Parecer sobre liberação de uso do WhatsApp Web nas estações de trabalho do TJPE

Este parecer é relativo aos questionamentos e solicitações repassados para SETIC sobre o uso da ferramenta WhatsApp Web (https://web.whatsapp.com/) nas estações de trabalho do TJPE. Para facilitar o entendimento esta introdução contém uma breve descrição do serviço Whats App Web em seu estado atual e nas seções seguintes encontram-se as avaliações pertinentes. Pode se considerar o conteúdo deste parecer extensível aos demais aplicativos de troca de mensagens que possuem módulo web.

O WhatsApp Web é uma forma de replicar o funcionamento do aplicativo WhatsApp de celular para a tela de um computador por meio de um navegador de Internet. Portanto, para o funcionamento da solução é necessário que o celular e o computador estejam conectados à Internet simultaneamente. Ao entrar no WhatsApp Web o usuário precisa sincronizá-lo com o WhatsApp do celular utilizando um código fornecido por meio de QR-Code. Ao finalizar os procedimentos de entrada as telas do WhatsApp nos dois dispositivos passam funcionar de forma sincronizada. O usuário poderá usar qualquer um dos dois para enviar e receber textos, imagens, áudios, vídeos, documentos PDF e outros formatos, etc.

Para uma melhor compreensão este parecer está organizado em duas avaliações: normativa e técnica-operacional. A seção normativa está dividida em três subseções: Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), Resolução Nº 349 de 2013, Instrução de Serviço nº 02, de 25 de maio de 2017 e Termos de Uso do WhatsApp.

1. Avaliação Normativa

1.1 Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD)

As características de funcionamento do WhatsApp Web tornam a sua utilização na rede de computadores do TJPE mais um ponto de vulnerabilidade em relação ao vazamento de dados pessoais (DPs). Como será melhor explicado ao longo deste parecer, controles tecnológicos para monitorar, registrar e auditar situações de possível vazamento de DPs são praticamente inviáveis de serem implementados sobre a ferramenta. Esta condição torna precário o atendimento à LGPD nas situações de uso do WhatsApp Web. A LGPD possui dispositivos muito claros sobre a responsabilização nos casos de incidentes envolvendo DPs, como por exemplo o Art. 38 e o seu Parágrafo Único:

> "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

1.2 Resolução Nº 349 de 2013 (Política de Segurança do TJPE)

Parecer sobre liberação de uso do WhatsApp Web nas estações de trabalho do TJPE

Quanto as normas internas do TJPE, é imprescindível considerar a Resolução Nº 349 de 2013 (Política de Segurança da Informação - PSI) que traz alguns dispositivos pertinentes à esta avaliação. A PSI do TJPE é clara em seu Art. 19:

> "Art. 19. O acesso aos ambientes físicos e recursos lógicos de TIC devem ser controlados e restritos às pessoas autorizadas pela SETIC, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível".

Sobre o Art. 19, a SETIC não dispõe de recursos para verificar se o WhatsApp Web está sendo utilizado para necessidades funcionais, bem como não conta com tecnologia que limite o uso apenas para atividades de trabalho. Mesmo que tivéssemos tais recursos, por se tratar de uma solução que sincroniza um dispositivo particular com um computador do TJPE, provavelmente interviríamos no funcionamento do celular privado do usuário e teríamos acesso as mensagens particulares trocadas durante o monitoramento. O parágrafo único do Art. 20 e corrobora e detalha o disposto no artigo anterior sobre o uso estritamente funcional da infraestrutura de TIC do TJPE:

> "Art. 20 Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente judiciário ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo do TJPE.
>
> Parágrafo único. Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais, dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional."

