ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

USO DE DISPOSITIVOS PESSOAIS NO AMBIENTE DE TRABALHO: A RELAÇÃO COLABORADOR E EMPRESA

Mauricio Sebastião de Barros[1]
Michael Cavalleri de Souza[2]

RESUMO

O crescente consumo de equipamentos como, *tablets*, *smartphones*, dentre outros equipamentos portáteis e de uso pessoal, deixa de ser uma exclusividade do uso particular e passa também a fazer parte de nossa vida profissional. Empresas começar a permitir o uso destes equipamentos para o desenvolvimento das atividades do seu funcionário (BYOD – *bring your own device*, ou traga o seu próprio dispositvo) visando uma maior produtividade e redução de custos. Porém, existem algumas contrapartidas desta prática, que podem trazer sérias consequências legais e de segurança da informação, que venham a prejudicar o empregador. Neste contexto a empresa precisa adotar algumas medidas para evitar processos trabalhistas e outros problemas relacionados a segurança da informação.

Palavras-chave: BYOD; CLT; Mobilidade; Segurança; Software.

INTRODUÇÃO

O uso de equipamentos tecnológicos começa cada vez mais cedo e já transformou itens que foram concebidos como ferramentas de trabalho, pertencentes a altos cargos dentro das empresas, em "brinquedos de criança". Dispositivos que antes pareciam insubstituíveis em suas tarefas já deram lugar para outros de menor tamanho, muitas vezes com maior capacidade de processamento e capazes de executar as mesmas tarefas. Esse é um caso muito familiar quando pensamos nos computadores pessoais (*desktops*), onde precisamos de um monitor, gabinete, teclado e mouse, sem contar a quantidade enorme de cabos e conexões. Tudo isso, aos poucos, perdeu mercado para os notebooks, logo em seguida para *smartphones* e *tablets*, os quais já conseguem executar diversas funções que antes fazíamos somente pelo computador.

No ano de 2013, em pesquisa[i] realizada pelo IDC, a venda de *tablets* ultrapassou pela primeira vez a venda de *desktops*. No período de outubro a dezembro de 2013 foram vendidos um total de 1,4 milhão de *desktops*, contra um total de 2,2 milhões de *notebooks* e 3 milhões de *tablets*. Embora as recentes pesquisas projetem uma queda na venda de *tablets*, de aproximadamente 6% em 2017

[1] Professor, Mestre em Educação, Perito Forense Computacional. mauriciobarros@acad.ftec.com.br
[2] Analista de Infraestrutura de TI graduado pela Faculdade SENAC no curso de Redes de Computadores. michael.souza@procempa.com.br

comparado a 2016, a diferença ainda é bastante grande[ii]. Nas últimas projeções realizadas pela IDC há uma estimativa de encerrar o ano de 2017 com uma venda de 1,6 milhão de *desktops* contra 2,9 milhões de *notebooks*[iii], 3,75 milhões de tablets e 49 milhões de *smartphones*[iv]. Ainda, neste contexto e segundo a consultoria Gartner Group

> As estratégias de BYOD são a mudança mais radical para a economia e a cultura da computação cliente nos negócios em décadas, disse David Willis, vice-presidente e analista destacado do Gartner. Os benefícios do BYOD incluem criar novas oportunidades de força de trabalho móvel, aumentar a satisfação dos funcionários e reduzir ou evitar custos (GARTNER, 2013).

Este cenário cria uma nova cultura nas empresas, permitindo aos colaboradores utilizarem seus dispositivos no ambiente de trabalho, pois o uso de tecnologia já é algo consolidado e é tarefa difícil encontrar pessoas que não tenham ao menos dois destes equipamentos (*tablet*, *smartphone* ou *notebook*). Esta tendência conhecida como BYOD (traga seu próprio dispositivo, do inglês *bring your own device*) traz muitos benefícios para as corporações, mas em contrapartida exige uma série de cuidados e medidas que serão discutidas ao longo deste artigo.

