade dos dados e informações.
- A Anatel iniciou procedimento de fiscalização para averiguar possíveis fragilidades nas redes.
- A Anatel considerou diversos temas para serem averiguados junto às **principais empresas de telecomunicações**.
- A quantidade de empresas pode ser ampliada de acordo com a necessidade da Agência.

Principais assuntos alcançados pelas perguntas:

- 1. Política de Controle de Acesso a Informações:** quais políticas adotadas, tanto para os dados dos usuários quanto para as comunicações em trânsito nas redes (por exemplo, casos de interceptação por ordem judicial);
- 2. Controles de Acesso (físico e remoto);**
- 3. Política de proteção contra códigos maliciosos** e vírus, inclusive contra ataques “Zero Day” e “Ataques Avançados Persistentes (APT)”;
- 4. Procedimentos de *Backup* e recuperação de dados e informações;**

Principais assuntos alcançados pelas perguntas:

- 5. Contratos Internacionais de *Roaming* e Interconexão;**
- 6. Procedimentos e Registros quanto a Incidentes de Segurança, Centros de Operações de Segurança (SOC) e coordenação com outros centros;**
- 7. Ações específicas em resposta à divulgação das notícias sobre a suposta espionagem feita pela *National Security Agency – NSA*.**

Principais assuntos tratados pela Anatel e respondidos pelas prestadoras

1. Política de Controle de Acesso a Informações: quais políticas adotadas, tanto para os dados dos usuários quanto para as comunicações em trânsito nas redes (por exemplo, casos de interceptação por ordem judicial)

- Todas as empresas consultadas afirmaram possuir controle de acesso;
- Nem todas seguem normas internas ou padrões e normas de órgãos certificadores (ex. ISO 27000);
- Nem todas mantém controle de acesso por meios de autenticação (senhas, logins).

Assuntos tratados pela Anatel e respondidos pelas prestadoras

3. Política de proteção contra códigos maliciosos e vírus, inclusive contra ataques “Zero Day” e “Ataques Avançados Persistentes (APT)”

- Afirmaram utilizar softwares específicos de proteção e segurança em estações/servidores;
- Possuem equipamentos programados para atuar em períodos pré-determinados de periodicidade para varredura, bem como para a atualização desses softwares.

Assuntos tratados pela Anatel e respondidos pelas prestadoras

4. Procedimentos de Backup e recuperação de dados e informações

- Todas as empresas afirmaram possuir rotinas de *backups*;
- Nem sempre o local de armazenamento dos dados se dá no Brasil;

Assuntos tratados pela Anatel e respondidos pelas prestadoras

5. Contratos Internacionais de Roaming e Interconexão

- Algumas operadoras brasileiras mantém contratos que tão somente normatizam os procedimentos de completamento de chamadas internacionais em território brasileiro e em território estrangeiro;
- Eses acordos são cobertos por cláusulas específicas de segurança e confidencialidade, **não incluindo qualquer aspecto de cooperação por parte das prestadoras brasileiras no que diz respeito à coleta de informações de chamadas e/ou usuários brasileiros** (ao menos no âmbito desses contratos formais firmados).

Assuntos tratados pela Anatel e respondidos pelas prestadoras

6. Procedimentos e Registros quanto a Incidentes de Segurança, Centros de Operações de Segurança (SOC) e coordenação com outros centros.

- Praticamente todas as empresas informaram que **não existiram** ocorrências ou suspeitas de violação dos sistemas ou rede de telecomunicações nos últimos 3 anos que colocassem em risco dados críticos dessas empresas;
- Nas tentativas de invasão detectadas, todas foram devidamente bloqueadas pelos sistemas de segurança implantados e tratavam apenas de dados institucionais divulgados em websites ou servidores utilizados para ferramentas de testes.