Um outro artigo impactado é o Art. 27, que trata dos conteúdos acessados e armazenados pela rede e nos computadores do TJPE:

> "Art. 27 É vedado aos agentes do judiciário acessar ou armazenar, a partir de dispositivos ou recursos de TIC do TJPE ou pessoais em seu proveito, conteúdo que caracterize atividade ilegal, que não condiga com as atividades a serem cumpridas ou que possa causar prejuízo ao bom funcionamento da infraestrutura de TIC do TJPE, a exemplo, mas não se limitando, de:
>
> - Arquivos de mídia, softwares e demais materiais protegidos por propriedade intelectual sem a devida licença ou autorização;
> - Material pornográfico ou que possua intenção de satisfazer a lascívia;
> - Conteúdo ou ambientes que ponham em risco a incolumidade da segurança dos dispositivos e ativos de TIC do TJPE, tais quais sítios de internet suspeitos de conterem scripts maliciosos ou consistirem em prática de fraude, instalação de softwares maliciosos, desconhecidos ou não homologados pelo NSI, vinculado à SETIC;
> - Conteúdos ou serviços de TIC de ordem pessoal dos agentes judiciários ou de terceiros, tais quais, repositórios de arquivos na internet, serviço de e-mail, mídias sociais não liberadas, rádios online e recursos de entretenimento em geral;
> - Qualquer outro que constitua crime, ato ilícito ou contrarie a Ordem Pública, os bons costumes, as normas em vigor do TJPE ou seus objetivos e função social."

Embora seja de muita utilidade prática, o WhatsApp é um aplicativo utilizado também para disseminar vírus, executar fraudes, repassar pornografia, etc. Pelas razões expostas anteriormente, na

prática, a SETIC não conseguiria viabilizar o controle para impedir ou verificar se tais conteúdos estão trafegando pela nossa rede ou sendo armazenado em nossos computadores utilizando o WhatsApp Web como meio. O Art. 31, transcrito abaixo, também sofreria com os mesmos impactos já citados, pois, mesmo que o WhatsApp fosse homologado pela SETIC, não teríamos como implementar controles:

> "Art. 31 As trocas de mensagens eletrônicas institucionais somente devem ser realizadas para fins laborais, utilizando sistemas fornecidos ou homologados pela SETIC, mantendo vocabulário formal e condizente com a reputação esperada, evitando subjetividades e intimidades em seus conteúdos."

O uso do serviço em questão pode ser considerado uma forma de acesso remoto intermediado por um serviço da empresa WhatsApp do grupo Facebook, embora com características limitadas. O Art. 33 dispõe sobre a responsabilidade da SETIC em implementar controles de segurança para acesso remoto, neste caso de implementação inviável:

> "Art. 33 O acesso remoto aos recursos de TIC do TJPE deve ser previamente homologado pela SETIC, que indicará as configurações adequadas e controles de segurança necessários para que haja o uso seguro pelos agentes judiciários."

O Art. 35 e seus §1º e §2º fala da permissão do porte e uso de dispositivos pessoais de TIC nas dependências do TJPE. Entretanto, não fala de qualquer possibilidade de integração deste dispositivo à infraestrutura de TIC. Os dispositivos também dispõem que não haja restrição profissional para o uso, não traga prejuízos ao TJPE, que a responsabilidade do conteúdo é do funcionário e que o uso não atrapalhe a produtividade no exercício das funções:

> "Art. 35. É permitido o uso de dispositivos pessoais de TIC pelos agentes judiciários nos ambientes do TJPE, desde que não haja restrição conforme seu perfil profissional e que não traga prejuízos para o TJPE.
>
> § 1º Os agentes judiciários serão integralmente responsáveis pelos conteúdo armazenados em seus dispositivos pessoais e pelos atos através deles praticados, sem ressalvas ou exceções.
>
> § 2º Os agentes judiciários poderão utilizar seus dispositivos pessoais de TIC durante o expediente profissional, isto é, desde que não atrapalhe a própria concentração ou dos demais a seu redor nas atividades que devem desempenhar, não prejudique o atendimento ao público ou atrase as tarefas que lhe cabem, não violem a Estrutura Normativa de Segurança da Informação ou gerem riscos ao TJPE, sob pena de perderem o benefício e sofrerem outras sanções disciplinares, mediante competente Processo Administrativo."