1 CUSTOS E PRODUTIVIDADE

À primeira vista, uma das principais vantagens para uma empresa parece ser a redução de custos com aquisição e manutenção de equipamentos. De fato, isto é uma realidade, pois utilizando uma política de BYOD estes custos de aquisição e manutenção, em princípio, ficariam a cargo do funcionário e proprietário do equipamento, porém é necessário que estas situações sejam bem especificadas no momento do contrato de trabalho, para evitar futuros problemas relacionados a aquisição ou manutenção do *tablet*, *notebook* ou *smartphone*. Em contrapartida, a implantação de uma política de BYOD pode acarretar em um custo considerável nos departamentos de T.I, especialmente no que se refere a segurança da rede e das informações, pois existirá um ambiente extremamente híbrido com diversos equipamentos de muitos fabricantes e que podem ter problemas de segurança, seja por falta de atualizações ou *softwares* instalados.

O aumento de produtividade é um item que muitas vezes gera controvérsias. De um lado a defesa de que o empregado trabalha melhor com seu equipamento, simplesmente pelo fato de já estar adaptado ao uso e também por poder utilizar a sua marca de preferência. Do outro lado, há quem diga que há uma diminuição de produtividade, pois existem muitos itens para distrair a atenção do colaborador para questões pessoais. O fato é que em pesquisa encomendada pela empresa Dell e realizada pelo IBOPE CONECTA, 54% das empresas permitem o uso de computadores pessoais dos

seus funcionários, dentre estas, 44% afirmam que há um aumento de produtividade. Das que não admitem a prática a justificativa refere-se em sua maioria a questões de segurança dos dados. A pesquisa IBOPE CONECTA, encomendada pela Dell, foi realizada com mais de 400 entrevistados, todos eles responsáveis pela decisão de compras referentes a T.I em empresas com até 99 funcionários em todo o Brasil, com respostas a questionários *on-line*, entre 1 e 9 de fevereiro de 2017[v].

2 DEFININDO OS LIMITES

2.1 Comportamento e Propriedade

É de extrema importância que sejam definidos de forma clara os limites para o uso de um equipamento pessoal por parte do funcionário dentro da empresa, a fim de evitar problemas jurídicos futuramente. Portanto as obrigações de cada parte, empregador e empregado, devem ser incluídas no contrato de trabalho. Serão apresentados agora alguns dos principais pontos a serem analisados.

A primeira questão é relacionada a jornada de trabalho, que deve estar esclarecida de forma que a utilização no equipamento pessoal fora das dependências da corporação, não caracterize jornada extra, ou até mesmo que a disponibilidade do seu telefone móvel não seja considerada um sobreaviso. Havendo necessidade de sobreaviso ou horas extras deve ser fixado os períodos que o colaborador precisa estar disponível.

Outro item que deve ser levado em conta é a propriedade do bem que será utilizado no trabalho. A recomendação seria incluir na documentação de admissão um termo afirmando que o proprietário do equipamento é o próprio colaborador, evitando desta forma que seja utilizado um dispositivo de terceiros que não possui nenhuma relação com a empresa. O risco de um terceiro envolvido seria a intenção de prejudicar a empresa alegando, por exemplo, o uso indevido por parte da mesma do seu bem.

O comportamento do funcionário com o seu equipamento nas dependências da empresa deve estar esclarecido de forma que indique o que e como pode ser utilizado. As políticas de BYOD devem contemplar normas de utilização de aplicativos e recursos seja do *notebook*, *smartphone* ou *tablet*. Itens como o acesso a aplicativos de troca de mensagens, sites, relacionados ou não a atividade exercida, uso da câmera fotográfica ou vídeo, documentos que podem ou não ser levados para fora da companhia, tudo isto deve ser de total ciência do empregado e preferencialmente documentado e assinado por ambas as partes.

