

Reflexão geral sobre a responsabilidade dos agentes no tratamento aos dados pessoais

Renato Leite Monteiro

VI Seminário sobre Privacidade e Proteção de Dados Pessoais
Setembro de 2015

Polêmicas no Brasil

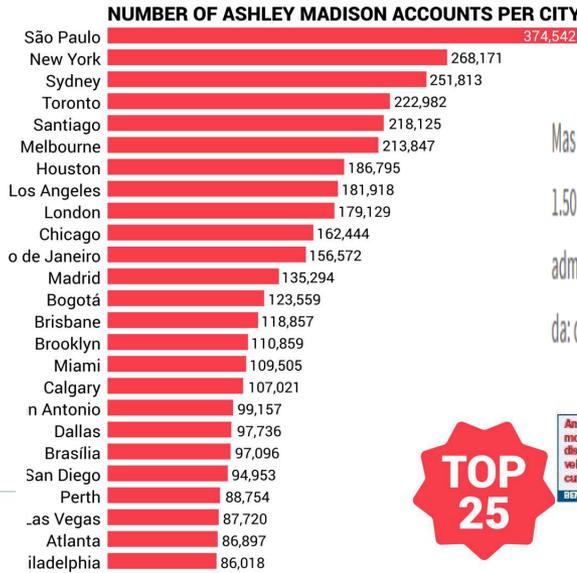
EXAME.COM

Tecnologia 10/12/2013 12:02

Banco do Brasil suspende aplicativo que provocou vazamento

Falha no site da AES Eletropaulo permitia alterações nos cadastros de 6,4 milhões de clientes

Por: Rodrigo Ghedin
6 de setembro de 2012 às 14:35



TOP 25

Fichas sobre estudantes de colégio tradicional de SP vazam na internet



Colégio Bandeirantes, em SP. Fichas sobre estudantes vazaram na internet

Mas um detalhe que chama a atenção é sobre as contas de e-mails. Foram encontrados cerca de 1.500 e-mails com o domínio .GOV.BR na base de dados. Dentre os diversos ramos da administração pública é possível encontrar e-mails da: camara.gov.br; senado.gov.br; planalto.gov.br e caixa.gov.br.



Risco de fraude para 12 milhões de estudantes

Juristas aconselham candidatos que tiveram dados expostos em página do MEC a se prevenirem contra uso indevido do nome e CPF

Os estudantes que tiveram nome, RG e CPF divulgados no site do Enem devem procurar a polícia e a Justiça para se prevenir contra o sequestro. Esse é o conselho de especialistas para os 12,5 milhões de alunos inscritos nos exames de 2007, 2008 e 2009 que foram afetados por falha no banco de dados do Instituto Nacional de Educação e Pesquisa (Inep), do Ministério da Educação (MEC), e cujos dados foram disponibilizados no site da instituição. Segundo o advogado criminalista Alexandre Moura Du-



Mandatory Data Breach Notification

Brasil:

- ✓ Status: inexistente
- ✓ APL de Dados Pessoais: mandatório.

Estados Unidos:

- ✓ Califórnia: 2002
- ✓ Status: 50 Estados

Europa:

- ✓ Directive on Privacy and Electronic Communications (E-Privacy Directive, Directive 2009/136/EC): específica para dados oriundos de empresas de telecomunicação e serviços de Internet;
- ✓ GDPR: mandatório para qualquer tipo de processamento de dados pessoais.



Legislação Nacional – Proteção Setorial

- ✓ Constituição Federal de 1988;
- ✓ Lei 8.078/90: Código de Defesa do Consumidor;
- ✓ Lei 9.472/97: Lei Geral de Telecomunicações (Art. 3º, IX);
- ✓ Lei 9.507/97: *Habeas Data*;
- ✓ Lei 9.983/2000: Crime de inserção de dados falsos em sistemas de informações da administração pública;
- ✓ Lei Complementar 105/2001: Sigilo das operações de instituições financeiras
- ✓ Lei 10.406/2002: Novo Código Civil;
- ✓ Portaria nº 5/2002 da SDE/MJ: Tornou abusiva cláusulas em contratos de consumo que autorizam o envio de dados pessoais sem o consentimento prévio.
- ✓ Resolução 245/07 do Denatran: Dispõe sobre a instalação obrigatório de equipamentos de rastreamento nos veículos saídos de fábrica;
- ✓ Resolução CFM Nº 1.821/07: Dispõe sobre prontuário eletrônico e pro. de dados médicos;



