White paper

A cibersegurança das mulheres durante a pandemia de COVID-19:

Experiências, riscos e estratégias de autocuidado na nova normalidade digital

OEA | Mais direitos para mais pessoas

Sumário

Créditos

Luis Almagro
Secretário-Geral
Organização dos Estados Americanos (OEA)

Arthur Weintraub
Secretário de Segurança Multidimensional
Organização dos Estados Americanos (OEA)

Alison August Treppel
Secretária Executiva
Comitê Interamericano contra o Terrorismo (CICTE)

Alejandra Mora Mora
Secretária Executiva
Comissão Interamericana de Mulheres (CIM)

Equipe Técnica da OEA
Programa de Cibersegurança
Kerry-Ann Barrett
Mariana Cardona
Mariana Jaramillo
Gabriela Montes de Oca Fehr

Comissão Interamericana de Mulheres /
Mecanismo de Acompanhamento da Convenção de Belém do Pará
Luz Patricia Mejía Guerrero
Alejandra Negrete Morayta

Autora
Katya N. Vera Morales

Desenho e Diagramação
Michelle Felguérez

01 Objetivos

> *O aumento acelerado dos processos de digitalização e transformação tecnológica é uma das características mais notáveis da evolução da pandemia de COVID-19, cuja gestão propiciou a construção de um ecossistema digital no qual novas identidades, experiências e interações estão surgindo, multiplicando-se e transformando-se em grande escala.*

Embora o cibercrime, o abuso e a violência digital já representassem um problema mundial antes da pandemia, estas novas condições criaram novas oportunidades para agressores e cibercriminosos, que durante esta etapa aumentaram o número e alcance de seus ataques, replicando velhas técnicas e ao mesmo tempo inovando em suas estratégias.

Desde março de 2020, diversos estudos no âmbito global e regional procuraram identificar as tendências e características das ameaças on-line e os desafios enfrentados em matéria de cibersegurança no novo ecossistema digital. Contudo, um exame desses estudos revela que se deu pouca atenção às experiências digitais das mulheres no âmbito das crescentes vulnerabilidades no espaço digital, persistindo uma falta de análise com perspectiva de gênero sobre a gama de riscos cibernéticos que enfrentam e os impactos da cibercriminalidade em suas vidas.

Esta falta de análise de gênero exemplifica o que acontece em grande escala no âmbito da cibersegurança, onde ainda prevalece um entendimento das tecnologias e dos riscos cibernéticos como neutros de gênero e, portanto, sem impactos diferenciados em função das identidades e expressões de gênero das pessoas (Millar et al., 2021: 8).

Neste contexto, diversas vozes no âmbito da academia, sociedade civil e fóruns multilaterais começaram a sublinhar a necessidade de analisar as dimensões de gênero da cibersegurança a fim de gerar uma melhor compreensão das dinâmicas que compõem a política e a prática neste setor, tendo surgido recentemente declarações oficiais, estratégias para o desenvolvimento de capacidades e pesquisas que estão abrindo caminho no tema.

Somando-se a estes sinais de mudança, a presente publicação tem por objetivo contribuir ao diálogo em torno dos vínculos entre a cibersegurança e as normas e papéis de gênero durante esta época crítica para o ciberespaço, apresentando um **quadro de análise para a identificação de possíveis vulnerabilidades e riscos que as mulheres enfrentam**[1] no novo ecossistema digital.

Para isso, propõe-se uma **análise do cenário de ciberataques** surgido a propósito da crise sanitária em **conjunto com as dinâmicas de acesso e uso** da internet por parte das mulheres, bem como das **condições de desigualdade de gênero** sistêmicas que incidem off-line e on-line, a fim de identificar algumas **ameaças cibernéticas que as estariam afetando especificamente durante esta etapa.**

[1] Destaca-se que, por questões de espaço, o presente documento focaliza unicamente as experiências diferenciadas das mulheres no âmbito da cibersegurança, embora se reconheça a urgência de abordar as experiências on-line e os riscos cibernéticos que outros coletivos marginalizados enfrentam atualmente, a partir de sua identidade ou expressão de gênero e sexual, bem como impulsionar o desenvolvimento de análises que permitam revelar de forma detalhada o impacto na segurança cibernética da intersecção entre o gênero e outros fatores de discriminação e exclusão.

Este quadro de análise procura fornecer elementos de utilidade para profissionais e responsáveis pelas políticas públicas de cibersegurança no contexto das estratégias implementadas para proteger as pessoas on-line durante a crise sanitária. Além disso, foi utilizado como base para a delimitação de um **bloco de medidas básicas de segurança digital cuja adoção é importante promover na nova normalidade digital.** Isto foi feito sob a premissa de que não basta identificar possíveis vulnerabilidades e riscos cibernéticos: é preciso normalizar o autocuidado digital como parte das estratégias para empoderar as mulheres no uso seguro das novas tecnologias.

O estudo das dimensões de gênero das normas, políticas e estratégias de cibersegurança é um campo de exploração em plena transformação e cujos avanços sem dúvida marcarão a pauta para um melhor entendimento do ciberespaço. Com isso em mente, o presente documento procura contribuir ideias para a reflexão que está em andamento, reconhecendo o grande potencial de se aplicar uma visão de gênero ao setor e o impacto de fenômenos mundiais como a COVID-19 em aspectos pontuais da indústria.

02 Os impactos da epidemia de COVID-19 no ecossistema digital

A pandemia de COVID-19 significa um ponto de inflexão no uso do ciberespaço, o qual se converteu no principal cenário comum global. A partir de março de 2020, a crise sanitária implicou a adoção de medidas de confinamento para reduzir a propagação do vírus, mantendo grande parte da população mundial dentro de suas casas e com reduzida capacidade de deslocamento físico. Ante este confinamento forçado, de forma abrupta nos vimos face à necessidade de reimaginar nossas sociedades e modificar aspectos básicos de nossas práticas cotidianas, adotando novas estratégias individuais e coletivas para paliar os efeitos da crise sanitária.

Mais do que nunca, os governos se valeram das tecnologias para proteger e preservar a saúde pública, manter o funcionamento da economia e levar os serviços públicos à cidadania, digitalizando aceleradamente seus processos administrativos e de gestão e oferecendo soluções digitais nas áreas de saúde, educação, comércio e trabalho. De igual forma, empresas, universidades, bancos, agências internacionais, igrejas, organizações e grupos de todo tipo, natureza e tamanho implementaram ferramentas e plataformas virtuais para migrar ao ciberespaço suas atividades baseadas previamente na presencialidade física[2].

Individualmente, voltamo-nos também ao ciberespaço num esforço para compensar o isolamento e manter proximidade digital com familiares e amigos apesar da separação física, buscando preservar essa sensação de normalidade que desapareceu com a chegada da pandemia. Transferimos para a web grande parte de nossas atividades laborais, educativas, comerciais, de entretenimento e relacionais[3], reforçando ainda mais aquela continuidade *on-line/off-line* que já se observava nas interações humanas antes do advento da pandemia.

[2] De acordo com a Comissão Econômica para a América Latina e o Caribe (CEPAL), entre abril e março de 2020 o número de sites empresariais aumentou 800% na Colômbia e no México e em torno de 360% no Brasil e no Chile. No México e no Brasil o número de novos sites de comércio eletrônico aumentou mais de 450% em abril, em comparação com o mesmo mês de 2019, e os sites com presença ativa na Colômbia e no México aumentaram cerca de 500%. Veja: Comissão Econômica para a América Latina e o Caribe (CEPAL) (2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.

[3] Na Europa, por exemplo, o uso da internet para atividades de lazer, interação em redes sociais ou plataformas de televisão paga aumentou tanto que a União Europeia solicitou a Netflix e HBO a redução da qualidade de vídeo para evitar a saturação da rede. Veja: José García (12 de março de 2020). "Netflix reducirá la calidad del contenido para evitar saturar la red a petición de la Unión Europea". https://www.xataka.com/streaming/netflix-reducira-calidad-contenido-para-evitar-saturar-red-a-peticion-union-europea. Consultado em 1° de fevereiro de 2021.

As tecnologias permitiram que as pessoas afetadas se conectassem com as autoridades e organismos de assistência, atuando como um canal para a expressão de suas necessidades, preocupações e experiências (UIT, 2020b: 17). Durante esta contingência, ficou mais claro que o acesso à internet já não é um mero luxo, mas uma linha de vida com o exterior e um direito humano que habilita o exercício de outros direitos fundamentais, como o direito à saúde, educação, cultura e liberdade de expressão (Agudelo et al., 2020: 3).

No caso das mulheres e meninas, a acelerada digitalização durante a pandemia permitiu romper preconceitos e estereótipos de gênero que por muito tempo as mantiveram afastadas das tecnologias digitais. Para algumas, esta é uma etapa em que pela primeira vez exploraram novas ferramentas e plataformas da internet ante a necessidade de manter-se conectadas, incursionando no uso de serviços financeiros digitais, compras pela internet, processos de escolarização à distância e atividades empresariais on-line. O período de confinamento motivou também sua ativa participação em debates digitais e a criação de laços com novas comunidades de mulheres on-line e lhes permitiu implementar novas formas de teletrabalho para conciliar suas responsabilidades laborais e familiares.

Em conjunto, esta mudança de práticas sociais durante a pandemia implicou modificações profundas no ciberespaço. Desde março de 2020 registraram-se recordes do tráfego na internet em âmbito mundial, alcançando em certos países um aumento entre 50% e 70% . De acordo com a Comissão Econômica para a América Latina e o Caribe (CEPAL), na região latino-americana durante o primeiro trimestre de 2020 o teletrabalho aumentou 324%, a educação on-line mais de 60%, o comércio eletrônico 157%, o *livestreaming* 12% e as transações bancárias eletrônicas 7% (CEPAL, 2020).

Atualmente, não se sabe ao certo quanto mais tempo durarão a crise sanitária da COVID-19 e as medidas de distanciamento físico, mas é claro que a digitalização chegou para ficar e será um elemento crucial da 'nova normalidade'. Durante esta etapa, o uso acelerado (e forçado em muitos casos) de ferramentas digitais trouxe uma sensação de maior comodidade no seu uso por parte de mulheres e homens, e é de esperar que uma vez passada a crise as pessoas optarão por utilizar a internet para mais coisas do que antes.

A. Os riscos no novo ecossistema digital

> *O aumento exponencial no âmbito mundial do uso da tecnologia para mitigar o impacto das medidas de mitigação da crise sanitária significa também um grande desafio para o ecossistema digital, revelando falhas estruturais tanto no acesso à internet como na segurança on-line.*

À medida que mulheres e homens direcionaram suas atividades ao ciberespaço, registrou-se um crescimento exponencial do nível de exposição a riscos on-line devido à falta de familiaridade com o uso em grande escala das tecnologias da informação e comunicação (TIC) e à carência generalizada de conhecimentos sobre ciberameaças e ferramentas de proteção e segurança digital.

[4] Mark Beech (25 marzo 2020). "COVID-19 Pushes up internet use 70% and streaming more than 12%, first figures reveal". https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=36a6e4ab3104. Consultado em 1° de fevereiro de 2021.

Mais pessoas on-line com poucos conhecimentos em cibersegurança (e expondo-se a mais riscos on-line do que fariam usualmente na escola ou em seu trabalho) configuraram um cenário propício para atacantes e cibercriminosos, que se aproveitaram rapidamente desta 'nova normalidade' digital explorando o medo e a incerteza geradas pela pandemia e o desejo de informação da população (UNODC, 2020)[5].

Segundo informaram diversas fontes, os cibercrimes tiveram um aumento diretamente proporcional à transformação digital iniciada em março de 2020, e no fim desse mês todos os países haviam recebido pelo menos um ciberataque temático de COVID-19[6]. A Organização das Nações Unidas (ONU) indicou que desde o início da pandemia houve um aumento de 600% nos e-mails maliciosos e 350% nos sites falsos, ocorrendo um ciberataque aproximadamente a cada 39 segundos[7]. Nos Estados Unidos, de acordo com informação do Internet Complaint Centre (IC3) do FBI, quadruplicaram as queixas apresentadas sobre cibercrimes[8]; na América Latina houve um aumento de 74% no número de crimes cibernéticos durante a pandemia[9], mais de 20,5 milhões de ataques cibernéticos a usuários em casa e 1,2 milhão de ataques a dispositivos móveis entre janeiro e setembro de 2020[10].

De acordo com análises das repercussões da COVID-19 no cibercrime realizadas por agências como o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), a Organização Internacional de Polícia Criminal (INTERPOL) e a EUROPOL, entre os ciberataques mais comuns observados desde março de 2020 encontram-se o uso de métodos de engenharia social, golpes pela internet e campanhas de *phishing*, infiltração de *malware* em dispositivos eletrônicos, a criação de sites falsos, sextorsão facilitada pelas TIC, ataques através de ferramentas de trabalho remoto, desinformação on-line e uso da *Dark Web* para atividades criminosas[11].

