Parecer sobre pedidos de utilização de plataformas de videoconferência na rede do TJPE

Com intuito de responder sobre eventuais solicitações de instalação ou uso do Zoom, Skype, Google Meet e softwares congêneres por meio dos dispositivos e rede do parque tecnológico do TJPE seguem os esclarecimentos.

Os referidos softwares são disponibilizados como serviço de comunicação instantânea, mensagens de texto, conferência em áudio e videoconferência. Em relação plataforma Zoom, Skype e Google Meet, todas tem sede nos Estados Unidos; país designado nos termos de uso para resolução de eventuais conflitos jurídicos.

Apesar da possibilidade de baixar gratuitamente os softwares, sua utilização implica na aceitação dos termos de uso das respectivas desenvolvedoras, que coletam informações dos utilizadores e realizam o processamento dos dados obtidos para viabilizar um modelo de negócio rentável para os respectivos proprietários dos serviços, o que vai de encontro a Política de Segurança da Informação do TJPE (Resolução 349, de 04 de Março de 2013 – da Corte Especial), uma vez que todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente do judiciário ou das quais tiver acesso no exercício de suas atividades são de propriedade e/ou direito de uso exclusivo do TJPE (Art. 23), não possuindo o TJPE contrato ou convênio firmado com as empresas para sessão dos dados.

Considerando os termos de uso das plataformas, convém destacar alguns pontos relevantes em relação aos impactos de segurança da informação:

Skype

A Skype coleta, armazena e usa todas as informações de comunicação, como, por exemplo, mas não se restringindo a: dados de cadastro, endereçamento, localização geográfica, comunicações por chat, correio de voz, transmissão de vídeo, dados de tráfego, resultados de pesquisas, contatos, localização de redes WiFi, dispositivos de redes WiFi, dados da operadora de telefonia móvel, informações sobre dispositivo móvel, como modelo, número de série, nome do fabricante, etc.

Os servidores da nuvem Skype estão nos EUA e podem ser realocados para qualquer outra posição geográfica de acordo com as necessidades da empresa. Todas as comunicações são intermediadas por esta nuvem de servidores.

A Skype prevê que qualquer informação que esteja sob seu poder será:

- Fornecida nos casos de obrigatoriedade legal para autoridades jurídicas, policiais ou governamentais (atualmente informações armazenadas nos EUA podem ser solicitadas legalmente por órgãos do Executivo, sem participação do Judiciário dos EUA, por meio *de National Security Letters*, com base no *Patriot Act*).
- Fornecida às empresas, operadores, parceiros de prestação do serviço e/ou agentes do grupo Skype.

Parecer sobre pedidos de utilização de plataformas de videoconferência na rede do TJPE

Google Meet

Termos de Uso

Conforme descrito nos termos de serviço,

> "Se você é um usuário comercial ou uma organização, então, na medida permitida por lei: você indenizará o Google e os diretores, executivos, funcionários e prestadores de serviço dele por quaisquer ações judiciais de terceiros (incluindo ações de órgãos do governo) decorrentes ou relacionadas ao uso ilegal dos serviços, a violações destes termos ou dos termos adicionais específicos do serviço. Essa indenização cobre qualquer responsabilidade ou despesa decorrente de ações judiciais, perdas, danos, julgamentos, multas, custos de litígios e honorários advocatícios; o Google não será responsável pelo seguinte: Perda de lucros, receitas, oportunidades de negócios, clientela ou economias previstas; Perda indireta ou emergente; Danos punitivos.
>
> As leis da Califórnia vão reger todas as disputas que surgirem com relação a qualquer um destes termos, dos termos adicionais específicos do serviço ou qualquer serviço relacionado, mesmo se houver conflito nas regras das leis. Essas disputas serão resolvidas exclusivamente nos tribunais federais ou estaduais do condado de Santa Clara, Califórnia, EUA, e você e o Google concordam com a jurisdição pessoal nesses tribunais.

