A guerra podre eleitoral está por vir com a propaganda paga na Internet e as fakenews

A guerra podre eleitoral está por vir com a propaganda paga na Internet

A Internet sempre foi o maior receito dos políticos de carreira. Em um cenário onde muitos tem a máquina, dinheiro, ou dominam algum meio de comunicação em massa como rádio, concessões ou afiliadas de TVs, liberar a rede para propaganda eleitoral era um perigo, considerando que não se sabe como os candidatos “sem condições” conseguiriam se projetar.

A campanha de OBAMA em 2008 e a da sua reeleição mostraram o poder do uso correto da Internet, de técnicas de otimização para os sites (SEO) a postagens recorrentes em horários estratégicos, passado por crowdfunding e pela presença em outras mídias pouco exploradas pela concorrência. Chegou-se a um resultado onde o mapa eleitoral se equivalia à curtidas e crescimento dos ativos digitais.

Em 2008, a primeira resolução que permitia a propaganda na internet era extremamente limitada e só permitia a propaganda via “sites”. Em 2009 a Lei eleitoral era alterada para permitir a internet como plataforma de propaganda de propaganda eleitoral. De lá para cá em todas as reformas eleitorais, um ponto nunca fora alterado: Não se poderia por dinheiro na Internet.

Na Internet era proibida qualquer tipo de propaganda eleitoral paga. E isso se justificava pois se na Internet fosse permitido “colocar dinheiro”, ela se equipararia à meios tradicionais, onde poucos tem acesso pleno (como revistas, jornais, etc.), mais uma vez se tornando uma forma de propaganda que privilegia alguns em detrimento da maioria dos

candidatos. Tudo mudou.

A reforma trazida pela Lei 13.488/2017 que alterou a Lei das Eleições liberou o impulsionamento de conteúdos contratados diretamente (e não via agências de marketing) com os provedores de aplicação de Internet, como Facebook, Instagram, etc, desde que com sede e foro no País.

Não bastasse, equiparou, para fins de impulsionamento, a priorização paga de conteúdos resultantes de aplicações de busca na Internet. Ou seja, está liberado pagar para "ser bem ranqueado" no Google (adwords) e outros buscadores. O cidadão está preparado para lidar com esta propaganda?

Quebra-se a isonomia e mais uma vez, quem tem mais irá aparecer em destaque, só que desta vez, não no rádio, TV, jornal ou nas ruas, mas na Internet. Mas não é só isso. Embora os gastos com impulsionamento sejam considerados gastos de campanha, sabe-se que existem formas de se impulsionar sem que necessariamente se tenha gastos. Estes meios "não oficiais" embora vedados pelo TSE, não encontram amparo investigativo e certamente serão utilizados para viralização de conteúdos e criação de caixas de ressonância, com destaque para os chatbots e botsprofiles, que são contratados a partir de outras aplicações que se conectam às redes sociais.

E não é só. A partir do primeiro dia de propaganda seremos bombardeados com posts pagos e impulsionados que terão a expressão "propaganda eleitoral", mas em meio a um mar de propaganda patrocinada e impulsionada, quem garantirá que terceiros não impulsionem propagandas negativas disfarçadas? Ou mesmo quem garantirá quem estará na frente de quem nas buscas? Mais uma vez estamos falando dos algoritmos das redes sociais. Eles são honestos? Ou os mais habilidosos em palavras chave e otimização de campanhas se destacarão?

Já se pode imaginar, por exemplo, o impulsionamento e patrocínio de postagens a partir de palavras chave envolvendo

o concorrente, ou mesmo de palavras negativas. Como reagir a isto na celeridade de um pleito eleitoral? A guerra podre da propaganda paga na Internet vai começar. Aos candidatos e comitês caberá monitorar as redes, reportar e representar ofensas, mas principalmente, em determinados casos, realizar judicialmente a quebra de sigilo e a busca de informações sobre os impulsionamentos e suas configurações, de modo a constatar se existe ou não alguma prática considerada abusiva ou impulsionamentos por meios não autorizados. Resta saber se o TSE, comitês e principalmente, provedores de aplicações, estão preparados para absorver estas demandas, impedindo que a internet seja usada para manipular a decisão de milhões de eleitores.

Quando os algoritmos falham e o combate ao Fakenews causa outros danos

A maior rede social do mundo enfrenta grandes problemas diante do vazamento de dados de 50 milhões de perfis a partir de aplicativo instalado em mais de 250 mil destes, que serviram de insumo para análises pela Cambridge Analítica, de uso na campanha eleitoral norte-americana para direcionamento de propaganda.