Assuntos tratados pela Anatel e respondidos pelas prestadoras

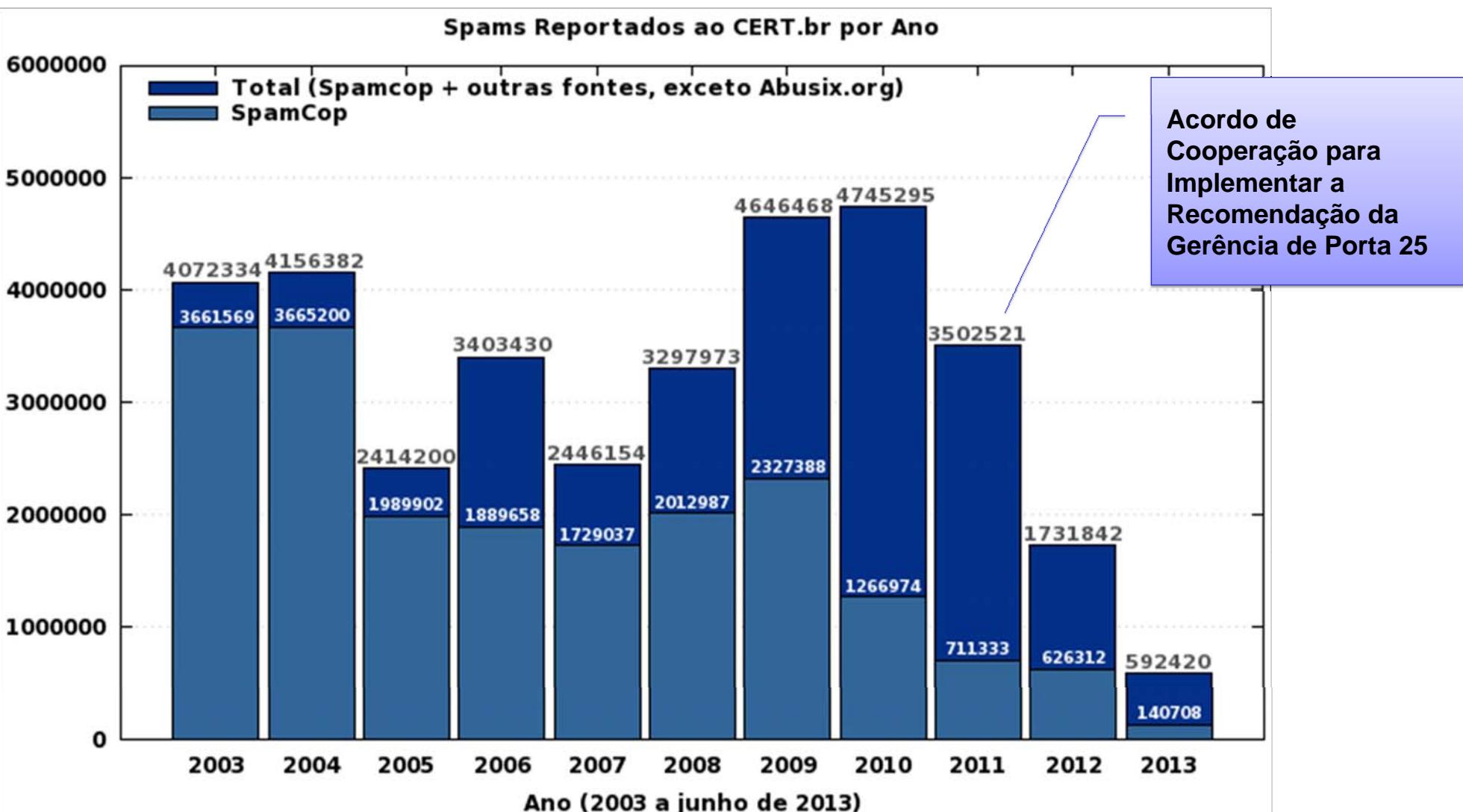
7. Ações específicas sobre a suposta espionagem NSA