1.3. Instrução de Serviço nº 02, de 25 de maio de 2017 (Norma de Acesso à Internet)

Cabe destacar o Art. 11 da Norma de Acesso à Internet, pois este, assim como alguns dispositivos da PSI, dispõe sobre a responsabilidade da SETIC de manter o controle de acesso aos serviços de Internet e critérios para autorizar ou não estes acessos:

> "Art. 11 Caberá à SETIC o controle de acesso aos sítios ou quaisquer serviços de Internet por critérios de identificação de vulnerabilidades e códigos maliciosos, justificativa de utilização para fins funcionais, viabilidade técnica e interesse da Instituição, sem prejuízo de normas internas e legislações vigentes."

O Art. 20 é ainda mais específico sobre o modelo adotado para o controle de acesso aos serviços de Internet e sobre a possibilidade do TJPE proibir o acesso aos sites que não atendam às necessidades funcionais:

> "Art. 20 No segmento de rede interno, o acesso padrão à Internet será realizado por meio do estabelecimento do mecanismo de lista negra mantida pela SETIC.
>
> § 2º Será de direito do TJPE proibir, a qualquer tempo, o acesso a qualquer página da Internet que não subsidie as atividades funcionais."

1.4. Termos de Uso do WhatsApp

O Termo de Uso do WhatsApp, disponibilizado como "Informação Legal do WhatsApp", é bastante explícito no que diz respeito ao acesso às mensagens trocadas via aplicativo. Segundo a empresa, por conta dos protocolos criptográficos utilizados, apenas as duas pontas envolvidas na troca de mensagem têm acesso ao conteúdo. Entretanto, discussões sobre mau uso do protocolo pela empresa levantam possibilidades de acesso pela empresa em situações não tão frequentes, como troca de aparelho, falta de conexão de uma das pontas no momento da conversa e troca de chip. Ver mais detalhes em:

- https://olhardigital.com.br/fique_seguro/noticia/brecha-na-criptografia-do-whatsapp-permite-que-mensagens-sejam-interceptadas/65316

Para este parecer assumimos as situações regulares de uso confirmadas pela empresa WhatsApp.

A empresa não ter acesso ao conteúdo da conversa é um ponto positivo, pois, teoricamente, assuntos institucionais do TJPE não seriam acessados por ela. Isto protegeria o TJPE inclusive em países onde eles mantêm infraestrutura e que as legislações permitem uso e compartilhamento de informações pelas mais diversas razões. O ponto negativo é que o próprio TJPE não teria acesso ao registro dessas conversas, que estariam disponíveis apenas nos celulares dos interlocutores. Desta forma a instituição fica desprovida de evidências, históricos e eventuais estatísticas sobre o conteúdo de conversas institucionais.

> "Suas mensagens. Não guardamos suas mensagens durante a prestação dos Serviços. Depois que suas mensagens (incluindo conversas, fotos, vídeos, mensagens de voz e compartilhamento de informações de localização) são entregues, elas são excluídas de nossos servidores. Suas mensagens ficam armazenadas em seu próprio dispositivo. Se uma mensagem não puder ser entregue imediatamente (por exemplo, se você estiver desconectado), podemos mantê-la em nossos servidores por até 30 (trinta) dias enquanto tentamos entregá-la. Se a mensagem não puder ser entregue nesses 30 (trinta) dias, nós a excluiremos. Para melhorar o desempenho e entregar mensagens com mídia de maneira mais eficaz, por exemplo, quando há o compartilhamento

> de fotos ou vídeos populares, podemos guardar esse conteúdo em nossos servidores por mais tempo. Nós também oferecemos a criptografia de ponta-a-ponta em nossos Serviços, esta por sua vez ativada por padrão quando você e as pessoas com quem troca mensagens, estiverem utilizando uma versão de nosso aplicativo que tenha sido lançada após o dia 2 de abril de 2016. Criptografia de ponta-a-ponta significa que suas mensagens estão criptografadas para que nós ou terceiros não as possam ler."

