REVISTA Mundi
Engenharia, Tecnologia e Gestão
INSTITUTO FEDERAL Paraná

SEGURANÇA TECNOLÓGICA NOS ATENDIMENTOS PSICOLÓGICOS A DISTÂNCIA

TECHNOLOGICAL SECURITY IN REMOTE PSYCHOLOGICAL CARE

Eloana Carine Pontes Fialho[1]
Isabela de Sá Leal[2]
Alison Antony Ribeiro[3]
Monia Karine Azevedo[4]

Resumo: A internet e o aumento da demanda por atendimento em psicologia resultaram no crescente contingente de estudos empíricos sobre eficácia e aspectos éticos dos atendimentos psicológicos pela internet. Este artigo busca apurar, de um ponto de vista tecnológico, a segurança e confidencialidade desses atendimentos, especificamente os que ocorrem por videochamadas, com foco na segurança dos dados necessária para a garantia da confidencialidade entre o psicólogo e os sujeitos por ele atendidos. Através de estudo teórico qualitativo de artigos acadêmicos e resoluções do Conselho Federal de Psicologia levantou-se o histórico das regulamentações e aplicações da psicoterapia remota. Ademais, discorreu-se os principais riscos na internet (*malwares*) e ferramentas para lidar com eles (*antivírus*, *antispyware* e *VPN*). Os resultados evidenciaram problemas relacionados à segurança no atendimento *on-line* e concluiu-se que é fundamental que a formação acadêmica das novas gerações de psicólogos contemplem o uso adequado das tecnologias de informação e comunicação.

Palavras-chave: Antivírus; Confidencialidade na internet; *Malwares*; Atendimentos psicológicos pela internet; Videochamada.

Abstract: The popularization of the internet and the increased demand for psychological care resulted in a growing contingent of empirical studies on the effectiveness and ethical aspects of psychological treatment through the internet. This essay seeks to investigate, from a technological point of view, the security and confidentiality of these services. Specifically the ones that occur through video-calls, with focus on the data security necessary to guarantee confidentiality between the psychologist and the subjects he/she serves. Through the qualitative theoretical study of academic articles and resolutions of the Federal Council of Psychology, the history of the regulations and applications of remote psychotherapy was raised. Moreover, its main risks on the Internet (malwares); tools to deal with them (antivirus, antispyware and VPN). The results showed problems related to security in online care and it was concluded that it is essential that the academic training of new generations of psychologists contemplate the appropriate use of information and communication technologies.

Keywords: Antivirus; Confidentiality on the internet; Malware; Psychological care through the internet; Video call.

[1] Técnica em Informática, IFPR, eloana.pontes@gmail.com
[2]Técnica em Informática, IFPR, isabelaleal713@gmail.com
[3]Mestre em Tecnologias Computacionais para o Agronegócio, UTFPR, alison.ribeiro@ifpr.edu.br
[4]Mestre em Psicologia, UEM, monia.azevedo@ifpr.edu.br

1. INTRODUÇÃO

Segundo Donnamaria (2013) psicólogos por todo o mundo buscam adaptar seus serviços de forma a atender a população e, por isso, o uso da internet representa grande possibilidade de ampliação na disponibilização de serviços. Apesar da pertinência dos atendimentos psicológicos através de ferramentas digitais, Siegmund et al. (2015) chamam a atenção para o fato de que a comunidade científica brasileira não possui muita pesquisa nessa área — tanto para as intervenções (seus métodos síncronos e assíncronos) quanto para a regulamentação destas (resoluções do Conselho Federal de Psicologia).

Diante desse contexto, esta pesquisa objetivou apurar a segurança dos atendimentos psicológicos pela internet — cujo uso, segundo Donnamaria (2013), só tende a crescer — especialmente no que diz respeito à segurança dos dados dos envolvidos e à confidencialidade durante encontros síncronos por meio de videochamadas.

A segurança dos dados é um problema que afeta todos os usuários, devido aos ciberataques através de *malwares* com o propósito de coletar informações pessoais (VIANNA, 2000). Esta questão, contudo, carrega um fator adicional ao se pensar no atendimento psicológico. Isto porque, segundo o código de ética profissional do psicólogo em seu Art. 9°: “É dever do psicólogo respeitar o sigilo profissional a fim de proteger, por meio da confidencialidade, a intimidade das pessoas, grupos ou organizações, a que tenha acesso no exercício profissional” (CONSELHO FEDERAL DE PSICOLOGIA, 2005, p.13). A confidencialidade também é, segundo Ormart (2013), essencial para criar um ambiente confortável para que todas as partes possam falar abertamente.

Para Anton (2013), a falta de proteção e de garantia da confiabilidade na internet formam o grande empecilho desta modalidade de atendimento psicológico. Isto posto, o presente artigo pretende dar luz às implicações, histórico e riscos dos atendimentos psicológicos mediados pela internet a partir de investigação teórica qualitativa sobre o assunto.

Foram utilizados artigos das bases de dados Academia.edu, SciELO e Google Acadêmico, a partir de buscas com os termos chave: “Psicoterapia pela

internet"; "Segurança de dados na internet"; "*Malwares*" e "Riscos à videochamadas". Sucederam-se, também, consultas às informações do Conselho Federal de Psicologia (CFP), órgão responsável pela regulamentação do exercício profissional do psicólogo.

2. ATENDIMENTOS PSICOLÓGICOS ATRAVÉS DA INTERNET

Os atendimentos psicoterápicos remotos, de acordo com Scharff (2012, apud PIETA e GOMES, 2014), acontecem em inúmeros países por telefone desde meados do século passado. O uso da internet na área da psicologia, no entanto, recebeu desconfianças em seu surgimento pelo receio de que dificultaria a formação de vínculo entre psicólogo e sujeito atendido.

Apesar dessa descrença inicial, com o decorrer dos anos a popularização da internet congregada ao aumento da demanda pela psicoterapia resultou no crescente contingente de estudos empíricos sobre eficácia, efetividade e aspectos éticos em diversos países, que em sua maioria tiveram resultados positivos ao atendimento remoto (PIETA & GOMES, 2014).

Dentre os argumentos de tais resultados favoráveis, Anton (2013) aponta a diminuição no custo de trabalho ao remover a necessidade de transporte tanto do psicólogo quanto do sujeito atendido. Ademais, Pachuk e Zadunaisky (2010, apud DONNAMARIA, 2013) sinalizam o anonimato propiciado em determinadas modalidades de atendimento *on-line*, que pode fazer com que o atendido sinta-se mais à vontade para discutir determinados temas. Outro ponto é trazido por Pieta e Gomes (2014), que argumentam que pessoas com questões mais específicas (tais como fobia social, agorafobia e problemas de imagem corporal), podem se sentir mais inclinadas a buscar atendimento *on-line*.

Em contrapartida, Tantam (2006, apud DONNAMARIA, 2013) ressalta a dificuldade na expressão do afeto entre psicólogo e sujeito atendido, mas este ponto é contraditório, já que Pieta e Gomes (2014) defendem que a relação terapêutica estabelecida não difere tanto em encontros presenciais ou pela internet. Também Pieta e Gomes (2014) destacam o risco de depender de

eletrônicos em situações de atendimento emergencial, uma vez que a possibilidade de assistência é limitada pela distância física.

Apesar de tais levantamentos, Donnamaria (2013) aponta que o Brasil ainda carece de literatura e pesquisa nessa área, mas reconhece o potencial terapêutico dos atendimentos psicológicos pela internet no país. Siegmund et al (2015) sublinham os esforços de psicólogos e do CFP em emparelhar as políticas de atendimento remoto às de países pioneiros como o Reino Unido, Canadá e Nova Zelândia.

2.1 Regulamentação dos atendimentos psicológicos ao longo dos anos pela internet

De acordo com Siegmund et al. (2015), no Brasil, a primeira regulamentação para atendimentos psicológicos através da internet foi no ano de 2000. Trata-se da Resolução nº 003/2000 do Conselho Federal de Psicologia[5]. A partir desta resolução passou a ser aceita a prestação de serviços psicológicos mediados por computadores, tais como orientação psicológica e afetivo-sexual, desde que pontuais e informativos, orientação profissional, orientação de aprendizagem e psicologia escolar, orientação ergonômica, consultorias a empresas, reabilitação cognitiva, ideomotora e comunicativa (Resolução 003/20000, Conselho Federal de Psicologia [CFP], 2000). Ademais, delimitou que a psicoterapia, especificamente, fosse aplicada com exclusiva finalidade de pesquisa. Pouco tempo depois — com o objetivo de validar, acompanhar e fiscalizar os sites utilizados — foi criada a Comissão Nacional de Credenciamento e Fiscalização dos Serviços de Psicologia pela Internet (DONNAMARIA, 2013).

A resolução de 2000 foi substituída pela N° 012/2005, que manteve a distinção entre a psicoterapia e as demais práticas profissionais. Também especificou como se daria a informação e comunicação com o Conselho

[5] A resolução CFP Nº 03/2000, foi a primeira resolução do CFP a regulamentar a prática de atendimento psicológico on-line. A mesma encontra-se disponível no endereço eletrônico https://www.crprs.org.br/upload/legislacao/legislacao40.pdf

Regional de Psicologia, assim como atualizou procedimentos de diretrizes para os sites. (SIEGMUND et al. 2015).

A partir de 2005, com a nova resolução, o CFP deveria conceder credenciais de autenticação eletrônica para que os atendimentos pudessem ocorrer. Outrossim, o Art. 3° chama a atenção para o fato de que, devido à natureza experimental dos atendimentos psicoterapêuticos mediados por Tecnologias da Informação e Comunicação (TICs), os psicólogos não poderiam cobrar por seus serviços. Aos demais serviços psicológicos, desde que não psicoterápicos, foi autorizada a cobrança de honorários (Resolução 012/2005, Conselho Federal de Psicologia [CFP], 2005).

Em 2012 entrou em vigor a Resolução CFP n.º 011/2012 que, segundo Siegmund et al. (2015), permitiu, entre outros, orientações psicológicas *on-line,* limitadas a 20 encontros, ou atendimento eventual destas em situações que o cliente se encontrasse impedido de comparecer presencialmente. Esta resolução exige que “em quaisquer modalidades destes serviços a(o) psicóloga(o) estará obrigada(o) a especificar quais são os recursos tecnológicos utilizados para garantir o sigilo das informações e esclarecer o cliente sobre isso” (Resolução 011/2012, Conselho Federal de Psicologia [CFP], 2012).

Ademais, a partir de 2012 o CFP passou a considerar os serviços psicológicos realizados por meios tecnológicos de comunicação tanto síncronos quanto assíncronos. De acordo com Siegmund et al (2015) os meios síncronos são aqueles em que a interação psicólogo-atendido acontece no mesmo espaço de tempo — exemplos incluem chamadas de voz e videochamadas. Já nos meios assíncronos não há a exigência de resposta imediata — como por mensagens de texto ou e-mails.

Segundo o *site* do Conselho Federal de Psicologia, em 2018 a demanda da categoria somada à popularização dos avanços tecnológicos levou à criação da resolução CFP n° 11/2018. Devido a ela o número de encontros não é mais limitado e foi removida a exclusividade experimental dos atendimentos psicoterapêuticos. Para que os atendimentos pela internet possam ocorrer os psicólogos devem estar devidamente cadastrados no Conselho Regional de Psicologia e a tecnologia escolhida deve ser aprovada pelo Sistema de Avaliação

de Testes Psicológicos (Resolução 011/2018, Conselho Federal de Psicologia [CFP], 2018).

Mesmo com maior liberdade no uso das TICs, ainda existem casos em que os atendimentos *on-line* não são autorizados. Segundo o Art. 6° da Resolução 011/2018: “O atendimento de pessoas e grupos em situação de urgência e emergência [...] é inadequado” e o Art. 8° veda o atendimento a quem passou por “violação de direitos ou de violência por meios de tecnologia e informação”.

A Resolução n° 4, de 26 de Março de 2020 é a mais recente tratando dos serviços psicológicos prestados por meio de TICs. Ela considera a declaração de pandemia de COVID-19 realizada pela Organização Mundial de Saúde - OMS em 11 de março de 2020 (UNA-SUS, 2020).

Para Viana (2020), além da maioria dos atendimentos que já ocorriam previamente terem passado a ser a distância em respeito ao isolamento social, também a demanda cresceu devido ao aumento significativo nas questões de saúde mental da população brasileira. Segundo o autor, dados apontam que com o isolamento social a qualidade do sono decaiu e houve um relativo aumento do estresse familiar. Ademais, é citada a questão financeira, várias famílias perderam suas fontes de renda diante o contexto de pandemia, que proporcionou o agravamento ou desenvolvimento de inúmeros problemas como fobias, insegurança e pânico.

Isto posto, a principal mudança da Resolução nº 4 de 2020 é a autorização da prestação de serviços psicológicos mesmo que o parecer de autorização do profissional ainda não tenha sido emitido pelo Conselho Regional de Psicologia (os profissionais, contudo, continuam com a obrigatoriedade de realizar o cadastro no *e-Psi*[6] — plataforma que lista os profissionais autorizados a prestarem serviços psicológicos *on-line*. Outra novidade é a autorização do atendimento de pessoas e grupos em situação de urgência e emergência, assim como de grupos em situação de violação de direitos ou de violência pelos meios de tecnologia e informação. Estas mudanças são válidas durante o período de

[6] Cadastro e-Psi. Disponível em: <https://e-psi.cfp.org.br/>. Acesso em 17 abr. 2021.

pandemia causada pelo coronavírus SARS-CoV-2 (Resolução 04/2020 & 11/2018, Conselho Federal de Psicologia [CFP], 2018 & 2020).

Como pode ser observado pelo panorama histórico supratranscrito, em apenas duas décadas os atendimentos *on-line* ganharam grande espaço no Brasil. Cabe refletir, no entanto, sobre a confidencialidade dos dados dos usuários dos atendimentos pela internet.

2.2. Segurança dos dados na internet e videochamadas

O Art. 7° da Lei Federal do Brasil Nº 12.965, assegura a proteção dos dados do usuário na internet. Entretanto, segundo Basílio (2003) a lei não é devidamente seguida pois há a ocorrência de crimes através de *malwares* que colocam a privacidade de usuários na internet em risco.

