BRAZIL'S LEGAL APPROACH ON CYBERCRIMES

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection

ITU & Secretaria de Comunicaciones de Argentina
Buenos Aires – Oct. 18, 2007

Gilberto Martins de Almeida
gmalmeida@mda.com.br

Agenda:

- Background history
- Brazil's local context
- Challenges, and possible solutions
- Convention on Cybercrime
- Brazil's bill of law on cybercrimes

Background history:

- **1986: 1st cases on computer crime submitted to Brazilian Courts, in Rio de Janeiro**
- **1995: Federal Law 9.100, Section 67 – Fraud in electronic political elections**
- **1995: Bill of law 1713 on cybercrimes - Dep. Cássio Cunha Lima**
- **1996: Bill of law on cybercrimes - Sen. Julio Campos**
- **1996: Federal Law 9.296, Section 10 – Crime of illegal electronic interception**
- **1998: Federal Law 9.609, Section 12 – Crime of software copyright infringement**
- **1998: 1st case on on-line child pornography adjudicated by the Supreme Court**
- **1999: Bill of Law on cybercrimes - 84/99 - Dep. Luiz Piauhylino**
- **2000: Bill of law 76 on cybercrimes - Sen. Renan Calheiros**
- **2000: Federal Law 9.983 – Amends crime of fraud to govt. systems in the Criminal Code**
- **2003: Federal Law 10.695 - Amends crime of copyright infringement in the Criminal Code**
- **2003: Law 10.764 – Amends crime of child pornography, in Child Protection Law**
- **2007: Expected approval of Bill of law 76, on cybercrimes, adapted to Budapest Convention**

Brazil’s local context

- **Conflicting Court decisions on key issues**

PESQUISAS JURISPRUDENCIAIS

(36/2003)

TEMA:	**PROVA OBTIDA ATRAVÉS DE CÂMERA DE VÍDEO. ILICITUDE**

HIPÓTESE I:	OCORRÊNCIA

Jurisprudência:

Tipo	*Número*	*Data*	*Juiz*	*Órgão*
Apel	156.524-6	25/10/01	Waldomiro Namur	TAPR

HIPÓTESE II:	INOCORRÊNCIA

Jurisprudência:

JTJ	150/324 (Cunha Bueno - 18/11/93 - TJSP)
RT	794/713 (Luiz B. Germano da Silva - 13/03/01 - TRF 4ª Região)

I - Corporations shall not monitor e-mail

TRT-SP Nº. 20000 34734 0

RECURSO ORDINÁRIO DA 37ª VT DE SÃO PAULO

EMENTA: Justa causa. “Email” não caracteriza-se como correspondência pessoal. O fato de ter sido enviado por computador da empresa não lhe retira essa qualidade. Mesmo que o objetivo da empresa seja a fiscalização dos serviços, **o poder diretivo cede ao direito do obreiro à intimidade** (CF, art.5º, inc.VIII). Um único “Email”, enviado para fins particulares, em horário de café, não tipifica justa causa. Recurso provido.

II – Corporations shall monitor e-mail

NÚMERO ÚNICO PROC: RR - 613/2000-013-10-00 **PUBLICAÇÃO:** DJ - 10/06/2005
PROC. Nº TST-RR-613/2000-013-10-00.7 A C Ó R D Ã O 1ªTurma JOD/rla/jc

PROVA ILÍCITA. "E-MAIL" CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO.

1. Os **sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência**, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual ("e-mail" particular). Assim, apenas o e-mail pessoal ou particular do
empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade.

2. Solução diversa impõe-se em se tratando do chamado "e-mail" corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é
disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma
ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço.

3. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita **parcimônia** dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o **princípio da proporcionalidade** e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente o "e-mail" corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo ao empregador.

I – No privacy rights over from / to data

"Investigação Criminal – Requisição para que seja apresentado o número de chamadas entre aparelhos telefônicos – Violação do art. 5.º, XII, da Constituição Federal – Inocorrência: 96(b) – Inocorre violação ao princípio constitucional da inviolabilidade do sigilo das comunicações telefônicas, caso para fins de investigação criminal, se pretenda somente a obtenção dos números de chamadas entre aparelhos telefônicos, não sendo pretendida a escuta ou a conversação telefônica entre pessoas, vez que, nessa hipótese, inocorre invasão da privacidade."

