10.52712/issn.1850-0013-553

La ciberseguridad necesita mujeres y las mujeres necesitan ciberseguridad *

A segurança cibernética precisa das mulheres, e as mulheres precisam da segurança cibernética

Cybersecurity Needs Women, and Women Need Cybersecurity

Jezabel Molina Gil y Pino Caballero-Gil **

Este artículo aborda la intersección de ciberseguridad, violencia digital y género para explorar desafíos y oportunidades en el panorama digital actual. La falta de representación femenina en ciberseguridad, con solo el 11% de roles ocupados por mujeres, plantea cuestionamientos sobre diversidad en una industria crítica. Simultáneamente, la ciberviolencia contra las mujeres emerge como una preocupación creciente, impactando en la salud mental y la participación en línea. Persisten desafíos, incluida la falta de perspectiva feminista en la investigación en ciberseguridad. En el ámbito laboral tecnológico, altos niveles de satisfacción entre mujeres contrastan con brechas salariales y de representación, especialmente en ciberseguridad. La baja presencia femenina en este campo afecta la investigación, limitando la comprensión de formas potenciales de abuso tecnológico. Abordar estas problemáticas desde una perspectiva de género es esencial para construir un entorno digital más equitativo y seguro. Este artículo refleja un llamado a la acción para fomentar la diversidad en ciberseguridad y promover soluciones inclusivas en la investigación y políticas digitales.

Palabras clave: ciberseguridad; violencia digital; género

* Recepción del artículo: 30/01/2024. Entrega del dictamen: 20/03/2024. Recepción del artículo final: 06/05/2024.

** *Jezabel Molina Gil:* Departamento de Ingeniería Informática y de Sistemas, Universidad de La Laguna, España. Correo electrónico: jmmolina@ull.edu.es. ORCID: https://orcid.org/0000-0001-7702-9264. *Pino Caballero-Gil:* Departamento de Ingeniería Informática y de Sistemas, Universidad de La Laguna, España. Correo electrónico: pcaballe@ull.edu.es. ORCID: https://orcid.org/0000-0002-0859-5876.

10.52712/issn.1850-0013-553

Este artigo aborda a interseção de segurança cibernética, violência digital e gênero, explorando desafios e oportunidades no cenário digital atual. A falta de representação feminina na segurança cibernética, com apenas 11% das funções ocupadas por mulheres, levanta questões sobre a diversidade em um setor essencial. Ao mesmo tempo, a violência cibernética contra as mulheres surge como uma preocupação crescente, afetando a saúde mental e a participação on-line. Internacionalmente, os desafios persistem, incluindo a falta de uma perspectiva feminista na pesquisa sobre segurança cibernética. No local de trabalho da tecnologia, os altos níveis de satisfação entre as mulheres contrastam com as diferenças salariais e de representação, especialmente na segurança cibernética. A baixa presença de mulheres nesse campo afeta a pesquisa, limitando a compreensão das possíveis formas de abuso tecnológico. Abordar essas questões a partir de uma perspectiva de gênero é essencial para criar um ambiente digital mais equitativo e seguro. Este artigo reflete um chamado à ação para fomentar a diversidade na segurança cibernética e promover soluções inclusivas na pesquisa e na política digital.

Palavras-chave: segurança cibernética; violência digital; gênero

This article addresses the intersection of cybersecurity, digital violence and gender, with the aim of exploring challenges and opportunities in today's digital landscape. The lack of female representation in cybersecurity, with only 11% of roles filled by women, raises questions about diversity in a critical industry. Simultaneously, cyberviolence against women emerges as a growing concern, impacting mental health and online participation. Challenges persist, including the lack of a feminist perspective in cybersecurity research. In technology workplaces, high levels of satisfaction among women contrast with wage and representation gaps, especially in cybersecurity. The low presence of women in this field affects research and limits the understanding of potential forms of technological abuse. Addressing these issues from a gender perspective is essential to building a more equitable and secure digital environment. This article reflects a call to action to foster diversity in cybersecurity and promote inclusive solutions in digital research and policy.

Keywords: *cybersecurity; digital violence; gender*

Introducción

La convergencia de ciberseguridad, violencia digital y cuestiones de género define un paisaje complejo en la era digital. Este diálogo ha explorado la intersección de estos temas cruciales, destacando la brecha de género en ciberseguridad, la problemática de la ciberviolencia contra las mujeres y la necesidad imperativa de perspectivas feministas en la investigación. Desde la protección de la infraestructura computacional hasta el impacto en la vida cotidiana de las mujeres en línea, cada faceta resalta desafíos significativos y oportunidades para un futuro digital más equitativo y seguro.