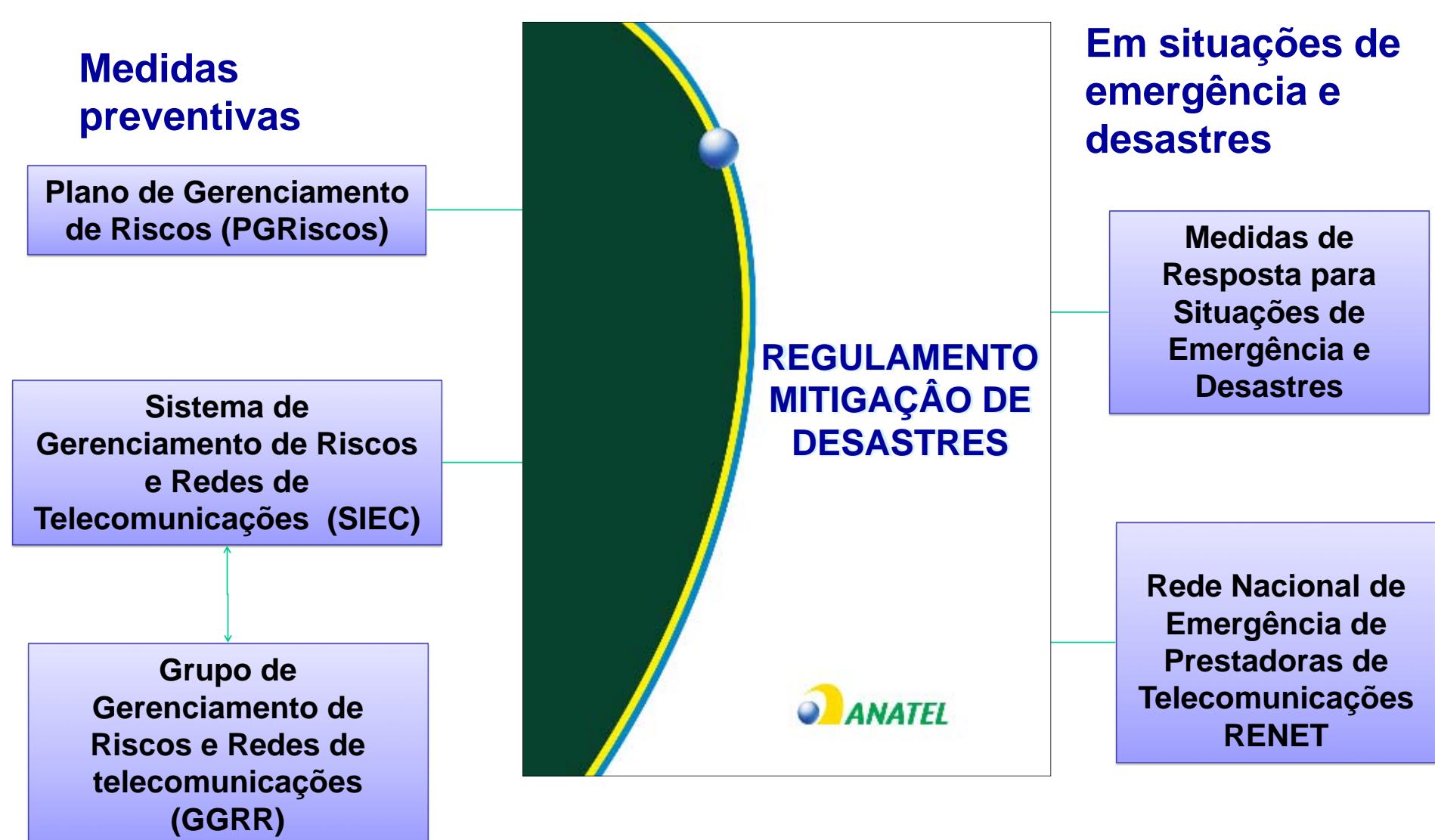
- As prestadoras responderam de forma alinhada por meio do Sinditelebrasil, informando que “nenhuma prestadora de serviços de telecomunicações associada provê ou facilita informações que possam quebrar o sigilo de seus usuários, salvo mediante ordem judicial na forma da lei brasileira”;
- Apenas uma prestadora informou que, diante das denúncias, ter realizado “procedimentos de auditorias extraordinárias, nas quais, também, não foram detectadas qualquer anormalidade ou atividade suspeita”.

- As informações encaminhadas pelas prestadoras foram consolidadas por temas. No momento, a documentação encontra-se em análise pelos técnicos da Agência que avaliam a necessidade da solicitação de mais informações e/ou demanda de ações de fiscalização presenciais.
- Por solicitação da Polícia Federal e Agência Nacional de Inteligência as informações prestadas pelas empresas foram encaminhadas como subsídios para as atividades de respectivas competência.
- A interação com esses órgãos continua, os quais tem demandado prestação/esclarecimento de informações.