Em tempos de novo regulamento de proteção de dados pessoais aprovado na União Europeia e enrijecimento da proteção aos dados dos norte-americanos (Já se discute o *Honest Ads Act*, proposta que obriga empresas de tecnologia a revelarem compradores de publicidade que sejam políticos) o descrédito e a queda do valor das ações estão fazendo Facebook tomar

medidas drásticas, sobretudo com vistas às eleições do Brasil e México.

Assim, o que já ocorre em outros países pode ocorrer aqui também, por meio da técnica de fact-cheking, ou seja, a partir de um link que o usuário pretende postar, o Facebook utilizará parceiros para avaliar a notícia e motivar o usuário a repensar antes de postar, além de estratégias convencionais, como reduzir alcance de páginas que costumam divulgar informações falsas.

Porém só isso não adianta, pois sabe-se que um bot irá aprender a postar a notícia falsa a despeito do aviso de que algo "não é bem assim". Por isso a rede está testando o aprendizado de maquina, de forma a detectar paginas e conteúdos enganosos e poderá até mesmo remover automaticamente os mesmos.

Recentemente identifiquei que rede já está "taggeando imagens", ou seja, a partir de inteligência artificial e algoritmos, consegue identificar o contexto das imagens postadas, certamente para detectar conteúdos abusivos e fakes também em formato visual. Na minha imagem que postei, o Facebook até detectou que eu estava de "terno".

Sabe-se que as vitimas de fakes podem recorrer ao Judiciário, por meio de um advogado em direito digital, em busca da exclusão do conteúdo, como recentemente ocorrido no caso da vereadora Marielle, onde um processo no Rio de Janeiro indaga o Facebook se o MBL pagou para impulsionar FakeNews, havendo risco de multa suspensão e bloqueio no Brasil, caso descumpra a ordem.

Na ânsia de frear o FakeNews, a rede corre um outro risco, o de ser responsabilizada por interferir no conteúdo, rotular indevidamente e excluir perfis que não espalhavam desinformações, além de gerar "bolhas de opiniões" ou "caixas

de ressonância", priorizando a usuários conteúdos que os mesmos possuem afinidade, ainda que proveniente de fontes duvidosas. Algoritimos falham ou podem ser usados para criar estados artificiais, fazer deduções equivocadas ou mesmo influenciar decisões. Não se sabe, até hoje, como o Facebook trabalha os seus códigos neste sentido.

Recentemente, até mesmo alguns novos chatbots foram bloqueados, diante das medidas anunciadas pela empresa para aprimorar a privacidade, englobando o seu Messenger.

Neste contexto, pessoas e empresas prejudicadas e que tiveram páginas excluídas podem recorrer ao Judiciário e processar a rede para manterem seus conteúdos no ar, ilegitimamente excluídos por erros, má intenções ou manipulações de códigos e algoritmos.

Não demais destacar, no entanto, a questão da onda de Fakenews e da violação a privacidade também pode ser evitada ou minimizada pela ação de usuários. De nada adianta as ações propostas como o Fatima (*chat bot que esclarece usuários sobre fakenews*) se estes continuam trocando sua privacidade por inutilitários que os mostram mais velhos, parecidos com algum artista ou mesmo no sexo oposto. Ao aceitar estes Apps, muitos usuários não vêem, mas estão concedendo acesso para que o token usado no App permita a coleta de informações e alimente o mercado de Fakenews, com nítida interferência no debate e no contraditório, que deveria ser o natural nas redes sociais, ameaçando a própria Democracia.

Medida sérias para provedores negligentes, lei de proteção de dados pessoais e educação digital, além de incentivo a aplicações ofereçam meios para o usuário detectar uma notícia aparentemente falsa. Não existem segredos para minimizarmos a onda de exposição indevida de dados e combate às notícias fraudulentas.

Ao leitores e usuários do Facebook, recomendo uma extensão do

Firefox, chamada Facebook Container (https://addons.mozilla.org/en-US/firefox/addon/facebook-container/), que acaba de ser lançada e assegura maior privacidade ao usuário de Internet, impedindo o compartilhamento de informações de outros sites com a rede social. Acaba assim com a publicidade segmentada e direcionada com base no que o usuário pesquisou ou acessou, atuando sobre os cookies do computador.

José Antonio Milagre é Advogado especializado em Direito Digital, Mestre e Doutorando em Ciência da Informação pela UNESP e pesquisador do Núcleo de Estudos em Web Semântica e Dados Abertos da Universidade de São Paulo.