Política de Privacidade

Conforme descrito na política de privacidade,

> Recolhemos informações para prestar um melhor serviço a todos os nossos utilizadores, desde perceber parâmetros básicos, como o idioma que fala, até dados mais complexos, como os anúncios que considera mais úteis, as pessoas mais importantes para si online ou os vídeos do YouTube que lhe podem interessar. As informações recolhidas pela Google, e a forma como são utilizadas, dependem de como utiliza os nossos serviços e como gere os seus controlos de privacidade.
>
> Quando não tem sessão iniciada numa Conta Google, armazenamos as informações recolhidas com identificadores únicos associados ao navegador, à aplicação ou ao dispositivo que está a utilizar.
>
> Também recolhemos o conteúdo que cria, carrega ou recebe de outras pessoas quando utiliza os nossos serviços. Este conteúdo inclui, por exemplo, e-mails que escreve e recebe, as fotos e os vídeos que guarda, os documentos e as folhas de cálculo que cria e os comentários que faz em vídeos do YouTube.
>
> Recolhemos informações sobre as aplicações, os navegadores e os dispositivos que utiliza para aceder aos serviços Google,

As informações recolhidas incluem os identificadores únicos, as definições e o tipo de navegador, as definições e o tipo de dispositivo, o sistema operativo e as informações da rede móvel, incluindo o nome e o número de telefone do operador, bem como o número da versão da aplicação. Também são recolhidas informações sobre a interação das aplicações, navegadores e dispositivos com os nossos serviços, incluindo o endereço IP, os relatórios de falhas, a atividade do sistema e a data, a hora e o URL referenciador do seu pedido.

Se utilizar os nossos serviços para fazer e receber chamadas ou enviar e receber mensagens, podemos recolher informações de registo telefónico, como o seu número de telefone, o número do autor da chamada, o número do destinatário, os números de encaminhamento, a hora e a data das chamadas e das mensagens, a duração das chamadas, as informações de encaminhamento e os tipos de chamada.

Recolhemos informações sobre a sua localização quando utiliza os nossos serviços, o que nos ajuda a fornecer funcionalidades como o trajeto de carro para a sua escapadela de fim de semana ou o horário de filmes em exibição perto de si.

A sua localização pode ser determinada com graus variáveis de precisão por:

- GPS
- Endereço IP
- Dados de sensores do seu dispositivo
- Informações sobre itens próximos do seu dispositivo, como pontos de acesso Wi-Fi, torres de redes móveis e dispositivos compatíveis com Bluetooth

Zoom

De acordo com a desenvolvedora, ao utilizar a solução o usuário concorda que confiará suas informações às políticas de tratamento de dados utilizadas, que destacam o seguinte:

- Inserção de marca d'água inaudível no streaming de áudio para identificar de forma única o usuário do serviço.
- Inserção de marca d'água sobreposta às imagens, contendo fragmentos do e-mail de seus utilizadores.
- Gravações das reuniões e arquivos transferidos são preservados em nuvem. (Podem ser fornecidas nos casos de obrigatoriedade legal para autoridades jurídicas, policiais ou governamentais. Atualmente informações armazenadas nos EUA podem ser solicitadas legalmente por órgãos do Executivo, sem participação do Judiciário dos EUA, por meio do *National Security Letters,* com *base no Patriot Act*).

Considerações sobre os termos e o modelo de prestação do serviço em face da dos normativos internos do TJPE

Os pontos acima ferem diretamente a RESOLUÇÃO Nº 349, de 04 de março de 2013 (Política de Segurança da Informação do Tribunal de Justiça de Pernambuco) que define em seu Art. 20º:

> Art. 20 º. 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.
>
> 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.

O Art 26º, especificamente, proíbe a gravação e divulgação de vídeo, imagem ou áudio sem autorização formal da instituição. Mesmo que este software viesse a ser liberado para uso, o conteúdo registrado por meio dele não estaria mais sob o controle do TJPE, mas sim das empresas *Microsoft (Skype)* e *Zoom Video Communications (Zoom).*

> Art. 26. Não é permitido aos agentes judiciários tirarem fotos, capturarem imagens, som ou vídeo do ambiente compreendido no perímetro físico sob gerenciamento do TJPE ou divulgar esses materiais sem uma autorização prévia da instituição.