Legislação Nacional – Proteção Setorial

A portaria nº 5/2002, da Secretaria de Direito Econômico do Ministério da Justiça, que complementou o elenco de cláusulas abusivas constantes do art. 51 do CDC, considerou abusiva qualquer disposição que:

I - **autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia**

II - **imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor**

III - **autorize o fornecedor a investigar a vida privada do consumidor**



Legislação Nacional – Proteção Setorial

- ✓ Decreto 6.135/2007: Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal;
- ✓ Decreto 6.425/2008: Dispõe sobre o censo anual da educação;
- ✓ Decreto 6.523/2008: Regulamenta o serviço de SAC;
- ✓ Lei 12.414/2011: Disciplinou o cadastro positivo e certos aspectos sobre proteção de dados pessoais no ambiente creditício (julgamento STJ);
- ✓ Lei 12.527/2011: Lei de acesso a informação (Art. 4º IV e Art. 31);
- ✓ Lei 12.737/2012: Crime de invasão de dispositivos informáticos (Lei Carolina Dieckmann);
- ✓ Decreto 7962/2013: Regulamentou comércio eletrônico;
- ✓ Lei 12.846/2013: Lei anticorrupção;
- ✓ **Lei 12.965/2014: Marco Civil da Internet;**
- ✓ **2015: Anteprojeto de Proteção de Dados Pessoais (PLS 330/13, PLS 181/14, PL 4060/12).**



Polêmicas – Caso Phorm

Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet



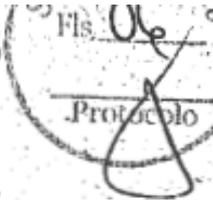
Brasília, 23/7/14 – O Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor (Senacon/MJ) multou a TNL PCS S/A (Oi) em R\$ 3,5 milhões por infrações às normas de defesa do consumidor. A condenação foi motivada em razão do serviço Navegador disponibilizado aos consumidores do Velox, serviço de banda larga da Oi. Durante o processo administrativo foram constatadas violações ao direito à informação, à proteção contra a publicidade enganosa, além do direito à privacidade e intimidade. A medida foi publicada no [Diário Oficial da União](#) desta quarta-feira (23).

As investigações começaram por iniciativa do próprio DPDC, que recebeu informações de que a parceria da Oi com a empresa britânica Phorm consistia no desenvolvimento do *software* chamado “Navegador”, que mapeava o tráfego de dados do consumidor na internet de modo a compor seu perfil de navegação. Tais perfis eram comercializados com anunciantes, agências de publicidade e portais da *web*, para ofertar publicidade e conteúdo personalizados.



Polêmicas - Caso Phorm





MINISTÉRIO DA JUSTIÇA
SECRETARIA NACIONAL DO CONSUMIDOR
DEPARTAMENTO DE PROTEÇÃO E DEFESA DO CONSUMIDOR
COORDENACÃO-GERAL DE CONSULTORIA TÉCNICA E PROCESSOS ADMINISTRATIVOS

Processo n.:	08012.003471/2010-22.
Nota técnica:	137/2014-CGCTPA/DPDC/Senacon/MJ.
Data:	22 de julho de 2014.
Representante:	Departamento de Proteção e Defesa do Consumidor <i>ex officio</i> .
Representado:	TNL PCS S/A (Oi).
Assunto:	Prática abusiva. Violação aos princípios da boa-fé e ao direito à privacidade.
Ementa:	Processo Administrativo. Infração aos direitos básicos do consumidor no que diz respeito ao reconhecimento de sua vulnerabilidade, ausência de boa-fé, ao equilíbrio entre consumidores e fornecedores, ao direito à privacidade e à intimidade, utilização de métodos comerciais coercitivos ou desleais, bem como a proteção às informações mantidas por fornecedores em banco de dados de consumidores. Descumprimento dos artigos 4º, inciso I e III; 6º, incisos II, III e IV; 31; 37; 39, inciso IV; 43 e 51, inciso XV e § 1º, todos do Código de Defesa do Consumidor. Aplicação de sanção de multa no valor de R\$ 3.500.000,00 (três milhões e quinhentos mil reais).