Esclarecimento aos Advogados: O que fazer diante do erro PETPG-99 no E-SAJ?Esclarecimeto aos Advogados: O que fazer diante do erro PETPG-99 no E-SAJ?

Muitos colegas me ligam ou enviam mensagem sobre o precitado erro. Infelizmente nem o suporte muitas vezes é capaz de informar do que se trata. Se a própria desenvolvedora do sistema não é clara, imagine suportes locais.

Muitas pessoas confundem com o erro AP-99, relativo a "certificados duplicados" e aplicam o procedimento de remoção de certificados da máquina com o "*certmgr.msc*" aqui explicado.

Ocorre que não se trata do mesmo erro. Algumas subseções ainda informam que se trata de arquivo PDF gerado em programa não homologado ou com mais de 300kb por página. Nada disso!

Infelizmente, nos casos que contornamos o erro, identificamos se tratar de um erro no próprio e-saj, especificamente no cadastro de uma "nova parte" ou "novo advogado". Nos casos de cadastramento de uma parte ou atualização dos dados das partes, o erro ocorre na hora da assinatura e envio.

Como contorno, a solução que encontramos (até o E-SAJ corrigir o erro) é distribuir o processo com dados desatualizados da parte (usando parte cadastrada, se existir) e posteriormente peticionar requerendo complementação do cadastro ou polo passivo.

Foi o que identificamos como "paliativo". Continuamos abismados com o descaso da responsável pelo software, que até o momento não comunica sobre a falha ou mesmo oferece uma orientação clara aos advogados sobre o que fazer diante deste erro e outros como AP-44, PETPG 35, etc. Aguardamos respostas da desenvolvedora sobre nossas cobranças envolvendo a descrição das falhas e procedimentos a serem tomados pelos Advogados diante dos erros reportados.

José Antonio Milagre, Presidente da Comissão de Direito Digital e Processo Eletrônico da OAB/SP Regional da Lapa.

Direito Digital ganha espaço no mercado

Leia mais em: Depois da ascensão do Direito Digital no mercado de trabalho e na vida das pessoas, a idéia de uma terra sem

lei ficou restrita aos filmes de bangue-bangue. Esta área do Direito, que mesmo sem legislação definida tenta colocar ordem no meio virtual e garantir segurança para os internautas, virou uma boa opção para quem escolheu ser advogado.

José Antonio Milagre, Escritório de Advocacia Especializado em Direito Digital

---

Advogados de Direito Eletrônico e Internet em São Paulo (SP)

É um campo do Direito que se propõe a estudar aspectos jurídicos do uso de computadores e da tecnologia da informação em geral, com fundamento no crescente desenvolvimento da Internet e na importância da tecnologia da informação e da informática nas relações jurídicas, sendo por isso, uma nova área do estudo do Direito.

Conheça o diretório do JusBrasil: https://www.jusbrasil.com.br/advogados/direito-digital-sp-sao-paulo/

José Antonio Milagre é Advogado Especialista em Direito Digital

---

A perícia digital e informática no Novo CPC

Dentre as significativas alterações trazidas pelo PLS 166/2010, conhecido como o "Novo Código de Processo Civil", pendente apenas de sanção presidencial, estão modificações introduzidas na Prova Pericial. A prova pericial, consistente em exame, vistoria ou avaliação, é necessária quando a questão objeto do litigio, para ser julgada, necessita de esclarecimentos técnicos.

Os peritos, no Código de 1973, seriam os escolhidos dentre profissionais de nível universitário, devidamente inscritos no órgão de classe competente. E nas localidades onde não houvessem profissionais qualificados que preenchiam tais requisitos, a indicação dos peritos era de livre escolha do juiz.

No Novo CPC, os peritos serão nomeados entre os profissionais legalmente habilitados e os órgãos técnicos ou científicos devidamente inscritos em cadastro mantido pelo Tribunal ao qual o juiz está vinculado.

Para a formação de tal cadastro, os Tribunais devem realizar consulta pública, por meio de divulgação na rede mundial de computadores ou em jornais de grande circulação, além de consulta direta a universidades, a conselhos de classe, ao Ministério Público, à Defensoria Pública e à Ordem dos Advogados do Brasil, para a indicação de profissionais ou órgãos técnicos interessados.

Por outro lado, permanece, com outras palavras, a regra de que na localidade onde não houver inscrito no cadastro disponibilizado pelo Tribunal, a nomeação do perito é de livre escolha pelo juiz e deverá recair sobre profissional ou órgão técnico ou científico comprovadamente detentor do conhecimento

necessário à realização da perícia.