Os Art 6º e Art. 7º abaixo atribuem aos agentes do Judiciário Pernambuco a responsabilidade por zelar por qualquer informação gerada, armazenada ou manuseada na execução das suas atividades. A utilização dessas plataformas por agentes do Judiciário implica em não conformidade com estes artigos:

> Art. 6 º Para os efeitos desta Política entende-se por classes de agentes do Judiciário: magistrados, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, voluntários e terceirizados que possuam um vínculo formal com o TJPE.
>
> Art. 7 º Cabe aos agentes do Judiciário: - Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não

> tenham nível de autorização suficiente; - Não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, por qualquer meio, informações sobre ativos ou de procedimentos do TJPE, exceto quando houver autorização prévia e formal por superior hierárquico ou de acordo com a legislação vigente para tanto; - Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle do Tribunal sem autorização formal; - Proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizados;

Não se limitando ao fato ser inviável gerenciar e auditar o uso dessas plataformas, a impossibilidade de monitoramento deste serviço também é algo crítico. As condições expostas acima vão de encontro a RESOLUÇÃO Nº 349:

> § 1º O TJPE também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação, podendo investigar fatos que comprometam seus ativos.
>
> Art. 20 º. ... 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.
>
> Art. 25. O TJPE, por meio da SETIC, monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo, o e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento.
>
> § 1º O TJPE também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação, podendo investigar fatos que comprometam seus ativos.
>
> 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: - 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;
>
> 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.

Como a utilização de serviços supostamente gratuitos de armazenamento na nuvem não se dá por um relacionamento institucional entre a empresa fornecedora e o TJPE, ficando este relacionamento restrito entre a pessoa física, o usuário, e o fornecedor, não há sequer possibilidade de incluir nesta relação a exigência exposta no Art. 36:

> Art. 36. Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC do TJPE ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por Termos de Confidencialidade e cláusulas contratuais que tratem especificamente da Segurança da Informação.

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:

> “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:

> “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.”

Avaliação Técnica-operacional

Uma vez que estas plataformas possuem mecanismos próprios de estabelecimento, manutenção, controle de banda, encriptação e demais funcionalidades referentes a conexão de dados para prestação do serviço, recursos como o download automático, inserção de *tags* passíveis de identificação do usuário, gravação da sessão etc. ficam impossibilitados de serem geridos e monitorados pela SETIC, colocando em risco a segurança da informação, da rede e dos sistemas do TJPE.

No que se refere ao uso de link de internet, considerando que o parque do TJPE possui mais de 10 mil computadores sob sua gestão, a adoção em massa de soluções de streaming de áudio e vídeo impacta diretamente no consumo de link de internet, sendo inviável, na conjuntura atual, garantir disponibilidade para todos os usuários.

Quanto ao suporte técnico, uma vez que os softwares em questão não passaram por um processo de homologação que analisa além dos aspectos de atendimento aos requisitos de segurança da informação, os aspectos de capacidade operacional para prestação do suporte técnico especializado dispensado a todos os sistemas que a SETIC mantém em funcionamento; tanto para seus usuários internos, quanto para o público externo que faz uso dos serviços publicados na internet.

Ademais, uma vez que não há contrato ou convênio firmado entre o TJPE e os proprietários das plataformas de serviços em questão, não há garantia de atendimento aos requisitos de segurança da informação (disponibilidade, integridade e confidencialidade) por parte das desenvolvedoras. Desta forma, o TJPE não pode exigir o cumprimento de quaisquer acordos de nível de serviço com nenhuma das empresas, nem requerer judicialmente reparos a quaisquer danos causados em virtude do mal funcionamento ou indisponibilidade das plataformas. Finalmente, eventuais conflitos jurídicos precisariam ser resolvidos nos locais designados pelos termos de uso das plataformas, nos Estados Unidos.

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

As características de funcionamento destas plataformas tornam a utilização na rede de computadores do TJPE mais um ponto de vulnerabilidade em relação ao vazamento de dados pessoais (DPs). Como explicado na seção anterior deste documento, 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 das plataformas supracitadas. 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."

Conclusão

O Núcleo de Gestão de Segurança da Informação recomenda que a prospecção de plataformas de videoconferência e comunicação instantânea considere, em todos os casos, a possibilidade de atendimento pleno a legislação de proteção de dados, normas e regulamentações de órgãos de controle, bem como o estabelecimento de controles que possibilitem a inspeção do tráfego, controle de banda e gestão dos recursos relacionados à segurança da informação. Desta forma, não existe a possibilidade de liberação deste tipo serviço para uso institucional. A recomendação do NGSI é que seja utilizada a plataforma de vídeo conferência Cisco Webex Meeting, já homologada para uso no TJPE;

Recife - 27/10/2021
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