Polêmicas - Caso Phorm

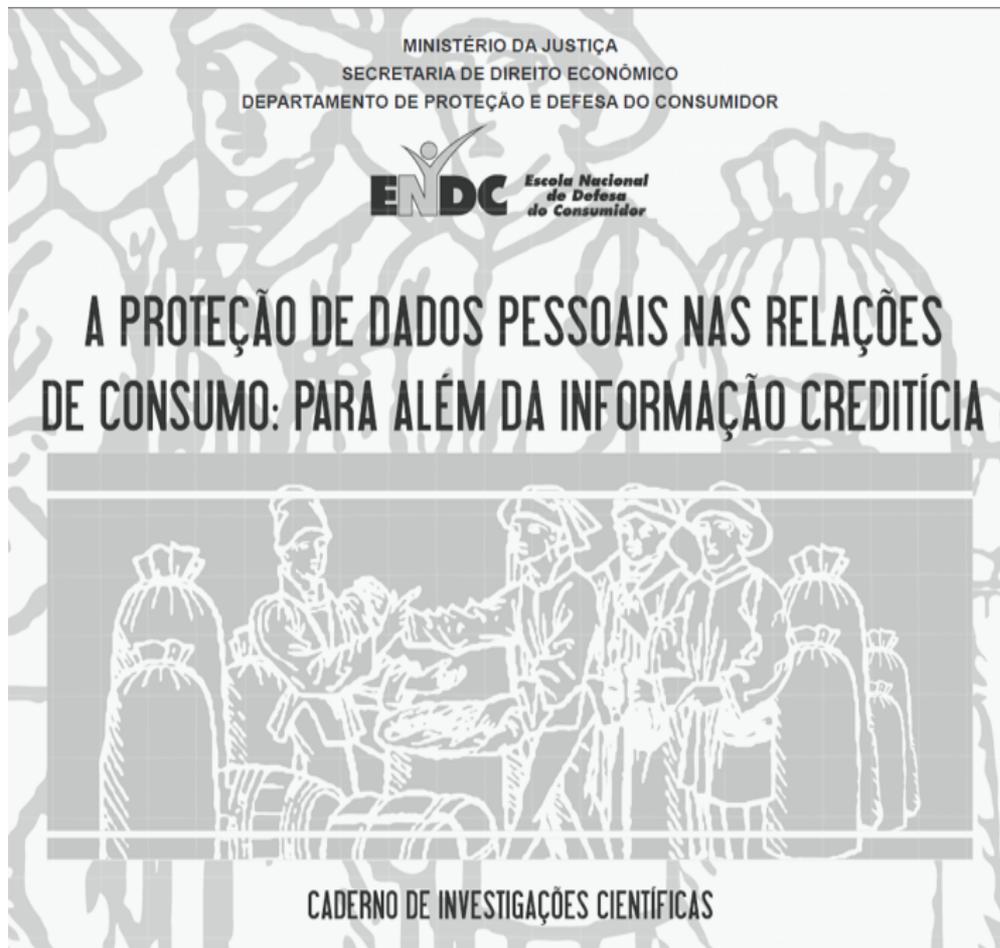
106. No presente caso, a TNE PCS S:A (“Oi”) implementou ferramenta tecnológica denominada *Navegador* capaz de mapear a navegação e interceptar as comunicações dos consumidores com o intuito de disponibilizar a outras empresas (portanto, comercializar) dados personalizados. A afronta, por conseguinte, é ao direito fundamental de proteção da dignidade e personalidade humana – o direito a privacidade e intimidade.

132. Em suma, o serviço *Navegador* agrava a vulnerabilidade, aumenta drasticamente a assimetria do consumidor em relação ao fornecedor alterando o equilíbrio da relação de consumo em favor deste último, confunde-se com método comercial e publicitário com características coercitivas ou desleais, torna precária a proteção das informações dos consumidores mantidas pelos fornecedores, retira do consumidor seu poder de autodeterminação em relação a utilização de dados ou informações geradas a partir de sua utilização da internet que deveria, por pressuposto, ser livre e autônoma. Essa passa a ser uma utilização monitorada para coleta de dados e informações com finalidades exclusivamente comerciais, especificamente voltadas para a publicidade *on line*. O *Navegador* retira do consumidor garantias específicas e eficazes para a tutela de sua privacidade e de sua autonomia.

Enfoque principal: Direito-dever de informação (BIONI, Bruno)



SENACON/MJ



<http://bit.ly/1OWfiOd>



Polêmicas – Caso Tudo Sobre Todos



Dados (pessoais) públicos

v.