O Termo de Uso do WhatsApp também chama atenção ao uso do WhatsApp integrado aos serviços de terceiros. Neste caso, coerentemente, a empresa orienta que o usuário observe os termos de uso destes serviços, por exemplo, na hora compartilhar algo por meio deles. O TJPE não exerce controle tecnológico sobre estas inúmeras possibilidades de integração, ficando ao encargo do usuário ler o termo adicional e decidir sobre compartilhar informações, sejam elas de propriedade do TJPE ou não:

> "Serviços de terceiros. Quando você usa serviços de terceiros que são integrados aos nossos Serviços, eles podem receber dados sobre seus compartilhamentos. Por exemplo, ao usar um serviço de backup de dados integrado aos nossos Serviços (como o iCloud ou o Google Drive), eles receberão informações sobre o que é compartilhado por você. Ao interagir com um serviço de terceiros conectado com nossos Serviços, você pode acabar fornecendo dados diretamente a eles. Observe que ao usar serviços de terceiros, os termos e as políticas de privacidade aplicáveis serão os elaborados para tais serviços."

A empresa WhatsApp faz parte do grupo de empresas da Facebook. O Termo de Uso do WhatsApp afirma que dados publicados em uma das duas ferramentas não serão automaticamente publicados na outra. Tal posicionamento é importante, pois evita que informações institucionais trocadas em conversas possam "vazar" no Facebook:

> "Nós nos juntamos ao Facebook em 2014. O WhatsApp agora, faz parte da família de empresas do Facebook. Nossa Política de Privacidade explica como estamos trabalhando juntos para melhorar nossos serviços e ofertas, como por exemplo, combater spam entre os aplicativos, dar sugestões sobre o produto, mostrar anúncios relevantes entre outros no Facebook. Nada que você compartilhe no WhatsApp, incluindo suas mensagens, fotos e dados da conta será compartilhado no Facebook ou em qualquer outro aplicativo de nossa família, para que outros vejam do mesmo modo que, nada do que você poste nestes aplicativos será compartilhado no WhatsApp para que outros vejam."

O item que trata da possibilidade do WhatsApp trafegar, processar ou armazenar informações em qualquer país merece atenção. Na prática os usuários do WhatsApp não possuem qualquer controle sobre a localização geográfica das instalações da empresa. Portanto, como é o mais natural, a legislação dos países por onde as informações possam passar pode se opor e preponderar sobre qualquer item do Termo de Uso do Serviço. Também é importante observar o disposto na Lei Geral de Proteção de Dados (LGPD) sobre transferência internacional de dados, pois os dados pessoais, mesmo encriptados, não estão necessariamente anonimizados. Portanto, neste caso, a LGPD seria aplicável.

> "O WhatsApp se preocupa com a sua privacidade. A Política de Privacidade do WhatsApp descreve as nossas práticas relativas à informação (e também mensagens), inclusive os tipos de informação que recebemos e coletamos e como usamos e divulgamos tais informações. Você concorda com as nossas práticas

> relativas a dados, inclusive com a coleta, o uso, o processamento e o compartilhamento de suas informações conforme descrito em nossa Política de Privacidade, assim como a transferência e processamento de suas informações nos Estados Unidos e em outros países onde temos ou usamos instalações, prestadores de serviço ou parceiros, independentemente do país onde nossos Serviços são usados por você. Você reconhece que as leis, regulamentos e normas do país no qual as suas informações são armazenadas ou processadas podem ser diferentes do que rege em seu próprio país."