Assim, a Lei não faz mais menção o pré-requisito "profissionais de nível universitário" devidamente inscritos no órgão de classe competente. Criou-se a expressão profissional "legalmente habilitado". Ora, legalmente habilitado seria aquele que por lei ou regulamentação teria condições de atuar em uma área do conhecimento de relevância para o juízo na análise de determinado caso. Logo, não havendo lei regulamentando determinada área de conhecimento, este profissional estaria exercendo atividade legal ou no mínimo, não teria nenhum impeditivo para peritar.

A Lei confirma o entendimento do STJ, que já se pronunciou recentemente no sentido de que a falta de formação específica do perito não anula laudo pericial (http://www.stj.jus.br/sites/STJ/default/pt_BR/noticias/noticias/Falta-de-forma%C3%A7%C3%A3o-espec%C3%ADfica-do-perito-n%C3%A3o-anula-o-laudo-pericial)

Problema antigo era a "reserva de perícias" ou varas que mantinham verdadeiras parcerias com peritos específicos, evitando que qualquer outro se habilitasse ou se habilitado, fosse nomeado. O novo CPC estabelece que será organizada lista de peritos na vara ou na secretaria, com disponibilização dos documentos exigidos para habilitação à consulta de interessados, para que a nomeação seja distribuída de modo equitativo, observadas a capacidade técnica e a área de conhecimento.

O novo CPC traz ainda a figura da "prova simplificada", que poderá ser determinada de ofício ou à requerimento das partes e consiste na substituição da perícia por uma simples inquirição pelo juiz a um especialista, sobre ponto controvertido da causa, o qual demanda conhecimento técnico ou científico.

Para a prova simplificada, o especialista deverá ter formação

acadêmica específica na área de objeto do seu depoimento e poderá ser valer de recursos tecnológicos de transmissão de sons e imagens com o fim de esclarecer os pontos controvertidos.

Formação acadêmica não significa “curso superior” na área de objeto do seu depoimento, mas a somatória de cursos e títulos que comprovam especialidade na área.

Fica prevista também em lei uma prática que já era comum hoje em dia, ou seja, a possibilidade do Juiz autorizar o pagamento de até cinquenta por cento dos honorários no início dos trabalhos, podendo o juiz reduzir os honorários do perito quando a perícia for considerada inconclusiva ou deficiente.

Há uma preocupação veemente do Novo CPC com a publicidade das diligências do perito. Hoje, quando nomeado judicialmente, cada perito agia de uma forma, sendo que alguns enviavam e-mails diretamente às partes designando o início dos trabalhos e outros protocolavam a data em juízo, requerendo ciência as partes por publicação oficial.

Agora, o perito deve assegurar aos assistentes das partes o acesso e o acompanhamento das diligências e dos exames que realizar, com prévia comunicação, comprovada nos autos, com antecedência mínima de cinco dias.

Novidade trazida com o Novo CPC é a possibilidade das partes, de comum acordo, já escolherem o perito, indicando-o mediante requerimento. Este instituto é chamado de “perícia consensual”. Sem dúvida um avanço que vai impedir que as partes tenham de “aceitar” a nomeação de alguns, muitas vezes, absolutamente despreparados para o exame técnico.

Continua valendo a regra quanto à possibilidade do juiz dispensar a prova pericial quando as partes, na inicial e na contestação, apresentarem sobre as questões de fato pareceres técnicos ou documentos elucidativos que considerar suficientes.

O Novo CPC agora traz elementos que o laudo pericial deve conter, como a exposição do objeto da perícia, a análise técnica ou científica realizada pelo perito e a indicação do método utilizado, esclarecendo-o e demonstrando ser predominantemente aceito pelos especialistas da área do conhecimento da qual se originou. É regra também que o laudo pericial apresente a resposta conclusiva a todos os quesitos apresentados pelo juiz, pelas partes e pelo órgão do Ministério Público.

Ainda, no laudo, o perito deve apresentar sua fundamentação em linguagem simples e com coerência lógica, indicando como alcançou suas conclusões.

Por fim, destaque-se que pelo Novo CPC, o prazo para manifestação das partes e dos assistentes técnicos em relação ao laudo juntado pelo perito é de quinze dias, que aliás, trata-se de prazo unificado que passa a ser a regra na legislação projetada.

As duas faces do direito ao esquecimento na Internet

Recentemente, o Tribunal de Justiça da União Européia deu causa a um advogado Espanhol e determinou que o mesmo teria direito de ter seu nome removido do resultados do Google.