- Projeto de **Segurança de Infraestruturas Críticas de Telecomunicações (SIEC)**, que tem como objetivo identificar e avaliar os riscos que possam afetar a segurança das redes de infraestruturas críticas de telecomunicações e que possam prejudicar a qualidade dos serviços de telecomunicações, com foco inicial nos grandes eventos internacionais;
- Desenvolvimento de **Regulamentação para Mitigação de Desastres**, que inclui Gerenciamento de Riscos em Redes de Telecomunicações;
- Implantação da **Gerência da Porta 25**, com impacto na redução de spams;
- **Regulamentos de Qualidade** para redes de banda larga fixa e móveis, com monitoramento da disponibilidade operacional e de parâmetros técnicos por uma entidade externa independente (EAQ);
- **Atuação Internacional**: UIT, CITEL, Mercosul e ações em outros organismos, como ABNT, ISO/IEC JTC1, IETF; IEEE, ATIS; ETSI; OASIS; W3C, 3GPP, ENISA, GSMA, que tratam de aspectos de segurança física e lógica das redes de telecomunicações;

Em 2009, Brasil ocupava a 1º posição, mais de 1 milhão de IPs listados (17%). Após acordo com as operadoras, em março de 2013: 12º posição, menos de 200 mil IPs listados (2%). Em agosto de 2013: 27º posição, menos de 50 mil IPs listados (0.73%).





- cumprindo seu papel de Agência Reguladora das Telecomunicações no Brasil, a Anatel colabora com o GS/PR nos aspectos de segurança das redes de telecomunicações;
- trabalha junto às operadoras do setor buscando identificar vulnerabilidades e preparar a reação a ataques, como por exemplo para os Grandes Eventos Internacionais sediados no Brasil (Rio+20, Copa, Olimpíadas, etc.) ;
- atua ainda, em particular, no Subgrupo Técnico de Segurança de Infraestruturas Críticas (SGTSIC) ;



Medidas legais

- abordagem de desafios legislativos relativos a atividades criminais cometidas nas redes das TICs em âmbito nacional e internacional.

Medidas técnicas e processuais

- promoção da segurança e da gestão de riscos no ciberespaço, incluindo esquemas de certificação, protocolos e normas;

Estruturas institucionais

- prevenção, detecção, resposta e gestão de crise ante ataques cibernéticos, para a proteção das infraestruturas de informação essenciais;

Capacitação

- estratégias e mecanismos de formação de pessoal, para promover consciência, transferência de conhecimento e aumento da segurança cibernética;

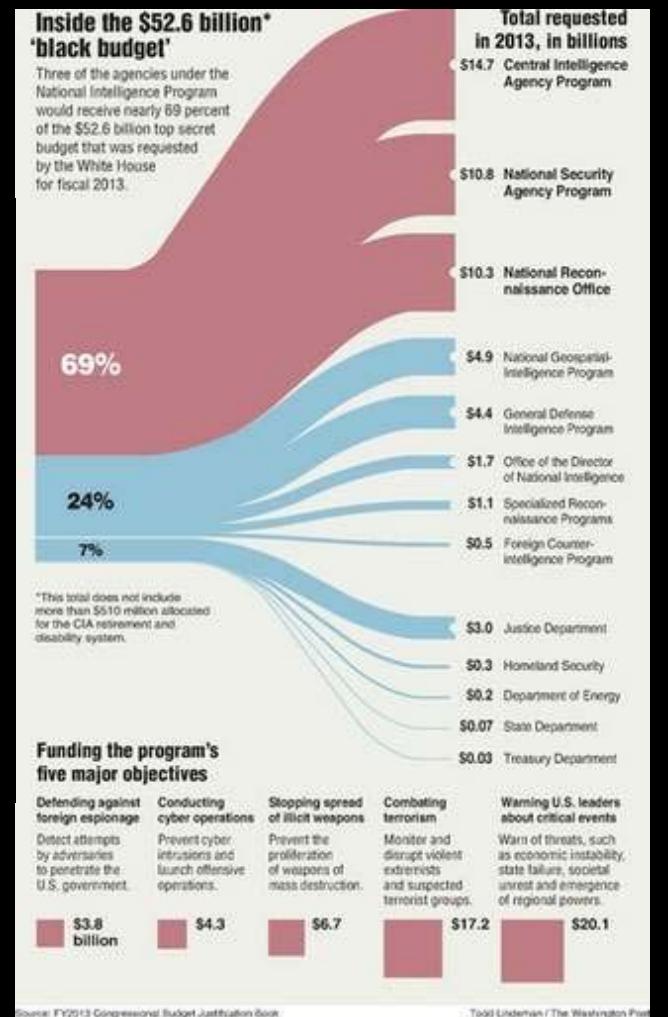
Cooperação Internacional

- promoção da colaboração, do diálogo e da coordenação de respostas às ameaças cibernéticas.

\$52.6 BILLION

The Black Budget

16 agências de inteligência
107.035 funcionários



OBRIGADO