OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Impacto do Projeto de Lei de Privacidade nos Negócios Bancários

Rubia Ferrão

rubia@opiceblum.com.br

Introdução - Legislação Nacional – Proteção Setorial

Evolução

Evolução

"Data is the currency of today's digital economy"

(European Commission – dez de 2015)

Privacidade em 1993 x Privacidade em 2013

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Today = *You Can Run, But You Can't Hide*

1993

On the Internet, <u>nobody</u> knows you're a dog.

"On the Internet, nobody knows you're a dog."

2013

On the Internet, <u>everybody</u> knows you're a dog.

KPCB

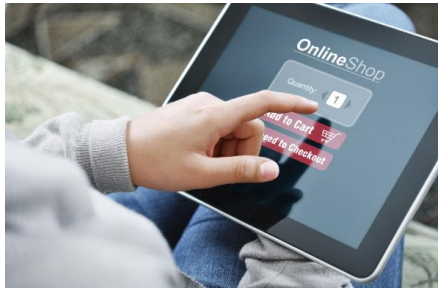
Source: Quote – Joe Louis (American heavyweight boxer), 1946. Left image – Peter Steiner, cartoonbank.com, The New Yorker, 1993. Right image – Tumblr user cachorro no computador.

rubia@opiceblum.com.br

Contratos Eletrônicos

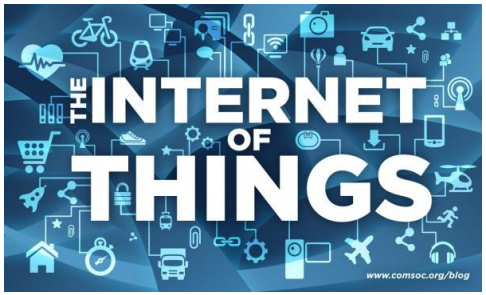
OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

CONTRATAÇÕES INTERPESSOAIS (pessoa e pessoa)



CONTRATAÇÕES INTERATIVAS (pessoa e sistema)

CONTRATAÇÕES INTERSISTEMÁTICAS (sistema e sistema)



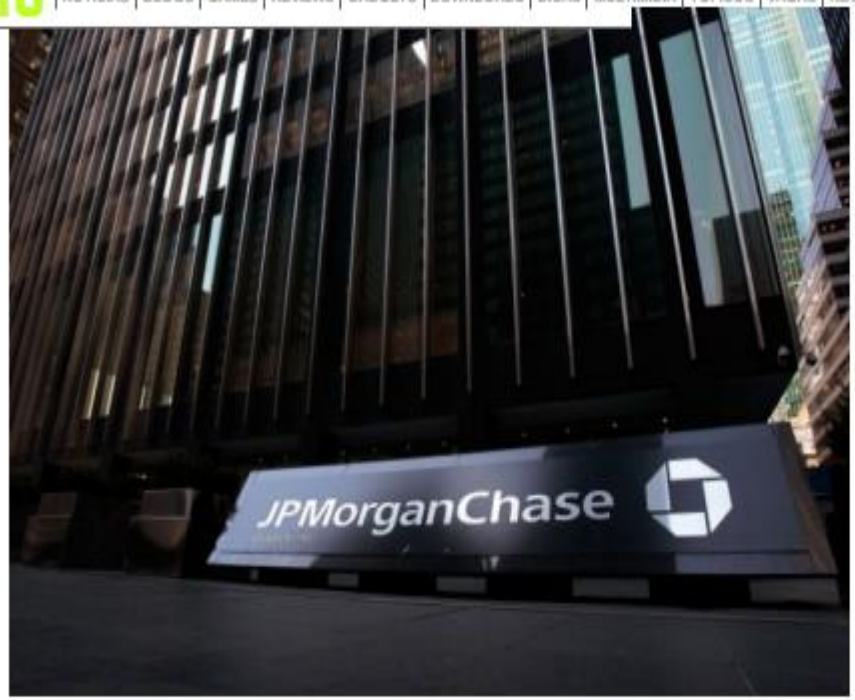
Vazamento de Informações

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

02/10/2014 20h57 - Atualizado em 02/10/2014 21h00

Dados de 76 milhões de clientes do banco JPMorgan foram violados

info | NOTÍCIAS | BLOGS | GAMES | REVIEWS | GADGETS | DOWNLOADS | DICAS | MULTIMÍDIA | TÓPICOS | VAGAS | REVISTA | SHOPPING | INFOStart |



Getty Images

O JPMorgan Chase informou nesta quinta-feira que dados de 76 milhões de clientes – nomes, endereços, e-mails e telefones – e de sete milhões de empresas foram comprometidos por uma violação de arquivos durante o último verão dos Estados Unidos.