II – Privacy rights over subscription data

ProcessoRHC **8493** / SP RECURSO ORDINARIO EM HABEAS CORPUS 1999/0024439-7

Relator(a) Ministro LUIZ VICENTE CERNICCHIARO (1084) **Órgão Julgador**T6 - SEXTA TURMA**Data do Julgamento**20/05/1999**Data da Publicação/Fonte**DJ 02.08.1999 p. 224 JSTJ vol. 9 p. 402 REVFOR vol. 350 p. 375

RHC - CONSTITUCIONAL - PROCESSUAL PENAL - **INFORMAÇÕES CADASTRAIS -SIGILO** - Quando uma pessoa celebra contrato especificamente com uma empresa e fornece dados cadastrais, a idade, o salário, endereço. É evidente que o faz a fim de atender às exigências do contratante.Contrata-se voluntariamente. Ninguém é compelido, é obrigado a ter aparelho telefônico tradicional ou celular. Entretanto, aquelas informações são reservadas, e aquilo que parece ou aparentemente é algo meramente formal pode ter conseqüências seríssimas; **digamos,uma pessoa, um homem, resolva presentear uma moça com linha telefônica que esteja no seu nome. Não deseja, principalmente se for casado, que isto venha a público.** Daí, é o próprio sistema da telefonia tradicional, quando a pessoa celebra contrato, estabelece,como regra, que o seu nome, seu endereço e o número constarão no catálogo; entretanto, se disser que não o deseja, a companhia não pode, de modo algum, fornecer tais dados. Da mesma maneira, temos cadastro nos bancos, entretanto, de uso confidencial para aquela instituição, e não para ser levado a conhecimento de terceiros.

Brazil’s local context

- Conflicting Court decisions on key issues
- **Need of international cooperation**

Extradition

Pedofilia na Web: Governo brasileiro admite extradição de israelense
Por André Felipe Lima
Repórter Canal Web

O ministro das Relações Exteriores, Luiz Felipe Lampreia, afirmou há poucos instantes ao **Canal Web** que **poderá articular um pedido de emergência solicitando ao Governo israelense a extradição do ex-vice-cônsul administrativo de Israel Arie Scher, caso a Justiça Brasileira venha a condená-lo**. “Ainda não avaliamos com cuidado o caso, mas podemos, sim, pedir a extradição dele”, disse o ministro.

Sher, que fugiu do Brasil em junho por ser acusado de praticar pedofilia e trafegar na Internet fotos de prática sexual com menores, teve a prisão preventiva decretada na semana passada pelo juiz em exercício na 31ª Vara Criminal, Humberto Amauri Ferraz.

Lampreia reconheceu que Scher não tem imunidade diplomática, ao contrário do que vem argumentando os advogados do foragido, que atualmente está em Israel. É esperado para hoje, que a defesa de Scher entre com um pedido de habeas-corpus.

A Justiça de Israel espera apenas que o Governo brasileiro envie as provas contra Scher para decidir qual rumo dar ao caso.
15/9/2000 - [Segurança]

Brazil’s local context

- Conflicting Court decisions on key issues
- Need of international cooperation
- **Prejudice against electronic evidence**

I - Criminal proceedings shall stop

Decisão da Justiça surpreende e pára caso de pedofilia na Web

Por André Felipe Lima
Repórter Canal Web

O combate à pedofilia na Internet no Rio de Janeiro sofreu um tropeção inesperado. Por decisão do Tribunal de Justiça do estado, um dos 15 réus que respondem por tráfego de fotos na Rede de abuso sexual contra crianças, teve um pedido de habeas corpus aceito. Com esta postura da Justiça, o caso fica suspenso.

Os inquéritos foram iniciados a partir de investigações da operação Catedral-Rio, realizada em outubro do ano passado, pelo Ministério Público do Estado do Rio. A grande maioria das residências investigadas na operação fica na zona sul do Rio, e todos os que respondem os inquéritos são de classe média para cima.
19/9/2000 - [Segurança]

II - Criminal proceedings shall not stop

(se a prova depende) “de informações técnicas de telemática, que pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial” (HC 76.689/PB, STF, 1a. Turma, 22/09/98, Min. Sepúlveda Pertence)

Brazil’s local context

- Conflicting Court decisions on key issues
- Need of international cooperation
- Prejudice against electronic evidence
- **How to adjudicate cyber crimes?**

Defamation on the Internet – Press law applicable

Calúnias na Internet – Lei de Imprensa

STJ nega fim de ação por calúnia via InternetO caso foi julgado anteriormente pela Terceira Câmara do Tribunal de Alçada Criminal do Estado de São Paulo, que também não concedeu o pedido de habeas-corpus**Brasilia/DF** - Acusado de caluniar juíza pela Internet continuará a responder à ação penal na Justiça. A Quinta Turma do Superior Tribunal de Justiça (STJ) negou o pedido de trancamento da ação movida contra Fábio de Oliveira Ribeiro pela juíza da Sétima Vara Cível da Comarca de Osasco/SP, Lígia Donati Cajon.