2.2 Uso de Softwares

Outro aspecto que deve ser levado em consideração ao elaborar uma política de BYOD é no que tange aos *softwares* que serão utilizados pelo colaborador para exercer sua função. Atualmente, há uma

preocupação muito grande no âmbito corporativo no que se diz respeito ao correto licenciamento de *software* e deve ser levado em conta a possibilidade de o colaborador possuir programas instalados sem as respectivas licenças, caracterizando pirataria. Portanto, se faz necessário a definição de todos os programas que são exigidos para o colaborador exercer suas atividades, de forma que ele seja responsabilizado por qualquer outro *software* não autorizado que esteja instalado no equipamento, sendo inclusive recomendado a proibição de uso dos mesmos nas dependências da empresa. A própria situação do licenciamento de *softwares* deve ser discutida, pois em muitos casos ao implementar o BYOD a empresa pode acordar que a compra das licenças e/ou das CDU´s (seção de direito de uso) deve ficar a cargo do colaborador, isto evitaria mais um custo, porém é preciso ter um certo cuidado, e garantir de alguma forma, seja através de alguma inspeção tecnológica ou humana que as aplicações utilizadas não estejam sem o devido licenciamento.

Empresas de desenvolvimento de *software*, que normalmente são as que mais aderem ao BYOD, especialmente aquelas que aceitam trabalhos de *freelancers* (profissionais liberais que prestam serviços sob demanda), precisam estar atentos também a Lei do Software de Computador.

> Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.[vi]

Interpretando este trecho da Lei 9.609/98, assumimos que programas de computador que forem desenvolvidos no equipamento do colaborador e não possuírem relação com seu contrato de trabalho e nem informações relacionadas a empresa pertencerão ao próprio desenvolvedor permitindo que neste caso sejam exercidas outras atividades de programação no seu equipamento que não tenha relação com a empresa contratante, mas é importante que esteja claro para o colaborador que o desenvolvimento do *software* sem relação, não pode ser realizado dentro da empresa a qual ele é contratado, de forma que utilize seus recursos ou as horas que constam em seu contrato de trabalho. Sendo assim, a empresa também não poderá alegar que, de alguma, forma o *software* desenvolvido sem o vínculo formal, pertença a mesma.

3 SEGURANÇA DA INFORMAÇÃO

Um dos principais motivos da rejeição de práticas de BYOD por determinadas empresas estão relacionados à segurança da informação. Em empresas com gestão mais conservadora é incompreensível

que um funcionário vá trabalhar com o seu próprio equipamento tendo acesso a partir dele às informações sigilosas da empresa, obviamente isto não quer dizer que uma empresa que não adota o BYOD não corre riscos de vazamento de informação, por outros meios ou formas.

Em suma, tem-se a situação de adotar práticas e conscientizar os funcionários sobre os riscos e punições cabíveis no caso de vazamento de dados sigilosos, ou apostar em serviços integrados a infraestrutura de T.I que possam até mesmo impedir que documentos sigilosos sejam visualizados fora das dependências da empresa, protegendo assim a propriedade intelectual.

O uso de serviços para gerenciar dispositivos móveis também pode ser uma solução para mitigar os riscos, estes *softwares* de *Mobile Device Management* (MDM), permitem gerenciamento remoto dos dispositivos, permitindo adicionar e remover aplicativos, também gerenciar e filtrar o conteúdo acessado, dentre outras funções que irão depender do fornecedor. Pode-se, por exemplo, restringir estas regras e monitorar o dispositivo apenas quando ele estiver dentro da empresa, pois é importante lembrar que o colaborador está utilizando o seu próprio bem e, portanto, pode-se incorrer na situação de invadir a privacidade do usuário.

Outra opção, de cunho técnico se dá a partir do uso de ferramentas de VPN (*Virtual Private Network*), muito utilizadas para acesso remoto (acessar um dispositivo a partir de outro), onde pode ser construído um ambiente de forma que o usuário precise se conectar a esta VPN para ter acesso a informações mesmo estando nas dependências da empresa. Esta solução, além contribuir na proteção da propriedade intelectual também é muito útil contra-ataques cibernéticos, pois com isso a conexão será estabelecida de forma privada entre o usuário e a empresa, sem ser intermediada por terceiros que possam estar se aproveitando de alguma fragilidade no equipamento usado.

Percebe-se que tudo se resume a estratégias de T.I e uma boa política de segurança que deve exigir do usuário, ao menos, medidas que sejam consideradas simples, como a configuração de uma senha e uso de antivírus (caso este não seja fornecido pela própria empresa), para que em caso de invasão do mesmo seja enquadrado como um crime informático e possa ser usado a favor da empresa, visto que a Lei 12.737/12 (Lei Carolina Dieckmann) tem como base que para que se caracterize como crime é preciso que haja "violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita", item que causa certa controvérsia sobre o que exatamente é um mecanismo de segurança, mas precisa ser respeitado facilitando a defesa no caso de algum incidente.