O maior banco americano disse que não há qualquer evidência de que informações como números de conta bancária, identidade do usuário ou senhas de segurança tenham sido roubadas pelos hackers.

O banco "não viu qualquer fraude incomum relacionada ao incidente". "Os clientes do JPMorgan Chase não são responsáveis por transações não autorizadas em suas contas, que devem ser imediatamente comunicadas à entidade", complementou.

O JPMorgan Chase disse em agosto que estava cooperando com as autoridades, após tomar conhecimento de que hackers da Rússia haviam invadido seus sistemas de computador.

No início desta quinta-feira, o New York Times informou que o JPMorgan Chase foi invadido pela segunda vez em três meses. Segundo a matéria, o banco descobriu que hackers da Itália e de outras partes do sul da Europa acessaram seu servidor.

Uma porta-voz do JPMorgan Chase, contudo, disse que a matéria era falsa e que o banco não estava ciente de nenhum novo ataque.

http://info.abril.com.br/noticias/seguranca/2014/10/dados-de-76-milhoes-de-clientes-do-banco-jpmorgan-foram-violados.shtml

Segurança da Informação

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

2014: A Year of Mega Breaches

Sponsored by Identity Finder

Independently conducted by Ponemon Institute LLC

Publication Date: January 2015

77% das empresas admitem que tiveram vazamento de dados no último ano, por conta de algum tipo de incidente. A principal causa citada para isso é a perda ou o roubo de equipamentos, seguida por ataques à rede, vulnerabilidades dos dispositivos móveis, Web 2.0 e e-mails enviados para remetentes errados.

http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf

Aos 40 anos, e-mail continua avesso a mecanismos de segurança

CSO/EUA Siga @idgnow

29 de abril - 15h15 - Atualizada em 15 de março - 13h47

Pesquisa revela que 3 em 4 funcionários de grandes empresas já violaram políticas de e-mail; combinar controle com facilidade de uso é desafio.

Notícias Relacionadas

- Um clique. E dados de 18 mil clientes são distribuídos em newsletter
- Malásia quer uma conta de e-mail por cidadão até 2015
- Gmail agora deixa colocar imagens na sua conta

Há 40 anos o e-mail era inventado. Mas, apesar da idade, o serviço permanece avesso à segurança, segundo uma pesquisa divulgada nesta semana.

De acordo com o estudo, realizado pela empresa de segurança em comunicações VaporStream, quase 75% dos entrevistados em grandes empresas informaram ter violado políticas de segurança em relação ao e-mail. E um terço afirmou ter feito isso de propósito.

O resultado lembra como é difícil fornecer segurança até para a mais utilizada das aplicações e levanta a questão: O que pode ser feito para torná-lo mais seguro sem comprometer sua funcionalidade?

http://idgnow.uol.com.br/internet/2011/04/29/aos-40-anos-e-mail-continua-avesso-a-mecanismos-de-seguranca/

PL de Proteção de Dados Pessoais

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Agenda – Impactos nos Negócios Bancários

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

- ***Privacy Officer*;**
- **Vazamentos de dados e notificações obrigatórias;**
- **Responsabilidade;**
- **Sanções.**

I – finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular;

II – adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

III – necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais; (...)

VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e (...)

Privacy Officer (art. 41)

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

- **Conceito:** definido como "*encarregado*" pelo tratamento de dados pessoais, ou seja, a pessoa responsável dentro da empresa pelas operações e políticas de tratamento de dados pessoais e pela comunicação com o órgão competente, a versão anterior determinava que toda empresa com mais de 200 funcionários deveria criar tal cargo. A nova versão não delimita um tamanho específico;

- **Atribuições: (I)** receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; **(II)** receber comunicações do órgão competente e adotar providências; **(III)** orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e **(IV)** demais atribuições determinadas pelo responsável ou estabelecidas em normas complementares.