La ciberseguridad, así como la criptografía que la sustenta, esenciales para salvaguardar nuestros activos digitales, se enfrentan a un déficit de representación femenina, evidenciando la urgencia de fomentar la diversidad en esta área crítica. Christofferson (2018) destaca la necesidad de una mayor inclusión y diversidad en el campo de la seguridad informática. Por su parte, el informe de (ISC)[2] (2018) subraya la importancia de la diversidad de género en el campo de la ciberseguridad. Según el informe, las mujeres representan solo el 24% de la fuerza laboral de la ciberseguridad.

Paralelamente, la ciberviolencia contra las mujeres y los menores ha emergido como un fenómeno preocupante, con consecuencias profundas en la salud mental y la participación en línea de las víctimas. Estas problemáticas se sitúan en un contexto internacional donde los esfuerzos por abordar la ciberviolencia y promover la igualdad de género en el ámbito digital han avanzado, pero persisten desafíos significativos. Palmer Padilla (2024) analiza los riesgos y las estrategias de prevención del *cyberbullying*, el *grooming* y el *sexting*, tres fenómenos que afectan a la seguridad y el bienestar de los menores en internet.

En el ámbito laboral de tecnología, las mujeres muestran altos niveles de satisfacción, pero las brechas salariales y de representación subrayan la necesidad de un enfoque más inclusivo. La baja representación femenina en ciberseguridad influye directamente en la investigación, afectando la comprensión de posibles formas de abuso tecnológico. En este contexto, abordar estos desafíos desde una perspectiva de género se revela como una necesidad crítica para construir un entorno digital equitativo y seguro. Este diálogo busca arrojar luz sobre estas complejidades y promover la reflexión hacia soluciones inclusivas y sostenibles.

1. La criptografía en la historia y la invisibilización de las mujeres

La criptología ha desempeñado un papel trascendental en momentos históricos cruciales, como las guerras mundiales, donde la criptografía emergió como una herramienta esencial para cifrar comunicaciones, especialmente durante conflictos armados.

Un hito notable en esta historia es la máquina Enigma, utilizada por los alemanes y Franco durante la Guerra Civil Española, desafiando a criptoanalistas de la época. Enigma representó un desafío formidable, pero fue finalmente descifrada por un equipo dirigido por Alan Turing en Bletchley Park, marcando un punto de inflexión no

solo en la guerra, sino también en la historia científica y tecnológica. El descifrado de Enigma sentó las bases de la computación moderna, mostrando cómo la criptografía militar puede impulsar avances tecnológicos significativos.

El legado de Enigma trasciende los logros militares para abarcar la intersección entre criptografía, historia militar y progreso tecnológico. Sin embargo, es crucial reconocer que esta narrativa histórica a menudo omite las contribuciones significativas de mujeres que desempeñaron un papel fundamental en el descifrado de Enigma y en la victoria de los aliados en la Segunda Guerra Mundial.

Si bien es aclamado por su liderazgo en el equipo de criptógrafos en Bletchley Park, Turing no estaba solo en esta hazaña monumental. La ruptura de Enigma fue el resultado de un esfuerzo colectivo, liderado en su mayoría por un grupo impresionante de 6600 mujeres con notables habilidades matemáticas e inteligencia excepcional. Sorprendentemente, eran más mujeres que hombres las involucradas en este proyecto clave.

A pesar de esta destacada participación femenina en el equipo de criptógrafos, la historia generalmente relega a estas mujeres al anonimato. La invisibilidad de sus nombres y logros es un ejemplo flagrante de la tendencia histórica de marginar las contribuciones femeninas, incluso en campos tan cruciales como la criptología. Es esencial reconocer a algunas de estas mujeres extraordinarias para rectificar este silencio histórico. Permítanme mencionar a tres de las 6600 mujeres que desempeñaron un papel vital en la ruptura de Enigma: Joan Clarke, una matemática excepcional que trabajó codo a codo con Turing; Mavis Batey, quien realizó contribuciones notables en descifrar los códigos enemigos; y Margaret Rock, una experta en lenguas y códigos que desempeñó un papel fundamental en el éxito del equipo.

Este episodio subraya la relevancia de reconocer y recordar las contribuciones femeninas en campos históricos, como la criptología, para desafiar la persistente invisibilidad de sus logros. A pesar de los obstáculos y la falta de reconocimiento, estas mujeres demostraron que su intelecto y destrezas eran esenciales para forjar el camino hacia el descifrado de Enigma y, en última instancia, hacia el fin de la Segunda Guerra Mundial. La culminación del proyecto para romper Enigma fue Colossus, una máquina gigantesca que contrastaba notablemente con la diminuta pero formidable máquina alemana. Este coloso mecánico, construido gracias al trabajo colectivo, representó el inicio de la informática tal como la conocemos hoy. Es crucial reconocer que las primeras personas que manejaron esta máquina pionera, y por ende las pioneras de la informática, fueron mujeres.