O caso foi julgado anteriormente pela Terceira Câmara do Tribunal de Alçada Criminal do Estado de São Paulo, que também não concedeu o pedido de habeas-corpus, mesma opinião da Subprocuradoria-Geral da República, ambos, porém, com argumentação diferente da proferida pelo STJ.

O relator do processo na Quinta Turma, ministro Gilson Dipp, explica, em seu voto, que Fábio Ribeiro foi denunciado por supostamente ter praticado calúnia, delito previsto na Lei de Imprensa. O pedido de trancamento da ação se baseou em ausência de justa causa. Em outras palavras, que não foram especificadas a calúnia contida no texto publicado na rede mundial, a intenção de calúnia por parte de Fábio Ribeiro nem a forma como os elementos de prova da suposta calúnia se dirigem à juíza Lígia Cajon.

Para o relator, tais hipóteses, entretanto, não foram verificadas no caso em questão, pois inexiste imprecisão quanto aos fatos atribuídos a Fábio Ribeiro, devidamente amparados em elementos de prova. **Também não se aplica o segundo argumento, de inaplicabilidade da Lei de Imprensa, por se tratar de texto veiculado na Internet.**

Defamation on the Internet – Criminal Code applicable

25.10.2004 - Inq 2130/DF
- Min. Ellen Gracie
"Carta Anônima. Veiculação pela 'Internet'. Calúnia. Imunidade Parlamentar Material O Tribunal rejeitou denúncia oferecida contra deputado federal pela suposta prática dos delitos de calúnia, injúria e difamação, previstos na Lei 5.250/67 (Lei de Imprensa), decorrentes de divulgação, por meio de informativo eletrônico semanal, do conteúdo de uma carta anônima que noticiava fatos ofensivos à honra de coronel da polícia militar do Estado de Minas Gerais e que o apontava como suposto autor de atos de corrupção passiva. Inicialmente, **o Tribunal asseverou que o caso deveria ser analisado com base no Código Penal e não na Lei de Imprensa, haja vista que informativo eletrônico semanal ou boletim impresso, gerado em gabinete de deputado federal, localizado na Câmara dos Deputados, não poderia ser considerado jornal ou publicação periódica e nem serviço de radiodifusão ou serviço noticioso** de que cuida o parágrafo único do art. 12 da citada Lei ('Art. 12. Aqueles que, através dos meios de informação e divulgação, praticarem abusos no exercício da liberdade de manifestação do pensamento e informação ficarão sujeitos às penas desta Lei e responderão pelos prejuízos que causarem. Parágrafo único. São meios de informação e divulgação, para os efeitos deste artigo, os jornais e outras publicações periódicas, os serviços de radiodifusão e os serviços noticiosos'). Entendeu-se, também, tratar-se, em tese, do crime de calúnia, praticado na modalidade de divulgação, previsto no §1º do art. 138 do CP ('Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.'), uma vez que os fatos divulgados noticiavam suposta prática de crimes de corrupção passiva. Não obstante, concluiu-se, tendo em conta ser o denunciado deputado federal e, ainda, de ser seu gabinete uma extensão da Casa Legislativa, que a divulgação efetivada, independentemente do meio utilizado, estaria acobertada pela imunidade parlamentar material por não estar desvinculada do exercício parlamentar, já que os fatos noticiados constituiriam, em tese, crimes contra a administração pública, incidindo, na hipótese, o disposto no art. 53 da CF/88, na redação dada pela EC 35/2001 ('Os deputados e Senadores são invioláveis, civil e penalmente, por quaisquer de suas opiniões, palavras e votos.'). Inq 2130/DF, rel. Min. Ellen Gracie, 13.10.2004. (Inq-2130)"