Dados (pessoais) publicamente acessíveis (dados de acesso público irrestrito)



Polêmicas – Condenação do SPC

SPC Brasil condenado por venda de dados de consumidores



(Imagem meramente ilustrativa/Wikipedia)

Ao fornecer um amplo e circunstanciado relatório com informações pessoais minudentes a ré viola a intimidade e a privacidade dos consumidores, os quais não podem ficar a mercê de ligações telefônicas, mensagens de marketing e telemarketing indesejadas, ainda mais em tempos que tais, em que são de domínio geral toda a sorte de fraudes cometidas contra a sociedade, inclusive de cunho criminoso. A reflexão é do Juiz Sílvio Tadeu de Ávila, da 16ª Vara Cível do Foro Central da Capital, em decisão que condenou a Confederação Nacional de Dirigentes Lojistas - SPC Brasil por prática abusiva ao fornecer, através do seu site, dados e informações pessoais de consumidores, sem a prévia aprovação. A decisão tem abrangência nacional.

Processo nº 001/11401789987, Agosto 2015
<http://www.tjrs.jus.br/site/imprensa/noticias/?idNoticia=282410>



Polêmicas – Condenação do SPC

“Restou incontroverso nos autos que há comercialização de dados cadastrais pela ré para ações de marketing, sem autorização prévia dos consumidores, através do site www.spcbrasil.org.br/ (...). Ao fornecer um amplo e circunstanciado relatório com informações pessoais minudentes a ré viola a intimidade e a privacidade dos consumidores, (...).

A disponibilização ampla e irrestrita de dados pessoais podem dar ensejo a um sem número de delitos civis e criminais, aí incluídos fraudes contratuais e sequestros, inclusive de familiares, não sendo demais mencionar que segurança pública eficiente tornou-se uma quimera.

Diversos dispositivos legais cuidam de determinar que a divulgação de dos dos consumidores seja submetida à ciência prévia destes, como é o caso dos 43 § 2º do CDC e do art. 3º, da Lei nº 14.414/2011.

Cabível, assim, que a demandada seja compelida a proceder o cancelamento do registro de consumidores que não tenham expressamente autorizado a inserção de seus dados cadastrais e informações pessoais nos bancos de dados (...)

001/1.14.0178998-7 (CNJ:.0220078-81.2014.8.21.0001), TJ/RS, Agosto de 2015



Polêmicas – Venda de dados

APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE REPARAÇÃO DE DANOS MORAIS. COMERCIALIZAÇÃO E DIVULGAÇÃO DE DADOS PESSOAIS DE CONSUMIDORES. PROCOP. “DADOS NÃO SENSÍVEIS”. AUSÊNCIA DE ILÍCITO. INEXISTÊNCIA DO DEVER DE INDENIZAR.

“A elaboração, organização, consulta e manutenção de bancos de dados sobre consumidores não é proibida pelo Código de Defesa do Consumidor; ao contrário, é regulada por este. **Hipótese em que o serviço colocado à disposição das empresas conveniadas pela ré não se reveste de ilegalidade, considerando que as informações expostas não são consideradas de caráter sigiloso ou íntimo, mas de fácil e ampla circulação no mercado de consumo**, para proteção do crédito e segurança nas relações comerciais. **Ausência de violação à vida privada, imagem ou intimidade**. Inexistência, ainda, de provas de que a divulgação de dados pela requerida tenha causado qualquer prejuízo à parte autora, ônus que lhe incumbia, não havendo como se conceder indenização por dano hipotético.”

(TJ/RS N° 70060163623 (N° CNJ: 0208925-06.2014.8.21.7000), Abril, 2015).



Juiz de Porto Alegre sugeriu a consumidora que se mudasse "para a floresta, deserto, meio do oceano ou para outro planeta", ao negar-se a analisar seu pedido para proibir uma empresa de comercializar seus dados pessoais para fazer publicidade de produtos e serviços.

Ao deixar de apreciar o pedido, o juiz afirmou que somente mudando-se para os lugares sugeridos seria possível assegurar à consumidora "seus direitos à privacidade na forma ou amplitude como defende".