En un paradójico giro de la historia, el campo de la informática nació de las manos de mujeres visionarias, pero, a medida que avanzamos en el tiempo, la participación femenina en esta área ha disminuido significativamente y el mundo de la informática y la ciberseguridad se ha vuelto desproporcionadamente masculino. Esta discrepancia entre los orígenes femeninos de la informática y la actual escasez de mujeres en estos campos sugiere que, en algún punto del camino, se han presentado obstáculos significativos para la participación y el avance de las mujeres en la informática y la ciberseguridad. La falta de modelos a seguir, estereotipos de género arraigados y

barreras sistémicas han contribuido a crear un entorno donde las mujeres, a pesar de sus capacidades y habilidades, enfrentan obstáculos significativos en su camino hacia carreras en estos campos.

El desequilibrio actual, donde las mujeres están infrarepresentadas en la informática y la ciberseguridad (Christofferson, 2018), no solo refleja una desafortunada disparidad en las oportunidades, sino que también plantea preguntas esenciales sobre los factores que han contribuido a esta brecha. Abordar la falta de mujeres en la informática y la ciberseguridad no es simplemente una cuestión de equidad, sino una necesidad estratégica para aprovechar todo el potencial de la innovación y el progreso tecnológico. Promover la diversidad de género en estos campos no solo enriquece la fuerza laboral con perspectivas diversas, sino que también asegura que el diseño y la implementación de tecnologías reflejen las necesidades y experiencias de toda la sociedad.

2. La doble cara de la moneda en Internet: desafíos y empoderamiento

Internet, a primera vista, se presenta como un espacio igualitario, un terreno donde no hay jerarquías preexistentes y se fomenta la participación en condiciones de equidad. Este escenario aparentemente perfecto se ha convertido en una plataforma clave para el empoderamiento de las mujeres, evidenciado por movimientos como #MeToo y el 8M, que han emergido como herramientas poderosas en la lucha feminista. Sin embargo, detrás de esta cara luminosa de la moneda, surge una realidad más oscura que revela la persistencia de estereotipos machistas y dinámicas de acoso en el ciberespacio.

El ciberfeminismo, un concepto que ha evolucionado con la llegada de las tecnologías de la información y la comunicación (TIC), se manifiesta como una forma de activismo feminista que aprovecha las herramientas digitales. El estudio (Núñez Puente y Sánchez Hernández, 2011) explora el papel de la identidad en línea en el ciberfeminismo. Se centra en el uso y creación de identidades en línea como un nuevo espacio de relación, y examina cómo estas prácticas pueden ser utilizadas para promover la igualdad de género y la inclusión en línea. La capacidad de Internet para propagar información ha transformado el paradigma de los medios de comunicación y ha emergido como una valiosa herramienta para la expansión del movimiento feminista. Convocatorias como el 8M y otras manifestaciones contra la violencia de género encuentran en la red un medio prioritario de divulgación y movilización.

A pesar de haber superado la primera brecha digital de género relacionada con el acceso a las TIC, la evolución del panorama digital ha introducido una segunda brecha significativa. Esta nueva disparidad no radica en el acceso en sí, sino en la forma en que hombres y mujeres utilizan Internet, manifestándose como la reproducción de estereotipos de género en la red. La persistencia de roles de género tradicionales se refleja en los patrones de comportamiento en línea, contribuyendo a la perpetuación de desigualdades y discriminación. La segunda brecha digital de género se manifiesta en la forma en que las mujeres a menudo enfrentan estereotipos y barreras que limitan su participación plena en espacios digitales. Abordar esta brecha requiere

no solo garantizar el acceso igualitario a la tecnología, sino también desafiar y cambiar las estructuras y actitudes que perpetúan los estereotipos de género en el ciberespacio. Solo mediante un enfoque integral podremos construir un entorno digital verdaderamente inclusivo y equitativo.

Internet se convierte en un campo de batalla, donde la autodefensa digital se vuelve imperativa. La otra cara de la moneda se manifiesta a través de la reproducción de estereotipos machistas que generan situaciones incómodas y perpetúan dinámicas de acoso. El machismo encuentra en la red un terreno fértil para continuar con sus prácticas nocivas, aprovechándose de la relativa anonimidad y la amplificación digital. Las mujeres, lamentablemente, a menudo se enfrentan a situaciones de acoso digital que van desde solicitudes de amistad con contenido sexual explícito hasta el troleo en foros digitales, donde se busca generar polémica, ofender y provocar, en gran medida dirigido contra mujeres. Este panorama destaca la urgencia de la autodefensa digital y la implementación de estrategias para contrarrestar el acoso en línea. La lucha por la igualdad de género en el ciberespacio es, por lo tanto, una tarea multidimensional que requiere no solo la promoción activa de los derechos de las mujeres, sino también la implementación de medidas para salvaguardar su seguridad y bienestar en línea.