A empresa WhatsApp afirma que a utilização da tecnologia de cookies serve para proporcionar uma melhor experiência para o usuário. Na prática isto se dá pelo registro e acompanhamento das suas ações no uso da ferramenta. Portanto, é importante que o usuário esteja ciente que todas as suas ações no uso, por exemplo, do WhatsApp Web estão sendo registradas e um perfil comportamental está sendo traçado com base nestes registros. Se o uso do WhatsApp é institucionalizado, o TJPE deve ter ciência e concordar com esta prática por parte da empresa.

> "Nós usamos os cookies para entender, proteger, operar e disponibilizar nossos Serviços. Por exemplo, usamos cookies para: (1) fornecer o WhatsApp para computador e web e outros serviços que são baseados na web, melhorar sua experiência, entender como nossos serviços estão sendo usados e para também customizar nossos serviços; (2) para entender quais de nossas páginas do FAQ são as mais populares e para mostrar somente conteúdo relevante aos nossos Serviços; (3)para lembrar suas escolhas, tais como configurações de idioma e também para customizar nossos Serviços para você; e (4) para classificar nossas páginas do FAQ em nosso site baseando-se em popularidade, entender usuários de celular versus usuários de desktop que usam nossos Serviços baseados em web ou para entender a eficácia de algumas de nossas páginas."

2. Avaliação Técnica-operacional

Como já foi afirmado, o WhatsApp Web é um "espelho" do aplicativo WhatasApp instalado no celular do usuário. A versão Web não oferece qualquer forma de administração corporativa da aplicação e possui menos opções de configuração do que a versão de aplicativo celular.

O conteúdo multimídia (vídeo, áudio, documentos, etc.) recebido em uma conversa pelo WhatsApp Web é automaticamente baixado para o computador (também é permitido salvar em um arquivo em disco). Não é fornecida uma forma de evitar o download. Nas opções disponíveis esta decisão fica a critério do usuário. Isto pode ter uma implicação direta sobre o desempenho da rede interna e do link de Internet do TJPE. Levando em conta que o envio de vídeos, imagens e áudio são comuns no aplicativo, poderíamos sofrer com baixo desempenho, indisponibilidades e aumento de despesas com link e infraestrutura para comportar tráfego que não é de interesse institucional.

Sem os controles necessários, qualquer conteúdo pode ser baixado a qualquer tempo para o computador. Não existe uma forma fácil e automática de evitar que conteúdo impróprio e nocivo ao ambiente de TIC seja baixado via WhatsApp Web. Resta apenas confiar que o agente de antivírus instalado no computador atue quando necessário. Como o WhatsApp é uma forma muito rápida de propagar mensagens em escala global, dificilmente o agente de antivírus estará preparado para, por exemplo, ameaças criadas recentemente. Portanto, trata-se de potencializar o uso da Internet como ponto de entrada de ameaças no ambiente interno do TJPE. Enquanto contratamos ferramentas (CheckPoint, IWSVA, IMSVA, OfficeScan, etc.) para evitar a entrada de conteúdo nocivo e impróprio por outros meios,

com o WhatsApp Web abre-se um caminho para que estas ferramentas sejam desconsideradas como controles de entrada de conteúdo.

O Termo de Uso do serviço do WhatsApp Web não oferece qualquer garantia quanto a disponibilidade. A ausência de garantias de disponibilidade é natural em serviços que não exigem pagamento em dinheiro. No Brasil, bem como em outros países, o WhatsApp já sofreu indisponibilidade total e parcial, tanto por ordem judicial como por problemas da empresa em suportar a sua própria demanda. Portanto, é preciso estar ciente que não há como cobrar garantias neste sentido. Se o uso do serviço se tornar institucionalizado, então será preciso avaliar impactos de eventuais indisponibilidades na prestação dos serviços.