A decisão favorável na justiça Européia ascendeu uma discussão que põe em confronto privacidade e honra com liberdade de expressão e comunicação. O Tribunal determinou que o site retirasse dos resultados das buscas uma página de um jornal, onde havia um anúncio relativo a uma suposta dívida do Advogado. A vice-presidente da Comissão Europeia, Viviane

Reding, comentou a decisão como “uma vitória clara para a proteção de dados pessoais dos europeus”. No entanto, nada é pacífico. Duas correntes advogam em sentido contrário nesta temática.

A primeira corrente, defendida pelo Google e parte dos ativistas entende que tal medida é inconstitucional à medida em que viola a liberdade de expressão, imprensa e comunicação, estabelecendo-se a censura.

Para a primeira corrente “não se pode apagar a história” e se uma pessoa fez algo na vida que hoje a envergonha, tais resultados seriam mera conseqüência de seus atos, vida desregrada, dentre outras. O Google, em seus processos, ainda, alega que o buscador apenas “indexa” conteúdo relevante, sendo que notícias mais populares ou linkadas por grandes sites tendem a aparecer no topo dos resultados. Alega, por fim, que não pode ser responsabilizado ou condenado a remover resultados do buscador.

O provedor indica em suas defesas que o ofendido procure se entender diretamente com o site que publica a ofensa, pois removendo-se a ofensa, automaticamente a busca será alterada com o tempo.

Outra corrente, em sentido contrário, defendida também por ativistas do direito a privacidade, entende que não se trata de “apagar a história”, mas do direito ao esquecimento ou do direito de ser deixado em paz. Pessoas que foram condenadas pelo Judiciário e já pagaram sua pena, ou que deviam e pagaram as dividas, não poderiam, segundo esta corrente, serem “eternos” condenados ou “eternos” devedores no mundo virtual. Para tal corrente, a liberdade de expressão não pode violar direitos de personalidade, a privacidade ou colocar em risco a integridade física e psíquica de pessoas.

Agora vamos ao caso concreto. Uma advogado, responsabilizado por um dívida que nunca contratou e que é publicada na

Internet em um site de informativo. Não bastasse, o Google pega a informação e a coloca em topo no ranking quando se pesquisa pelo nome da pessoa, claramente sendo o "controlador da informação".

Até que ponto uma informação inverídica, associada aos dados pessoais de alguém, pode permanecer na rede, no maior buscador do mundo? Perceba. Não se trata de "apagar a história" ou "censura", mas de correção de um equívoco, abuso ou injustiça. Trata-se da remoção de uma informação falsa. Repise-se, o advogado nunca foi devedor.

Outros casos que merecem reflexão, por exemplo, relacionados a blogs com difamação e injuria criados para ofender alguém utilizando como palavras chaves o nome do ofendido. Em muitos casos, blogs insignificantes, sem relevância, que poucas pessoas acessariam diretamente, não fosse o Google, que pega o blog e o coloca em posição de destaque, quando se pesquisa pelo nome do ofendido.

Tomemos o exemplo de alguém que é processado e ao final absolvido, mas as notícias do processo permanecem nos primeiros resultados do buscador. A pessoa deveria conviver com isso para o resto de sua vida? Imaginemos agora que o Blog é anônimo, publicado em qualquer localidade do globo terrestre, sem que os serviços estejam sujeitos às ordens judiciais brasileiras. O que é mais fácil à vítima? Remover a postagem ofensiva no blog, mediante ordem judicial, ou remover a referência ao Google, que vem dando publicidade ao mesmo quando o nome da vítima é digitado? Se a notícia é da imprensa, veiculada por órgão jornalístico, não podendo ser removida na fonte, tal impossibilidade de remoção se estenderia ao buscador que insiste em classificar a notícia antiga em primeiro lugar quando se busca o nome de uma pessoa?

Não existe ponto pacífico. Cada caso é um caso e é preciso discernimento e proporcionalidade. Embora o caso espanhol tenha recebido destaque, temos casos mau digeridos no Brasil,

como o de uma atriz, onde “do nada” e após pressão midiática, misteriosamente o “ranking” com o links para as fotos da atriz foram alterados, foram limpos da Internet, especificamente, dos resultados de um buscador.

Outros casos podem ser citados, como por exemplo, o caso de uma mulher que, após ter feito fotos sensuais para uma revista, foi associada ao termo “acompanhante” pelo “pesquisas relacionadas” e “sugestões de busca” do buscador. Como? Não se sabe. O que se sabe é que a caixa preta dos algoritmos do buscador em algum momento, avaliando as informações sobre a mulher, a classificou de forma mais que errônea à condição de prostituta.