3. Violencia digital: una amenaza creciente en la era digital

La expansión de la tecnología ha dado paso a una nueva dimensión de violencia, aquella que se perpetra y se expande a través de medios digitales como redes sociales, correo electrónico y mensajería móvil. Esta forma de violencia, conocida como violencia digital, causa daños sustanciales a la dignidad, la integridad y la seguridad de las víctimas. Entre las numerosas formas de violencia digital, se incluyen el acoso, el control, la monitorización y el acecho, la extorsión, el troleo, la difamación, el desprestigio, las amenazas, la suplantación y el robo de identidad, el abuso sexual, entre otras.

El ciberacoso, en particular, ha emergido como una de las manifestaciones más perniciosas de la violencia digital. A lo largo de la historia, las mujeres han enfrentado la violencia machista en diversas formas, y en la era digital este fenómeno persiste y adquiere una relevancia aún mayor. La vida cada vez más digitalizada ha proporcionado un terreno fértil para que la violencia machista digital cause estragos significativos en las vidas de las víctimas.

La violencia digital, en sus diversas formas, inflige daños profundos en la integridad, la dignidad y la seguridad de las personas. Además, puede tener consecuencias físicas de la misma magnitud que otras formas de violencia machista más tradicionales. El ciberacoso es solo la punta del iceberg, ya que cada día surgen nuevas formas de violencia digital, haciendo que la lista sea interminable. El control digital sobre las víctimas, el acecho, la monitorización, la extorsión, el troleo, la difamación por redes y el desprestigio son solo algunas de las expresiones de esta amenaza digital. Las amenazas que utilizan herramientas de ciberseguridad, como la suplantación y el robo de identidad, añaden una capa de complejidad y malevolencia, especialmente dolorosa para aquellos que trabajan en campos como la ciberseguridad al evidenciar un desconocimiento de la especialidad.

La violencia digital es una realidad que se manifiesta de diversas maneras, impactando directamente la vida de las víctimas y destacando la necesidad urgente de abordar este fenómeno. La ciberseguridad, además de proteger la infraestructura digital, debe extender sus esfuerzos hacia la protección de individuos contra estas formas de violencia digital que, de manera alarmante, están en constante evolución en nuestra sociedad digitalizada.

4. Diferencias entre violencia *offline* y violencia *online*: la ciberviolencia desenfrenada

En el mundo *offline*, la violencia ha sido tradicionalmente caracterizada por la interacción directa entre víctima y agresor, a menudo en un ámbito privado o familiar. Esta forma de violencia, aunque devastadora, generalmente involucra a un número limitado de participantes, con la posibilidad de incluir a hijos e hijas en la ecuación. Sin embargo, en el ámbito digital, la violencia adquiere una dimensión diferente y desafiante.

La ciberviolencia, en el mundo *online* se distingue por dos características fundamentales que la diferencian de su contraparte *offline*. En primer lugar, la participación en estos ataques se expande significativamente. El agresor no solo se limita a la víctima y al entorno cercano, sino que, de manera alarmante, puede sumar a comunidades enteras en sus acciones. Estas comunidades pueden ser amigos en manadas, colegas de trabajo o incluso los usuarios de una red social, multiplicando así el impacto de la violencia digital de una manera que rara vez se ve en la violencia física.

La segunda característica distintiva es la amplitud de posibles víctimas. Mientras que en la violencia *offline* es más probable que el agresor sea alguien conocido o tenga acceso físico a la víctima, en el mundo digital, cualquier desconocido tiene el potencial de convertirse en agresor. Esta falta de restricciones geográficas o de conocimiento personal crea un escenario donde cualquiera puede convertirse en víctima de ciberviolencia, independientemente de su relación previa con el agresor.

La violencia digital, aunque no deja huellas físicas tangibles, tiene un impacto psicológico y emocional profundo en sus víctimas. A pesar de esto, persiste una percepción subestimada de la importancia de la ciberviolencia. Es esencial reconocer que la magnitud y las consecuencias de la violencia *online* son tan reales como las de la violencia *offline*, y abordar este problema requiere una comprensión profunda de sus características únicas y su alcance en constante evolución.

5. ¿Quiénes son las cibervíctimas? Un vistazo a la realidad desafiante

En el complejo entramado de la ciberviolencia, surge una pregunta fundamental: ¿quiénes son las cibervíctimas? La respuesta revela una realidad impactante que destaca la vulnerabilidad específica de ciertos grupos, principalmente las mujeres.