Challenges, and possible solutions

- **How to fill in the blanks, without analogy?**

No need of analogy (*in mala partem*)

(“It is not a matter of filling in the blanks of criminal law with analogy (...) “The invention of powder did not require redefinition of homicide (...)” (Habeas Corpus 76.689/PB, Supreme Court, 1st. Chamber, 22/09/98, Min. Sepúlveda Pertence)

Challenges, and possible solutions

- How to fill in the blanks, without analogy?
- **Who is empowered to request data?**

In special cases, no need of judicial order

TRIBUNAL DE ALÇADA CRIMINAL DE SÃO PAULO RECURSO DE HABEAS CORPUS Nº 1236031/4
Ementa: TELECOMUNICAÇÕES – QUEBRA DE SIGILO – “e-mail” enviado a partir do Brasil ao endereço eletrônico da Casa Branca, na cidade de Washington D.C., com mensagem redigida na língua inglesa, contendo ameaças à integridade física da pessoa do presidente americano e de seus familiares – identificados, pelos serviços técnicos de varredura na internet, o provedor de acesso e o número do IP (Internet Protocol) de que se serviu o autor das ameaças para o envio da mensagem através da rede mundial, além do dia e hora da remessa – notificação policial ao provedor para fornecer a identidade, qualificação e endereço do usuário conectado naquele instante ao referido número de “IP” – Recusa em atender à notificação sob a alegação de que os dados requisitados estariam acobertados pelo sigilo garantido pela Constituição Federal aos serviços de telecomunicações, de modo que sua quebra estaria sujeita às formalidades impostas pela lei nº. 9.296/96, principalmente no que se refere à necessidade de ordem judicial – Hábeas Corpus impetrado para não se ver processado por desobediência

Challenges, and possible solutions

- How to fill in the blanks, without analogy?
- Who is empowered to request data?
- **What personal data are required?**

Lan houses – São Paulo

Lei Estadual nº 12.228, de 11-01-2006: Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências.

O GOVERNADOR DO ESTADO DE SÃO PAULO:

Faço saber que a Assembléia Legislativa decreta e eu promulgo a seguinte lei:

Artigo 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à Internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como "lan houses", cibercafés e "cyber offices", entre outros.

Artigo 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

I - nome completo;

II - data de nascimento;

III - endereço completo;

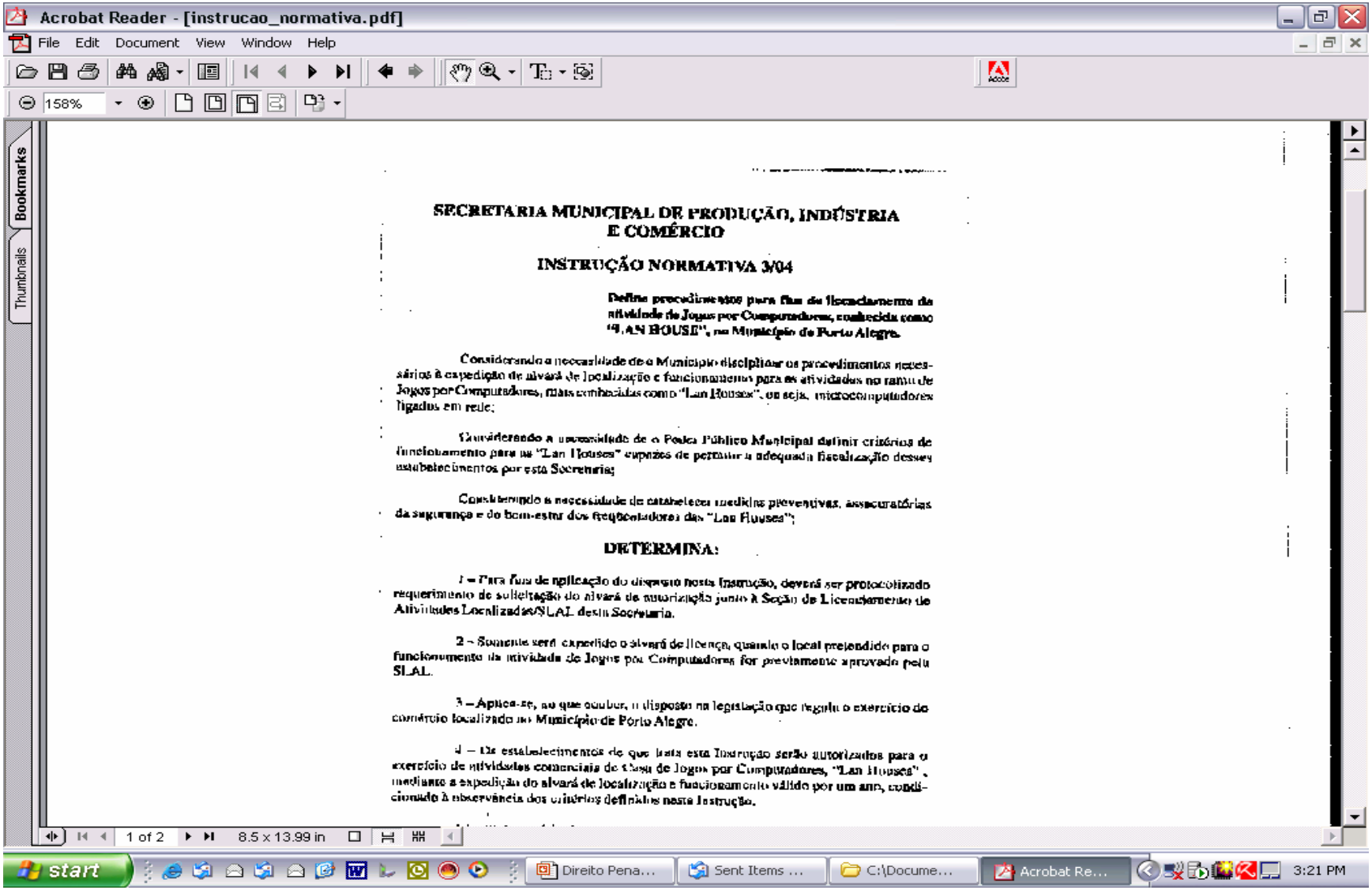
IV - telefone;