Polêmicas – Inexistência de privacidade

Julgador:

Luiz Augusto Guimarães de Souza

Despacho:

Vistos... 1. Se a suplicante, de fato, sente-se incomodada com publicidades encaminhadas a seu endereço ou telefone, a partir de informes, alegadamente, de iniciativa da ré, sugiro-lhe mude-se para a floresta, deserto, meio do oceano ou para outro planeta..., quando, então sim, ser-lhe-ão assegurados seus direitos à privacidade na forma ou amplitude como defende. Impõe-nos o convívio em sociedade, no entanto, todo dia e toda hora, restrições as mais diversas. Inclusive, o recebimento - ou não - de panfletos, em cada semáforo, enquanto passeamos com a família, especialmente, no final-de-semana, interferindo, diretamente, com nossos constitucionais direitos à privacidade, ao descanso e ao lazer ! Entretanto, como dito, não somos obrigados a abrir o vidro e receber tais encartes. Como podemos usar, gratuitamente, os serviços da operadora de telefonia para bloquear ligações, de qualquer natureza; e, finalmente, ainda podemos por no lixo publicidades enviadas pelo correio que nos estejam sendo inconvenientes ou inoportunas. Agora, medida judicial para atingimentos de finalidades que tais afeiçoa-se como mais uma aventura jurídica, de que os foros de todo País estão atonetados. Não falta mais nada, pois até o ar que respiramos e o direito de defecar e mictar em banheiro público, amanhã, não duvide, serão passíveis de judicialização ! Quem viver, verá. Para litisconsórcio à chicana, todavia, não contem comigo. 2. JULGO EXTINTO O PROCESSO, SEM RESOLUÇÃO DE MÉRITO, por falta de interesse processual (art. 267, VI, do CPC1), ficando suspensa a exigibilidade de custas em razão de a requerente litigar sob o pálio da AJG, que ora lhe concedo. INTIMAR; nada mais sendo requerido, baixa e arquivado.

Processo:

**0103154-84.2014.8.2
1.0001, TJ/RS,**

**23 de Abril
de 2014**



Marco Civil da Internet

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 12. (...) seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - **advertência**, com indicação de prazo para adoção de medidas corretivas;

II - **multa de até 10%** (...), considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - **suspensão temporária das atividades** (...); ou

IV - **proibição de exercício das atividades** (...).

Credit Scoring

O desrespeito aos limites legais na utilização do sistema “credit scoring”, configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a **responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente** (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

RESP Nº 1.419.697 - RS (2013/0386285-0)



Federal Trade Commission - FTC

122 3237

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeney

In the Matter of

GOOGLE INC.,
a corporation.

DOCKET NO.

Aplicação (“enforcement”) de ordens

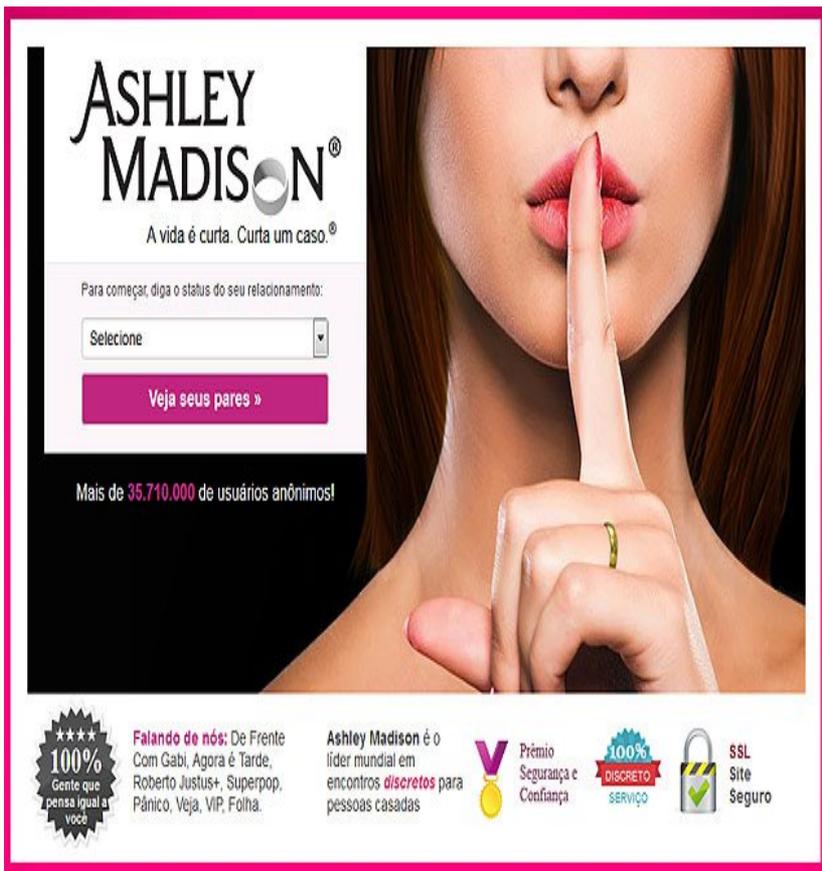
- Casos terminam em ordens de consentimento, “cercando” práticas:
 - Proibindo empresa de implementar práticas enganosas sobre a privacidade dos usuários.
 - Supressão de informação obtida ilegalmente
 - Programa abrangente de privacidade & segurança.
 - Pena civil por violação da ordem.
- Exemplo: Google, \$ 22,5 milhões.