Con base en un informe publicado por la Organización de Naciones Unidas (2015), se estima que tres de cada cuatro mujeres en todo el mundo han sido expuestas a alguna forma de ciberviolencia. Este alarmante porcentaje, en lugar de disminuir, podría haber aumentado, especialmente a raíz de la pandemia de la COVID-19, un periodo en el que las interacciones digitales se han multiplicado. En un análisis más detallado, se descubre que el 80% de las víctimas de ciberviolencia son mujeres, subrayando la desproporcionada carga que recae sobre este género. En cuanto a los perpetradores, el 67% son hombres. Es importante destacar que, aunque existe un porcentaje menor de mujeres agresoras, los hombres representan una preocupante mayoría del total. Otro dato particularmente triste y preocupante es que, antes de cumplir los 15 años, el 18% de las mujeres ya ha experimentado algún tipo de violencia digital. Este elevado porcentaje señala una realidad alarmante: niñas que, desde una edad temprana, se ven afectadas por la ciberviolencia. Por último, tenemos a las mujeres defensoras de los derechos humanos, periodistas, activistas y, en general, aquellas con perfiles feministas que participan en actividades públicas son blanco frecuente de la ciberviolencia. Este es el perfil preferido de los ciberagresores, lo que resalta cómo la ciberviolencia a menudo se dirige a mujeres que desafían el *statu quo* y defienden causas justas en el ámbito público.

Este panorama arroja luz sobre la urgente necesidad de abordar la ciberviolencia desde una perspectiva de género y tomar medidas significativas para proteger a las mujeres, especialmente a aquellas que desempeñan roles destacados en la promoción de los derechos humanos y la igualdad.

6. Conceptos clave

6.1. Del acoso digital al *doxing*

En el complejo mundo del ciberacoso, diversos conceptos delinean las distintas formas en que esta violencia digital puede manifestarse. Uno de estos conceptos fundamentales es el propio ciberacoso, que consiste en el uso de medios digitales para molestar o acosar a una persona. Este comportamiento se materializa a través de ataques personales, la divulgación de información confidencial o falsa, aprovechándose comúnmente del anonimato que proporciona el entorno digital. Un término vinculado al ciberacoso es el *doxing*. Esta práctica implica la publicación en Internet de datos personales de la víctima, como números de teléfono, direcciones o correos electrónicos. El *doxing* agrega una capa adicional de invasión de la privacidad, exponiendo información sensible de la víctima y aumentando el impacto emocional y psicológico del acoso digital.

Es importante resaltar que el 80% de las personas afectadas por ciberacoso son mujeres, subrayando la desproporción de impacto que experimenta este género en el entorno digital. Ante esta problemática, se aconseja no borrar las pruebas de ciberacoso, certificar los mensajes acosadores con un sello temporal y denunciar ante la Agencia Española de Protección de Datos (AEPD) o la Policía. El ciberacoso es un delito penal con penas de prisión de hasta dos años, subrayando la gravedad y

las consecuencias legales de estas acciones perjudiciales en el mundo digital. La conciencia, prevención y denuncia son pilares fundamentales en la lucha contra el ciberacoso y el *doxing*.

Se están recreando dinámicas machistas que se aprovechan de las tecnologías y que requieren de un mayor número de mujeres y una perspectiva feminista en el mundo de la ciberseguridad. La inclusión de más mujeres en este ámbito no solo es esencial para abordar las crecientes amenazas digitales, sino también para combatir activamente la ciberviolencia y garantizar un entorno digital más seguro y equitativo.

6.2. "Troleo" de género

Se refiere a la práctica de realizar descalificaciones y ataques contra mujeres que expresan discursos feministas o muestran empoderamiento en plataformas digitales. Este tipo de ciberacoso tiene como objetivo desacreditar y menospreciar la voz y perspectiva de mujeres que defienden la igualdad de género y demuestran autonomía en línea.

En el Reino Unido y Estados Unidos, el "troleo" de género es considerado un delito que puede conllevar penas de prisión, subrayando la seriedad y las consecuencias legales de tales comportamientos. Como medida preventiva, se aconseja a las personas incrementar al máximo la privacidad de sus perfiles en redes sociales y limitar quién puede responder a sus publicaciones. Estas precauciones buscan resguardar la seguridad y bienestar de las mujeres en línea, proporcionando un entorno digital más protegido y respetuoso. La conciencia sobre la criminalidad y el impacto perjudicial del troleo de género es esencial para combatir activamente esta forma de ciberacoso.

6.3. *Sexting*

El *sexting* se define como la acción de intercambiar imágenes u otros materiales de naturaleza erótica o sexual. Esta práctica puede constituir un acto delictivo cuando implica la divulgación, exposición o transferencia a terceros de imágenes o grabaciones audiovisuales que representan a una persona sin su consentimiento explícito. Esta acción conlleva una seria invasión a la privacidad y puede tener repercusiones significativas en el bienestar emocional y psicológico de la persona afectada.

Dentro de esta definición se encuentra el mal llamado "porno de venganza", que consiste en la difusión sin consentimiento de imágenes sexuales con la intención de amenazar, coaccionar, intimidar o perjudicar a la persona que aparece en ellas, generalmente una mujer. Quienes comparten o reenvían una foto o vídeo privado de otra persona sin su consentimiento incurren en un delito penal. Como medida preventiva, se aconseja no compartir jamás información multimedia sensible. Además, en caso de tener dicha información en el ordenador o móvil, se recomienda cifrarla y activar un control de accesos robusto al sistema. Estas precauciones son esenciales para proteger la privacidad y seguridad de las personas en línea, así como para prevenir el impacto devastador del *sexting* y el "porno de venganza".

