

Recomendação n. 01 / 2018

Inquérito Civil Público - ICP n. 08190.044813/18-44

Considerando que incumbe ao **Ministério Público** a defesa dos interesses sociais e individuais indisponíveis;

Considerando que a unidade e a indivisibilidade são princípios institucionais do **Ministério Público**;

Considerando que ao **Ministério Público** incumbe promover, privativamente, a ação penal pública;

Considerando que são funções institucionais do **Ministério Público** promover o inquérito civil e a ação civil pública para a proteção de interesses difusos e coletivos;

Considerando que, segundo dicção do Código de Defesa do Consumidor, a defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo;

Considerando que o **Ministério Público** poderá propor ação civil coletiva de responsabilidade pelos danos individualmente sofridos a ser ajuizada no foro da Capital do Estado ou no do Distrito Federal, para os danos de âmbito nacional ou regional;

Considerando que compete à **Comissão de Proteção dos Dados Pessoais** do **Ministério Público do Distrito Federal e Territórios** receber comunicações

sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo aos titulares dos dados pessoais (*data breach notification*), bem como sugerir, diante da gravidade do incidente de segurança, ao responsável pelo tratamento dos dados a adoção de outras providências, tais como: pronta comunicação aos titulares; ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente;

Considerando que, nos termos do artigo 6º, inciso XX, da Lei Complementar n.75/1993, compete ao **Ministério Público** "*expedir recomendações, visando à melhoria dos serviços públicos e de relevância pública, bem como o respeito, aos interesses, direitos e bens cuja defesa lhe cabe promover, fixando prazo razoável para a adoção das providências cabíveis*";

Considerando o incidente de segurança¹ (*data breach*) envolvendo a base de dados de clientes da empresa **Netshoes** (Ns2.Com Internet S.A.) - datado de dezembro de 2017;

tec

Hackers vazam dados cadastrais de 17,9 mil clientes da Netshoes



Fachada da Netshoes em loja física

NATÁLIA PORTINARI
DE SÃO PAULO

14/12/2017 © 19043

¹ PORTINARI, Natália. tec. *Folha de São Paulo*, São Paulo, 14 dez. 2017. **Hackers vazam dados cadastrais de 17,9 mil clientes da Netshoes.** Disponível em: <<http://www1.folha.uol.com.br/tec/2017/12/1943327-hackers-vazam-dados-cadastrais-de-179-mil-clientes-da-netshoes.shtml>>. Acesso em: 19 jan. 2018.

Considerando as informações ofertadas pela empresa em resposta às perguntas requisitadas por meio do Ofício n. 60/2017 - 2PJCRIM - datado de 11 de dezembro de 2017;

Considerando que já foi requerida à **Polícia Federal** a instauração de inquérito policial para identificar os responsáveis pela tentativa de extorsão da empresa com uso dos dados pessoais objeto do incidente de segurança;

Considerando a notícia de novo incidente de segurança² envolvendo a mesma empresa que supostamente comprometeu mais de 1 milhão de contas - datada de janeiro de 2018;



Considerando que o **Ministério Público do Distrito Federal e Territórios** teve acesso aos dados "vazados", contendo informações de **1.999.704** (um milhão novecentos e noventa e nove mil e setecentos e quatro) contas (*order_history1M.txt* = **1.499.767** contas e *order_history500k.txt* = **499.937** contas);

² PAYÃO, Felipe. *TECMUNDO*, São Paulo, 16 jan. 2018. **Vazam mais dados sensíveis de 1 milhão de clientes da Netshoes**. Disponível em: <<https://www.tecmundo.com.br/seguranca/126198-vazam-dados-sensiveis-1-milhao-clientes-netshoes.htm>>. Acesso em: 19 jan. 2018.

Considerando que se trata de um dos maiores incidentes de segurança registrados no Brasil, colocando em risco milhares de titulares dos dados pessoais;

Considerando que a análise inicial dos dados comprovou o comprometimento das seguintes informações pessoais dos clientes **Netshoes**:

Joao Joao Joao ; 000000000000 ; exemplo123@exemplo123.com.br ; 00/00/0000 ; 000000000000 ; R\$00,00 ; 00/00/0000 ; CreditCard ; COL-1660-006-02³

- **Nome do cliente**

Sequência alfabética: Joao Joao Joao

- **Número do Cadastro de Pessoa Física da Receita Federal - CPF**

Sequência de 11 números: 000000000000

- **E-mail**

Sequência alfanumérica com o símbolo "@" (arroba):

exemplo123@exemplo123.com.br

- **Data de nascimento do cliente**

Sequência numérica com 2 caracteres "/" (barra): 00/00/0000

- **Número do Pedido - informação interna da empresa**

Sequência de 11 números: 000000000000

- **Valor do produto adquirido no site da empresa**

Sequência alfanumérica: R\$00,00

- **Data da compra do produto**

Sequência numérica com 2 caracteres "/" (barra): 00/00/0000

- **Forma de pagamento do produto**

CreditCard ou Boletto

- **Código de referência do produto⁴**

COL-1660-006-02

³ Informações meramente exemplificativas para demonstrar a forma que estão estruturados os dados pessoais comprometidos pelo incidente.

⁴ Esta variável indica o tipo de produto que foi adquirido no site da **Netshoes**, podendo ser revelado com o simples ato de digitar o código em uma plataforma de busca como o **Google**.