AGREEMENT CONTAINING CONSENT ORDER

Guilherme Roschke



Federal Trade Commission - FTC





Index. These groups of data were disclosed by facebook (click for more details):

- | | | | |
|--|--------------------------------------|---|---|
| 00. Target | 13. Date of Birth | 28. Machines | 43. Privacy Settings |
| 00. Date Range | 14. Education | 29. Messages | 44. Profile Blurb |
| ----- | 15. E-Mails | 30. Minifeed | 45. Realtime Activities |
| 01. About Me | 16. Events | 31. Name | 46. Recent Activities |
| 02. Account End Date | 17. Family | 32. Name Changes | 47. Registration Date |
| 03. Account Status History | 18. Favourite Quotes | 33. Networks | 48. Relationship |
| 04. Address | 19. Friend Requests | 34. Notes | 49. Religious Views |
| 05. Alternate Name | 20. Friends | 35. Notification Settings | 50. Removed Friends |
| 06. Applications | 21. Gender | 36. Notifications | 51. Screen Names |
| 07. Chat | 22. Groups | 37. Password | 52. Shares |
| 08. Checkins | 23. Hometown | 38. Phone Numbers | 53. Status Updates |
| 09. Connections | 24. Last Location | 39. Photos | 54. Vanity |
| 10. Credit Cards | 25. Linked Accounts | 40. Physical Tokens | 55. Wallposts |
| 11. Currency | 26. Locale | 41. Pokes | 56. Website |
| 12. Current City | 27. Logins | 42. Political Views | 57. Work |

Original Files. These are some excerpts and altered versions of the original files we got from facebook. Because of privacy concerns all personal information was edited out, some files were altered in order to make editing easier.

initials and userID	date	original file	blackened excerpt	blackened file
L.B. (747****)	2011-06-07	PDF (780 pages, 34 MB)		PDF (7.7 MB)
P.E. (129****)	2011-06-07	PDF (1.142 pages, 165 MB)	PDF (138 KB)	
M.S. (509****)	2011-06-09	PDF (18 pages, 56 KB)		PDF (95 KB)
M.S. (509****)	2011-07-11	PDF (1.222 pages, 496 MB)		PDF (11 MB)
"Removed" content that was still held by Facebook			PDF (206 KB)	



Risk Based Approach – GDPR - Europe

- **Risk assessment:** “the determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat” (RFC 4949);
- **Acceptable risk:** risk that is understood and tolerated usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss (RFC 4949);
- **Risk-based approach:** identifying “specific risks”, assessing and categorising the rights of third parties and making decisions based on this in order to reduce administrative burden (Council of EU).

Direitos Fundamentais v. Risk Based Approach



APL de Proteção de Dados Pessoais (2010) Mackenzie

Art. 6º **O tratamento de dados pessoais é atividade de risco** e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarcí-lo, nos termos da lei.

Atividade de risco = Responsabilidade objetiva

Responsabilidade objetiva = incentivo para proteger os dados de forma adequada



APL de Proteção de Dados Pessoais (2015)

Versão original

Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarcí-lo.

§ 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;

§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.