10.52712/issn.1850-0013-553

6.4. *Grooming*

Se refiere a una forma de ciberviolencia pedófila en la cual un adulto establece contacto con un o una menor a través de Internet, teléfono o redes sociales con la intención de controlar emocionalmente al menor y ganarse su amistad para obtener una satisfacción sexual. Este comportamiento manipulador y peligroso tiene como objetivo último la explotación sexual de menores, constituyendo un delito grave y una amenaza seria para la seguridad de los niños y adolescentes en línea.

Es preocupante observar que los casos de *sexting* y *grooming* han experimentado un aumento significativo, superando el 30% en los últimos cinco años. Como medida preventiva, se aconseja encarecidamente limitar el acceso de las cuentas de menores en redes sociales y plataformas en línea. Estas restricciones buscan proteger a los menores de posibles contactos inapropiados y prevenir situaciones de *grooming* que podrían tener consecuencias devastadoras. La conciencia sobre los riesgos del *grooming* es fundamental para educar a padres, tutores y menores sobre la importancia de la seguridad en línea y la prevención de la explotación sexual infantil.

6.5. Cibercontrol

Se refiere a la vigilancia, por parte de la pareja o expareja, de la actividad en línea de una persona, como saber con quién habla o dónde se encuentra accediendo a su teléfono móvil o redes sociales. Este comportamiento, también conocido como *stalking*, se ha convertido en una manifestación contemporánea del control ejercido en relaciones de pareja y forma parte de la violencia de género.

Históricamente, el control por parte de maltratadores incluía la supervisión de la correspondencia, llamadas telefónicas y la red de amistades. En la era digital, este control se ha trasladado al ámbito virtual, donde los agresores pueden monitorear correos electrónicos, conocer contraseñas de redes sociales, y espiar perfiles en plataformas como Twitter o WhatsApp. Según las estadísticas, el 35% de los jóvenes considera aceptable el cibercontrol, mientras que el 25% de las chicas ha experimentado esta forma de violencia.

Desde 2015, el cibercontrol está definido como delito penal. Como medida de protección, se aconseja utilizar contraseñas robustas en las redes sociales, así como controlar las sesiones abiertas para evitar accesos no autorizados. También se recomienda bloquear a ciberacosadores y desactivar la geolocalización para proteger la privacidad y seguridad personal en línea.

7. Riesgos de ciberacoso en hogares inteligentes

En hogares inteligentes, la proliferación de dispositivos conectados como termostatos, cerraduras, altavoces, micrófonos, cámaras y luces, puede transformarse en herramientas potenciales para el acoso y control de víctimas que no están familiarizadas con las tecnologías inteligentes de su hogar. Este fenómeno ilustra una

creciente preocupación respecto a la invasión de la privacidad y la seguridad personal en el entorno doméstico digital.

El *stalkerware, software* diseñado para monitorizar la actividad y acceder a las cámaras y micrófonos de dispositivos, ha experimentado un aumento alarmante del 35%. Este tipo de herramientas se convierte en una peligrosa arma en manos de acosadores, permitiéndoles vigilar de manera invasiva la vida cotidiana de sus víctimas.

Como medida de prevención, se aconseja a las mujeres ser administradoras de todos los dispositivos inteligentes en su hogar. Este enfoque no solo implica un mayor control sobre la configuración y accesos, sino que también promueve la autonomía y seguridad de las mujeres en sus propios espacios.

8. Consecuencias de la ciberviolencia

La ciberviolencia representa una forma insidiosa de silenciar y excluir a las mujeres en el espacio digital. Las consecuencias para aquellas mujeres que han sido víctimas de violencia en línea son:

- *Reducción de la presencia en línea:* casi un tercio de las mujeres que han experimentado violencia digital (28%) toma la decisión consciente de reducir su presencia en línea. Este acto refleja cómo la ciberviolencia puede influir negativamente en el acceso y participación de las mujeres en entornos digitales (Secretaría General de la Organización de los Estados Americanos, 2021).
- *Modificación del uso de redes sociales:* un impactante 76% de las mujeres afectadas modifica la forma en que utiliza las redes sociales, especialmente evitando expresar sus opiniones sobre determinados temas. Este cambio revela cómo la ciberviolencia puede coartar la libertad de expresión y contribuir a la autocensura de las mujeres en línea (ONTSI, 2022).

Además de estas repercusiones, la ciberviolencia mina la confianza en sí mismas y el bienestar emocional de las víctimas, generando consecuencias significativas en su salud mental (ONU, 2021). El 54% de las mujeres que ha sufrido acoso a través de redes sociales ha experimentado ataques de pánico, ansiedad o estrés. Y el 42% de las niñas y jóvenes que ha sufrido acoso *online* mostró estrés emocional, baja autoestima y pérdida de autoconfianza (ONTSI, 2022).