É utópico imaginar que buscadores só indexam conteúdo, mas na verdade, hoje, classificam ou rotulam pessoas. Em outro caso ainda, uma família cujo filho morreu de forma trágica, em um acidente que foi fotografado pelo titular de uma página sensacionalista anônima: Quando se busca pelo nome da família ou do filho falecido, o primeiro resultado é o site com fotos do jovem morto, ensangüentado. A família tem que aceitar e conviver com isso para sempre? Liberdade de expressão? Qual o interesse público nesta divulgação?

Explanadas as duas correntes, nossa opinião é pela flexibilizarão entre as duas óticas, pela proporcionalidade e pela análise de cada caso, com muita cautela. Dois direitos constitucionais estão em conflito. Não se pode admitir que um pedófilo condenado queira limpar notícias referentes aos crimes que praticou. Não se pode admitir que um político corrupto queira “ficar bem na foto” do ambiente de um buscador. Por outro lado, não nos parece aceitável que pessoas tenham que conviver com informações comprovadamente falsas a seu respeito amplamente rankeadas pelo buscador e associadas a seus dados pessoais, como nome, cpf, dentre outros dados, como nos exemplos acima citados.

Longe de ser a palavra final sobre o tema, o presente artigo

tem o papel de fomentar a discussão sobre o assunto, considerando que como explanado, nem tudo é "apagar o passado", censura ou violação à liberdade de expressão, mas grave violação a direitos de personalidade, honra, imagem e privacidade de pessoas, direitos estes, tal como a liberdade de expressão, também previstos na Constituição Federal. A discussão é necessária, pois o "direito ao esquecimento" pode ser erroneamente interpretado e ser encarado, sempre, como ato de censura, ou mesmo usado maliciosamente para apagar conteúdos legítimos da Internet. É preciso pensar fora dos condicionamentos de quem não analisa a questão em sua dupla face. Apresentadas as correntes divergentes, cabe ao cidadão avaliar e formar seu entendimento.

Decisão do TJ da União Européia: http://s.conjur.com.br/dl/tj-ue-google-direito-esquecimento.pdf

---

Responsabilidade dos provedores de hospedagem por invasão: Culpa do sistema ou do provedor?

Você mantém um site rodando sobre o motor wordpress, disponível via painel de controle em uma hospedagem qualquer. Estima-se que 19% dos sites rodem sobre WordPress. Seguiu todos os passos para o hardening, revisou http://codex.wordpress.org/pt-br:Blindando_o_WordPress e mesmo assim está encontrado problemas com injection, file include ou invasões.

Alterou a senha do blog, ftp e do banco de dados. Nada resolve. Alterou os prefixos das tabeas wp_, alterou as permissões, criou um novo usuário administrativo, removeu plugins, criou index.html em diretórios, ocultou a versão do seu CRM, tunou o .htaccess, instalou plugins de scannes de vulnerabilidades e nada…

Então, ao identificar o ip (no Bing, Ip:seu número de IP) para seu site descobre se tratar de um servidor com dezenas de sites. Um servidor compartilhado. Não há hardening de WordPress que resista a um servidor compartilhado comprometido.

Quais as medidas de segurança que o provedor está adotando para proteger seus arquivos? Em servidores compartilhados as permissões de alterações de arquivos pode ser fatal. E o pior, o provedor pode "abafar" sua vulnerabilidade, alegando que não encontrou problema algum. E o usuário, muitas vezes consumidor, se complica para provar pois não tem acesso à infra do provedor.

O grande problema é que diante de tais incidentes, o primeiro cenário é buscar entender o que aconteceu com o provedor de hospedagem. Lamentavelmente, muitos provedores irão sempre jogar a culpa no código do cliente, nunca no servidor. Em alguns casos, simplesmente dizem que nada aconteceu, mesmo você mostrando para o helpdesk registros na tabela wp_posts cheios caracteres "estranhos" e posts não criados pelo administrador.

Sob o prisma jurídico, não há duvida que o provedor pode ser responsável, sobretudo quando alega que o problema é no seu código. É possível provar com um pentest que não é o código o problema!

O provedor, diante de um incidente, deve restaurar backup anterior a invasão e imediatamente encaminhar os logs (access) e outras informações. O backup deve envolver o banco de dados

e é questionável a cobrança pela restauração de backups dos clientes.

Já se decidiu na justiça brasileira que a ausência de backup ou a corrupção do mesmo pelo cracker, pode ensejar responsabilização do provedor de hospedagem.

Mesmo o provedor tendo restabelecido o serviço, é direito do consumidor de serviços descobrir data e hora do acesso indevido, vulnerabilidade explorada e técnica utilizada. Se o provedor alega que se trata de um injection ou uma vulnerabilidade no seu código que permitiria a injeção de um shell, mas não existe nada nos logs, esta afirmação pode não corresponder à realidade, sobretudo se o incidente se repetir.

Cabe, neste caso, a atuação com uma perícia ou auditoria externa, para constatar efetivamente se a afirmação do fornecedor de hospedagem realmente procede. Com a perícia em informática, pode-se identificar, por exemplo, vulnerabilidade no servidor ou serviços desnecessários rodando, não iniciados pelo cliente, sendo o caso de responsabilização do provedor.

Em Minas Gerais, ao julgar o recurso de apelação 433.758-0 (2.0000.00.433758-0/000.), o então Tribunal de Alçada responsabilizou provedor de hospedagem em caso em que defacer invadiu site e anexou fotos pornográficas no site da vítima. Por outro lado, nos termos do inciso II, parágrafo 3o. do Art. 14 do Código de Defesa do Consumidor, o provedor poderá provar culpa exclusiva da vitima, que por exemplo, não protegia o arquivo wp-config.php, permitindo que qualquer um conhecesse a senha para acesso ao banco de dados, ou mesmo mantinha uma senha fraca para seus serviços.

Recentemente, em 2013, um provedor foi condenado por não garantir segurança ao cliente, permitindo a invasão (http://www.ebc.com.br/tecnologia/2013/08/microsoft-e-condenada-a-indenizar-consumidora-que-teve-perfil-invadido)

Outro julgado pode ser encontrado em

http://www.migalhas.com.br/arquivo_artigo/art20130828-11.pdf

A controvérsia é técnica e será decidida pela justiça. Vale quem produzir a melhor prova. Mais uma vez a perícia informática é fundamental, desta vez, para o prestador de serviços de hospedagem que pretenderá demonstrar que o problema não era com sua infra.

Seja como for, recomenda-se a ambas as partes o registro de todas as telas e detalhes da invasão, bem como das conversações (suporte, chamados, helpdesk, etc.) envolvendo o incidente. A coleta de evidências dever ser ágil sim, mas sempre preceder qualquer medida para "apagar" o exploit ou arquivos plantados pelo atacante no FTP, pois serão provas em juízo. O contrato deve ser revisto, sempre, pois ele limitará, no que não for nulo ou abusivo, os direitos e deveres entre as partes, diante de um incidente.

Recomenda-se, em caso de servidor aberto ou compartilhado, mediante um ajuste com o prestador de serviços, a utilização do OSSEC (http://www.ossec.net/), que permite a análise de logs rapidamente, permitindo ainda monitorar arquivos quando os mesmos são alterados, garantindo a possibilidade de uma resposta rápida a um incidente.

Para segurança em WordPress, por fim, recomendamos o ebook http://ithemes.com/wp-content/uploads/downloads/2013/12/WordPress-Security-ebook.pdf

---

Análise forense de redes

sociais e Facebook

Quanto tratamos de perícias em redes sociais, temos que fazer uma grande distinção. A primeira área é aquela que envolve coleta de grandes volumes de dados ou a utilização de data minning aplicado a computação forense. Esta área é embrionária e esbarra em questões de privacidade e desafios para a computação forense.

Nicole Beebe, uma pesquisadora da Universidade do Texas, tem um trabalho interessante sobre o tema. Uma outra área envolve a análise de uma máquina que realizou o acesso à redes sociais. A este padrão, já é possível aplicar muitos conceitos da Forense Convencional e as pesquisas já estão mais avançadas.

Para quem pretende pesquisar a área, alguns artigos são leitura obrigatória:

1. https://www.sba-research.org/wp-content/uploads/publications/socialForensics_preprint.pdf
2. http://www.fbiic.gov/public/2011/jul/facebook_forensics-finalized.pdf
3. Este mapa pode lhe auxiliar a simular um ambiente para realizar a Forense em Facebook http://www.marshall.edu/forensics/files/2012/09/Helenek-Kathy-Poster-4-12-12.pdf

Já existem softwares desenvolvidos para a Perícia Digital em Facebook, como o FFS A aplicação permite que o examinador faça um clone de um perfil, realizando um parsing dos dados para uma análise na estação forense.