Ver exemplos indisponibilidade do WhatsApp em:

- http://jconline.ne10.uol.com.br/canal/economia/nacional/noticia/2017/05/04/whatsapp-pede-desculpas-por-instabilidade-mundial--281602.php
- http://www1.folha.uol.com.br/mercado/2016/05/1766886-whatsapp-sai-do-ar-por-72-horas-no-brasil-por-determinacao-da-justica.shtml
- http://exame.abril.com.br/tecnologia/entenda-por-que-juiz-do-piaui-mandou-tirar-o-whatsapp-do-ar/

3. Conclusões

Em termos práticos é preciso ponderar entre os benefícios do uso do WhatsApp Web nas estações do TJPE e os riscos e impactos negativos do uso da ferramenta. A tabela a seguir resume os principais aspectos identificados:

Vantagem direta	Riscos e impactos
• Usuários não precisam do celular para troca de mensagens institucionais via WhatsApp; • O WhatsApp afirma que não tem acesso ao conteúdo das mensagens trocadas por usuários.	• Inconformidade com o normativo atual que define o uso de recursos de TIC apenas para fins funcionais; • O TJPE não tem acesso as eventuais mensagens institucionais trocadas entre usuários; • Não é viável fazer *backup* de conversas; • Impacto sobre a produtividade devido ao uso para finalidades de cunho particular; • Nenhuma garantia de disponibilidade do serviço do WhatsApp; • Maior exposição aos riscos de ameaças eletrônicas (vírus, fraudes, crimes, etc.); • Possibilidade de uso dos computadores do TJPE para tráfego e armazenamento de conteúdo ilegal e impróprio (protegidos por direitos autorais, pornografia, conteúdo ilegal, etc.); • Aumento de tráfego na rede interna e link de Internet, que pode ocasionar pior desempenho, indisponibilidade e aumento de custos com infraestrutura; • Impossibilidade/inviabilidade de implementação de controles por parte da SETIC;

	• Integração com serviços de terceiros (exceto Facebook) pode oferecer risco de vazamento ou uso indesejado de informações institucionais; • Estar submetido às legislações de países cujo o Brasil não tem qualquer acordo internacional para acesso e uso de informações; • Ter o comportamento dos funcionários no uso do WhatsApp registrado e analisado pela empresa.

Levando em conta que não é viável restringir ou controlar o uso do WhatsApp apenas para fins funcionais dos funcionários e ainda todos os riscos e impactos, a situação de liberação se encaixaria em uma concessão. O Art. 22 da Resolução Nº 349 de 2013 prevê que esta concessão seja formalmente divulgada pelo TJPE:

> Art. 22. A utilização de qualquer recurso da infraestrutura de tecnologia deve ser restrita à execução de atividades inerentes e previamente previstas para o desempenho de suas funções ou concessões formalmente divulgadas pelo TJPE, seguindo a política de conceder apenas as permissões indispensáveis para realização das suas atividades.

Apenas como um exemplo de aplicação desta solução de formalização dentro do TJPE, o próprio WhatsApp foi explicitamente liberado para a rede sem fios (*wi-fi*) de visitantes por meio da Instrução de Serviço nº 02, de 25 de maio de 2017 da Presidência do TJPE.

Finalmente, o NSI recomenda a prospecção de plataformas de troca de mensagens que possam ser utilizadas como solução interna de forma ampla por todos os servidores do TJPE, com garantias de segurança e maior conformidade com as normas internas do TJPE. Essa prospecção está fora do escopo deste parecer, mas o NSI pode ser acionado a qualquer tempo pela área responsável pela atividade para apoiar nos itens relacionados à segurança. Caso a gestão da SETIC não entenda que a prospecção seja interessante, o NSI sugere que sejam considerados na decisão os pontos levantados neste parecer.

Recife - 14/08/2020

Poder Judiciário de Pernambuco
Núcleo de Gestão de Segurança da Informação – NGSI
Assessoria de Governança de Tecnologia da Informação e Comunicação – AGTIC
Secretaria de Tecnologia da Informação e Comunicação – SETIC