Recordemos que Internet y las TIC en general juegan un papel fundamental en la sociedad actual para el fortalecimiento de las identidades, las interacciones sociales, el poder económico y todo en general. En la era digital, la existencia y participación en línea se han vuelto elementos esenciales para la validación y el reconocimiento social, lo que lleva a la afirmación de que hoy en día, si no estás *online*, prácticamente no existes en diversos aspectos de la vida moderna. Por este motivo es necesario abordar

la ciberviolencia de manera integral, implementando medidas que no solo prevengan la agresión en línea, sino que también apoyen la recuperación y el empoderamiento de las mujeres afectadas.

El desconocimiento de las víctimas sobre cómo afrontar el problema de la ciberviolencia contribuye a la perpetuación del fenómeno. A pesar de la prevalencia del fenómeno, la violencia cibernética contra mujeres y niñas (CVAWG, por sus siglas en inglés) sigue estando infradenunciada en la UE y hay una falta significativa de datos exhaustivos. Las víctimas no siempre creen que sus casos serán tomados en serio por las autoridades policiales y, en consecuencia, a menudo deciden no denunciar. Incluso en encuestas anónimas, los encuestados pueden no ser conscientes de que sus experiencias pueden considerarse como violencia cibernética. La infradenuncia contribuye a una falta de datos exhaustivos y comparables, y oculta la verdadera escala y prevalencia del problema. (EIGE, 2022). Por ejemplo, en lugares como India, solo el 35% de las cibervíctimas se atreve a presentar una denuncia, revelando la falta de confianza en la efectividad de las medidas legales.

El anonimato del agresor agudiza la vulnerabilidad de las víctimas, quienes, lamentablemente, se ven obligadas a enfrentar la violencia digital por sí mismas en muchos casos. Cuando las vejaciones a través de las redes sociales son consideradas leves, los juzgados tienden a no adoptar medidas de protección ni realizar diligencias de investigación. Este escenario deja a las víctimas en una posición precaria, temerosas de denunciar por temor a que el problema se agrave, contribuyendo así a la perpetuación de la ciberviolencia.

9. Acciones para abordar la ciberviolencia contra las mujeres

A lo largo de los años, las instituciones internacionales han reconocido la importancia de proteger los derechos de las personas en el ámbito digital y han tomado medidas para abordar específicamente la ciberviolencia contra las mujeres:

- *2013 - Consejo de Derechos Humanos de las Naciones Unidas:* ese año el Consejo de Derechos Humanos de las Naciones Unidas afirmó que los derechos fundamentales de las personas deben estar protegidos tanto en el ámbito *offline* como *online*, reconociendo la necesidad de salvaguardar los derechos humanos en el entorno digital.
- *2016 - Asamblea General de las Naciones Unidas:* la Asamblea General reconoció oficialmente que las mujeres son más propensas a ser afectadas por violaciones del derecho a la privacidad en la era digital. Este reconocimiento marcó un paso significativo hacia la comprensión de los desafíos específicos que enfrentan las mujeres en el ciberespacio.
- *2020 - Informe de Evaluación sobre la Implementación de la Plataforma de Acción de Beijing:* el informe destacó la ciberviolencia como una problemática crítica que obstaculiza el avance de los derechos de las mujeres y las niñas. Esta inclusión subraya la necesidad de abordar la violencia digital como parte integral de la agenda global para promover la igualdad de género.

- *Agenda 2030 y el ODS 5:* En la Agenda 2030, el quinto objetivo de desarrollo sostenible (ODS) se propone alcanzar la igualdad de género y empoderar a las mujeres. La meta 5.2 se centra en eliminar todas las formas de violencia contra las mujeres en los ámbitos público y privado, mientras que la meta 5.9 busca aumentar la utilización de las TIC para promover el empoderamiento de las mujeres.

Estas acciones internacionales reflejan un compromiso global para abordar la ciberviolencia, reconociendo su impacto específico en las mujeres y estableciendo metas concretas para avanzar hacia la igualdad de género en el ciberespacio.

10. Brecha de género en ciberseguridad y tecnología

A pesar de los avances en la inclusión de mujeres en el campo de la tecnología, la ciberseguridad sigue siendo una industria mayoritariamente masculinizada, con solo el 11% de los roles ocupados por mujeres. Esta disparidad de género se refleja también en las diferencias salariales, con una brecha del 25% en la industria tecnológica en general y del 21% específicamente en ciberseguridad (Standard Chartered & Cyber Women Community, 2022).

A pesar de estos desafíos, las mujeres que trabajan en tecnología muestran niveles significativos de satisfacción laboral. El 80% de las mujeres en el sector de tecnologías de la información (TI) está satisfecho con sus posiciones, y nueve de cada diez mujeres estarían dispuestas a repetir sus carreras. Sin embargo, la representación femenina en ciberseguridad sigue siendo baja, con solo el 18% de las estudiantes especializándose en esta área.