CONCLUSÃO

Não é tarefa simples possuir um gerenciamento centralizado dos dispositivos quando não há um padrão nas plataformas de trabalho, afinal o equipamento do funcionário não vai ser aquilo que a empresa dispõe, terá prioridade o dispositivo da marca de sua preferência, transformando o ambiente tecnológico em um ambiente híbrido, que dependendo da situação não vai conseguir estabelecer nem um padrão de uso de softwares iguais para todos. O fato é que se exige um grande esforço de equipes de gestão, recursos humanos, jurídico e T.I para que o BYOD não se torne um pesadelo para estas áreas.

A segurança da informação tem um papel extremamente importante neste cenário, pois terá de implementar mecanismos de defesa e proteção que acompanhem esta diversidade de cenários, assim como campanhas de conscientização e treinamentos relacionados a segurança. As equipes de gestão, recursos humanos e departamento jurídico terão que, em conjunto, elaborar as políticas de utilização, termos de compromisso e conexos, até mesmo possíveis alterações nos contratos de trabalho para dirimir ao máximo as possibilidades de ações trabalhistas que poderão ocorrer, caso algum colaborador se sinta lesado ou em desacordo com a CLT, seja por ter que pagar pelo conserto do seu equipamento ou até mesmo alegações de trabalho além da carga horária que consta em contrato.

As empresas que implantam estas políticas sem estarem devidamente preparadas correm sérios riscos de ataques ou vazamento de informações sigilosas que podem comprometer a integridade e confidencialidade dos dados, portanto deve ser muito discutido sobre qual será o retorno das práticas de BYOD e se estas serão vantajosas, pois embora exista uma redução de custos com equipamentos, pode ser necessário um alto investimento em T.I para suportar um ambiente dito multiplataforma.

REFERÊNCIAS

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 20 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 18 out. 2017.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 3 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 18 out. 2017.

GARTNER. **Half of Employers will Require Employees to Supply Their Own Device for Work Purposes.** Stamford. Mai. 2013. Disponível em: <https://www.gartner.com/newsroom/id/2466615>. Acesso em: 30 out. 2017.

GLOBO, G1. **Tablet ultrapassa vendas de desktop e notebook pela primeira vez no Brasil.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/03/tablet-ultrapassa-vendas-de-desktop-e-notebook-e-pela-1-vez-no-brasil.html> Acesso em: 18 out. 2017.

UOL, Convergência Digital. **BYOD aumenta produtividade em micro e pequenas empresas**. Disponível em < http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&_infoid =45328&sid=147 > Acesso em 18 out. 2017.

LATIN, IDC. **Mercado brasileiro de tablets cai 8% em vendas no segundo trimestre, segundo IDC Brasil**. Disponível em <http://br.idclatin.com/releases/news.aspx?id=2215> Acesso em: 18 out. 2017.

LATIN, IDC. **Mercado brasileiro de PCs cresce 5% em vendas no segundo trimestre, revela estudo da IDC Brasil**. Disponível em <http://br.idclatin.com/releases/news.aspx?id=2211> Acesso em: 18 out. 2017.

LATIN, IDC. **Mercado brasileiro de celulares volta a apresentar números positivos no segundo trimestre, revela IDC Brasil**. Disponível em <http://br.idclatin.com/releases/news.aspx?id=2213> Acesso em: 18 out. 2017.

[i] Divulgada em http://g1.globo.com/tecnologia/noticia/2014/03/tablet-ultrapassa-vendas-de-desktop-e-notebook-e-pela-1-vez-no-brasil.html.
[ii] Divulgado em http://br.idclatin.com/releases/news.aspx?id=2215.
[iii] Divulgado em http://br.idclatin.com/releases/news.aspx?id=2211.
[iv] Divulgado em http://br.idclatin.com/releases/news.aspx?id=2213.
[v] Disponível em http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=45328&sid=147.
[vi] BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998, disponível em http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm.