“Vivemos o 5º poder, que está nas mãos de quem domina tecnologia e internet”

A sociedade brasileira avançou no uso de tecnologia nos últimos anos e grande parte das regras para estas novas relações foram criadas em âmbito privado, por contratos, termos de uso ou até mesmo mecanismos de auto-regulamentação. No entanto, chegamos a um patamar em que para dar o próximo passo evolutivo, para o crescimento sustentável do Brasil Digital, há necessidade de se preencher algumas lacunas jurídicas. Só o Legislativo tem alçada para tal.

Não sou a favor de que existam leis para Internet em si, mas a mesma já deixou de ser apenas mais um meio, uma mídia, e passou a ser o ambiente principal de relacionamento, realização de atividades, obrigações, responsabilidades e transações para muitos indivíduos e instituições. A interatividade, somada à infra-estrutura viabilizada pela banda larga, permite que o mundo virtual, na verdade, ocupe o lugar do mundo real. A tal ponto que a ONU elevou o direito de acesso à internet a uma garantia de direito digital do indivíduo. Sem isso, ele está “fora do mundo”, fica excluído e marginalizado, sem opção inclusive para se desenvolver.

Por isso, a tramitação mais rápida de projetos de lei como o PL 84/99, o Marco Civil da Internet, a nova Lei de Direitos Autorais, a regulamentação da atividade de Compra Coletiva, ou mesmo normas que permitam melhorar a segurança da informação no nível público, e combater crimes eletrônicos, terrorismo digital e guerra cibernética. Não pode levar mais de 10 anos para tramitar projetos de lei sobre o tema de Direito Digital. Além disso, o Legislativo precisa estar mais capacitado para enfrentar temas técnicos, o que exige, inclusive, uma redação mais aprimorada das leis.

Tem crescido os ataques a sites de Governo, principalmente porque os mesmos são extremamente vulneráveis, não foram criados dentro de uma estratégia de plano de contingência e continuidade, visto que no início eram meramente institucionais. Mas, evoluíram para se tornarem verdadeiros ambientes de governo eletrônico, prestando serviço essencial ao cidadão que não pode ficar indisponível, não pode sofrer interrupção, muito menos vazamento de dados.

Apesar de estar em vigor o Decreto 3505/2000, uma pesquisa feita pelo Tribunal de Contas da União em 2010 mostrou que a maioria das instituições públicas ainda não possui política de segurança da informação implementada, com campanha de conscientização realizada. Há a nítida impressão de que isso ainda não ocorreu, passados mais de 10 anos, visto que aumentar o nível de monitoramento nos ambientes da administração pública pode vir a revelar condutas indevidas do próprio gestor público, e que ficariam então mais expostas, além da dificuldade de dar continuidade neste tipo de tema que exige um trabalho permanente e não se encerra com um mandato.

Muitos países já têm discutido sobre qual o limite que distingue a prática de um Crime Eletrônico comum e quando o mesmo se torna um ato de Cyberterrorismo ou mesmo de Guerra Cibernética, visto que o ataque intencional a site de governo com objetivo de retirar do ar e furtar dados é considerado de altíssima gravidade. No Brasil foi criado um Núcleo de Defesa Cibernética, a cargo do Exército e do Ministério da Defesa, conforme portarias 666 e 667 de 2010, mas o trabalho ainda está no início, deveria

ser acelerado. Vivemos o 5º. poder, que está nas mãos de quem domina tecnologia e internet. O Governo Brasileiro tem que ter política para tratar risco digital especificamente. Hoje, cada Órgão trata do seu jeito.

No tocante ao aspecto de direito internacional digital, a Lei 10.744/2003, trata em seu artigo 2º de que é responsabilidade da União tratar sobre atentados terroristas e atos de guerra, e pela leitura seria possível enquadrar a conduta tanto no § 3º *"entende-se por atos de guerra qualquer guerra, invasão, atos inimigos estrangeiros, hostilidades com ou sem guerra declarada, guerra civil, rebelião, revolução, insurreição, lei marcial, poder militar ou usurpado ou tentativas para usurpação do poder*" como no § 4 º "*entende-se por ato terrorista qualquer ato de uma ou mais pessoas, sendo ou não agentes de um poder soberano, com fins políticos ou terroristas, seja a perda ou dano dele resultante acidental ou intencional*". O próprio Pentágono declarou que ataque cibernético será considerado ato de guerra.

O que pode ser feito, em caráter emergencial, para melhorar o nível de proteção do ente público e também dos dados dos cidadãos brasileiros, que devem ser cuidados pelo mesmo são: revisar nível de segurança da informação dos sites de governo, melhorando programação dos códigos fontes e criptografando bases de dados; implementar plano de contingência e continuidade e demais medidas para evitar interrupção; realizar monitoramento permanente do ambiente, podendo usar estratégia "*honey pot*" para pegar um ataque logo no início e identificar seu autor; criar policiamento online (não apenas a delegacia de crimes eletrônicos); aprovar leis que melhorem tipificação e guarda de provas, devem trazer os novos tipos de Crime Eletrônico, Cyberterrorismo e Guerra Cibernética, definir modelo de identidade digital obrigatório e prazo mínimo de guarda de dados de conexão e tráfego por provedores de internet, email, páginas de conteúdo, redes sociais; implementar campanha de conscientização de segurança da informação pública, voltada aos servidores e ao cidadão, orientando sobre proteção de senha, bloqueio de estação de trabalho, necessidade de desligar o equipamento quando não estiver sendo usado e de manter atualizados os softwares de antivírus. Inclusão digital com educação digital é fundamental para prevenção.

Date Created
11/09/2011