Segurança e Sigilo de Dados

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

- **Medidas de Segurança (art. 45):** O operador deve adotar ***medidas de segurança técnicas e administrativas*** aptas a ***proteger os dados pessoais*** de ***acessos não autorizados*** e de ***situações acidentais ou ilícitas*** de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- **Vazamentos de dados e notificações obrigatórias (art. 47):** O responsável deverá **comunicar**, em ***prazo razoável***, o órgão competente sobre a ocorrência de qualquer ***incidente de segurança*** que possa acarretar risco ou prejuízo relevante aos titulares.

Requisitos da Comunicação e Providências (art. 47, parágrafo único)

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Art. 47. O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso da comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

Art. 48. O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de outras providências, como:

I - pronta comunicação aos titulares;

II - ampla divulgação do fato em meios de comunicação; e

III - medidas para reverter ou mitigar os efeitos do incidente.

LIMINAR BUSCA E APREENSÃO – 18ª VT ZONA SUL/SP

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Para a concessão da medida pleiteada é necessário que o pedido preencha os requisitos de verossimilhança da alegação e o fundado receio de dano irreparável ou de difícil reparação.

No caso dos autos, vislumbro a presença do *fumus boni iuris*, uma vez que a autora carreou aos autos documentos hábeis a demonstrar que a ré utilizou-se de seu e-mail corporativo para o envio de arquivo contendo as referidas informações sigilosas para seu e-mail particular o que, por si só, indica eventual pretensão de utilização ou divulgação das informações ali constantes, o que pode gerar graves danos não somente à autora como também a todos os seus clientes cujos dados ali estão inseridos.

Presente, também, a urgência da medida, pois é sabido que os meios informáticos são notoriamente fluidos e com eventual demora a ré poderá efetuar cópias dos arquivos em mídias móveis de fácil ocultação ou efetuar a transferência dos arquivos para eventual provedor de internet com sistema de depósito "nas nuvens", o que permitiria o seu acesso pela ré em qualquer dispositivo informático e em qualquer local com acesso à internet. Ademais, poderia a ré efetuar o envio dos arquivos através de seu e-mail pessoal para diversas outras contas de e-mail ou, até mesmo, divulgá-los nas redes sociais. Evidente, portanto, o *periculum in mora*.

Nessas circunstâncias, havendo fortes indícios de que a conduta da ré violou os direitos de sigilo de dados e de propriedade da autora (art. 5º, X e XII, da CF), sendo imperioso destacar que a autora é instituição financeira que tem o dever legal de conservar o sigilo em suas operações, cabível a medida pleiteada em sede de liminar *inaudita altera parte*.

Ante o exposto, nos termos do art. 804 do Código de Processo Civil, **defiro parcialmente o pedido de liminar** para determinar:

- Busca e apreensão de cópias de todo o conteúdo armazenado em discos rígidos, mídias removíveis e outros meios de guarda de arquivos encontrados no local da diligência;
- Cópia de todas as mensagens de e-mail da ré, inclusive os registros de webmail (área de swap), apenas em relação ao recebimento e encaminhamento do arquivo mencionado pela autora;
- Busca e apreensão de todos e quaisquer outros documentos físicos ou informáticos relacionados ao objeto da perícia, incluindo banco de dados, tabelas e similares;

Passo a examinar o pedido de tutela antecipada preventiva. Pretende o requerente a antecipação de tutela de obrigação de não fazer, com respaldo no Art. 461 do CPC. Para a concessão da medida postulada, o dispositivo processual tem como pressuposto o justificado receio de que um ato contrário ao direito seja praticado antes do trânsito em julgado.