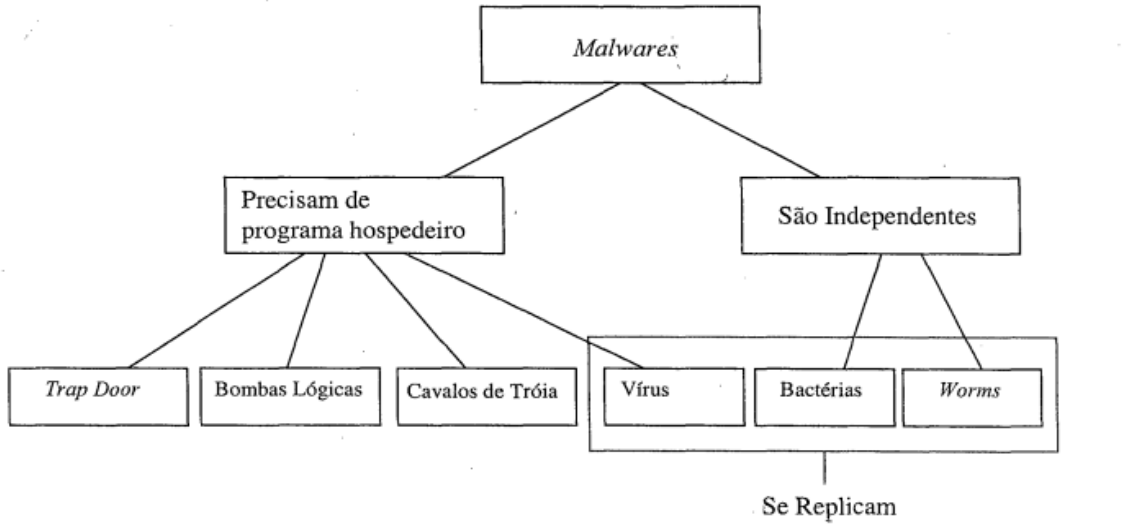
Caldas (2016) afirma que grande parte da pesquisa contra tais ataques é voltada para a prevenção e detecção. Dentre os mecanismos para tal, citamos o uso de antivírus, antispyware e *VPN*.

2.2.1 Malwares

De acordo com Lima et al. (2015) *malware* é uma junção dos termos ‘malicioso’ e ‘*software*’. O *malware* tem como principal objetivo acessar um dispositivo alheio sem permissão explícita de seu proprietário. Vasudevan e Yerraball (2006) descrevem o *malware* como "um termo genérico que engloba vírus, trojans, *spywares* e outros códigos intrusivos”.

Uma forma de taxonomia de *malwares* segundo Stallings (1999, apud Pereira, 2001) pode ser vista na FIGURA I. O diagrama na imagem faz uma divisão a partir da necessidade ou não do *malware* ter um programa hospedeiro e, ainda, os subdivide baseando-se em suas características reprodutivas (se eles podem ou não se replicar).

Quadro 1 - Taxonomia dos *Malwares*



Fonte: Adaptado pelo autor com base em Pereira (2001, p. 43).

Exemplos de *malware* incluem, mas não são limitados a:

- *Trap Door* é, de acordo com Pereira (2001), uma entrada secreta no programa que dá acesso a partes do sistema com o acesso comumente negado. Desenvolvedores de *software* utilizam *trap doors* para testar programas, mas isso se provou uma prática de risco quando *hackers* começaram a utilizá-las.
- *Backdoor*, segundo CERT.BR (2016, apud Caldas, 2016), é um meio para *hackers* ou outros tipos de *malware* retornarem a um computador comprometido. Pode ser adquirido quando o microcomputador já está infectado por outro programa malicioso e propicia que ele seja manipulado remotamente (F-SECURE, 2016, apud CALDAS, 2016).
- Bomba Lógica é um dos tipos mais antigos de *malware*. Trata-se de um código infiltrado em um programa comum que entra em ação (apagando alterando arquivos) quando algum tipo de "gatilho" é ativado (PEREIRA, 2001).
- Cavalo de Tróia**,** para Weber (1989, apud Pereira, 2001), é um módulo de ataque disfarçado de normal. Ele é um programa que aparenta ter uma utilidade, quando na realidade tem um código oculto, que geralmente objetiva permitir outro usuário executar funções indesejadas, como apagar arquivos ou conceder permissões (CALDAS, 2016).

- Vírus, segundo Pereira (2001) são códigos que se autorreproduzem. Eles fazem parte de algum arquivo executável ou de um *software* modificado. De acordo com Bernstein (1997, apud Pereira, 2001) esses *malwares* podem eliminar e alterar dados e arquivos do sistema, além de negar disponibilidade em alguns casos.
- *Worms* são, de acordo com Caldas (2016), *malwares* que se propagam em redes de computadores em grande velocidade. Para tal, eles buscam sistemas remotos na tabela de *hosts* e estabelecem conexões com estas e, em seguida, criam cópias de si para sistemas remotos e as executam (PEREIRA, 2001).
- *Spywares* oferecem algum tipo de serviço em troca da permissão para coletar informações sobre o comportamento de navegação na web do usuário ou aplicativos preferenciais (F-secure, 2016, apud CALDAS, 2016). Segundo Egele et al (2007), uma vez ativado em seu dispositivo, o *spyware* monitora silenciosamente todo o comportamento do usuário atingido.
- *Phishing*, segundo Caldas (2016) é uma maneira de obter dados pessoais como senhas e dados de cartão de crédito se passando por plataformas ou pessoas confiáveis. Como um e-mail de, aparentemente, um membro oficial de uma empresa com um endereço de um site que pareça seguro com o intuito de coletar informações pessoais inseridas nele.

2.2.2 Antivírus e antispyware

Segundo Pereira (2001), o *software* antivírus é: "responsável pela detecção, identificação e eventual remoção de código malicioso executável." O *software* detecta um arquivo malicioso de várias formas, dentre elas a mais comum é utilizando um conjunto de assinaturas digitais para encontrar o arquivo suspeito. Após encontrar o arquivo, o *software* toma medidas defensivas para que o código malicioso não se espalhe pela máquina.

De acordo com Bär (2017), os *antispyware* são *softwares* muito similares aos antivírus, o programa de *antispyware* é utilizado para a remoção de um ou mais *spywares* de uma máquina ou rede. O *software* possui dois objetivos

básicos: remover e desinstalar *spywares* e prevenir a instalação destes arquivos mal intencionados em seu computador.

2.2.3 Rede privada virtual

Visando a integridade e segurança das informações compartilhadas, foi criada a Rede Privada Virtual, que tem origem do inglês *Virtual Private Network* (VPN). De acordo com Augusto et al. (2019) ela tem seu fundamento em garantir a segurança na troca e transporte das informações.

Esta rede constitui-se de um modo de compartilhamento das informações entre aparelhos não necessariamente conectados fisicamente por uma rede, essa conexão se dá através de um canal de comunicação em uma rede pública onde é aplicado um protocolo que permite que apenas aparelhos autorizados possam acessar tais informações (AUGUSTO et al, 2019; CARDOSO, 2010). Cardoso (2010) aponta o uso de VPN como a alternativa mais barata e eficaz para a transmissão de vídeo.

2.2.4 Ferramentas adequadas para videochamadas

De acordo com a *Electronic Frontier Foundation* (EFF) — organização que defende o direito à privacidade — alguns dos fatores que devem ser levados em conta ao escolher um software de comunicação seguro são: o uso de criptografia; privacidade em relação aos provedores de internet; garantia da identidade dos contatos; uso de *Perfect Forward Secrecy* (protocolos que garantem que as chaves da sessão não serão comprometidas); *design* de segurança propriamente documentado e, por fim, verificações de código feitas, no máximo, a cada 12 meses (GUSMÃO, 2016).

O Webex encontra-se entre as ferramentas que mais se aproximam de se adequar a esses parâmetros. Segundo Sevilla (2020), essa ferramenta da CISCO — disponível como aplicativo *mobile*, *software* e através de navegadores — apresenta bons níveis de segurança por suas salas protegidas por senha. Outra possibilidade é o Jitsi, que de acordo com Maciel (2020), é um dos melhores aplicativos de videoconferência por usar a tecnologia *peer-to-peer* —

que segundo Rocha (2004), são redes virtuais com objetivo de compartilharem recursos entre os usuários da rede sem que haja uma hierarquia entre esses usuários.

Exclusivamente para dispositivos *mobiles*, e com opções de chamada de vídeo, *chat* e chamadas de voz, Gusmão (2016) afirma que o Silent Phone foi um dos mais bem colocados na avaliação da EFF. Entretanto, o autor chama a atenção para o fato de que nenhuma dessas ferramentas é perfeita, são apenas melhores entre as outras no mercado (GUSMÃO, 2016).

3. DISCUSSÃO

Atendimentos *on-line* já são uma realidade no campo da psicologia há alguns anos, entretanto, assim como em qualquer prática inovadora, existem pontos favoráveis a esta modalidade de trabalho, mas também questões desvantajosas.

A videoconferência, a título de exemplo, é uma ferramenta muitas vezes adotada como recurso para atendimento *on-line* por possibilitar que sujeito atendido e psicólogo possam compartilhar suas expressões faciais, tom de voz, postura e outros elementos que a tornam mais próxima a um atendimento presencial. Apesar de tantos benefícios, diversos casos reportados — exemplificados a seguir — mostram seus problemas de segurança que colocam em risco a confidencialidade.

A matéria de Germano (2020) demonstra que um dos aplicativos que mais cresceu no período de pandemia do COVID-19 — a ferramenta de videoconferência Zoom Meetings — teve exposta sua fragilidade quando *hackers* o invadiram a partir da sua URL (*Uniform Resource Locator* — localizador uniforme de recursos). Também foi apontado um erro no sistema do *software* que possibilita invasores controlarem câmeras e microfones dos usuários que estão participando da videoconferência. Com a repercussão da fragilidade da ferramenta o governo da Califórnia nos Estados Unidos, e até mesmo o FBI (Departamento Federal de Investigação) começaram a apurar as

ocorrências de invasões. Situações semelhantes em que os dados dos usuários entraram em risco ocorreram com as videochamadas do Whatsapp (ARSTECHNICA, 2019) e Google Meet (SHARMA, 2020).

Para lidar com adversidades como essas, é necessário principalmente o uso de *antimalware* e de antivírus — além de um *firewall* confiável. Nomeamos também o uso de redes privadas virtuais, para garantir segurança em relação a provedores e qualquer outro dispositivo não autorizado. Existem diversas variantes gratuitas disponíveis para *download como PrivadoVPN, ProtonVPN* e Hide.me (MARKS, 2021).

Donnamaria (2013) cita também o emprego de senhas com caracteres especiais e números; a realização dos atendimentos em ambientes privados e a utilização assinaturas digitais nos atendimentos síncronos e assíncronos.
Para lidar especificamente com o *phishing* — citado previamente em '3. 1 *Malwares*' — psicólogo e sujeito a ser atendido podem empregar uma "palavra-chave", dita cada vez que uma conversa por texto é iniciada.

Mencionadas tais medidas, cabe discorrer sobre o uso e conhecimento a respeito delas na prática nacional da psicologia. Pieta e Gomes (2014) argumentam que os principais impasses dos atendimentos psicológicos *on-line* podem ser resolvidos com uma delimitação clara pelas diretrizes de conduta legal e ética do Conselho Federal de Psicologia.

Em contato realizado por e-mail pelos pesquisadores no dia 10 de janeiro de 2021 ao Conselho Federal de Psicologia, questionou-se acerca da existência de alguma norma técnica ou recomendação para garantir o sigilo e confidencialidade dos dados nos atendimentos síncronos e assíncronos. O conselho em questão, remeteu ao Conselho Regional do Paraná que, diante o questionamento, informou que não faz recomendações nem aprovação de plataformas ou *sites*, e que o profissional tem autonomia para a escolha. Citaram que as resoluções disponíveis são as CFP n° 11/2018 e CFP n° 04/2020, ambas já analisadas no item 2.1.

Em contrapartida, Siegmund et al (2015) interpretam a realidade do atendimento psicológico como algo além da regulamentação do CFP. Os autores alegam que não basta que estes atendimentos remotos sejam permitidos e

regulamentados, é necessário que os profissionais da área estejam aptos a superar os desafios emergentes das especificidades dessa prática profissional. Em citação a Suler (2002, *apud* SIEGMUND et al. 2015), os autores inferem que parâmetros de treinamento (referentes à confidencialidade e garantia de sigilo) devem ser estipulados aos profissionais que desejarem atuar com atendimentos a distância.

Fica evidente a necessidade desta capacitação ao analisar os dados de segurança de rede no país. De acordo com uma pesquisa realizada pela empresa DFNDR LAB em 2018, aproximadamente 34% dos brasileiros foram alvo de ataques cibernéticos no segundo trimestre de 2018, sendo que a maioria destes poderia ser evitada por proteções básicas, como uso de antivírus e maior prudência com as próprias senhas.

Isto posto, e considerando a exigência de confidencialidade dos atendimentos psicológicos, o ponto chave para a formação de profissionais aptos a superar os desafios da segurança de dados é a interdisciplinaridade, através de pontes com áreas como a informática, seria possível a consolidação dos atendimentos psicológicos pela internet de forma eficaz e segura segundo a Associação Americana de Psicologia (APA) (2009). Desta forma, ao optar pelo uso de TICs seria imprescindível que os psicólogos tivessem ciência de propostas como as da literatura estrangeira para promover a proteção dos usuários da psicoterapia pela internet.

4. CONCLUSÃO

Seja por limitações éticas ou técnicas, é impossível julgar que os atendimentos psicológicos prestados através da internet irão eventualmente substituir por completo os realizados em consultórios. O uso das TICs, no entanto, apresenta um campo extremamente vasto de possibilidades e benefícios — quando realizado de maneira adequada.

Em oposição ao cenário atual, que apresenta resoluções e estudos da área que focam mais na eficiência e factibilidade dos atendimentos via internet do que na preocupação com a segurança, é necessário uma série de dianteiras

interligadas para a execução com confidencialidade da prática profissional mediada por TICs.

Sendo a privacidade e confidencialidade exigidas em todas as áreas de atuação profissional da psicologia (ORMART, 2013), a questão levantada neste trabalho diz respeito à segurança das informações nos atendimentos *on-line*. A resposta simplificada para a questão “é possível garantir plenamente, e de forma ininterrupta, o sigilo e a privacidade necessários aos atendimentos através das tecnologias disponíveis?”, infelizmente, é que **não**.

As tecnologias de informação e comunicação transmutam-se em grande velocidade, e tentar afirmar que existem meios para barrar qualquer ameaça despontante seria um equívoco. Vale ressaltar, entretanto, que diante da necessidade e importância que estas modalidades vêm tomando, evoluem também as proteções e protocolos de segurança relativos à elas. Eles garantem o máximo de segurança alcançável.

Isto posto, para garantir eficácia e segurança nos atendimentos psicológicos à distância é necessário, além da especificação das plataformas com bons níveis de segurança a serem utilizadas por parte das resoluções, também maior conhecimento dos profissionais da psicologia sobre os meios tecnológicos, a fim de compreenderem a melhor forma de lidar com tais ferramentas — tanto as utilizadas diretamente (como de videochamadas ou aplicativos de troca de mensagens assíncronas) quando aquelas feitas para promover a segurança de dados (antivírus, *antimalwares* e VPN).

Sugere-se algumas medidas a serem tomadas a curto prazo, como por exemplo: o CFP oferecer oficinas e cursos de capacitação para os profissionais que atuam na área e que o Conselho indique ferramenta especialmente desenvolvida para o uso dos psicólogos.

Já a longo prazo seria primordial que os profissionais atuantes se mantenham atualizados quanto as novas tecnologias disponíveis, em especial as ferramentas de segurança da informação. Outra medida urgente é a inclusão de disciplinas relacionadas à tecnologia da informação nos cursos de graduação de psicologia.

5. REFERÊNCIAS

ANTON, Juleine. O Atendimento Psicológico Online: aspectos éticos do uso da Internet. **Psicologado**. 10 abr. 2013. Disponível em: https://psicologado.com.br/atuacao/psicologia-clinica/o-atendimento-psicologico-online-aspectos-eticos-do-uso-da-internet. Acesso em: 05 out. 2020.

AUGUSTO, Filipe; FERNANDES, Juliana; DOS ANJOS, Lidiana Souza. **Virtual Private Network.** 2019, Universidade Federal do Rio de Janeiro, Rio de Janeiro. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/vpn/. Acesso em: 09 jul. de 2020.

BÄR, Hugo. O que é antispyware?. **Tripla**, Belo Horizonte, 31 ago. 2017. Disponível em: https://triplait.com/voce-sabe-o-que-e-antispyware/. Acesso em: 07 mai. 2020.

BASÍLIO, Felipe Augusto. Crimes na internet. **Revista Direito**, v. 4, n. 6, p. 63-76, 2003.

BRAY, James.**President's column: Vision for the future of psychology practice**. American Psychological Association, v. 40, n. 2, p. 5, fev. 2019.

CALDAS, Daniel Mendes. **Análise e extração de características estruturais e comportamentos para perfis de *malware.*** 2016. 105 f. Tese (mestrado em engenharia elétrica) — Universidade de Brasília, Faculdade de tecnologia: departamento de engenharia elétrica. Brasília, 2016.

CARDOSO, Felipe. Cesar. **Conceitos de rede virtual privada para streaming de vídeo.** 2010. 82 f. Monografia (Engenharia da Computação) — Universidade São Francisco, Itatiba, 2010.

Código de Ética Profissional do Psicólogo. **Conselho Federal de Psicologia**, Brasília, ago. de 2005. Disponível em: <http://site.cfp.org.br/wp-

content/uploads/2012/07/codigo-de-etica-psicologia.pdf>. Acesso em:19 set. 2020.

CFP - Conselho Federal de Psicologia. Resolução CFP nº 12/2005. Regulamenta a atuação da(o) psicóloga(o) no âmbito do sistema prisional. **Conselho Federal de Psicologia**, Brasília, DF, 18 ago. 2005. Disponível em: https://cadastrosite.cfp.org.br/docs/resolucao2005_12.pdf. Acesso em: 02 jul. 2020.

_____. CFP publica nova resolução sobre atendimento psicológico online. **Conselho Federal de Psicologia**. Brasília, DF, 2018. Disponível em: <https://site.cfp.org.br/cfp-publica-nova-resolucao-sobre-atendimento-psicologico-online/>. Acesso em: 06 jul. 2020.

_____. Resolução CFP nº 04/2020. Dispõe sobre regulamentação de serviços psicológicos prestados por meio de Tecnologia da Informação e da Comunicação durante a pandemia do COVID-19. **Conselho Federal de Psicologia**, Brasília, DF, 26 mar. 2020. Disponível em: https://atosoficiais.com.br/cfp/resolucao-do-exercicio-profissional-n-4-2020-dispoe-sobre-regulamentacao-de-servicos-psicologicos-prestados-por-meio-de-tecnologia-da-informacao-e-da-comunicacao-durante-a-pandemia-do-covid-19?q=04/2020. Acesso em: 10 mai. 2020.

_____. Resolução CFP nº 11/2020. Regulamenta a prestação de serviços psicológicos realizados por meios de tecnologias da informação e da comunicação e revoga a Resolução CFP N.º 11/2012. **Conselho Federal de Psicologia**, Brasília, DF, 11 mai. 2018. Disponível em: https://atosoficiais.com.br/lei/orientacao-psicologica-pela-internet-cfp?origin=instituicao. Acesso em: 01 mai. 2020.

_____. Resolução CFP nº 03/2020. Regulamenta o atendimento psicoterapêutico mediado por computador. **Conselho Federal de Psicologia**, Brasília, DF, 25 set. 2020. Disponível em: www.crprs.org.br/upload/legislacao/legislacao40.pdf. Acesso em: 05 mai. 2020.

DE LIMA, Sidney Marlon Lopes *et al.* **Antivírus dotado de Rede Neural Artificial visando a Diferenciação entre Executáveis Benignos e Malwares. EJITEC-Electronic Journal of Information Technology and Communication**, Faculdade São Miguel, v. 1, n. 1, 2017.

DFNDR LAB. **Relatório de Segurança Digital no Brasil**. Online, 2018. Disponível em https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2-trimestre-2018.pdf. Acesso em: 05 mai. 2021.Disponível em: http://www.apa.org/monitor/2009/02/pc.aspx. Acesso em: 21 abr. 2020.

DONNAMARIA, Carla Pontes. **Experiências de atendimento psicológico grupal via internet: uma perspectiva psicanalítica**. 2013. 198 f. Tese (Doutorado em Psicologia) – Pontifícia Universidade Católica de Campinas, Centro de Ciências a Vida, Programa de Pós-Graduação em Psicologia, Campinas, SP, 2013.

EGELE, Manuel *et al.* Dynamic Spyware Analysis. In **USENIX annual technical conference**, 2007, p. 233–246. Disponível em: https://static.usenix.org/event/usenix07/tech/full_papers/egele/egele.pdf. Acesso em: 21 jul. 2020.

GERMANO, Felipe. Por que o Zoom é um desastre de privacidade para você. **Portal UOL**, São Paulo, 02 abr. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/02/bombou-na-quarentena-por-que-o-zoom-e-um-desastre-de-privacidade-para-voce.htm. Acesso em: 03 jul. 2020.

GOODIN, Dan. WhatsApp vulnerability exploited to infect phones with israeli spyware. **Ars Technica**, 5 mar. 2019. Disponível em: https://arstechnica.com/information-technology/2019/05/whatsapp-vulnerability-exploited-to-infect-phones-with-israeli-spyware/. Acesso em: 23 mar 2020.

GUSMÃO, Gustavo. Os 10 apps de mensagem mais seguros. **Revista Exame, São Paulo,** 13 set. 2016**.** Disponível em: https://exame.com/tecnologia/os-10-apps-de-mensagem-mais-seguros/. Acesso em: 29 jul. 2020.

HANNEL, KELLY. **Contribuições ao Processo de Comunicação na Internet Baseado em Videoconferência e Streaming de Áudio e Vídeo**. Monografia (graduação). Bacharelado em Ciência da Computação. Instituto de Física e Matemática. Universidade Federal de Pelotas: Pelotas, 2005.

MACIEL, Rui. Jitsi: plataforma de videoconferências usa a mesma criptografia do WhatsApp. **Canaltech**, 26 abr. 2020. Disponível em: https://canaltech.com.br/seguranca/jitsi-plataforma-de-videoconferencias-usa-a-mesma-criptografia-do-whatsapp-163799/. Acesso em: 30 jul. 2020.

MARKS, Tove. Os 6 principais provedores de VPN verdadeiramente gratuitos de janeiro de 2022. **Vpnoverview**, Holanda, 29 dez. 2021. Disponível em: https://vpnoverview.com/pt/melhores-fornecedores-vpn/servicos-vpn-gratuitos/. Aceso em: 02 fev. 2022.

ORMART, Elizabeth Beatriz. El secreto profesional en psicología: aspectos deontológicos, legales y clínicos. **Psicología para América Latina**, n. 24, p. 191-205, 2013. Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1870-350X2013000100012&lng=pt&nrm=iso. Acesso em: 03 abr. 2020.

PEREIRA, Kariston. **Uma proposta de metodologia para o controle e defesa contra vírus e outros *malwares* em ambientes corporativos.** 2001. 122 f. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós -Graduação em Computação. Universidade Federal de Santa Catarina, Florianópolis, 2001. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/79958. Acesso em: 10 jun. de 2021.

PIETA, Maria Adélia Minghelli e GOMES, William B. Psicoterapia pela Internet: viável ou inviável?. **Psicologia: Ciência e Profissão** [online]. 2014, v. 34, n. 1,

p. 18-31. Disponível em: https://doi.org/10.1590/S1414-98932014000100003. Acesso em: 04 de fev. de 2022.

ROCHA, João et al. Peer-to-peer: Computaçao colaborativa na internet. In: **Minicursos do XXII Simposio Brasileiro de Redes de Computadores (SBRC 2004)**. 2004. Disponível em: https://www.cin.ufpe.br/~cak/publications/sbrc2004_minicurso_p2p.pdf. Acesso em: 30 jul. 2020.

SEVILLA, Gadjo. Zoom vs. Webex: The Best Video Conferencing Apps Face Off on Features. **PCMag,** 07 abr. 2020. Disponível em: https://www.pcmag.com/news/zoom-meeting-vs-cisco-webex-meetings. Acesso em: 29 jul. 2020.

SHARMA, Shubham. Hackers are using Zoom, Google Meet for phishing attacks. **NewsBytes,** 12 mai. 2020. Disponível em: https://www.newsbytesapp.com/timeline/science/60955/285174/hackers-use-zoom-google-meet-for-phishing. Acesso em: 13 jul. 2020.

SIEGMUND, Gerson. *et al*. Aspectos éticos das intervenções psicológicos *online* no Brasil: Situação atual e desafios. **Psicologia em Estudo**, Universidade Estadual de Maringá, Maringá, vol. 20, p. 437-447, 2015.

UNIVERSIDADE ABERTA DO SUS. Organização Mundial de Saúde declara pandemia do novo Coronavírus. **UNA-SUS,** Brasília, 11 mar. 2020. Disponível em: https://www.unasus.gov.br/noticia/organizacao-mundial-de-saude-declara-pandemia-de-coronavirus. Acesso em: 02 de fev. de 2021.

VASUDEVAN, Amit; YERRABALLI, Ramesh. Spike: engineering malware analysis tools using unobtrusive binary-instrumentation. In: **Proceedings of the 29th Australasian Computer Science Conference**, Volume 48. 2006. p. 311-320.

VIANA, Diego Mendonça. Atendimento psicológico online no contexto da pandemia de covid-19. **Cadernos ESP-Revista Científica da Escola de Saúde Pública do Ceará**, v. 14, n. 1, p. 74-79, 2020.

VIANNA, Túlio Lima. Dos crimes pela internet. **Revista do CAAP**, p. 367-385, 2000.

Enviado em: 14 set. 2021.
Aceito em: 02 jul. 2022.
Editora responsável: Bianca Neves Machado.