Considerando que levantamento preliminar realizado pelo **Ministério Público do Distrito Federal e Territórios**, por meio de amostragem, demonstrou a veracidade dos dados pessoais comprometidos, inclusive a genuinidade do **código interno da empresa referente à ordem efetivada pelo cliente - Número do Pedido**;

Considerando que o citado levantamento do **Ministério Público**, também por amostragem, comprovou que os produtos adquiridos no site da empresa, indicados no vazamento como **código de referência do produto**, foram efetivamente entregues pela **Netshoes** aos clientes;

Considerando que incidente de segurança comprometeu os dados pessoais de servidores públicos **politicamente expostos**, conforme a análise dos e-mails tornados públicos pelo incidente de segurança, como por exemplo: **Tribunal de Contas da União** (@tcu.gov.br), **Câmara dos Deputados** (@camara.leg.br), **Tribunal de Justiça do Distrito Federal e Territórios - TJDF** (@tjdft.jus.br), **Polícia Federal** (@dpf.gov.br), **Superior Tribunal de Justiça** (@stj.jus.br), **Supremo Tribunal Federal** (@stf.jus.br), **Ministério da Justiça** (@mj.gov.br), **Advocacia-Geral da União** (@agu.gov.br), **Presidência da República** (@presidencia.gov.br), dentre outros;

Considerando as diversas classes profissionais afetadas pelo incidente de segurança, como **advogados** (adv.com.br), **médicos** (med.com.br), **engenheiros** (eng.com.br), **veterinários** (vet.com.br), dentre outras;

Considerando que os **códigos de referência dos produtos** indicaram a aquisição de produtos de saúde, como por exemplo monitor de pressão arterial, caracterizando, assim, **dados pessoais sensíveis**⁵ dos titulares;

⁵ Dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos.

Considerando a instauração de **Inquérito Civil Público - ICP**⁶ pelo **Ministério Público do Distrito Federal e Territórios** para " *Investigar as circunstâncias e as causas do incidente de segurança que comprometeu os dados pessoais dos clientes da Netshoes (Ns2.Com Internet S.A.), bem como apurar as responsabilidades pelos danos causados*";

Considerando as insuficientes medidas adotadas pela empresa **Netshoes** no sentido de informar os clientes prejudicados pelo incidente de segurança, consubstanciado no envio de e-mail genérico para a base de consumidores:



Considerando a gravidade dos fatos, o risco de prejuízos graves aos consumidores e a quantidade de titulares dos dados pessoais afetados, o **Ministério Público do Distrito Federal e Territórios**, por meio da **Comissão de Proteção dos Dados Pessoais**, da **2ª Promotoria de Justiça Criminal** e da **1ª Promotoria de Justiça de Defesa do Consumidor**, resolve

⁶ Inquérito Civil Público - ICP n. 08190.044813/18-44 - Comissão de Proteção dos Dados Pessoais, 2ª Promotoria de Justiça Criminal e 1ª Promotoria de Justiça de Defesa do Consumidor.

RECOMENDAR à empresa **Netshoes** (Ns2.Com Internet S.A.), na pessoa do seu C.E.O., Sr. **Marcio Kumruian**, que:

1º) Informe aos clientes afetados pelo incidente de segurança (*order_history1M.txt* = 1.499.767 contas e *order_history500k.txt* = 499.937 contas), através de correspondência, com aviso de recebimento (AR), ou por meio de ligação telefônica, que os seguintes dados pessoais foram comprometidos:

- Nome do cliente
- Número do **Cadastro de Pessoa Física** da Receita Federal - CPF
- E-mail
- Data de nascimento do cliente
- Número do **Pedido** - informação interna da empresa
- Valor do produto adquirido no site da empresa
- Data da compra do produto
- Forma de pagamento do produto
- Código de referência do produto

O descumprimento deste item implicará no ajuizamento de Ação Civil Pública por danos morais e materiais causados aos consumidores.

2º) Abstenha-se de efetuar qualquer tipo de pagamento ao suposto autor do incidente de segurança (*Hacker*), seja na forma de moeda física ou de criptomoeda, sob pena de configuração do **crime de fraude processual**⁷ na modalidade "*inovar artificialmente, na pendência de processo administrativo, o estado de coisa*".

Confere-se o **prazo de 3 (três) dias úteis**, a contar do recebimento desta, para que a empresa se manifeste sobre a presente Recomendação, informando se a acatará ou não, expondo as razões de eventual recusa.

⁷ **Fraude processual**

Art. 347 - Inovar artificialmente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito:

Pena - detenção, de três meses a dois anos, e multa.

Parágrafo único - Se a inovação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro.

A manifestação poderá ser encaminhada para o e-mail xxxxxxxxxxx@xxxxx.xx.xx e somente será considerada válida com mensagem de confirmação de recebimento por parte do destinatário.

Em caso de acatamento, a empresa deverá elencar, de maneira clara, objetiva e precisa, quais serão as medidas implementadas.

Ademais, a ausência de manifestação será interpretada como recusa de acatamento.

Brasília-DF, 25 de janeiro de 2018.

Frederico Meinberg Ceroy⁸

Promotor de Justiça
*Coordenador da Comissão de
Proteção dos Dados Pessoais*

⁸ Original assinada e enviado à sede da empresa na rua Vergueiro, 943.