Não resta dúvida que o Big Data vai mudar a forma de se coletar e analisar informações de incidentes. O mercado anseia por scripts, soluções ou mesmo um padrão de interconexão que atenda a demanda das autoridades e ao mesmo tempo preserve a privacidade dos cidadãos e estrangeiros, não esbarrando em

normas de proteção. Já existe um projeto do tradicional software forense Sleuth Kit para o Hadoop Framework, o que permitirá implantar soluções para processamento de grandes volumes de dados, mas muito precisa ser desenvolvido ainda neste setor.

Este ponto de equilíbrio é o desafio para os próximos tempos, considerando que as Redes Sociais são o "combustível do Big Data", riquíssimas em informações que podem ser transformadas em predição e conhecimento sobre crimes e incidentes, mas por outro laudo, não se pode coletar e analisar dados de todos, sob o pretexto de "combater o crime". Alguém já ouviu esta fala antes?

Uma abraço e até a próxima!

NOTAS

Um excelente parser para Facebook pode ser encontrado aqui

Aspectos jurídicos sobre o aplicativo Lulu: Quando uma hashtag viola sua personalidade

O aplicativo Lulu vem levantando polêmica no Brasil e já lidera downloads no Google Play e na Apple Store (http://idgnow.uol.com.br/mobilidade/2013/11/25/app-lulu-para-mulheres-avaliarem-homens-ja-lidera-downloads-no-brasil/)

Basicamente, uma ferramenta, disponível apenas para mulheres e que interage pelo Facebook, fazendo com que estas possam

avaliar homens da rede social, de forma anônima, por meio de #hashtags, podendo também dar uma nota para o homem.

Até ai tudo bem, o problema são as ofensas vindas em tais hashtags, sobretudo que possam agredir a honra e a privacidade de usuários. Acrescente-se a isso o anonimato proporcionado pela ferramenta, que obsta que o avaliado conheça os avaliadores.

Embora muitos juristas tenham comentado de uma suposta violação ao art. 43 do Código de Defesa do Consumidor (considerando que o Facebook exporta os dados pessoais ao aplicativo – mas não sabemos a profundidade), fato é que muitos dos usuários avaliados sequer sabiam da existência da aplicação. Logo, não restam dúvidas de que existe violação a privacidade, a imagem e a honra, direitos protegidos pelo inciso X, do art. 5º. da Constituição Federal.

Isto porque, quando supostas amigas anônimas comentam sobre um homem, por vezes revelam situações íntimas, ou mesmo ofendem sua honra objetiva, com comentários jocosos. Não bastasse, em nenhum momento os avaliados autorizaram que seus dados fossem inseridos na aplicação, nem que os mesmos fossem "ranqueados" ou avaliados na Internet, avaliação disponível a todos.

Diga-se, o direito a privacidade não envolve tão somente controlar as informações pessoais que são reveladas, mas também como as informações reveladas serão utilizadas por terceiros. Igualmente, a empresa ou sua filial no Brasil não podem exigir que avaliados baixem programas para se verem livres de avaliações.

Ao que parece a empresa disponibilizou um site em http://company.onlulu.com/deactivate onde permite que pessoas possam remover seus perfis da possibilidade de avaliações. Igualmente, disponibiliza um e-mail, privacy@onlulu.com, onde pessoas (homens) podem requerer a remoção.

Em que pese a diretora no Brasil afirmar que o aplicativo é legal (http://www.techtudo.com.br/noticias/noticia/2013/11/justica-brasileira-nao-garante-anonimato-do-app-lulu.html) fato é que ao usuário não cabe o ônus de notificar a empresa manifestando seu não interesse em ser avaliado, sendo que resta comprovada a violação a direitos de personalidade em caso de avaliação com termos ofensivos, sendo cabível ação reparatória, inclusive com pedidos judiciais de identificação dos responsáveis por comentários. Aliás, o uso indevido dos dados pelo Lulu, sem autorização do titular, já é violação.

Tanto é que em São Paulo já existe uma ação indenizatória em andamento, movida em face do Facebook (o que entendemos errônea pois o Facebook, em tese, não é responsável pelo aplicativo), e que teve sua liminar indeferida, mas que está em andamento (http://esaj.tjsp.jus.br/cpo/pg/show.do?processo.foro=16&processo.codigo=0G0002S3I0000) Na ação, a suposta vítima pede uma indenização de R$ 27.120,00, pois teria sido agredido em sua honra e imagem pelo uso da ferramenta Lulu.

Vamos aguardar para avaliar como o Judiciário irá se pronunciar em relação à questão.