V - número de documento de identidade.

§ 1º - O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina.

§ 2º - O estabelecimento deverá **registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.**

Lan houses – Porto Alegre



SECRETARIA MUNICIPAL DE PRODUÇÃO, INDÚSTRIA E COMÉRCIO

INSTRUÇÃO NORMATIVA 3/04

Define procedimentos para fins de licenciamento de atividade de Jogos por Computadores, conhecida como "LAN HOUSE", no Município de Porto Alegre.

Considerando a necessidade de o Município disciplinar os procedimentos necessários à expedição de alvará de localização e funcionamento para as atividades no ramo de Jogos por Computadores, mais conhecidas como "Lan Houses", ou seja, microcomputadores ligados em rede;

Considerando a necessidade de o Poder Público Municipal definir critérios de funcionamento para as "Lan Houses" capazes de permitir a adequada fiscalização desses estabelecimentos por esta Secretaria;

Considerando a necessidade de estabelecer medidas preventivas, assecuratórias da segurança e do bem-estar dos frequentadores das "Lan Houses";

DETERMINA:

1 – Para fins de aplicação do disposto nesta Instrução, deverá ser protocolizado requerimento de solicitação do alvará de autorização junto à Seção de Licenciamento de Atividades Localizadas/SLAL desta Secretaria.

2 – Somente será expedido o alvará de licença, quando o local pretendido para o funcionamento da atividade de Jogos por Computadores for previamente aprovado pela SLAL.

3 – Aplica-se, ao que couber, o disposto na legislação que regula o exercício do comércio localizado no Município de Porto Alegre.

4 – Os estabelecimentos de que trata esta Instrução serão autorizados para o exercício de atividades comerciais de Casa de Jogos por Computadores, "Lan Houses", mediante a expedição do alvará de localização e funcionamento válido por um ano, condicionado à observância dos critérios definidos nesta Instrução.

Challenges, and possible solutions

- How to fill in the blanks, without analogy?
- Who is empowered to request data?
- What personal data are required?
- **What are the sources of “contents”?**

ISO LAWS

9000 (1987)

Consumer Protection Code (1990)

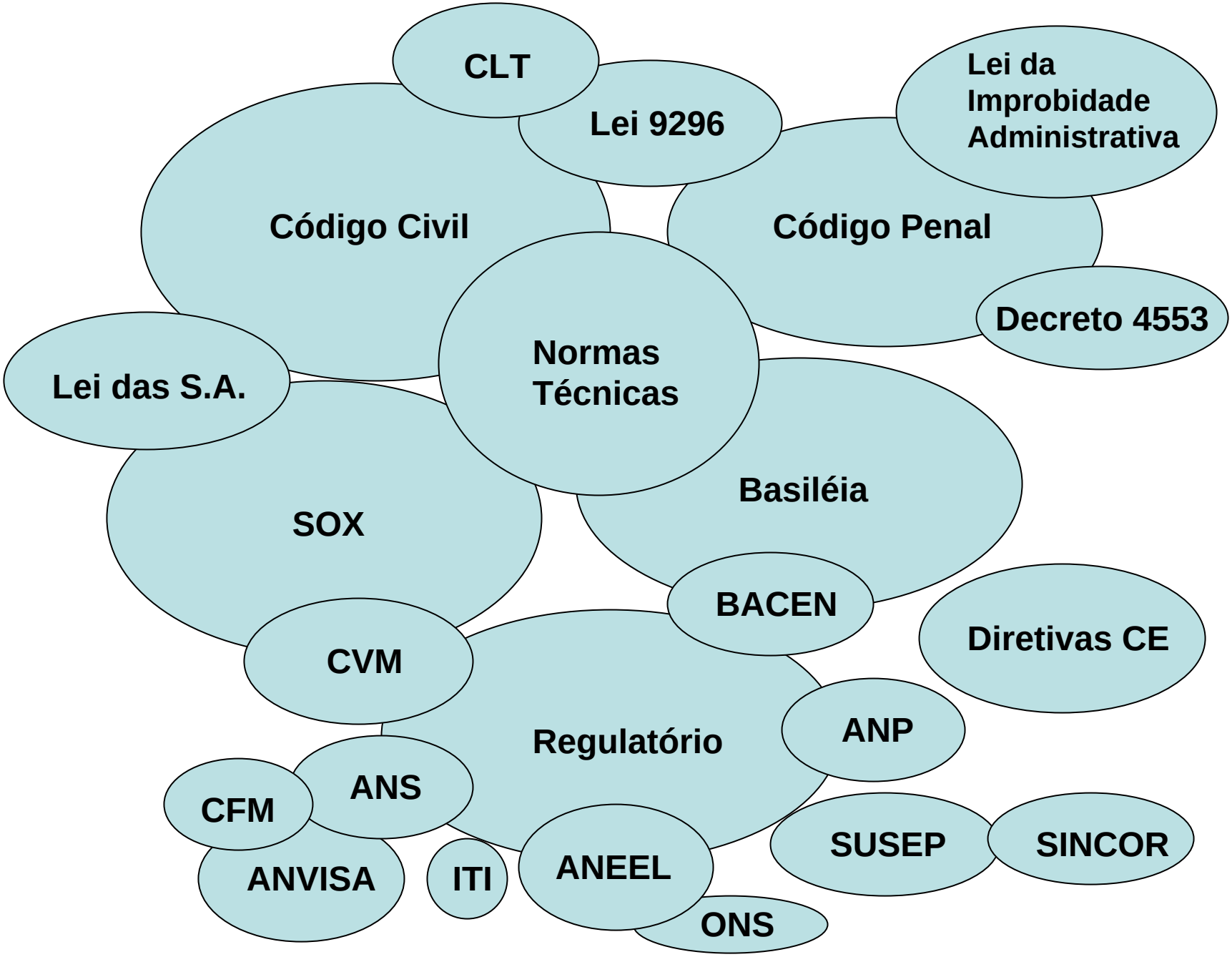
14000 (1996)

Civil Code (2002)

20000 / 27000 (2005) (2005)

Crim. Law (2007?)

ITIL: 1a. versão (80´s); 2a. versão (2001); 3a. Versão (2007?)


CLT
Lei 9296
Lei da Improbidade Administrativa
Código Civil
Código Penal
Decreto 4553
Lei das S.A.
Normas Técnicas
SOX
Basiléia
BACEN
Diretivas CE
CVM
Regulatório
ANP
ANS
CFM
SUSEP
SINCOR
ANVISA
ITI
ANEEL
ONS

Challenges, and possible solutions

- How to fill in the blanks, without analogy?
- Who is empowered to request data?
- What personal data are required?
- What are the sources of “contents”?
- **What are the trends?**

Security v. Privacy

- References in the Federal Constitution:
  - Security: 15; ii) Privacy: 1

- References in quick search at Rio de Janeiro's Higher Court web site:
  - Security: 300; Privacy: 37

Damage v. Danger

- 1942 – 1957: instituted 100 crimes of damage, 14 of danger, and 8 hybrid
- 1985-2000: instituted 200 crimes of damage, 144 of danger, and 28 hybrid

(Juliana Cabral, “Os tipos de perigo & a pós-modernidade”, Revan, RJ, 2005, p. 143)

ABNT – Associação Brasileira de Normas Técnicas

Sede:
Rio de Janeiro
Av. Treze de Maio, 13 / 28º andar
CEP 20003-900 – Caixa Postal 1680
Rio de Janeiro – RJ
Tel.: PABX (21) 210-3122
Fax: (21) 220-1762/220-6436
Endereço eletrônico:
www.abnt.org.br

ICS 35.040	DEZ 2005	**Projeto 21:204.01-012**

Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos

Origem: ISO/IEC 27001:2005

ABNT/CB-21 - Comitê Brasileiro de Computadores e Processamento de Dados

CE-21:204.01 - Comissão de Estudo de Segurança Física em Instalações de Informática

21:204.01-012 - Information technology — Security techniques — Information security management systems — Requirements

Descriptors: Information technology. Security

Esta Norma é equivalente a ISO/IEC 27001

Palavra(s)-chave: Tecnologia da informação. Segurança	30 páginas

i) Recomendações para melhoria.

7.3 Análise crítica das saídas

As saídas da análise crítica devem incluir quaisquer decisões e ações relacionadas ao seguinte:

a) Melhoria da efetividade do SGSI;

b) Atualização da avaliação de risco e plano de tratamento de risco;

c) Modificação de procedimentos e controles que efetuam segurança da informação, quando necessário, para responder a eventos internos ou externos que podem impactar no SGSI, inclusive mudanças de:

1) Requisitos de negócio;

2) Requisitos de segurança;

3) Processos de negócio que efetuam os requisitos de negócio existentes;

4) Requisitos legais ou regulatórios;

5) Obrigações contratuais; e

6) Níveis de risco e/ou critérios de aceitação de risco.

d) Recursos necessários; e

e) Melhoria de como a efetividade dos controles está sendo medida.

8 Melhoria do SGSI

8.1 Melhoria contínua

A organização deve melhorar a efetividade do SGSI continuamente pelo uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e revisões gerenciais (ver 7).

Convention on cybercrime

- **Provides substantive and procedural criminal legal basis**
- **Leaves balance between security and privacy for national laws**
- **Defines Investigative powers and relevant safeguards / limits**
- **Guidelines for relationship with service providers**
- **Guidelines for development of national legislation**
- **Framework for international cooperation**

Convention on cybercrime

- **The Convention serves as a guideline for the development of national cybercrime legislation**
  - **Coherent approach to national legislation**
  - **Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries**
  - **Procedural measures for more efficient investigations**

- **Tools for the gathering of electronic evidence, including tools for the investigation of cyberlaundering, cyberterrorism and other serious crime**
  - **Through the Convention these tools can also be applied in international cooperation**

Brazil’s Bill of Law on Cybercrimes

Matters adressed:

- Aggravation of crimes against honor
- Punishes unauthorized access, possession, forwarding
- Glossary (communication device, computer system, computer network, computer data, etc.)
- Qualified theft
- Malicious code
- Data as “thing” (“coisa”) for legal purposes
- Attacks to utillity services
- Credit cards and electronic devices: private documents
- Cloning of mobile phone or of other communication devices

Brazil's Bill of Law on Cybercrimes

- Amends Criminal Code, Criminal Procedure Code, Military Criminal Code, Consumer Protection Code, etc.
- Imposes obligations to Internet access providers
- Determine creation of proper investigation forces
- Incentivates denounces to authorities

Thank You / Muchas Gracias

- **Gilberto Martins de Almeida**:

- Teacher of Computer Law at the Catholic University / Rio de Janeiro, Superior School of Lawyers / São Paulo Bar, and at the School of Preparation of Judges / Rio de Janeiro
- Arbiter accepted by the World Intellectual Property Organization (WIPO)
- Member of Association of Judicial Experts of Rio de Janeiro
- Member of the Advisory Board of the Brazilian Association of Computer Law and Telecommunications – ABDI
- Advisor for government and for private parties
- Partner at Martins de Almeida – Advogados (www.mda.com.br)