Por Patricia Peck Pinheiro (*)

Para começar o debate, uso dos mensageiros no ambiente corporativo exige uma norma específica e atualização da Política de Segurança da Informação (PSI)

Como as empresas devem lidar com o uso de aplicativos sociais e de comunicação como WhatsApp, SnapChat, Viber, Voxer, Facebook Messenger, Telegram e Chaton, e tantos outros que surgem a cada dia? Aceitar e permitir? Ou proibir? O que é melhor do ponto de vista técnico? E do ponto de vista jurídico?

Independente da escolha da empresa, os colaboradores estão usando. Então, de qualquer modo, este novo cenário exige regras claras! Isso tem provocado a necessidade de implementação de uma norma específica sobre o tema, bem como atualização da Política de Segurança da Informação (PSI), para que a diretriz não trate apenas da informação e dos dispositivos, mas também do ambiente de aplicativos e nuvem.

Do ponto de vista estratégico, visando mobilidade e competitividade internacional, a TI deve servir ao negócio, logo, a opção de permitir sob certas condições e com requisitos claros de conformidade legal e segurança da informação é o caminho mais sustentável.

A primeira coisa que deve ser feita é definir claramente o escopo desta norma sobre uso de aplicativos sociais como sendo, com referência no ITIL, um conjunto de código e instruções compiladas, executadas ou interpretadas por um Recurso de TIC, hospedadas em um dispositivo ou na nuvem, que é usada para troca rápida de mensagens, conteúdos e informações multimídia.

A partir do momento que a informação que circular no aplicativo for da empresa, a mesma pode determinar qual a regra aplicável.

Portanto, é fundamental haver uma orientação clara sobre questões como: procedimento de backup (para não perder a documentação da comunicação corporativa), nível de segurança aplicável conforme a classificação da informação (ex: se terá que usar codificação, criptografia ou se há restrição para uso deste canal devido ao grau de sigilo e confidencialidade), entre outros.

Uma das alternativas é prever que o uso destes recursos é uma prerrogativa relacionada a alçadas e poderes, ou a função e cargo, ou ainda que depende de uma autorização prévia acompanhada da justificativa do negócio. No entanto, em que pese o desejo de controlar a informação, ela circula entre chefes e subordinados, se o superior tem WhatsApp é muito provável que seu time acabe se comunicando com ele por este ambiente, a pedido dele mesmo, para facilitar a própria gestão.

A maioria dos aplicativos sociais está na nuvem, logo, a norma que trata do uso dos mesmos acaba por também tratar do uso da própria nuvem. Com o crescimento dos tablets pessoais em reuniões de trabalho, é emergencial determinar regras clara sobre a guarda ou transferência de informações através dos repositórios digitais tais como Google Drive, SkyDrive, Dropbox, iCloud, Box e SugarSync.

Para estes casos devemos aplicar a máxima “se não pode vencê-los, junte-se a eles”. Mas isso deve ser feito acompanhado de um trabalho de blindagem legal com documentação formal escrita e de campanha de conscientização de segurança, já que a decisão entre proteger ou tornar público está a cada dia mais na mão do usuário dos dados.

Por último, deve-se sempre reforçar o dever de cautela e sigilo profissional de todo e qualquer colaborador, inclusive dos terceirizados. Ademais, deve-se deixar claro que quando o conteúdo tiver algum tipo sigilo legal, seja ele bancário, fiscal, judicial ou de propriedade industrial ou

intelectual, deve-se buscar usar um canal mais seguro de comunicação, sempre!

A melhor regra é a que é implementável. Não importa onde está a pessoa, a informação, se no âmbito pessoal, profissional, dentro ou fora da empresa. Por isso, fazendo uma redação simples mas objetiva, consegue-se tratar o tema sem paralisar a operação ou gerar riscos desnecessários para o negócio.

Minha sugestão é atualizar o quanto antes a PSI pois o pior risco é justamente não ter regra definida ainda sobre o assunto. Algo como: “sempre ao compartilhar assuntos de trabalho, em qualquer local, dentro ou fora do ambiente de trabalho, a partir de qualquer tipo de canal, mídia, ferramenta ou tecnologia, o colaborador deve respeitar a ética, a legislação vigente no Brasil e cumprir com seu dever de sigilo profissional, aplicando a melhor técnica disponível na época para garantir a segurança da informação no nível exigido pela classificação da mesma”. E vamos focar no resultado, pois é para isso que usamos tecnologia, para servir ao negócio!

(*) **Patricia Peck Pinheiro** é advogada especialista em Direito Digital.

Fonte: Computerworld, em 03.03.2016.