[5] Trend Micro (11 de novembro de 2020). "Developing Story: COVID-19 Used in Malicious Campaigns". https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. Consultado em 1° de fevereiro de 2021.
[6] News Center Microsoft Latinoamérica (16 de junho de 2020). "Explotar una crisis: Cómo se comportaron los cibercriminales durante el frote". https://news.microsoft.com/es-xl/explotar-una-crisis-como-se-comportaron-los-cibercriminales-durante-el-brote/. Consultado em 1° de fevereiro de 2021.
[7] Business Standard (7 de agosto de 2020). "UN reports sharp increase in cybercrime during coronavirus pandemic". https://www.business-standard.com/article/technology/un-reports-sharp-increase-in-cybercrime-during-coronavirus-pandemic-120080700289_1.html; Phil Muncaster (1° abril 2020). "Cyber-Attacks up 37% over past months as #COVID19 bites". https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/. Consultado em 1° de fevereiro de 2021.
[8] Maggie Miller (16 de abril de 2020). "FBI sees spike in cybercrime reports during coronavirus pandemic". The Hill. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
[9] Unisys. Unisys Security Index. https://www.unisys.com/unisys-security-index; Mundo Contact (1° de julho de 2020). "Cibercrimen aumenta 74% en AL durante la pandemia". https://mundocontact.com/cibercrimen-aumenta-74-en-al-durante-pandemia/. Consultado em 1° de fevereiro de 2021.
[10] Em setembro de 2020, registrou-se um aumento exponencial de ciberataques em toda a região latino-americana, sendo Argentina, Brasil e México os países com maior risco. Veja: Agencia EFE (30 de setembro de 2020). "Argentina, Brasil y México, más vulnerables al cibercrimen en Latinoamérica". https://www.efe.com/efe/america/tecnologia/argentina-brasil-y-mexico-mas-vulnerables-al-cibercrimen-en-latinoamerica/20000036-4355566. Consultado em 1° de fevereiro de 2021.
[11] Para mais detalhes sobre as características dos ciberataques mais comuns durante a pandemia de COVID-19, veja: Programa de Cibersegurança da Organização dos Estados Americanos (OEA) (2021), "Alfabetismo y Seguridad Digital. Mejores prácticas en el uso de Twitter". https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf . Veja também: Escritório das Nações Unidas sobre Drogas e Crime (UNODC) (14 de abril de 2020). Cibercrime and Anti-Money Laundering Section. "Cybercrime and COVID19: Risks and Responses". https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf; INTERPOL (4 de agosto de 2020). "Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19". https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19; EUROPOL (5 de outubro de 2020). "Internet Organised Crime Threat Assessment (IOCTA)". https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020; Conselho da Europa (27 de março de 2020). "Cybercrime and COVID-19". https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19; INTERPOL, "COVID-1a Cyberthreat". https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. Cibersecurity & Infraestructure Security Agency (8 de abril de 2020). "UK and US Security Agencies Issue COVID-19 Cyber Threat Update". https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update. Consultado em 1° de fevereiro de 2021.

Evidentemente, esta lista de cibercrimes é exemplificativa do que está ocorrendo nos espaços digitais, sendo previsível que as ameaças continuem evoluindo conforme se modifiquem as condições da pandemia de COVID-19. Contudo, é importante notar que o aumento no cibercrime observado durante os últimos meses não é algo acidental. Em muitos casos, a **COVID-19 simplesmente intensificou os problemas preexistentes em matéria de cibersegurança,** deixando entrever o alto grau de vulnerabilidade e de exposição a riscos on-line das pessoas.

O novo contexto evidenciou o paradoxo tecnológica que enfrentamos há alguns anos: a **grande maioria das pessoas está utilizando a tecnologia sem ter plena consciência dos riscos e das consequências de seu uso** e, para satisfazer suas necessidades de conectividade, descartam facilmente a possibilidade de que a internet possa ser um campo fértil para agressores e cibercriminosos.

B. Diversos contextos, diversos riscos cibernéticos

> *Estar ao corrente das tendências gerais que a cibercriminalidade adotou durante a pandemia de COVID-19 é crucial para conhecer os potenciais riscos cibernéticos que as pessoas enfrentam e enfrentarão na nova normalidade digital e as possíveis medidas de segurança digital a serem implementadas.*

Não obstante, ao considerar esta radiografia do novo ecossistema digital é necessário também ter em mente que as experiências *on-line* das pessoas, inclusive seu nível de **exposição a ameaças e os cibercrimes** que as afetam, não são uniformes ou unívocas, mas **variam dependendo dos contextos pessoais e de fatores sociais** como o gênero, a localização geográfica, a idade, o grau de escolaridade e a origem étnica.

Embora persista ainda certo idealismo baseado na neutralidade da web, o certo é que, conforme avança a digitalização, fica cada vez mais claro que o ciberespaço não é o mesmo para todas as pessoas nem está separado dos problemas sociais off-line. A era tecnológica destacou que as pessoas não são seres unidimensionais, mas existe uma continuidade entre suas realidades *on-line* e *off-line*. Isto implica que suas identidades e os papéis sociais que desempenham off-line se trasladam também ao ciberespaço, condicionando suas experiências e interações digitais e, portanto, os riscos cibernéticos que enfrentam.

A partir disso, um entendimento integral das necessidades de segurança digital durante esta época de crise implica necessariamente o reconhecimento de que o mundo *on-line* é um reflexo das realidades *off-line* e que as tecnologias digitais replicam (e potencialmente aprofundam) o contexto em que as pessoas vivem.

Sob esta premissa, e a fim de poder identificar os possíveis riscos cibernéticos que as mulheres enfrentam durante esta época, adiante examinaremos **como o gênero[12] das pessoas condiciona os efeitos da pandemia de COVID-19 no ciberespaço e na cibercriminalidade**, entendendo-se que incorporar esta perspectiva é uma tarefa ineludível para a formulação de estratégias de segurança digital que sejam realmente efetivas durante esta época de mudança acelerada.

[12] O gênero refere-se aos papéis, comportamentos, atividades e atributos que uma sociedade numa época determinada considera apropriados para homens e mulheres, bem como às relações entre mulheres e homens. Estes atributos, oportunidades e relações são construídos socialmente, aprendidos através do processo de socialização e específicos do contexto ou época e passam por alterações. O gênero determina o que se espera, o que se permite e o que se valoriza numa mulher ou num homem num contexto determinado. Veja: ONU Mulheres, "Important Concepts Underlying Gender Mainstreaming". https://www.un.org/womenwatch/osagi/pdf/factsheet2.pdf

03 Como as mulheres habitam a nova normalidade digital? Uma análise com perspectiva de gênero do ecossistema digital que surgiu a partir da epidemia de COVID-19

Comprovou-se que existem **acentuadas diferenças entre o tipo de cibercrimes, abuso e violência cometidos on-line contra as mulheres e aqueles que afetam os homens,** cujas manifestações adotam formas específicas e geram impactos diversos em função do gênero (Millar, Shires e Tropina, 2021; Brown e Pytlak, 2020).

Embora o reconhecimento destas diferenças tenha avançado no âmbito da cibersegurança, quase um ano depois de iniciada a crise sanitária **ainda são escassas as análises com perspectiva de gênero sobre os impactos da pandemia na cibercriminalidade.** Até agora, os estudos sobre as ameaças cibernéticas contra as mulheres se concentraram nas diversas formas de violência de gênero *on-line* que surgiram ou aumentaram durante a pandemia, deixando de fora os outros riscos e ataques que elas enfrentam no ciberespaço. Infelizmente, esta carência de dados impede conhecer com certeza como as mulheres e as meninas estão vivendo o aumento nos níveis de cibercrime durante este período crítico.

Em resposta a esta lacuna, esta seção destaca alguns elementos que devem ser considerados ao realizar uma análise com perspectiva de gênero sobre as ameaças cibernéticas que as mulheres enfrentam na nova normalidade digital, com o que se espera contribuir a um melhor entendimento do que está ocorrendo no ciberespaço.

Em termos gerais podemos dizer que a adoção de um enfoque ou perspectiva de gênero implica analisar o impacto das características biológicas e de gênero das pessoas em suas interações, oportunidades e papéis sociais e revelar as dinâmicas de desigualdade e diferenças de poder entre homens e mulheres[13].

Em consequência, trazer esta **perspectiva para o âmbito da cibersegurança permite revelar como as experiências on-line das pessoas e as ameaças cibernéticas e danos que enfrentam são diferentes dependendo de sua identidade de gênero e orientação sexual.** Além disso, também se expõe **como as relações entre homens e mulheres e a desigualdade de gênero podem influir em questões tais como os usos e riscos na internet.** Esta visão de gênero implica formular as seguintes perguntas:

[13] "O enfoque de gênero é uma forma de olhar a realidade identificando os papéis e tarefas que homens e mulheres realizam numa sociedade, bem como as assimetrias, relações de poder e desigualdades entre eles. Permite conhecer e explicar as causas que produzem essas assimetrias e desigualdades e formular medidas (políticas, mecanismos, ações afirmativas, normas, etc.) que contribuam para superar as disparidades sociais de gênero". Rworld. Glosario de términos relacionados al enfoque de igualdad de género. https://www.refworld.org.es/pdfid/5af1c8114.pdf

De que forma os homens e as mulheres habitam o ciberespaço e quais são os riscos específicos que enfrentam?

Quais são as experiências das mulheres e meninas no contexto atual da cibercriminalidade?

Quais são os danos diferenciados que as mulheres sofrem ante ciberataques?

Implementar esta perspectiva também revela uma questão a ser considerada: as tecnologias digitais não são neutras; pelo contrário, o gênero das pessoas influi e condiciona o acesso e o uso da internet e seus riscos. São diferenças que se mantêm ao longo das etapas da vida e interatuam com outras determinantes sociais, tais como o grau de escolaridade, a idade, a localização, o nível socioeconômico, a orientação sexual e a origem étnica de homens e mulheres.

Como a Organização Mundial da Saúde (OMS) reconheceu, os **impactos das pandemias nunca são neutros com relação ao gênero das pessoas;** portanto, os planos estratégicos mundiais e nacionais de preparação e resposta à COVID-19 devem basear-se numa sólida análise de gênero e na forma em que este interatua com outras esferas de desigualdade (OMS, 2020). Evidentemente, esta afirmação se estende aos impactos que a pandemia tem no ciberespaço e às políticas e medidas de cibersegurança que devem ser adotadas para frear o atual surgimento acelerado de ameaças on-line e cibercrimes.

Consequentemente, uma análise de gênero do novo ecossistema digital propiciado pela pandemia de COVID-19 permitirá identificar os diferentes padrões de exposição a ciberameaças que homens e mulheres enfrentam e as medidas de segurança digital mais adequadas para protegê-los.

Tendo isso em mente, **propõe-se um quadro de análise** composto de três componentes que permitem revelar as experiências diferenciadas das mulheres na internet, bem como suas necessidades especiais. Estes componentes são básicos para conhecer o nível de vulnerabilidade e os tipos de riscos que podem enfrentar no novo ecossistema digital. Os três componentes são:

UM — **As condições nas quais as mulheres acessam o ciberespaço.**

DOIS — **A desigualdade de gênero e os impactos *on-line/off-line* da pandemia de COVID-19.**

TRÊS — **Os usos que as mulheres fazem da internet.**

A. Que obstáculos as mulheres enfrentam para habitar o ciberespaço? As brechas digitais de gênero

> *O primeiro elemento a ser considerado ao analisar os impactos diferenciados das ciberameaças nas mulheres é o fato de que* ***estas não gozam em pé de igualdade de um acesso pleno e de qualidade à internet nem dos conhecimentos necessários*** *para proteger-se e aproveitar tudo o que ela pode oferecer.*

A pandemia de COVID-19 evidenciou as consequências devastadoras de um acesso à rede inadequado ou nulo, pois sem esta via de contato e informação as pessoas ficam mais vulneráveis ao vírus, desconectadas de seus seres queridos e segregadas das estratégias governamentais para compensar a crise. Infelizmente, este é o cenário enfrentado por milhões de mulheres e meninas que ainda não têm acesso adequado à web (Brown e Pytlak, 2020).

Embora se tenha informado que as mulheres utilizam com cada vez mais frequência a internet, as brechas digitais de gênero[14] persistem em múltiplos níveis. De acordo com os últimos relatórios da União Internacional de Telecomunicações (UIT), 51% da população mundial (aproximadamente 4 bilhões de pessoas) estavam on-line em 2019[15]. Desse total, somente 48% das mulheres tinham acesso à internet, em comparação com 55% dos homens, o que em termos relativos significa que a disparidade mundial de gênero é de 17% (UIT, 2020). Além disso, a UIT informou que em países de renda baixa e média as mulheres têm 10% menos probabilidades que os homens de ter um telefone celular (UIT, 2020b), o que implica impactos importantes por ser este o meio mais utilizado de acesso à internet[16].

[14] O termo brecha de gênero se refere a qualquer disparidade entre a condição ou posição dos homens e mulheres na sociedade. São as diferenças de oportunidades, acesso, controle e uso dos recursos construídas com base nas diferenças biológicas, produto histórico de atitudes e práticas discriminatórias que obstaculizam o gozo e exercício dos direitos por parte de homens e mulheres.

[15] Em 2020 a UIT identificou importantes brechas de conectividade que persistem nas áreas rurais dos países em desenvolvimento. Globalmente, 72% dos domicílios em áreas urbanas têm internet, face a 38% nas áreas rurais.
Quanto à conectividade regional, a CEPAL indicou que em 2019 67% dos domicílios urbanos estavam conectados à internet, enquanto somente 23% das zonas rurais estavam conectadas.
Por sua vez, o Banco Interamericano de Desenvolvimento (BID) identificou que no período compreendido entre 2017 e 2018 a porcentagem de acesso à internet na América Latina e no Caribe era de 63% para os homens e 57% para as mulheres, enquanto o uso do telefone celular era de 80% para mulheres e 83% para homens. A World Wide Web Foundation informou também que os homens têm 21% mais probabilidades de estar on-line do que as mulheres, elevando-se a 52% nos países menos desenvolvidos do mundo. Veja: World Wide Web Foundation (2020). The gender gap in internet access: using a women-centred method. https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/. Consultado em 1° de fevereiro de 2021; CEPAL (2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19; BID (2020). ¿Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.

[16] Documentou-se também que os meninos tem 1,5 vez mais probabilidades de ter um telefone que as meninas. Veja: Jessica Posner Odede (2 de agosto do 2019). "Yes, technology can liberate girls around the world-but it must be managed properly". World Economic Forum. https://www.weforum.org/agenda/2019/08/getting-girls-online-first-step-achieving-gender-equality/. Consultado em 1° de fevereiro de 2021.

Não se deve perder de vista que esta disparidade de acesso básico à internet faz parte de uma brecha digital de gênero muito maior que envolve todas as formas em que as mulheres são menos capazes de usar a tecnologia, e que é agravada pela conjunção com outros fatores de exclusão, como o grau de escolaridade, a localização geográfica, idade, nível socioeconômico e origem étnica (Chair et al, 2020).

Documentou-se que as mulheres e meninas não só sofrem uma maior desconexão do mundo digital, mas, quando estas têm acesso à internet, não contam com uma conectividade significativa[17] e alcançam uma maior porcentagem de analfabetismo digital, o que implica que possuem menos habilidades para entender, controlar e gerar vínculos de confiança com a tecnologia[18]. Além disso, em comparação com os homens, as **mulheres possuem um nível mais baixo de competências em matéria de segurança digital,** o que impacta profundamente o gozo e exercício de seus direitos humanos on-line e sua possibilidade de navegar com liberdade e autonomia na web (Chair et al, 2020).

Existem também **limitações de tempo e conteúdo que as mulheres enfrentam ao acessar a internet** (Brown e Pytlak, 2020). Por exemplo, alguns estudos indicam que as mulheres têm 25% menos probabilidades que os homens de saber como aproveitar a tecnologia digital para realizar tarefas básicas (UIT, 2020b: 13)[19] e, em geral, é exíguo seu uso da internet com fins de empoderamento econômico ou para o exercício de seus direitos (Chair et al, 2020). As mulheres também permanecem alheias ao comércio on-line e ao dinheiro móvel, estimando-se que representam 56% das pessoas excluídas financeiramente da economia digital[20]. Além disso, dado que estas têm a seu cargo a maior parte do trabalho doméstico e de cuidado não remunerado, frequentemente dispõem de menos tempo para explorar o ciberespaço e desenvolver novas habilidades digitais e costumam ceder o uso dos dispositivos eletrônicos a outros membros da família quando há um número limitado em casa.

Estas disparidades no acesso e uso de internet e no nível de competência e cultura digital propiciam a perpetuação de desigualdades de gênero, inclusive desigualdades relacionadas com a pobreza informacional, pois "colocam as mulheres numa posição desfavorável em relação às oportunidades que as novas ferramentas digitais oferecem não só para o emprego, mas também para a participação política e social e o exercício dos direitos de cidadania" (Sainz et al, 2020).

[17] De acordo com Alliance for Affordable Internet, a conectividade significativa inclui contar com umbrais mínimos de acesso regular à internet, um dispositivo apropriado, dados suficientes e uma conexão rápida. Veja: Alliance for Affordable Internet. "Meaningful Connectivity- unlocking the full power of internet access". https://a4ai.org/meaningful-connectivity/. Consultado em 1° de fevereiro de 2021.
[18] World Wide Web Foundation (agosto de 2018), Advancing Women´s Rights Online: Gaps and Opportunities in Policy and Research. http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf; Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (2018). Bridging the Digital Gender Divide: Include, Upskill, Innovate. http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf; Araba Sey y Nancy Hafkin (eds.) (2019). Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University. https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf. Consultado em 1° de fevereiro de 2021.
[19] Na região, 35% das mulheres informaram não saber como usar um smartphone e 40% indicaram não saber como utilizar a internet. Veja: BID (2020). ¿ Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.
[20] World Bank Group (2018), "La base de datos Global Findex 2017. Medición de la inclusión financiera y la revolución de la tecnología financiera. Reseña", https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ovSP.pdf. Consultado em 1° de fevereiro de 2021.

Em particular, no **contexto da pandemia de COVID-19 a falta de acesso às TIC e os baixos níveis de alfabetização digital têm propiciado a exclusão das mulheres** das ações em matéria de saúde, educação[21] e trabalho que estão utilizando as tecnologias digitais para enfrentar a contingência e limitam seu acesso à informação e notícias públicas sobre medidas de isolamento e quarentena, bem como aos programas de apoio ou subsídios (CIM, 2020b; CEPAL, 2020: 5). Sem acesso nem habilidades digitais suficientes, as mulheres têm menos capacidade para receber informação vital, compreendê-la e atuar oportunamente (UIT, 2020a: 14), o que põe em risco sua saúde e seu bem-estar.

Por último, é importante ter em mente que, numa época de digitalização crescente como a que se vive atualmente, estas brechas digitais não só colocam as mulheres em situação de maior vulnerabilidade, mas impactam toda a sociedade em seu conjunto. Dado que as mulheres "desempenham um papel desproporcional como trabalhadoras da linha de frente, cuidadoras e educadoras, a brecha de gênero tem custos adicionais para as famílias, as comunidades e as economias" (Chair et al, 2020b: 5), que dependem delas para poder preservar seu bem-estar, sua saúde e, em muitos casos, sua vida.

B. A continuidade das realidades on-line/off-line: a discriminação de gênero e os impactos da pandemia de COVID-19 nas mulheres

> *O segundo elemento a ser considerado ao realizar uma análise dos impactos de gênero da pandemia no ciberespaço é o fato de que as experiências on-line e as ciberameaças que as mulheres enfrentam não podem ser separadas das realidades que elas vivem off-line (Brown e Pytlak, 2020), as quais são determinadas pelas condições sistêmicas de desigualdade que as afetam em todos os âmbitos de sua vida e que se agravaram durante a crise sanitária.*

Como reconheceu a ONU, as mulheres estão abaixo dos homens em todos os indicadores de desenvolvimento sustentável e representam a maior porcentagem de pessoas em situação de pobreza e sem acesso à educação[22]. Este **contexto de desigualdade se replica também na área das TIC**[23], onde a participação das mulheres apenas alcança um porcentagem aproximada de 20% (com 22% na área de inteligência artificial e 11% no âmbito da cibersegurança)[24], estimando-se que levará ao menos 100 anos para alcançar a paridade de gênero no setor das tecnologias digitais[25].

---

[21] Dado que com frequência não têm acesso a métodos de escolarização on-line (incluindo a falta de dispositivos eletrônicos e/ou de dados para conectar-se), as meninas e jovens também estão em risco de sofrer uma exclusão cada vez maior ante o fechamento geral das escolas durante a crise sanitária. Se levarmos em conta que as mulheres e meninas compõem a porcentagem mais alta de pobres no mundo e que os meninos têm 1,5 vez mais oportunidades que as meninas de ter um celular, é previsível que muitas meninas e adolescentes tenham sua educação truncada durante este período crítico, seja porque em sua casa não têm dados ou um dispositivo para conectar-se ou porque, se o têm, tradicionalmente muitas famílias valorizam mais a educação dos meninos do que a das meninas, sendo provável que estes utilizem os dispositivos disponíveis em casa. Veja: Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), ¿Cómo estás aprendiendo durante la pandemia de COVID-19? https://es.unesco.org/covid19/educationresponse; Vodafone Foundation, MITD-Lab e Girl Effect, Executive summary. Real girls, real lives, connected. A global study of girls' access and usage of mobile, told through 3000 voices, https://static1.squarespace.com/static/5b8d51837c9327d89d936a30/t/5bbe7cbe9140b7d43f282e21/1539210748592/GE_VO_Executive+Summary+Report.pdf

[22] No âmbito mundial, somente 49,6% das mulheres fazem parte da população economicamente ativa em comparação com 76% dos homens, e persiste uma disparidade salarial de 16%, que é uma causa fundamental de desigualdade em termos de renda ao longo de toda a vida das mulheres. Além disso, as mulheres continuam representando mais de dois terços das pessoas analfabetas no mundo e, apesar dos avanços registrados nos últimos anos, sua taxa de escolaridade continua sendo menor do que a dos homens (sobretudo na educação secundária e superior); as meninas enfrentam obstáculos tais como casamento forçado e gravidez precoce, violência de gênero e atitudes tradicionais que fazem com que a educação dos meninos seja privilegiada. A violência também continua sendo uma condição sistêmica que mantém as mulheres em situação de subordinação. Uma de cada três mulheres foi vítima de violência física ou sexual, principalmente por parte de um companheiro, situação qualificada como uma pandemia mundial estendida também ao ciberespaço. Veja: ONU Mulheres (25 de setembro de 2015). "Infografía: Igualdad de género- ¿Dónde nos encontramos hoy?"; Notícias ONU (14 de fevereiro de 2018). "Las mujeres están por debajo de los hombres en todos los indicadores de desarrollo sostenible", https://www.unwomen.org/es/digital-library/multimedia/2015/9/infographic-gender-equality-where-are-we-today; ONU Mujeres, "Mujeres y Pobreza". https://news.un.org/es/story/2018/02/1427081; https://beijing20.unwomen.org/es/in-focus/poverty. Consultado em 1° de fevereiro de 2021.

[23] PWC, "Women in Tech. time to close the gender gap". https://www.pwc.co.uk/who-we-are/women-in-technology/time-to-close-the-gender-gap.html. Consultado em 1° de fevereiro de 2021

[24] Fórum Econômico Mundial. "Assessing Gender Gaps in Artificial Intelligence". Global Gender Gap Index 2018, http://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/; The Conversation (2020). "The lack of women in cybersecurity put us all at greater risk". The Next Web. https://thenextweb.com/syndication/2020/06/28/the-lack-of-women-in-cybersecurity-puts-us-all-at-greater-risk/ Consultado em 1° de fevereiro de 2021.

[25] Cade Metz (21 junio 2019). "The gender gap in computer science research won't close for 1000 years". The New York Times. https://www.nytimes.com/2019/06/21/technology/gender-gap-tech-computer-science.html. Consultado em 1° de fevereiro de 2021.

Estas condições de desigualdade e vulnerabilidade foram magnificadas pela pandemia. Como sublinhou a Comissão Interamericana de Mulheres, "a emergência derivada da COVID-19 está provocando impactos específicos sobre as mulheres e aprofundando as desigualdades de gênero existentes" (CIM, 2020b: 4), sobretudo para as mulheres e meninas que enfrentam formas múltiplas de discriminação por fatores como raça, origem étnica, religião ou crença, deficiência, idade, orientação sexual, classe social e situação migratória (European Women's Lobby, 2020).

A pandemia elevou os níveis de pobreza das mulheres e afetou seu trabalho e as brechas de gênero no emprego. Antes da contingência sanitária, as mulheres ocupavam a maior parte dos empregos na área de serviços e dos empregos inseguros, precários e informais[26], setores especialmente afetados durante os últimos meses[27].

As mulheres constituem também 70% do pessoal do setor da saúde e de cuidados e assistência social e são a maioria do pessoal médico que se encontra na linha de frente de resposta à crise, assumindo maiores custos físicos e emocionais e maior risco de infecção[28] . Além disso, em diversos países têm sido vítimas de crescentes atos de discriminação, xenofobia eestigmatização devido à ansiedade e ao medo do contágio pela COVID-19 (ONU Mulheres, 2020d).

A isso se soma o fato de que para muitas mulheres aumentou o trabalho doméstico e de cuidados em detrimento de seu trabalho produtivo remunerado[29]. Antes da pandemia, as mulheres em todo o mundo faziam quase três vezes mais trabalhos domésticos e de cuidado não remunerados do que os homens, cifra que se elevou durante a contingência[30]. A saturação dos sistemas de saúde, o fechamento das escolas e as medidas de confinamento fizeram com que haja mais pessoas em casa que necessitam alimentos, cuidados e educação, e muitas mulheres tiveram que renunciar a seus empregos, reduzir suas jornadas de trabalho ou abandonar empregos de tempo integral para assumir trabalhos de cuidados e domésticos e a supervisão dos processos de aprendizagem de seus filhos, com importantes impactos em sua saúde física e mental, em sua independência e no tempo que têm disponível (CIM, 2020c; CIM 2021; ONU Mulheres 2020f).

O contexto gerado pela emergência aumentou a violência contra as mulheres e meninas, chegando-se a afirmar que, à sombra da pandemia de COVID-19, está ocorrendo também uma pandemia de violência de gênero (CIM, 2020a; ONU Mulheres, 2020c). Em todos os países foram registradas taxas mais elevadas de violência doméstica devido às medidas de confinamento, as quais aumentaram as tensões e conflitos dentro dos domicílios e o isolamento de mulheres e meninas, que se viram obrigadas a conviver permanentemente com agressores (CIM, 2020a). Segundo estimativas da ONU, por cada três meses que continue o confinamento, haverá 15 milhões de casos adicionais de violência de gênero em todo o mundo[31]. Isto certamente limitará seu acesso à internet e sua aquisição de habilidades digitais.

[26] A No âmbito regional, antes da pandemia 54% das mulheres trabalhavam no setor informal como empregadas domésticas, vendedoras ambulantes, agricultoras de subsistência e temporárias (aproximadamente 126 milhões de mulheres, segundo a Organização Internacional do Trabalho). Veja: ONU Mulheres. "Las mujeres en la economía informal". https://www.unwomen.org/es/news/in-focus/csw61/women-in-informal-economy. Consultado em 1° de fevereiro de 2021.

[27] De acordo com a Organização Internacional do Trabalho (OIT), a redução da atividade econômica afetou em primeiro lugar as trabalhadoras informais, que perderam sua renda intempestivamente e terão dificuldades para encontrar trabalho na já prognosticada recessão econômica. Veja: Organização Internacional do Trabalho (OIT) (2020). Policy Brief. A Gender-responsive employment recovery: Building back fairer.

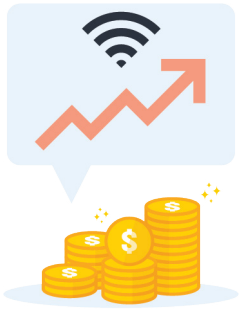
[28] Pesquisas revelaram que na Alemanha, Itália, Espanha e Estados Unidos a taxa de contágio de mulheres que trabalham na saúde é entre duas e três vezes mais alta do que a dos homens. Veja: Global Health 5050. The COVID-19 Sex-Disaggregated Data Tracker. https://globalhealth5050.org/the-sex-gender-and-covid-19-project/. Consultado em 21 de fevereiro de 2021.

[29] Estima-se que o tempo dedicado à educação dos filhos aumentou 36%, enquanto o tempo dedicado a realizar compras para a família aumentou 24%. Ver: ONU Mulheres (20 de outubro de 2020). "El avance de las mujeres hacia la igualdad se estanca" https://news.un.org/es/story/2020/10/1482722; Matt Krentz et al. (21 de maio de 2020). "Easing the COVID-10 burden on working parents". BGG; https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19; Richard Blundell et al. (11 de junho de 2020). "COVID-19: the impacts of the pandemic on inequality". Institute for Fiscal Studies. https://www.ifs.org.uk/publications/14879. Consultado em 1° de fevereiro de 2021.

[30] Nos Estados Unidos e na Europa, as mulheres assumiram uma carga extra de trabalho doméstico e de cuidado não remunerado de 15 horas semanais. Esta situação torna-se ainda mais crítica no caso das mulheres que são chefes de famílias monoparentais, que representam 75% no âmbito mundial. Além disso, as evidências indicam que durante a pandemia as mães têm maiores probabilidades do que os pais de perder seus empregos de maneira temporária ou permanente, registrando perdas de até 60% em sua renda. Veja: Matt Krentz et al. (21 de maio de 2020). "Easing the COVID-10 burden on working parents". BGG. https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19

[31] Nações Unidas (28 abril 2020). "Millones de mujeres sufrirán embarazos no deseados durante la pandemia de coronavirus". Noticias ONU. https://news.un.org/es/story/2020/04/1473572. Consultado em 1° de fevereiro de 2021.

Antes da pandemia de COVID-19, mulheres não conectadas em países do Sul Global já indicavam os altos custos como uma das principais razões para não acessar a internet (World Wide Web Foundation, 2015)[32], situação que será exacerbada pela perda de renda e empregos durante esta etapa.



Também deve haver impactos negativos no médio e longo prazo no desenvolvimento de habilidades digitais por parte de meninas e jovens ante as repercussões da pandemia em sua educação. Em anteriores surtos epidêmicos comprovou-se que o fechamento de escolas afeta desproporcionalmente as meninas, muitas das quais nunca retomam sua educação ao serem obrigadas a trabalhar para compensar a perda de renda familiar, ou ao serem vítimas de casamentos infantis, violência ou exploração sexual (ONU Mulheres, 2020e: 14-15). Assim, é muito provável que as alterações educativas durante a pandemia de COVID-19 significarão um obstáculo para o acesso e uso significativo da internet por parte de meninas e jovens; está comprovado que a educação é um dos fatores mais importantes da brecha de gênero no acesso às TIC: alguns estudos indicam que as mulheres com educação básica têm seis vezes menos probabilidades de estar na internet do que as que concluíram a educação média (World Wide Web Foundation, 2015).

A isso se somam as múltiplas formas de ciberabuso e violência on-line que aumentaram durante a crise da COVID-19 quase no mesmo nível do aumento da violência doméstica (APC, 2020; ONU Mulheres, 2020a; Brudvig et al, 2020). Conforme informado por diversas fontes, houve um aumento dos casos de abuso de gênero on-line de até 38% (Glitch UK, 2020), sendo comum a distribuição não consentida de imagens íntimas e atos de sextorsão, ciberbullying, ciberassédio e violência sexual on-line, bem como atos de *grooming* e exploração sexual facilitada pelas TIC contra mulheres e meninas (ONU Mulheres, 2020a; CIM, 2020a; Derechos Digitales, 2020)[33].

A violência on-line, que é uma das manifestações mais claras da desigualdade de gênero no ciberespaço, aumenta também a brecha digital que mulheres e meninas enfrentam; em consequência, elas se autocensuram ou decidem manter um perfil discreto na internet por temor de que sua privacidade ou segurança sejam violadas. Além disso, afeta sua capacidade para mover-se livremente e sem medo nos espaços on-line, negando-lhes a oportunidade de interatuar com as tecnologias para a construção autônoma de suas identidades digitais (REVM-ONU, 2018: par. 29)[34].

Conforme indicado na seção IV, estas condições de desigualdade e discriminação por motivo de gênero que afetam as mulheres se refletem no ciberespaço e são a base de muitas das ameaças cibernéticas que elas enfrentam, pois determinam os padrões de uso da internet e suas possíveis vulnerabilidades on-line.

[32] De acordo com a pesquisa Direitos Digitais das Mulheres da Fundação World Wide Web realizada em 10 países em desenvolvimento, o custo nesses países de dados pré-pagos de 1GB (equivalente a 13 minutos de internet por dia sem considerar custos de vídeo) era equivalente a 10% da renda per capita média, que é 10 vezes mais alto em relação à renda per capita nos países da OCDE e o dobro do que uma pessoa gasta em saúde nos países em desenvolvimento. Veja: World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment. http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf. Consultado em 1° de fevereiro de 2021.

[33] De acuerdo com um estudo realizado por Glitch UK e a coalizão End Violence Against Women, 46% das pessoas pesquisadas afirmaram ter sido vítimas de abuso on-line. Das pessoas que sofreram abuso on-line um año antes da pandemia, 29% indicaram que o abuso se tornou mais grave, cifra que aumenta para 38% no caso de mulheres negras ou pessoas não binarias.

[34] De acuerdo com pesquiusas mencionadas pela Relatora Especial da ONU sobre a violência contra a mulher, 28% das mulheres vítimas de violência de gênero on-line reduziram deliberadamente su presença on-line. Veja: Relatora Especial sobre a violência contra a mulher, sus causas e consecuencias (2018). Informe acerca de la violencia en línea contra las mujeres y niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. Organização das Nações Unidas.

C. Que sabemos acerca dos usos que as mulheres fazem da internet durante a pandemia de COVID-19?

> *Finalmente, como um terceiro elemento de análise é importante levar em consideração que os* ***usos da internet são condicionados quantitativa e qualitativamente pelo gênero das pessoas,*** *encontrando-se variações importantes entre a forma em que homens e mulheres navegam no ciberespaço e os objetivos que buscam ao conectar-se (Brown e Pytlak, 2020).*

Antes da pandemia, estudos na matéria registravam que os propósitos de uso da internet pelas mulheres estavam mais relacionados com o bem-estar social, comunicação com familiares e amigos (receber ou fazer chamadas e conversar) e buscar informação sobre saúde (Agüero, Bustelo e Viollaz, 2020; Sainz, 2020; Brown e Pytlak, 2020). Os homens, por sua vez, tendem a utilizar a internet para enviar mensagens, buscar informação sobre notícias, clima e transporte, acessar serviços bancários e realizar atividades de entretenimento, como videogames, escutar música ou ver vídeos. Além disso, costumam utilizar de forma mais intensiva e variada os dispositivos eletrônicos e fazem uso maior da internet para realizar atividades econômicas, de trabalho e administração, como, por exemplo, trâmites on-line (Agüero, Bustelo e Viollaz, 2020; Sainz, 2020).

Documentou-se também que as mulheres dependem mais da internet do que os homens para exercer certos direitos. Por exemplo, a internet pode lhes permitir acessar a educação se suas responsabilidades domésticas as impedem de frequentar um centro educativo, expressar-se se vivem em comunidades particularmente opressoras, acessar informação sobre direitos sexuais e reprodutivos quando não está disponível *off-line* ou proteger sua segurança pessoal em casos de violência doméstica (Brown e Pytlak, 2020).

Embora a digitalização acelerada durante a pandemia de COVID-19 tenha propiciado para todas as pessoas uma modificação radical nos hábitos de uso de dispositivos eletrônicos e da internet, **dados os papéis e normas de gênero que persistem dentro e fora do ciberespaço, é muito provável que durante e após a crise se mantenham algumas destas tendências de uso.** Conforme assinalado previamente, ainda faltam estudos na matéria que nos permitam conhecer com certeza como as mulheres estão utilizando a internet durante este período. Contudo, **podemos projetar alguns possíveis cenários a partir de tendências prévias de navegação e dos impactos que a pandemia** tem atualmente em suas vidas.

Já que durante esta etapa as mulheres assumiram em maior medida que os homens a carga de trabalho doméstico e de cuidado não remunerado, é de esperar que elas estejam usando preponderantemente a **internet como um meio para manter-se em contato com familiares e amigos,** a fim de estar ao corrente de seu estado de saúde, bem como para realizar compras de alimentos e medicamentos on-line, obter notícias sobre a evolução da doença e facilitar a educação à distância de seus filhos. Além disso, dado que elas constituem a maior parte do pessoal do setor da saúde, é possível que estejam utilizando a tecnologia para oferecer **teleconsultas e coordenar suas tarefas de cuidados e assistência** social nas comunidades.

Outros impactos da pandemia na vida das mulheres podem nos dar indícios adicionais sobre seus usos, necessidades e prioridades durante esta época quando acessam a internet. Por exemplo, dada a alta porcentagem de mulheres que trabalhavam como autônomas ou no setor informal, é previsível que algumas procurem manter seus negócios **incursionando em plataformas de *e-commerce* ou estejam acessando pela primeira vez sites de ofertas de trabalho** ante o grande aumento na taxa de desocupação feminina. Seguindo esta mesma lógica, e dado o número de meninas inscritas na educação primária, é previsível também que elas (e suas famílias) tenham sido obrigadas a vencer rapidamente estereótipos de gênero que as mantinham afastadas das tecnologias a fim de inscrever-se em aulas não presenciais.

Algumas outras tendências de uso já se confirmaram conforme avança a crise sanitária. Por exemplo, seguindo uma tendência anterior, as mulheres e jovens estão utilizando a internet durante esta época **para obter informação sobre sua saúde sexual e reprodutiva,** cujos serviços foram suspensos em muitas partes do mundo ante a redução de orçamentos e as medidas preventivas de distanciamento físico[35].

Além disso, ante o aumento da violência de gênero dentro e fora da internet durante esta etapa, as mulheres estão utilizando os dispositivos digitais como uma linha de defesa **para solicitar ajuda e manter contato com sua rede de apoio** por meio de serviços de mensagem instantânea com função de geolocalização, chamadas gratuitas a linhas de ajuda contra o abuso doméstico ou aplicativos que proporcionam apoio e informação a sobreviventes caso sejam vigiadas por seus abusadores. Também estão recorrendo em maior número à internet **para notificar e divulgar atos de violência de gênero** on-line cometidos contra elas e para criar redes de apoio a vítimas.

Sem dúvida, ainda falta muito por explorar quanto às experiências de uso da internet pelas mulheres e meninas durante esta etapa e seriam necessários mais estudos com perspectiva de gênero sobre os impactos da pandemia no novo ecossistema digital. Contudo, conforme assinalado anteriormente, uma leitura conjunta das dinâmicas de acesso e uso do internet por parte das mulheres, bem como dos impactos que a própria pandemia tem em suas vidas *off-line*, pode nos dar uma orientação preliminar para conhecer suas experiências digitais e, a partir disso, suas necessidades, interesses e vulnerabilidades quando acessam a internet.

[35] Ximena Casas (12 Mayo 2020). "Protecting Women's Reproductive Health During the Pandemic". Human Rights Watch. https://www.hrw.org/news/2020/05/12/protecting-womens-reproductive-health-during-pandemic. Consultado em 1° de fevereiro de 2021.

04 As ciberameaças e riscos específicos que as mulheres enfrentam no novo ecossistema digital: uma reflexão em curso

> *Ante a falta de estudos e dados desagregados por sexo sobre a prevalência do cibercrime durante a pandemia, esta seção* ***realiza uma projeção sobre quais são as possíveis ameaças que as mulheres enfrentam no ciberespaço durante a pandemia de COVID-19.***

Como examinaremos mais adiante, as experiências das mulheres no ciberespaço revelam que os riscos e ameaças que enfrentam on-line têm características específicas e as afetam de forma diferenciada em função dos papéis de gênero e da discriminação e desigualdade que vivem on-line e off-line (Brown e Pytlak, 2020).

Destaca-se que esta identificação de ciberameaças é enunciativa e não limitativa, pois, ante as constantes mudanças observadas no ciberespaço e nas interações *on-line/off-line*, é de esperar que o tipo de ameaças e riscos cibernéticos que as mulheres enfrentam mudem conforme a evolução da pandemia de COVID-19.

A. Um fator de risco comum: a falta de habilidades em matéria de segurança digital

Neste cenário de identificação de riscos, deve-se mencionar especialmente o nível de habilidades de segurança digital das mulheres. Este é um fator que determina em grande medida o tipo de ciberataques que elas enfrentam e as consequências em sua vida.

Conforme assinalado anteriormente, a pandemia de COVID-19 expos a carência generalizada de conhecimentos básicos para prevenir riscos e ameaças on-line e o alto grau de exposição a riscos cibernéticos. Contudo, ante as dificuldades que as mulheres enfrentam na aquisição de habilidades digitais em geral, e de cibersegurança em particular, elas se encontram em situação particularmente vulnerável face a ataques cibernéticos.

Além disso, ainda persistem estereótipos de gênero que as impedem de fortalecer a segurança digital. Muitas delas percebem o ciberespaço como um lugar irremediavelmente inseguro para mulheres e meninas, o que tem origem em preconceitos sobre sua suposta incapacidade natural para entender e controlar as tecnologias. A isto se somam também os efeitos da violência de gênero sistêmica que permeia o ciberespaço e normaliza as agressões on-line contra as mulheres.

Isto implica que um grande número de mulheres tem ao seu alcance muito poucos recursos para enfrentar comportamentos ilícitos e abusivos on-line, o que as coloca em situação de maior risco do que os homens face a certos ciberataques, muitos dos quais se dirigem contra quem pode ser um alvo fácil (UNODC, 2020).

Além disso, deve-se mencionar que esta falta de habilidades em matéria de cibersegurança tem efeitos em cadeia ao permear todas as interações digitais que as mulheres mantêm on-line e ir além do ciberespaço, dada a continuidade entre sua vida dentro e fora da internet. A segurança digital é também uma questão de direitos humanos, e o fato de que as mulheres se sintam inseguras on-line afeta não só seu acesso à internet, mas todas as oportunidades que este proporciona para exercer seus direitos *on-line e off-line*.

Esta falta de habilidades tem impactos em suas famílias e comunidades. Durante esta época de crise sanitária as mulheres assumiram a maior parte do trabalho de cuidado não remunerado e a supervisão dos processos de aprendizagem de seus filhos ante o fechamento das escolas, motivo pelo qual seu desconhecimento sobre as ameaças cibernéticas que as crianças e adolescentes ou idosos podem enfrentar na nova normalidade digital coloca também as pessoas sob seu cuidado em situação de risco[36].

B. Explorando alguns riscos que as mulheres enfrentam na nova normalidade digital

Embora ainda falte muito por conhecer acerca da dimensão de gênero dos incidentes de segurança e ameaças específicas que as mulheres enfrentam no ciberespaço durante a pandemia de COVID-19, ao realizar um análise dos ciberataques mais comuns notificados no mundo durante a pandemia de COVID-19, em conjunto com as experiências das mulheres dentro e fora do ciberespaço, podemos identificar alguns tipos de ameaças on-line que as estariam afetando especialmente:

Certo tipo de fraudes e golpes através de campanhas de *phishing* ou difusão de *malware*.

Ante o papel preponderante que as mulheres têm durante a crise sanitária no trabalho doméstico e de cuidado não remunerado de famílias e comunidades, pode-se estimar que o tipo de ataques de phishing que significariam maior risco para elas estão relacionados a compras de alimentos e medicamentos ou informação de saúde.

[36] No caso do cuidado de crianças e adolescentes, por exemplo, a falta de conhecimento dos processos de educação virtual e medidas básicas de proteção digital pode colocá-los em maior risco de grooming, violência sexual, sextorsão ou acesso a informações falsas.

Fraudes e golpes dirigidos contra mulheres que realizam comércio on-line, usam dinheiro móvel ou recebem transferências de programas sociais.

Já que antes da pandemia as mulheres representavam mais da metade das pessoas financeiramente excluídas da economia digital, é previsível que os ciberataques se dirijam especificamente contra novas usuárias dada sua falta de familiaridade com as ferramentas financeiras digitais e de conhecimentos de cibersegurança para proteger suas transações on-line. É previsível também que estes ataques tenham maiores impactos na economia das mulheres do que no caso de ciberataques dirigidos a homens, dadas as taxas elevadas de desigualdade de gênero no emprego e na renda.

Fraudes via *phishing* dirigidas contra mulheres de idade avançada.

Alguns relatórios indicam um aumento de ataques a pessoas de idade avançada durante esta etapa na forma de e-mails fraudulentos, chamadas telefônicas ou serviços de mensagem instantânea, mediante os quais os cibercriminosos se fazem passar por alguém de confiança para a vítima (como o banco ou pessoal médico) a fim de obter dados pessoais. No contexto atual de maior uso da internet, as mulheres idosas são especialmente vulneráveis a ciberataques, dada sua carência de habilidades informáticas em geral, e de segurança digital em particular, que é maior do que a dos homens do mesmo grupo de idade[37].

Campanhas de desinformação.

A infodemia e a distribuição de informação falsa são riscos on-line que afetam particularmente as mulheres, dado o uso preponderante que elas fazem da internet para obter notícias relacionadas com a saúde. Estudos demostram que existe uma forte dimensão de gênero nas atividades de desinformação, dado que a identidade de gênero e a orientação sexual podem ser a base para que alguém receba informação ao se fazer suposições sobre os interesses da pessoa e sua capacidade de ser influenciada (Brown e Pytlak, 2020).

[37] As mulheres estão sobrerrepresentadas entre as pessoas idosas (representam 57% das pessoas com mais de 70 anos e 62% das que têm mais de 80 anos) e são três vezes mais propensas que os homens a viver sozinhas. Estudos realizados na Europa indicam que somente 48% das pessoas maiores de 65 anos contam com habilidades digitais e que as mulheres idosas têm menos habilidades que os homens idosos com uma diferença de 10 pontos. Registrou-se que somente metade das pessoas entre 65 e 74 anos que usaram a internet no último ano contava com algum tipo de software ou ferramenta de segurança informática em seus dispositivos, enquanto 13% indicaram não a conhecer. Além disso, grande número de pessoas idosas não utiliza senha em seus dispositivos por medo de não se lembrar ou utiliza senhas que são facilmente identificáveis por hackers. A empresa de segurança informática McAfee indicou que 50% dos usuários de redes sociais maiores de 60 anos compartilham voluntariamente informação pessoal com indivíduos que não nunca viram pessoalmente e sem nenhuma segurança. Veja: Abby Ellin (12 de setembro de 2019). "Scammers Look for Vulnerability, and find it in Older People". The New York Times. https://www.nytimes.com/2019/09/12/business/retirement/scams-elderly-retirement.html; ONU Mulheres (maio de 2020). "Informe de políticas: Los efectos de la COVID-19 en las personas de edad". https://www.un.org/sites/un2.un.org/files/old_persons_spanish.pdf; Enrique Arieas Fernandez et al. (2018). "Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria". Prisma Social. Revista de Ciencias Sociales. No. 21. https://revistaprismasocial.es/article/view/2458. Consultado em 1° de fevereiro de 2021.

Ataques via *software*, redes ou ferramentas de trabalho remoto.

É comum que os ciberatacantes se aproveitem do uso distraído de ferramentas de trabalho remoto para ingressar nos sistemas corporativos, o que é um risco latente quando a pessoa que trabalha é afetada pelo cansaço ou fontes de distração constantes, como é o caso das mulheres que durante esta etapa têm que combinar o trabalho produtivo remunerado com o aumento das atividades domésticas e de cuidado não remuneradas, suportando uma dupla ou mesmo tripla jornada de trabalho (CIM, 2020c; ONU Mulheres, 2020f).

Ataques de *ransomware* a hospitais através dos dispositivos eletrônicos das mulheres que integram o pessoal médico.

Embora falte realizar pesquisas nessa matéria, é previsível que os ataques de *ransomware* a hospitais ou centros de saúde tenham um componente de gênero, já que as mulheres constituem a maioria das pessoas que trabalham no setor e podem ser um alvo fácil de ciberataques ante seu menor grau de conhecimentos de segurança digital em comparação com os homens que trabalham no setor da saúde.

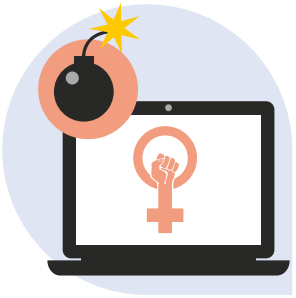
Violência de gênero on-line.

Comprovou-se que a violência de gênero on-line contra as mulheres aumenta de forma diretamente proporcional ao seu acesso à internet (REVM-ONU, 2018; EIGE, 2017; Van Der Wilk, 2018;). Seguindo esta tendência, estudos feitos durante a crise sanitária comprovaram que, ante o aumento de sua participação no ciberespaço, as mulheres estão sendo vítimas de forma desproporcional de ciberassédio, ciberbullying, distribuição não consentida de imagens íntimas e sexuais, doxing, violência sexual, recebimento de imagens e vídeos sexuais sem consentimento e ameaças de violência sexual (ONU Mulheres, 2020a; Glitch UK; APC, 2020).

Além disso, seguindo tendências observadas antes da pandemia, a violência de gênero digital está afetando particularmente mulheres ativas em redes sociais, como, por exemplo, jornalistas que informam sobre a evolução da doença, ativistas, *bloggers*, defensoras de direitos humanos e mulheres com um perfil público que utilizam as redes sociais para promover a igualdade de gênero e que informaram ser vítimas de campanhas de desinformação e desprestígio (AI, 2018; REVM-ONU, 2018; ONU Mulheres, 2020a)[38].

[38] Veja: Julie Posetti et al. (2020). Online violence against women journalists. A global snapshot of incidence and impacts. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136. Consultado em 1° de fevereiro de 2021; Maria Giovanna Sessa (4 de dezembro de 2020). "Misogyny and Misinformation: An analysis of Gender Disinformation Tactics during the COVID-19 Pandemic". EU Disinfo Lab. https://www.disinfo.eu/publications/misogyny-and-misinformation:-an-analysis-of-gendered-disinformation-tactics-during-the-covid-19-pandemic/. Consultado em 1° de fevereiro de 2021.

Ataques a organizações feministas ou grupos de mulheres que trabalham no âmbito da igualdade de gênero e direitos sexuais e reprodutivos.



Documentou-se também que a violência de gênero on-line se dirige de forma específica a organizações de mulheres que utilizam a internet durante esta etapa para se manterem conectadas e organizar-se, reivindicar seus direitos e prestar apoio e acompanhamento a vítimas de violência de gênero. Estas organizações informaram sabotagens de chamadas de vídeo e ataques via *zoombombing*[39] mediante o envio de material sexualmente explícito, racista e sexista, ataques a seus canais de expressão mediante hackeamento das páginas de internet, redes sociais ou contas de e-mail e ataques de negação de serviço (DDoS), entre outros (APC, 2020).

Estratégias de sextorsão digital.

Comprovou-se que este ataque, cujos índices aumentaram de forma significativa durante a pandemia, tem um importante componente de gênero, concentrando-se preponderantemente em mulheres, jovens e meninas[40], dado que a difusão pública de imagens íntimas tem maiores consequências para elas ante as normas e estereótipos de gênero em torno do controle da sexualidade feminina[41]. O aumento deste cibercrime é consequência de uma combinação de fatores, entre os quais podemos destacar as medidas de distanciamento físico e a necessidade de manter proximidade com outras pessoas utilizando as ferramentas virtuais, práticas inseguras de *sexting* e golpes de sextorsão via *phishing*.

Grooming e assédio sexual de meninas e adolescentes.

Com o aumento do tempo on-line registrou-se um aumento paralelo na vigilância, assédio, contato sem consentimento e imposição de condutas de caráter sexual indesejadas contra menores de idade, ciberataques realizados através de espaços de interação, como jogos on-line, redes sociais e salas de chat (INTERPOL, 2020).

[39] Véase: Lizle Loots et al. (14 abril 2020). "Online safety in a changing world- COVID-19 and cyber violence". Sexual Violence Research Initiative. http://www.svri.org/blog/online-safety-changing-world-%E2%80%93-covid-19-and-cyber-violence; Sophie Davies (18 marzo 2020). "Risks of online sex trolling as coronavirus prompts home working". https://www.reuters.com/article/us-women-rights-cyberflashing-trfnidUSKBN2153HG. Consultado el 1° de febrero de 2021.

[40] Benjamin Wittes et al (11 mayo 2016). "Sextortion: Cybersecurity, teenagers, and remote sexual assault". Brookings. https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases; Katherine Kelley (19 marzo 2019). "New Data on Sextortion: 124 additional public cases". Lawfare. https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/. Véase también: Claudia Long (3 junio 2020). "Coronavirus shutdown prompts spike in reports of sextortion toe Safety Commissioner", ABC News. https://www.abc.net.au/news/2020-06-03/spike-reports-esafety-commissioner-coronavirus-shutdown/12314442 Consultado el 1° de febrero de 2021.

[41] Christina Elia (11 agosto 2020). "My sextortion birthday: Digital violence during COVID-19". Genderit.org. https://genderit.org/feminist-talk/my-sextortion-birthday-digital-violence-during-covid-19. Consultado el 1° de febrero de 2021.

Embora ainda falte coletar dados desagregados por sexo sobre a prevalência destes cibercrimes, pode-se estimar que o *grooming* e assédio sexual são um risco cibernético que afeta particularmente mulheres e meninas. Pesquisa realizadas antes da pandemia confirmaram que elas têm o dobro de probabilidades de ser assediadas sexualmente na internet[42] e que os tipos de comentários violentos que recebem on-line são qualitativamente diferentes dos que recebem os meninos e rapazes, baseando-se em sua aparência física e incluindo ameaças de violência sexual[43].

Exploração sexual e tráfico de mulheres e meninas facilitado pelas novas tecnologias.

Levando em consideração tendências observadas antes da pandemia, pode-se estimar que as mulheres e meninas têm maior risco de serem vítimas da rede internacional de tráfico de pessoas em consequência do aumento em seus níveis de pobreza. Estudos na matéria documentaram que 80% das vítimas de tráfico de pessoas são mulheres, número que ascende a 95% em casos de exploração sexual[44].

[42] Angus Reid (2016). Trolls and Tribulations: One-in-Four Canadians Say They're Being Harassed on Social Media. http://angusreid.org/wp-content/uploads/2016/10/2016.10.04-Social-Media.pdf

[43] De acordo com um estudo de Plan International, quase 60% das meninas e adolescentes de todo o mundo foram vítimas de diferentes formas de ciberassédio on-line, enfrentando esta forma de violência a partir dos 8 anos. Veja: Plan International (2020). Inseguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online. https://plan-international.es/inseguras-online. Consultado em 1° de fevereiro de 2021.

[44] Parlamento Europeu (2016). Briefing. The gender dimension of human trafficking 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf; Sylvia Walby et al. (2016). Study on the gender dimension of trafficking in human beings. Final Report. Comissão Europeia. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf

05 A segurança digital das mulheres no novo ecossistema digital: um núcleo duro de medidas de autocuidado

> *A identificação dos possíveis riscos que as mulheres enfrentam na nova normalidade digital é apenas o primeiro passo na construção de uma cultura de cibersegurança atenta ao gênero. Já que não se conta com informação de qualidade sobre as características desses novos cenários, é necessário determinar estes riscos digitais a fim de gerar um esquema de autocuidado para as mulheres.*

Esta identificação de riscos deve ser acompanhada de esforços específicos de todos os setores envolvidos para visibilizar as ferramentas que permitam às mulheres proteger-se e navegar seguras e com confiança, no pressuposto de que no ciberespaço existe um contexto de risco e discriminação que as afeta pelo simples fato de serem mulheres, e que é um reflexo do mesmo contexto de violência por razões de gênero presente na vida off-line.

Conforme mencionado anteriormente, a falta de práticas pessoais de segurança digital por parte das mulheres é um problema generalizado em consequência da pouca informação de qualidade que recebem. Esta falta de adoção de medidas de segurança digital não é um problema atribuível às mulheres; pelo contrário, são necessários mais esforços por parte dos atores implicados para fechar a brecha de gênero na alfabetização digital e diminuir os impactos negativos dos estereótipos de gênero que as afastam do controle das tecnologias.

Diante disso, uma das principais mensagens a destacar numa estratégia de cibersegurança com perspectiva de gênero é que, apesar de o ciberespaço ser um ambiente que implica riscos, as mulheres não estão irremediavelmente condenadas a serem vítimas, mas é preciso proporcionar-lhes a informação necessária para proteger-se e para prevenir ciberataques e atos de violência on-line mediante a implementação de medidas básicas de autocuidado.

Além disso, é de suma importância ter em mente que a identificação destas práticas de segurança digital não deve ser entendida no sentido de colocar a responsabilidade nas mulheres e meninas pela violência on-line e pelos ciberataques cometidos contra elas, responsabilidade que recai invariavelmente nos atacantes e cibercriminosos responsáveis pelos danos, que devem ser punidos por estas condutas.

Tendo em vista os riscos que enfrentam, nesta seção condensou-se um núcleo duro de medidas básicas de proteção para mulheres durante a atual crise sanitária. É crucial promover sua adoção paralelamente ao desenvolvimento de políticas de cibersegurança focadas na identificação das condições que facilitam estes ciberataques e na persecução e punição dos responsáveis.

A. Kit básico de medidas de segurança digital para a nova normalidade

Adotar uma política pessoal de cibersegurança em resposta à pandemia

- **Dar-se conta de que é um alvo. A conscientização é a primeira linha de defesa** contra as novas ameaças cibernéticas surgidas durante a pandemia.
- É importante realizar um **exercício pessoal de análise de risco:** Quais são as novas condutas de risco adotadas ante o aumento do tempo *on-line* e o uso de novas ferramentas (por exemplo, navegando por sites que não são habituais, instalando aplicativos desconhecidos ou fazendo compras em sites pouco seguros)? O que estou fazendo para me proteger de possíveis ataques?
- **Precaução acima de tudo.** É crucial manter-se vigilante e ter muita precaução na forma como se interage no mundo digital. Agora que a pandemia forçou a adoção de novas tecnologias num curto período de tempo, é importante planejar, treinar e se fortalecer em proteção digital, já que cada passo no ecossistema digital tem o potencial de criar riscos.
- O êxito dos **ciberataques frequentemente depende de erros humanos.** Quando as pessoas estão em um estado prolongado de estresse, tensão ou cansaço ou estão distraídas são mais propensas a cometer erros e a baixar a guarda frente a possíveis riscos cibernéticos.
- **A busca de informação sobre a COVID-19 é especialmente importante.** Muitos dos ataques atuais se dirigem a quem busca informação sobre a pandemia; por isso, deve-se confiar unicamente em sites oficiais ou verificados, não só pela qualidade da informação, mas pelo aumento no número de sites maliciosos que exploram essa necessidade de informação.
- **O cibercrime está se aproveitando do medo e da incerteza** que a COVID-19 provoca e se adapta às notícias locais sobre o desenvolvimento da pandemia. As "iscas" quase sempre replicam as notícias no âmbito nacional e se adaptam à localização das vítimas.

- Muitos **ataques não ocorrem de forma isolada, mas combinada.** Por exemplo, um acesso não autorizado a um dispositivo eletrônico pode facilitar uma fraude ou o hackeamento de uma conta de redes sociais pode servir para disseminar *spam* promovendo compras fraudulentas de produtos médicos.

- É **fundamental estar atenta e informada** acerca de novos enganos e ameaças cibernéticas e as possíveis respostas.

- **Conversar com a família**, inclusive crianças e idosos, sobre a importância de se proteger *on-line*. Deve-se promover em família uma corresponsabilidade digital, já que o cuidado em ambientes digitais compreende não somente práticas individuais, mas também o cuidado e segurança de outras pessoas.

Senhas seguras são a primeira linha de proteção

As senhas são o primeiro passo para acessar contas e dispositivos e, portanto, oferecem uma primeira capa de proteção ante ameaças e ciberataques. Por isso, uma parte crucial da segurança digital continua sendo ter bons hábitos pessoais com relação às senhas *on-line*.

- É importante contar com **senhas únicas, longas, aleatórias e difíceis de prever** (não devem conter informação pessoal).

- Para oferecer uma proteção efetiva, as senhas têm que incluir uma mistura de pelo menos 12 letras **maiúsculas e minúsculas, números e caracteres especiais.**

- Deve-se utilizar uma **senha diferente para cada conta e mudá-la frequentemente**, em especial a das contas mais confidenciais

- Usar geradores automáticos e/ou **administradores de senhas *on-line***, os quais criam senhas aleatórias e seguras para cada uma das contas.

- Utilizar as **perguntas de segurança** nos sites que disponibilizam esta opção, mas sem respondê-las com informação pessoal.

- Não guardar as senhas na configuração do navegador, na nuvem ou em um documento pouco seguro dentro do computador ou celular.
- Não compartilhar senhas através de uma conexão não segura, como mensagens de texto ou SMS.
- Para acrescentar uma segunda capa de proteção, **ativar a verificação em dois passos** (autenticação de dois fatores ou 2FA) que se encontra disponível no correio eletrônico e redes sociais.

Navegação segura

- Conectar-se unicamente em redes **Wi-fi privadas e confiáveis.**
- Nas redes domésticas é importante que o roteador não possa ser acessado do exterior e que conte com uma senha de administrador forte e difícil de adivinhar. Também é preciso monitorar com regularidade quais são os equipamentos conectados à rede.
- Assegurar-se de **navegar sempre de modo seguro.** Sempre verificar que o endereço no qual se está navegando seja reconhecido pelo protocolo de segurança HTTPS, sobretudo para compras on-line, movimentações bancárias ou quando se envia informação sensível e dados pessoais. Estas páginas também podem ser identificadas por ter um cadeado verde na barra do navegador, o que significa que a informação circula com criptografia de ponta a ponta.
- Instalar complementos para bloquear publicidade, rastreadores e software malicioso no navegador.

Outras medidas de proteção básicas

- **Fazer backup periodicamente** de todos os dados e informações pessoais importantes, cifrá-los e armazená-los em um disco rígido ou na nuvem. Uma cópia de segurança feita de forma oportuna e regular pode evitar a perda de materiais e dados sensíveis no caso de hackeamento de dispositivos e ataques de ransomware.

- Utilizar a versão mais atualizada de um **software antivírus**. Embora os antivírus não possam detectar todos os *malwares*, oferecem uma capa de proteção adicional aos dispositivos.

- Manter o sistema operacional, navegador e aplicativos nos **dispositivos** eletrônicos sempre atualizados, o que não só ajuda a serem mais rápidos, mas oferece maior segurança, já que podem proteger de ameaças e reforçar as vulnerabilidades das versões anteriores.

- Cuidar da informação pessoal. Não a compartilhar em sites não seguros ou publicá-la em redes sociais.

- Revisar e se familiarizar com as opções de **privacidade e segurança de contas de redes sociais** e verificar qual informação pessoal está exposta em redes.

- Desconfiar de mensagens sobre a COVID-19 e links ou arquivos anexos suspeitos ou promoções demasiado atraentes.

- **Examinar com cuidado os aplicativos sobre a COVID-19** que se instalam nos dispositivos eletrônicos, já que muitos deles imitam fontes fidedignas, como a OMS.

- Baixar aplicativos ou qualquer outro **software exclusivamente de plataformas seguras** (Google Play Store ou App Store), desconfiar de aplicativos que pedem permissões desnecessárias no dispositivo e revisar as qualificações de outras pessoas usuárias. Revisar os aplicativos que já não são utilizados e eliminá-los, pois podem ser uma porta de entrada para *malware*.

B. Medidas de segurança digital contra riscos específicos

a. Proteção contra phishing e smishing

Uma das formas mais comuns que os atacantes atualmente utilizam para instalar *malware* em computadores ou celulares é através de ataques de *phishing* ou pesca de dados fraudulenta. Este tipo de ciberataque baseia-se no envio fraudulento de correios, mensagens SMS ou mensagens instantâneas em redes sociais (Whatsapp) que parecem inocentes porque suplantam a identidade de uma pessoa, empresa ou entidade reconhecida, mas na realidade disfarçam programas maliciosos ou redirecionam a sites falsos para arrecadar informação pessoal, nomes de usuários, palavra-chave, senhas ou dados bancários. Através de ataques de *phishing* cibercriminosos podem também tomar controle dos dispositivos e de toda a informação armazenada.

Durante a pandemia, muitas destas tentativas de phishing suplantaram a identidade de entidades de governo ou organizações de saúde ou filantrópicas, apresentando informação sobre a COVID-19, atualizações sobre o desenvolvimento da doença, supostas curas, vacinas e material médico, apoios governamentais, benefícios fiscais, falsas ofertas de trabalho ou serviços gratuitos. Outros ataques comuns são os de *smishing*, mediante os quais se envia um SMS se fazendo passar por uma entidade do governo compartilhando um link onde se solicitam dados pessoais.

Recomendações de autoproteção:

- A melhor estratégia é **tomar consciência sobre a recorrência das tentativas de phishing.** Como regra geral, desconfie ao receber um e-mail ou mensagem estranha ou de um usuário desconhecido que solicite informação privada ou a realização de ações rápidas ou de urgência ou seja ameaçador.
- **Suspeitar de todos os e-mails sobre a COVID-19**, especialmente se não reconhecer o endereço eletrônico.

- **Suspeitar também de cadeias de WhatsApp.** Circulam via WhatsApp milhares de mensagens com links para uma grande variedade de sites onde supostos especialistas oferecem recomendações e soluções sobre o vírus. Grande parte dessas mensagens contém links maliciosos ou busca desinformar.

- Suspeitar se a mensagem tem **erros gramaticais ou semânticos, um desenho ou qualidade suspeita** e se não está personalizada (que diga, por exemplo, 'prezado colega', 'estimado amigo', 'querido cliente').

- Revisar com atenção o remetente e o endereço.

- **Não clicar nos links** recebidos através de uma mensagem sobre a COVID-19 (de texto, WhatsApp ou e-mail), ainda que pareçam ser de uma fonte oficial como o Ministério da Saúde ou a OMS. Muitos desses links redirecionam a sites falsos onde se engana para identificar ou introduzir dados confidenciais que os golpistas utilizam para acessar os dispositivos e roubar dinheiro.

- **Proteger a informação pessoal.** Nenhuma fonte oficial solicita dados por e-mail.

- **Não abrir arquivos anexos** de mensagens estranhas nem acessar ou baixar links ou arquivos pouco confiáveis (sobretudo se têm terminação .exe). Se há dúvidas e o arquivo anexo parece importante, pode-se abrir dentro do Google Drive para maior proteção.

- Escanear links suspeitos utilizando ferramentas como VirusTotal (embora esta ferramenta não reconheça todos os tipos de malware, pode revelar alguns programas maliciosos comuns).

- **Não responder** em nenhum caso a essas mensagens. Se tiver dúvida, consulte diretamente a empresa ou serviço que representa para confirmar a veracidade da mensagem, pois é possível que tenham falsificado ou hackeado seu e-mail.

- **Contar com firewall** instalado (as versões mais recentes de Windows e Mac OS já têm firewall pré-instalado, e também pode-se utilizar ferramentas como Comodo Firewall, ZoneAlarm e Glasswire).

- Bloquear os anúncios integrados em sites ou anúncios emergentes, pois podem levar a baixar arquivos maliciosos (pode-se utilizar complementos como uBlock Origin para evitar clicar nesses anúncios emergentes).

- No caso de publicações de ofertas de trabalho, revisar o site da empresa e a redação da oferta, não revelar informação privada, revisar a política de proteção de dados e utilizar portais confiáveis de busca de emprego.

b. Teletrabalho seguro

Para muitas mulheres esta época de confinamento significou começar o teletrabalho e dentro de sua casa combinar o trabalho produtivo remunerado com o trabalho doméstico e de cuidado não remunerado. Nesta nova normalidade digital, é necessário tomar precauções especiais, pois as redes domésticas podem não estar corretamente configuradas e/ou controladas, o que poderia supor a abertura da porta da empresa aos cibercriminosos ou o envolvimento em uma brecha de segurança acidental. Além disso, a dupla carga de trabalho pode gerar cansaço e distrações que tornam as mulheres mais vulneráveis do que os homens que trabalham de forma remota e sem o mesmo grau de responsabilidades no lar.

- **Sempre se conectar em uma rede Wi-fi segura** (não pública) e configurar de maneira segura a rede doméstica sem fio (mudar a senha padrão do roteador e atualizá-la regularmente), o que oferecerá maior proteção face a acessos não autorizados à informação da organização por parte de cibercriminosos. Se possível, conectar-se ao ambiente corporativo utilizando uma rede privada virtual (VPN), que cria uma conexão privada e cifrada.

- Manter a informação de trabalho no computador do trabalho e evitar usar o computador ou dispositivos pessoais para questões de trabalho. **Separar contas pessoais das contas de trabalho**, inclusive de correio eletrônico e redes sociais.

- Fazer uma **criptografia completa** dos dispositivos de trabalho.

- Se não contar com dispositivos corporativos para trabalhar, instalar no dispositivo pessoal um sistema de detecção proativa de ameaças, que se obtém instalando uma solução integral de segurança e mantendo-a atualizada.

- Prestar atenção na instalação de programas, pois o download de um *software* malicioso pode pôr em risco a segurança de toda a organização.

- Realizar backups periódicos da informação.

- Verificar sempre se está no site legítimo da empresa antes de introduzir os dados de acesso ou informação confidencial. Além disso, contar com senhas robustas e utilizar fator duplo de autenticação para acessar contas importantes.

- Utilizar de forma segura as ferramentas colaborativas na nuvem.
- Tomar precauções de segurança ao fazer videoconferências.
- Se for preciso enviar informação confidencial ou delicada, é conveniente utilizar um serviço que encripte a informação e não o fazer por mensagem instantânea.
- Estar atenta a tentativas de *phishing* e e-mails externos e solicitações incomuns das credenciais de acesso (inclusive chamadas telefônicas inesperadas da equipe de suporte de tecnologia da empresa solicitando as credenciais de acesso).
- Ter sempre à mão os contatos de suporte tecnológico e, se ocorrer um incidente de segurança, denunciá-lo o quanto antes.

c. Realizar reuniões on-line seguras

Durante a pandemia, os aplicativos de chamada de vídeo se converteram em ferramentas imprescindíveis para continuar com as atividades cotidianas. Muitos atacantes se aproveitaram da popularidade das ferramentas de videoconferência (Zoom, Webex, Hangout, Skype) para distribuir malware ou acessar e boicotar reuniões (*zoombombing*); por isso, deve-se garantir a segurança para prevenir a intrusão e garantir a confidencialidade das conversas e da informação compartilhada.

Algumas medidas de proteção básicas a serem adotadas:

- **Controlar a privacidade da reunião.** Exigir senhas para acessar a reunião (muitos aplicativos já o fazem como padrão).
- Conhecer a política de privacidade do aplicativo de chamada de vídeo (Como trata a informação confidencial?).
- **Ter precaução com a convocação e acrescentar somente contatos.** Fazer convites pessoais, evitar o uso de canais de comunicação inseguros para lançar a convocação e solicitar uma pré-inscrição.

- Ativar a sala de espera, onde pode-se verificar a identidade de cada participante antes de admiti-los na reunião. É importante verificar que o usuário que desejar entrar tenha nome e sobrenome previamente identificados.
- Se for feita uma videoconferência pela primeira vez com um contato novo, **verificar sua identidade** por outros meios.
- Uma vez que os participantes forem incorporados na chamada, **bloquear o acesso** a novas pessoas para assegurar que intrusos não possam entrar e espiar as conversas.
- Baixar o aplicativo do site oficial ou repositórios oficiais (Google Play ou Apple Store).
- Ativar as **atualizações automáticas do *software*** e aceitar cada vez que o solicitar, pois ajuda a ter as características mais recentes e a versão mais segura.
- **Aplicar a criptografia** de forma predeterminada e assegurar que seja do início ao fim.
- **Ter cuidado ao compartilhar arquivos e telas,** pois poderiam revelar acidentalmente informação confidencial ou ser utilizados para difundir programas maliciosos.
- **Desabilitar o compartilhamento de tela e arquivos e o recebimento de vídeo** como padrão (default).

d. . Internet banking e compras on-line

- Utilizar uma senha segura para as contas bancárias on-line e a autenticação por fator duplo.
- Instalar *software* de segurança em todos os dispositivos utilizados para compras on-line ou movimentações bancárias e mantê-los atualizados.
- **Não utilizar computadores públicos ou redes de wi-fi públicas** para fazer movimentações bancárias, pois isto aumenta as possibilidades de que pessoas estranhas possam acessar a informação bancária.
- É recomendável utilizar um só cartão de crédito para transações on-line a fim de expor ao mínimo a informação bancária.

- Revisar a conta bancária frequentemente para detectar atividades suspeitas.
- Estar **prevenida para tentativas de golpe através de mensagens de *phishing*** nas quais se solicita os dados da conta bancária ou se redireciona a sites para ingressar estes dados. Se houver dúvida sobre a veracidade da mensagem, contatar diretamente o banco para corroborar sua legitimidade.
- Uma cura para a COVID-19? Não se deixe enganar por ofertas on-line e mantenha-se alerta. Se uma oferta é boa demais para ser verdade, provavelmente é falsa.
- Criar um **e-mail exclusivo para compras on-line.**
- Convencer-se da fiabilidade dos provedores antes de comprar on-line. Comprar sempre de vendedores estabelecidos, reconhecidos e confiáveis, revisar a antiguidade de suas atividades, suas qualificações on-line e seu histórico de venda.
- Fazer compras on-line com provedores que utilizam sites seguros para as transações e pagamentos. Um site seguro terá "https://" no endereço do site, e às vezes um ícone de cadeado fechado na barra de endereço do navegador.
- Desconfiar se a página não tiver aviso legal com informação sobre a empresa, condições de venda, devoluções e reclamações, entre outras coisas.
- Verificar todos os detalhes dos bens e serviços que estão sendo comprados (descrição do produto, cobrança pelo envio, moeda e taxa de câmbio, termos e condições, garantia, devoluções).
- Notificar se houver fraude.

e. Infodemia e campanhas de desinformação

A pandemia de COVID-19 tem sido acompanhada de uma infodemia, a qual gerou ansiedade e confusão ante o excesso de informação que circula em tuítes, mensagens de Facebook, cadeias de WhatsApp, vídeos e notícias. Esta saturação de informação torna complicado discernir entre

a informação que é confiável e útil e a que busca confundir, o que dificulta para as pessoas guiar suas ações e decisões em momentos críticos como os que se vivem agora.

A informação que circula cotidianamente através da internet é composta por um conjunto de notícias falsas, campanhas de desinformação e manipulação, teorias conspiratórias, rumores, mitos e pseudociência sobre os efeitos da COVID-19 e informação para promover supostas curas, tratamentos e vacinas, o que é um cenário perfeito para fraudes e enganos. Tornar-se vítima desta infodemia ou sobrecarga informativa pode afetar a economia pessoal, elevar os níveis de ansiedade e produzir graves danos à saúde, não só para quem consulta esta informação, mas para toda a família.

- **Selecionar uma ou duas fontes de informação** confiáveis para consultar notícias e evitar ler relatórios falsos ou não científicos.
- Gerar **capacidade crítica** para distinguir notícias falsas e desconfiar de artigos sensacionalistas sobre resultados positivos de tratamentos experimentais em pequena escala.
- Confiar somente em sites oficiais ou verificados, não só pela qualidade da informação, mas pelo aumento de sites maliciosos que exploram esta situação.
- **Verificar a informação:** fazer uma busca do(a) autor(a) ou organização, comprovar se a informação provém de um site de boa reputação, revisar a URL (começa com HTTPS?) ou utilizar sites de verificação de fatos (Fullfact, Snopes).
- Problemas de redação e nas imagens ou problemas nas datas.
- **Contribuir para a luta contra a desinformação.** Não compartilhar informação não verificada que proceda de fontes duvidosas.
- **Para as crianças e jovens, pode ser mais difícil** discernir entre a realidade e notícias falsas; por isso, é importante conversar sobre o tema para desenvolver seu pensamento crítico e ajudá-los a identificar informação falsa ou mitos perigosos.

f. Extorsão sexual

A extorsão sexual se manifesta mediante uma chantagem com base na posse (ou suposta posse) por parte do agressor de imagens íntimas, que ameaça distribuí-las caso não receba dinheiro ou imagens adicionais ou para manter uma relação. O agressor pode ser um companheiro íntimo, uma pessoa que se conheceu na internet ou um agressor desconhecido.

Durante a pandemia um golpe comum consiste no envio de mensagem ou e-mail de alguém desconhecido que afirma haver hackeado o dispositivo ou conta ameaçando publicar imagens privadas se não for realizado o pagamento de uma determinada quantia. A maioria desses e-mails procura assustar a vítima indicando que o dispositivo foi infectado com um malware, que se monitorou a atividade do computador e gravou práticas sexuais, fazendo referência a alguma senha utilizada pela destinatária em uma de suas contas. Ante isso, recomenda-se:

- Nunca abrir uma mensagem não solicitada ou de uma pessoa desconhecida.
- Desconfiar de qualquer mensagem que pareça provir da própria conta. Muitas vezes, para tornar a fraude mais crível, o cibercriminoso falsifica o endereço do remetente mediante uma técnica conhecida como spoofing de e-mails.
- Não responder a estas mensagens nem ceder ante ameaças ou pagar o resgate. O mais provável é que seja uma tentativa de golpe e o agressor não tenha em sua posse imagens íntimas nem tenha infectado o equipamento, mesmo se mencionar uma senha pessoal.
- Mesmo se o agressor tiver em sua posse imagens íntimas, é recomendável não responder, interromper todo contato imediatamente, não pagar e denunciá-lo o quanto antes. Realizar o pagamento fará com que peça mais dinheiro e, em muitos casos, o material é publicado apesar de efetuado o pagamento.
- Fazer capturas de tela das ameaças e das contas envolvidas para guardá-las como evidência caso se deseje fazer um relatório na polícia.
- Relatar nas redes sociais e bloquear a conta para evitar contato.
- Revisar as configurações de segurança de todas as contas e redes sociais.
- Falar com o círculo próximo e as pessoas que podem ser afetadas. Os chantagistas se refugiam no silêncio da vítima
- Denunciar às autoridades.

g. Cibersegurança em família

Os principais tipos de violência on-line sofridos por crianças e adolescentes são a exposição a conteúdos de caráter sexual e/ou violento sem consentimento, o ciberassédio e o grooming. De acordo com um estudo realizado por Save the Children, 52% dos menores de idade não tinham restrições por parte de seus pais e mães para acessar a internet, e entre quem tinha as limitações se baseavam unicamente no número de horas.

- ☑ É impossível estar todo o tempo com as crianças e adolescentes enquanto estão on-line; por isso, é importante manter um diálogo aberto e ajudá-los a desenvolver um pensamento crítico sobre os riscos que podem enfrentar on-line e as ferramentas de segurança a seu alcance para se proteger.

- ☑ Explicar aos menores a importância da privacidade e cibersegurança, inclusive a proteção de sua identidade digital.

- ☑ Prestar atenção em suas experiências on-line e conhecer seus hábitos de navegação. Supervisar o acesso de crianças à internet para prevenir que publiquem informação pessoal e privada (endereço, telefone, nome do colégio), assim como o tipo de canais de entretenimento que visitam com frequência.

- ☑ Estabelecer alguns limites de quando e onde podem utilizar os dispositivos eletrônicos (recomenda-se que isto seja em áreas comuns).

- ☑ Instalar um programa de controle parental da atividade on-line de crianças (estes programas estão disponíveis em quase todos os dispositivos eletrônicos, televisões e consoles de videogame). É possível também baixar controles de segurança em família e estabelecer buscadores de internet para crianças a fim de evitar que entrem em sites inapropriados.

- ☑ Revisar os controles de privacidade de videogames, aplicativos e jogos inteligentes, pois podem revelar os detalhes pessoais e a localização de crianças e adolescentes.

- ☑ Recordar que os jogos on-line são uma rede social que deve ser levada em conta na hora de revisar a informação compartilhada (permitem também estabelecer chamadas e contatos com terceiros)

- ☑ Manter-se em dia sobre os sites, aplicativos, redes sociais, videogames e serviços de chat utilizados pelas crianças e adolescentes, e explorá-los juntos, inclusive como proteger a informação e como relatar conteúdo ou conduta inapropriada nessas plataformas.

- Às vezes compartilham-se em família dispositivos móveis nos quais se costuma guardar informação sensível, como senhas, números de cartão de crédito ou informação de trabalho. É importante assegurar que não possam acessar essas contas e proteger esses dispositivos com sistemas de proteção.

Para prevenir o *grooming*:

- Assegurar que as contas de redes sociais e funções de chat em videogames sejam privadas, revisar as configurações de segurança e estabelecer regras acerca do tipo de conteúdo que podem compartilhar on-line. Instá-los a excluir contatos que não conhecem pessoalmente.
- Relatar e bloquear qualquer pessoa suspeita.
- Indicar que podem falar sempre que receberem um contato inapropriado ou se sentirem incômodos.
- Instá-los a eliminar amizades ou solicitações de seguidores de pessoas que não conhecem (verificar se a pessoa que faz a solicitação tem amizades em comum).
- Prestar atenção nas pessoas com quem socializam on-line e off-line
- Estar atenta a sinais de angústia.