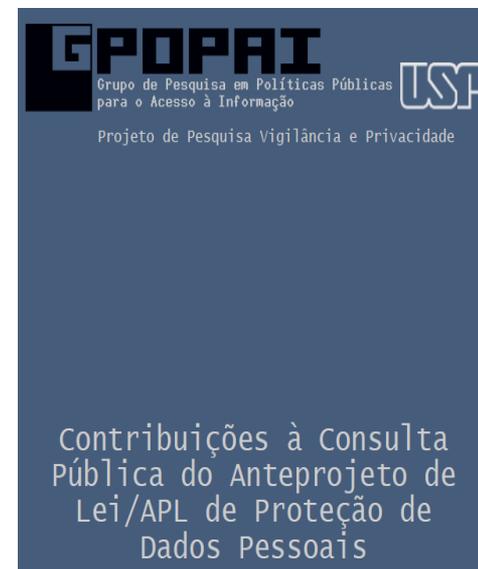
Sugestão de alteração

Art. 35. O tratamento de dados pessoais é atividade de risco e todo aquele que, em razão do exercício de tal atividade, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarcí-lo, independentemente de culpa, nos termos desta lei.

§ 1º A exclusão da responsabilidade do operador e dos demais agentes que integram a cadeia de tratamento de dados pessoais somente se dará nos casos de culpa exclusiva da vítima ou força maior.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;

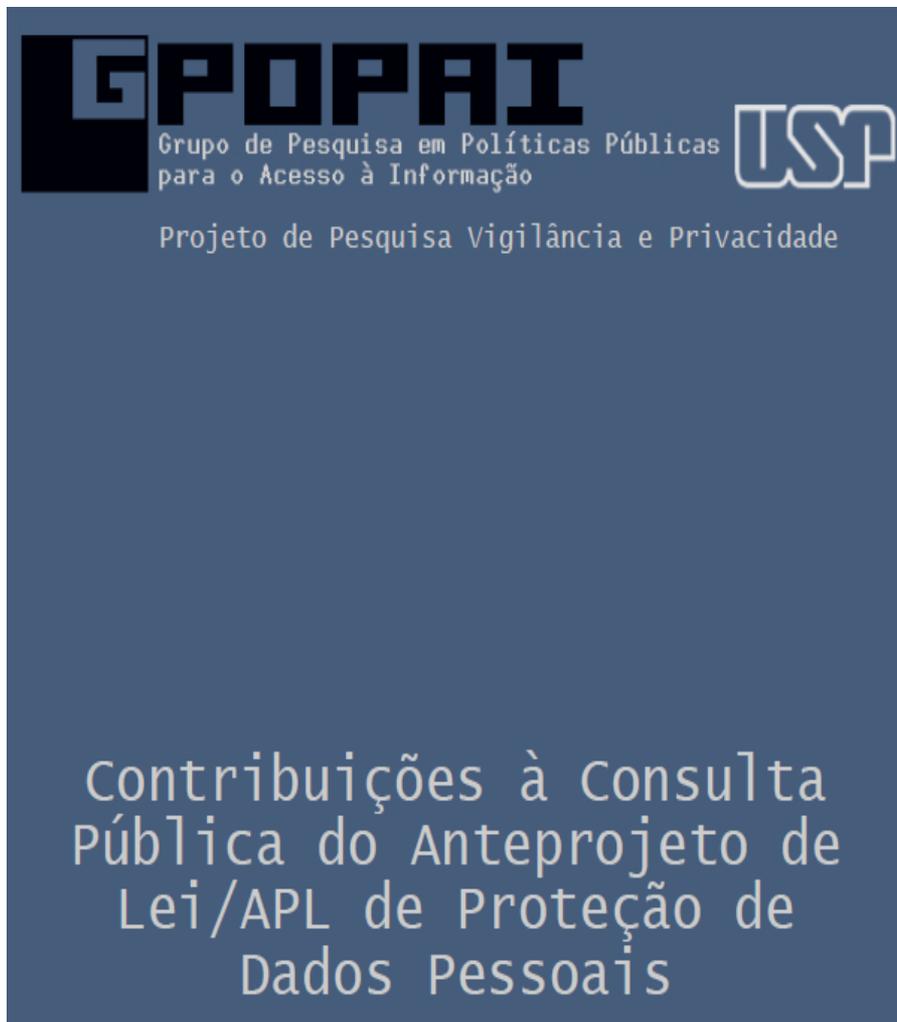
Art. 38. Os órgãos e entidades públicas responderão, independentemente de culpa, pelos danos morais, patrimoniais, individual ou coletivo causados a outrem decorrentes da gestão das suas bases dados.



<http://bit.ly/1OrtGQt>



Bibliografia



<http://bit.ly/1OrtGQt>



RENATO LEITE MONTEIRO



renato.monteiro@mackenzie.br



Renato Leite Monteiro



@RenatoLMonteiro