Esta falta de representación femenina tiene consecuencias más amplias, ya que afecta la perspectiva feminista en la investigación en ciberseguridad. La escasa presencia de mujeres en este campo implica que muchas posibles formas de abuso tecnológico pueden pasar desapercibidas en los estudios. Para fomentar la diversidad de perspectivas y abordar de manera más completa los desafíos en ciberseguridad, es crucial trabajar hacia una mayor inclusión de mujeres en esta industria.

Conclusiones

La intersección entre ciberseguridad, violencia digital y género revela una compleja red de desafíos y oportunidades en la era digital. La ciberseguridad se ve afectada por la persistente brecha de género existiendo una clara falta de representación que influye en la perspectiva y enfoque de la investigación en este campo.

La ciberviolencia, por otro lado, emerge como un fenómeno que impacta desproporcionadamente a las mujeres. La falta de conocimiento sobre cómo abordar este problema, combinada con la percepción de ineficacia en las acciones legales, contribuye a la sensación de desamparo entre las víctimas. El impacto en la salud

mental, la autoestima y la disminución de la participación en línea resaltan la urgencia de medidas integrales para abordar este tipo de violencia. A nivel internacional, los esfuerzos para reconocer y abordar la ciberviolencia contra las mujeres han sido progresivos. Desde la afirmación de los derechos en el entorno digital por el Consejo de Derechos Humanos de las Naciones Unidas en 2013 hasta la inclusión de la violencia digital en la Agenda 2030, se evidencia un compromiso global. Sin embargo, la falta de perspectiva feminista en la investigación en ciberseguridad resalta la necesidad de una mayor diversidad de voces en este campo.

El ámbito laboral en tecnología presenta tanto desafíos como oportunidades. Aunque persisten brechas salariales y de representación en ciberseguridad, las mujeres que trabajan en TI muestran altos niveles de satisfacción laboral. Sin embargo, la baja representación femenina en ciberseguridad influye en la investigación, omitiendo posibles formas de abuso tecnológico.

En conclusión, abordar la ciberseguridad y la violencia digital desde una perspectiva de género es esencial para construir un entorno digital inclusivo y seguro. La diversidad de voces y experiencias, especialmente las de las mujeres, debe ser prioridad en la investigación, la industria y las políticas para forjar un futuro digital más equitativo y resiliente.

Bibliografía

Christofferson, D. A. (2018). Women in security: Changing the face of technology and innovation. Greenwood Village: Springer. Recuperado de: https://link.springer.com/book/10.1007/978-3-319-57795-1.

Comisión de las Naciones Unidas para la Banda Ancha (2015). Combatir la violencia en línea contra las mujeres y las niñas: una llamada de atención al mundo.

European Institute for Gender Equality (2022). Gender-based violence. Combating Cyber Violence against Women and Girls. Luxemburgo: Oficina de Publicaciones de la Unión Europea. Recuperado de: https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf.

(ISC)^2 (2018). Women in Cybersecurity: An Cybersecurity Workforce Report: Young, educated and ready to take charge. Recuperado de: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Women-in-Cybersecurity-Report.pdf?rev=d9c1e6269f8d43b19ee8fae5972a1bf5.

Núñez Puente, S. & Sánchez Hernández, M. F. (2011). Prácticas del Ciberfeminismo: Uso y creaciones de identidades en la red como nuevo espacio de relación. Instituto de la Mujer: Madrid. Recuperado de: https://www.inmujeres.gob.es/areasTematicas/estudios/serieEstudios/docs/practicasCiberfeminismo.pdf.

Observatorio Nacional de Tecnología y Sociedad (2022). Violencia digital de género: una realidad invisible. Ministerio de Asuntos Económicos y Transformación Digital. Recuperado de: https://www.ontsi.es/sites/ontsi/files/2022-07/_violenciadigitalgenero_unarealidadinvisible_2022.pdf.

Organización de las Naciones Unidas (2021). ‘‘Bodyright’ campaign launched, to end rise in gender-based violence online. UN News, 2 de diciembre. Recuperado de: https://news.un.org/en/story/2021/12/1106972.

Palmer Padilla, F. J. (2024). Seguridad y riesgos: Cyberbullying, Grooming y Sexting [Trabajo final de maestría]. Barcelona: Universidad Oberta de Catalunya. Recuperado de: https://openaccess.uoc.edu/bitstream/10609/67105/6/fpalmerpTFM0617memoria.pdf.

Secretaría General de la Organización de los Estados Americanos (2021). La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. Recuperado de: https://www.oas.org/es/sms/cicte/docs/Guia-conceptos-basicos-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf.

Standard Chartered & Cyber Women Community (2022). Women in IT and Cybersecurity.