Glossário

Análise de gênero. Forma sistemática de observar o impacto diferenciado de desenvolvimentos, políticas, programas e legislações sobre os homens e as mulheres. *4, 9, 10, 13*

Brecha de gênero: Refere-se a qualquer disparidade entre a condição ou posição das mulheres e homens na sociedade (diferenças no acesso a recursos, direitos e oportunidades). *11, 12, 13, 14, 15, 18, 24*

Controle parental. Conjunto de ferramentas para bloquear, restringir ou filtrar o acesso de menores de idade a determinados conteúdos ou programas a fim de evitar que se exponham a riscos através da internet. *37*

Criptografia de informação. É um processo para converter dados digitais em códigos, os quais tornam a informação ilegível exceto para a pessoa que possui a chave para decifrá-los. *31, 33*

***Dark Web* ou internet obscura.** É uma parte da internet intencionalmente oculta aos motores de busca na qual existem páginas que não estão indexadas e contam com IP oculto acessíveis somente com navegadores especiais. Essas páginas são dedicadas a todo tipo de atividades criminosas e incluem conteúdo ilegal. *7*

Discriminação por razão de gênero. Toda distinção, exclusão ou restrição baseada no sexo e que tenha por objetivo ou resultado prejudicar ou anular o reconhecimento, gozo ou exercício pela mulher, independentemente de seu estado civil, com base na igualdade do homem e da mulher, dos direitos humanos e liberdades fundamentais nos campos político, econômico, social, cultural e civil ou em qualquer outro campo [Fonte: Artigo 1 da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra a Mulher]. *13, 15, 24*

Engenharia social. São técnicas para enganar potenciais vítimas a fim de que compartilhem suas informações pessoais (por exemplo, senhas, detalhes de contas bancárias ou dados sensíveis) de forma quase voluntária. Estes métodos costumam se valer da boa vontade e da falta de precaução da vítima. *7*

Estereótipos de gênero. É uma opinião ou um preconceito generalizado acerca de atributos ou características que homens e mulheres possuem ou deveriam possuir ou das funções sociais que desempenham ou deveriam desempenhar [Fonte: ACNUDH, *Estereótipos de gênero e sua utilização*]. *6, 17, 18, 22, 24*

***Firewall*.** Sistema físico ou digital que tem o objetivo de permitir ou proibir o acesso a partir ou para uma rede a fim de assegurar que todas as comunicações entre a rede e a internet se realizem conforme as políticas de segurança de uma organização ou empresa. *30*

Gênero. Refere-se aos papéis, comportamentos, atividades e atributos que uma sociedade numa época determinada considera apropriados para homens e mulheres. O gênero também se refere às relações entre mulheres e às relações entre homens. Esses atributos, oportunidades e relações são construídos socialmente e aprendidos através do processo de socialização [Fonte: ONU Mulheres, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24*

***Grooming* ou aliciamento.** São atos deliberados de um adulto para se aproximar de um menor de idade (possivelmente cultivando uma conexão sentimental) com o objetivo de estabelecer uma relação e um controle emocional que lhe permita cometer abusos sexuais, iniciar relações virtuais, obter pornografia infantil ou realizar tráfico de menores. *15, 19, 22, 23, 37, 38*

HTTPS. Corresponde à sigla em inglês de *Hypertext Transfer Protocol Secure* e consiste em um protocolo de rede destinado à transferência segura de dados criptografados. *27, 34, 35*

Igualdade de gênero. Refere-se à igualdade de direitos, responsabilidades e oportunidades das mulheres e homens e das meninas e meninos [Fonte: ONU Mulheres, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *21, 22*

Incorporação de uma perspectiva de gênero. É uma estratégia para que as preocupações e experiências das mulheres, da mesma forma que as dos homens, façam parte integrante da elaboração, implementação, monitoramento e avaliação de políticas e programas em todas as esferas políticas, econômicas e sociais, de maneira que as mulheres e os homens possam se beneficiar deles igualmente e não se perpetue a desigualdade [Fonte: UNICEF, UNFPA, PNUD, ONU Mulheres. *Gender Equality, UN Coherence and you*]. *8*

Livestream. É uma plataforma de vídeo ao vivo que permite aos usuários ver e difundir conteúdo de vídeo utilizando uma câmera e um computador através da internet. *6*

Malware. O termo nasce da união das palavras em inglês *malicious software* (*software* mal-intencionado) e se refere a um tipo de *software* que tem como objetivo se infiltrar e/ou danificar um sistema de informação sem o consentimento do usuário. *7, 19, 28, 29, 30, 32, 36*

Negação de serviço. Ciberataque que tem por objetivo saturar um servidor com pedidos de serviço a fim de impedir que usuários legítimos possam utilizá-lo. Um método mais sofisticado é o ataque de Negação de Serviço Distribuído (DDoS), mediante o qual os pedidos são enviados de forma coordenada entre várias equipes. *22*

Papéis de gênero. Normas sociais e de conduta que, dentro de uma cultura específica, são amplamente aceitas como socialmente apropriadas para as pessoas de um sexo específico. Costumam determinar as responsabilidades e tarefas tradicionalmente atribuídas a homens, mulheres, meninos e meninas [Fonte: UNICEF, UNFPA, PNUD, ONU Mulheres. *Gender Equality, UN Coherence and you*]. *4, 16, 18*

Perspectiva de gênero. Mecanismo de análise que consiste em observar o impacto do gênero nas oportunidades, papéis e interações sociais das pessoas [Fonte: ONU Mulheres, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *4, 8, 9, 10, 17, 24*

Phishing. É um golpe cometido através de uma comunicação eletrônica enganosa e aparentemente oficial (e-mail, mensagem de texto ou telefone) mediante a qual o golpista ou *phisher* suplanta a personalidade de uma pessoa ou empresa de confiança para que a pessoa receptora forneça informação confidencial (senhas, dados bancários, etc.). Denomina-se *smishing* quando o golpe é realizado via SMS e *vishing* quando recria uma voz automatizada. *7, 19, 20, 22, 29, 32, 34*

Ransomware. É um programa de software malicioso mediante o qual se toma o controle do equipamento infectado e se 'sequestra' a informação do usuário (criptografando-a) com o objetivo de solicitar o pagamento de um resgate. *21, 28*

Rede Privada Virtual. Também mencionada como VPN (*Virtual Private Network*), é uma tecnologia de rede de computadores que estabelece uma extensão segura de uma rede de área local (LAN) sobre uma rede pública ou não controlada, permitindo que o computador na rede envie e receba dados sobre redes públicas como se fosse uma rede privada (conseguindo que esta conexão seja segura graças à criptografia da informação). *31*

Sexo (biológico). Refere-se às características biológicas que definem os seres humanos como mulheres e homens. *18, 23*

Spoofing. Consiste em uma série de técnicas de suplantação de identidade de entidades ou pessoas na rede realizadas mediante um processo de investigação ou com o uso de *malware*, com o objetivo de obter informação privada ou para conseguir acessar páginas com uma credencial falsa. Segundo a fonte do ataque, o *spoofing* pode ser classificado em IP *spoofing* (suplantação de endereço IP), mail *spoofing* (suplantação de e-mail), web *spoofing* (mediante um falso site), DNS *spoofing* (suplantação de identidade por fonte de domínio), ARP *spoofing* (suplantação de tabela ARP, um protocolo de nível de rede que relaciona um endereço MAC com o endereço IP do computador). *36*

Trabalho de cuidado não remunerado. Refere-se a todas as atividades diárias para manter a vida e saúde humana, tais como as tarefas domésticas (preparação de alimentos, limpeza, lavagem de roupa) e cuidados pessoais. O mais comum é que estas atividades sejam feitas pelas mulheres no lar de forma gratuita [Fontes: Orozco, Amaia. *Cadenas globales de cuidados. ¿Qué derechos para un régimen global de cuidados justo?*]. *12, 14, 16, 19, 21, 31*

URL (*Uniform Resource Locator*) Refere-se ao endereço específico que se atribui a cada um dos recursos disponíveis na rede (páginas, locais, documentos) para que possam ser localizados ou identificados. *35*

Violência contra a mulher. Qualquer ato ou conduta baseada no gênero que cause morte, dano ou sofrimento físico, sexual ou psicológico à mulher, tanto na esfera pública como na esfera privada. [Artigo 1 da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher). *9, 14, 15, 17, 18, 21, 22, 24*

Vírus. É um programa informático autopropagado que tem por objetivo alterar o funcionamento normal de um dispositivo eletrônico. Os vírus se diferenciam de outros tipos de *malware* por se replicarem automaticamente, isto é, são capazes de passar de um arquivo ou computador para outro sem o consentimento do usuário. *5, 11, 30*

Wi-fi. É uma rede de dispositivos sem fio interconectados entre si e geralmente também conectados à Internet através de um ponto de acesso sem fio. *27, 31, 33*

Zoombombing. Refere-se à intrusão sem consentimento de uma videoconferência através de conteúdo obsceno, pornográfico, sexista, racista, homofóbico, etc., usualmente resultando na finalização da videoconferência. O termo foi cunhado primeiramente para se referir a incidentes ocorridos durante a pandemia de COVID-19 na plataforma de Zoom, mas agora se aplica a intrusões em outras plataformas de videoconferências. *32*

Referências

- Agudelo, Mauricio, Eduardo Chomali, Jesús Suniaga, et al (2020). Las oportunidades de la digitalización en América Latina frente al COVID-19. CEPAL, ELAC, Corporação Andina de fomento, DPL Consulting e Telecom Advisory Services.
- Agüero, Aileen, Monoserrat Bustelo y Mariana Viollaz (2020). ¿Desigualdades en el Mundo Digital? Brechas de género en el Uso de las TIC. Nota técnica No. IDB-TN-01879. Banco Interamericano de Desarrollo.
- Association for Progressive Communications (APC) (2020). COVID-19 and the increase of domestic violence against women: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on Violence against Women, its causes and Consequences.
- Brown, Deborah y Allison Pytlak (2020). Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom y Association for Progressive Communications (APC).
- Brudvig, Ingrid, Chenai Chair y Adriane van den Wilk (2020). COVID-19 and increasing domestic violence against women: The pandemic of online gender based violence. World Wide Web Foundation.
- Chair, Chenai, Ingrid Brudivg, Calum Cameron et al (2020a). Women's rights online. Closing the digital gender gap for a more equal world. World Wide Web Foundation.
- (2020b). Derechos de la mujer en línea. Cerrar la brecha digital de género para lograr un mundo más igualitario. Resumen ejecutivo.
- Comissão Econômica para a América Latine e o Caribe da Organização das Nações Unidas (CEPAL) (2020). Informe Especial COVID-19 No. 7. Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.
- Comissão Interamericana de Mulheres (2020a). La violencia contra las mujeres frente a las medidas dirigidas a disminuir el contagio del COVID-19.
- (2020b). COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados.
- (2020c). COVID-19 en la vida de las mujeres: Emergencia global de los cuidados.
- (2021). COVID-19 en la vida de las mujeres: Los cuidados como inversión
- Relatora Especial sobre a violência contra a mulher, suas causas e consequências (REVM-ONU) (2018). Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. Conselho de Direitos Humanos. Organização das Nações Unidas. Consultado em 9 de setembro de 2020.
- Derechos Digitales América Latina (2020). COVID-19 and the increase of domestic violence against women in Latin America: A digital rights perspective.
- European Union Agency for Law Enforcement Cooperation (EUROPOL) (2020a). Internet Organised Crime Threat Assessment.
- (2020b). Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic.
- (2020c). Catching the virus. Cybercrime, disinformation and the COVID-19 pandemic.
- European Women's Lobby (2020). Policy Brief Women must not pay the price for COVID-19. Putting equality between women and men at the heart of the response to COVID-10 across Europe.
- Glitch UK y End Violence against Women Coalition (2020). The Ripple Effect: COVID-19 and the Epidemic of Online Abuse.

- Instituto Europeu da Igualdade de Gênero (EIGE) (2017). La ciberviolencia contra mujeres y niñas
- Millar, Katherine, James Shires y Tatiana Tropina (2021). Gender Approaches to Cybersecurity. Instituto das Nações Unidas para Pesquisa sobre Desarmamento (UNIDIR)
- Escritório das Nações Unidas sobre Drogas e Crime (UNODC) (2020). Cybercrime and COVID-19: Risks and Responses.
- ONU Mulheres (2020a). Online and ICT facilitated violence against women and girls during COVID-19.
- (2020b). From Insights to Action. Gender Equality in the Wake of COVID-19.
- (2020c). COVID-19 and Ending Violence against Women and Girls.
- (2020d). COVID-19 en América Latina y el Caribe: Cómo incorporar a las mujeres y la igualdad de género en la gestión de la respuesta de la crisis.
- (2020e). Spotlight on Gender, COVID-19 and the SDGS. Will the Pandemic Derail Hard-Won Progress on Gender Equality?"
- (2020f). COVID-19 y la Economía de los Cuidados: Acciones inmediatas y transformación estructural para una recuperación con perspectiva de género. Documento de Políticas No. 16.
- Organização Mundial da Saúde (OMS) (2020). El género y la COVID-19.
- Sainz, Milagros, Lidia Arroyo y Cecilia Castaño (2020). Mujeres y digitalización. De las brechas a los algoritmos. Instituto de la Mujer para la Igualdad de Oportunidades. Ministério da Igualdade do Governo da Espanha.
- Slupska, Julia (2019). "Safe at Home: Towards a Feminist Critic of Cybersecurity". St Antony's International Review, 15, no. 1: 83-100.
- Organização Internacional de Polícia Criminal (INTERPOL) (2020). Cybercrime COVID-19 Impact.
- União Internacional de Telecomunicações (ITU) (2020a). Measuring digital development. Facts and Figures 2020.
- (2020b). "Las mujeres, las TIC y las telecomunicaciones de emergencia: Oportunidades y limitaciones".
- World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment.

OAS Cataloging-in-Publication Data

La ciberseguridad de las mujeres durante la pandemia del COVID-19 : experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital / [Preparado por la Secretaría General de la Organización de los Estados Americanos].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.16)
ISBN 978-0-8270-7184-1
1. Women's rights. 2. COVID-19 (Disease). 3. Computer security. I. Title. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Serie Libro Blanco. VII. Series.
OEA/Ser.D/XXV.16

Secretariat for Multidimensional Security (SMS)

White paper

A cibersegurança das mulheres durante a pandemia de COVID-19:

Experiências, riscos e estratégias de autocuidado na nova normalidade digital

OEA | Mais direitos para mais pessoas