Conforme demonstrado na petição inicial, **o ato praticado pelo requerido de enviar os dados da cartela de clientes, cujas contas gerenciava, a um endereço eletrônico estranho à ambiência laboral, realizado no mesmo dia em que pediu a rescisão do seu vínculo empregatício, configura justificado receio de que esses dados possam ser usados pelo destinatário do e-mail para as mais variadas e inusitadas finalidades, inclusive por outra instituição financeira, o que configuraria o desvio ilícito de clientela.** (...) **Ante o exposto, DEFIRO a antecipação de tutela**, determinando apenas que: a) **o requerido se abstenha, a partir desta decisão, de utilizar, explorar ou divulgar, de qualquer forma, para quaisquer fins, e por qualquer meio ou processo, de quaisquer informações do requerente que estejam em seu poder**, bem como das informações ilicitamente desviadas, conforme comprova a Ata Notarial colacionada (doc. 09), sob pena de multa de R$ 1.000,00 por cada utilização, exploração ou divulgação comprovada, limitada a R$ 50.000,00;

Responsabilidade e Penas

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

- **Responsabilidade subjetiva (art. 42)**: a versão anterior atribuía responsabilidade objetiva aos responsáveis pelo tratamento de dados pessoais. A nova versão atribui responsabilidade subjetiva. Possibilidade de inversão do ônus da prova.

- **Sanções (art. 52): (I)** multa simples ou diária; **(II)** publicização da infração; **(III)** anonimização dos dados pessoais; **(IV)** bloqueio dos dados pessoais; **(V)** suspensão de operação de tratamento de dados pessoais; **(VI**) cancelamento dos dados pessoais; e **(VII)** suspensão de funcionamento de banco de dados.

Resolução do Bacen
Abertura de contas por meio eletrônico

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Resolução 4.480/16

1)COMPROVAÇÃO DOCUMENTAL: deve ser garantida a comprovação de integridade, autenticidade e confidencialidade dos documentos eletrônicos relacionados aos procedimentos de abertura de conta - isso pode se dar, não apenas por meio de certificação digital, mas por outros métodos, inclusive a assinatura em dispositivos eletrônicos, a qual terá equivalência funcional ao "cartão com autógrafo" mencionado na Resolução 2.025/1993 do Bacen.

2)REGRAS DE SEGURANÇA DA INFORMAÇÃO: as Regras de Segurança da Informação (RISI) devem ser revisitadas, com o objetivo de que expressamente protejam os dados e os documentos dos correntistas, contra acesso não autorizado, sendo importante confirmar, também, que todo o disposto na Resolução 4.474/2016 do Bacen está sendo contemplado, especialmente os artigos 5º a 8º.

3)BACKUP: os procedimentos de backup devem ser rigorosamente seguidos, no que recomendamos que esse assunto seja incluído com ainda maior detalhamento, quando dos ajustes às Regras de Segurança, também observando o disposto na Resolução 4.474, acima mencionada.

4)CADEIA DE CUSTÓDIA: deve haver cadeia de custódia das ações realizadas na plataforma eletrônica, sendo possível auditar e rastrear a utilização dela e das tecnologias utilizadas, caso seja necessária a realização de perícia.

5)MANUAL DE PROCEDIMENTOS: todos os procedimentos correlacionados à abertura e ao encerramento de contas de depósito devem constar em manual próprio, elaborado pela instituição financeira, cabendo à auditoria interna validá-lo, e realizar testes periódicos na plataforma, confirmando a sua plena segurança.

Fonte: https://www.linkedin.com/pulse/5-pontos-de-aten%C3%A7%C3%A3o-em-rela%C3%A7%C3%A3o-%C3%A0-resolu%C3%A7%C3%A3o-do-bacen-carvalho-lima?trk=prof-post

Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes **diretrizes sobre padrões de segurança**:

I - o **estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários**;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, **sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros**;

III - a **criação de inventário detalhado dos acessos** aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e

IV - o uso de soluções de gestão dos registros por meio de **técnicas que garantam a inviolabilidade dos dados**, como encriptação ou medidas de proteção equivalentes.

OBRIGADA!

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

rubia@opiceblum.com.br

Rubia Ferrão

- Advogada atuante na advocacia consultiva, preventiva e contenciosa, com ênfase em Direito Digital.
- Sócia do Opice Blum, Bruno, Abrusio, e Vainzof Advogados Associados.
- Especialista em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo.
- Professora da Faculdade de Direito da Universidade São Francisco.
- Professora do curso de Especialização em Computação Forense do Mackenzie.
- Professora convidada de algumas instituições de ensino como USP, FGV, EPD, UNICID e UNIGRAN.
- Currículo Plataforma Lattes: http://lattes.cnpq.br/6919075258032289

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF