

مكافحة العنف الرقمي ضدّ النساء في لبنان

توصيات سياسية

إعداد: د. ربي الحلو¹
إشراف: حياة مرشاد



مقدمة²

يعاني لبنان من نقص الإطار الحمائي ومسار الآليات القانونية لتناول بعض أشكال العنف التي تحدث عبر الإنترنت أو ما يُسمى أيضًا "العنف الرقمي". وتُشير الدراسات إلى أن النساء والفتيات هنّ الأكثر عرضةً للعنف الرقمي، وتشمل هذه الإساءات التهديدات الجنسية، ونشر الصور الحميمة دون موافقة، والتحرش الإلكتروني³. هذا النوع من العنف يترك الضحايا/ الناجيات عرضةً للأذى ويمنح امكانية الجناة للإفلات من العقاب إن لم تنتبه لمشاكله ونتائجه على الضحايا/ الناجيات والمجتمع⁴. وبالرغم من اعتناء المشرع/ة اللبناني/ة بوضع قوانين تتعلق بالقذف والتشهير والتحرش في مكان العمل، كان مجلس النواب اللبناني قد أقرّ في كانون الأول 2020 القانون رقم 205 لتجريم التحرش الجنسي وتأهيل ضحاياه⁵/ الناجيات منه، ما شكل خطوة مهمة نحو تحديث القوانين في لبنان. لكن ومع كلّ هذه الجهود، تزداد حوادث العنف الرقمي وجرائمه المختلفة إن كان تجاه النساء والفتيات، الأطفال والكبار على حد سواء، حيث لا يوجد حاليًا نظام عالمي واضح وثابت للإبلاغ عن العنف عبر الانترنت. ناهيك عن صعوبة تنظيم العالم الرقمي⁶.

واعتبرت منظمة هيومن رايتس ووتش أن القانون رقم 205، إيجابي "إذ يحمي الضحايا من الثأر عبر المس براتبهنّ أو ترقيتهنّ، أو نقلهنّ إلى قسم آخر، أو عدم تجديد عقدهنّ، أو اتخاذ إجراءات تأديبية بحقهن". ويتضمّن القانون تدابير لحماية كاشفي/ات التحرش ويمنع التمييز ضدهم/ن⁷. ورأت أنه وعلى الرغم من كونه خطوة مهمة في تجريم هذا السلوك، إلا أنه لم يتمكن المشرع/ة من ربطه بشكلٍ مباشرٍ مع قضايا إصلاح قوانين العمل، والرقابة، والتعويضات المدنية⁸ والإجراءات الوقائية وسياسات الحماية في مكان العمل⁹.

عالمياً يمثل قانون السلامة على الإنترنت¹⁰ The Online Safety Act (the Act) 2023 في المملكة المتحدة نموذجًا تشريعيًا هام لنا في لبنان. يهدف هذا القانون إلى حماية الأطفال/الطفلات والبالغين/ات في الفضاء الرقمي. كما يُحمّل شركات وسائل التواصل الاجتماعي وخدمات البحث المسؤولية، ما يجعلها مسؤولة بشكلٍ أكبر عن سلامة المستخدمين/ات على منصاتها ويفرض مجموعة واجبات جديدة منها حماية المستخدمين/ات من كافة الفئات العمرية، منع المحتوى الضار وتوفير آليات للإبلاغ، ويُلزم المنصات الكبرى بالشفافية حول أنواع المحتوى التي تَسمح بها، كما يمنح المستخدمين/ات قدرة أكبر على التحكم في المحتوى الذي يشاهدونه.



1 هي زميلة برنامج مستقبل الحقوق والحوكمة (FORGE) في كلية الحقوق بجامعة نيويورك حيث تعمل على مشروع بحثي تحت عنوان حقوق الإنسان في الموارد البشرية(HR6HR)كما تشغل منصب الأمانة العامة للمركز اللبناني لحقوق الإنسان (CLDH) وعضوة في مجلسه التنفيذي. تتمتع بخبرة واسعة في مجال الإعلام والتنمية التنظيمية خاصةً، في تدقيق المعلومات، التخطيط والتطوير الاستراتيجي، وتصميم السياسات وتنفيذها والإصلاحات الهيكلية. عملت أكاديمية ومهنية، وطورت العديد من أدوات التدريب والمنشورات حول الموارد التعليمية المفتوحة (OER)بالإضافة إلى منشورات حول إصلاح المنظمات والاتصالات ومجتمع الشبكات، ومقالات محكمة حول الدراسات التسوية واللاكورية والدراسات الثقافية ما بعد الاستعمارية والنقاطية والإثنوغرافيا الذاتية. تشمل مجالات أبحاثها التواصل السياسي، والعنف القائم على النوع الاجتماعي كما دراسات النوع الاجتماعي النقطية والتنظيم الذاتي لوسائل الإعلام، والحقوق الرقمية، وحكم سيادة القانون. تعمل كمصاحفة وأستاذة محاضرة في التواصل والنوع الاجتماعي ومُستشارة متخصصة في التخطيط الأكاديمي وضمان الجودة في التعليم العالي والتدريب. كما عملت على نطاق واسع في قطاع الإعلام في مجالات التطوير التنظيمي، والتواصل والإعلام، وتصميم السياسات وتنفيذها، والإصلاح الهيكلي

2 ملاحظة: تم مراجعة ورقة السياسات هذه من قبل خبيرات وخبراء في مجال المراقبة الرقمية الحقوق الرقمية، الحركة النسوية، وحقوق الإنسان، وذلك لضمان التشاركية، الشمولية وفعالية البحث كما التوصيات.نقدم لهم/ان خالص الشكر على مساهمتهم/ان القيّمة وتعبير الباحثة عن امتنانها لكل من سمر حلال (خبيرة الحقوق الرقمية والامن الرقمي)، نورهان ابو زيد (محامية وناشطة نسوية)، عبد قطايا (مدير المحتوى الرقمي في منظمة سمكس)، نورهان شرف الدين (قسم التواصل والمناصرة في المركز اللبناني لحقوق الانسان)، دلال سعود (صحافية والمستشارة الاقليمية لمنظمة النساء في الاخبار Women In News)ميادة عبدالله (منسقة مشروع برنامج الماجستير العربي في الديمقراطية وحقوق الإنسان في جامعة القديس يوسف وعضوة الهيئة الإدارية في منظمة لادي(LADE)لما قدموه من مراجعة ودعم خلال العمل البحثي

<https://onlineviolencewomen.eu.com/> 3

<https://www.amnesty.org/en/what-we-do/technology/online-violence/> 4

<https://blogs.worldbank.org/ar/arabvoices/sexual-harassment-workplace-lebanon-where-are-we-headed> 5



في المملكة المتحدة مسؤولية تنظيم السلامة الرقمية، كجهة مستقلة ومراقب على تطبيق OfCom (The Office of Communication) وتتولى أوفكوم أو هيئة تنظيمية الاتصالات القانون والامتثال له. كما تلتزم نشر مدونات سلوك، قواعد ممارسة وإرشادات حول كيفية امتثال الشركات الخاضعة للقانون لواجباتها. وتملك الهيئة صلاحيات واسعة لتقييم مدى التزام المنصات بالقانون وفرض العقوبات عليها، بما في ذلك غرامات مالية كبيرة قد تشمل شركات مقدمة الخدمة خارج المملكة المتحدة، إذا كان لها روابط مع المملكة.

يواجه تطبيق قوانين مماثلة لقانون السلامة على الإنترنت في لبنان تحديات كبيرة. تتضمن هذه التحديات الحاجة إلى تقنيات متقدمة من تطبيقات وبرمجيات، ومخاطر إساءة استخدام هذه الأدوات ضد الناشطين/ات، بالإضافة إلى الصعوبات القانونية في تعريف خطاب الكراهية، والمخاوف المتعلقة بالمراقبة، Surveillance وضرورة ضمان المساءلة كما حماية الخصوصية الفردية.

في هذا السياق، تبرز "الإعلانات المستهدفة" Target Ads عبر الإنترنت، كأداة للتضليل السياسي، ما يثير تساؤلات حول تأثير المنصات على الانتخابات ونتائجها. يهدف البحث إلى اقتراح سياسات ورؤى تدعم التوجهات القانونية والحماية للمجتمع اللبناني، مع الاستفادة من تجارب دولية كالمملكة المتحدة، ومراعاة التحديات التي تواجه تطبيقها في السياق اللبناني.

أخيراً، لا يمكننا البدء في مسار مكافحة العنف الرقمي بشكل فعال في لبنان دون تبني النهج الشمولي-التشاركي والمتعدد الأطراف، يشمل متطلبات مؤسساتية، تقنية ومالية. وذلك عن طريق تنظيم نقاشات جدية برلمانية متاحة للجمهور من أجل كل فرد في لبنان، بناء الثقة اللازمة وتفعيلها وتعزيز التعاون بين كافة المؤسسات الرسمية والخاصة، وتأمين الميزانية اللازمة لتنفيذ القوانين. ثانياً، فيما يتعلق بالشفافية والمساءلة، هنالك حاجة إلى نقاش عام مفتوح مع المجتمعات الأهلية. بالإضافة إلى ذلك هناك حاجة لوضع جدول أعمال، واتخاذ القرارات وتنفيذها، كما ضمان شفافية تطبيقها على جميع أصحاب المصلحة.

ما هو هدفنا؟

تهدف هذه المعالجة البحثية إلى وضع إطار لسياسة عامة تُساهم في حماية مستخدمي/ات الإنترنت في لبنان من العنف الرقمي، من خلال توفير آليات وقائية واضحة ورسم مسار تنظيمي فعال للتعامل مع هذه الجرائم وتحديد أصحاب المصلحة وإشراكهم/ن في إيجاد حلول مُستدامة. حيث يُمكن أن يؤدي العنف الرقمي إلى تراجع مشاركة العديد من الأشخاص في النقاشات العامة الرقمية ومنهن النساء. وذلك سيؤدي حتماً إلى تجنب استخدام وسائل التواصل الاجتماعي أو التعبير عن آرائهن بحرية. كما يُمكن أن يؤثر ذلك سلباً على فرصهن في التعليم والتوظيف والمشاركة السياسية.

إن سجل لبنان الضعيف في مجال إصلاح السياسات وتنفيذها يمثل تحدياً كبيراً لنا. ومع ذلك، يمكن الاستفادة من التجربة المتواضعة في مجال التنظيم الذاتي لقطاع الإعلام كنموذج للإصلاح الشامل. يمكن أن تكون مبادرة إصلاح ناجحة ونقطة انطلاق للتغيير في مجالات أخرى. وكما يقول المثل، رحلة الألف ميل تبدأ بخطوة؛ ولتحقيقها ولمس التغيير يجب التغلب على عقبات الطائفية السامة والمذهبية، كما ثقافة الإفلات من العقاب، ونظام المحسوبيات المتأصل في لبنان. تقدم هذه الورقة مجموعة من الإرشادات لبدء نقاش وطني حول مجالات حيوية محددة للغاية للعمل على الإصلاح في المجال الرقمي.

⁶ Song, Haoming and Holzer, Angie (2023) "Online Safety Laws by Country," Journal of Nonprofit Innovation: Vol. 3: Iss. 3, Article 3. URL: <https://scholarsarchive.byu.edu/joni/vol3/iss3/3>

⁷ <https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/114675/205.pdf>

⁸ <https://www.hrw.org/ar/news/2021/03/05/378078>

⁹ <https://www.openglobalrights.org/human-rights-of-human-resources-workplace-justice-in-lebanon/>

¹⁰ <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-does-the-online-safety-act-do>

¹¹ عملت الباحثة طوال ثلاث سنوات على تطبيق التنظيم الذاتي لوسائل الإعلام في لبنان مع عدة مؤسسات وقطاعات محلية. يمكن لهذه التجربة أن تكون مثال يُبنى عليه للمستقبل

العنف الرقمي والتحديات الدوليّة

بالرغم من أن التكنولوجيا أداة قوية لتفعيل قدرة مستخدمي/ات الانترنت وتعزيز الحقوق، إلا أنها تُستخدم بشكل متزايد كوسيلة لممارسة العنف ضد النساء والفتيات، من خلال التحرش والتمييز والتنمر الإلكتروني. هذا العنف الرقمي هو امتداد للتمييز الهيكلي ضد النساء والفتيات، ويصبح مُضخم بفعل خصائص الإنترنت، ما يخلق تحديات جديدة في مجال الحقوق الرقمية.¹² لذلك، نحتاج إلى سياسات شاملة تُعالج هذه القضايا من خلال: تضيق الفجوة الرقمية الجندرية، ووضع قوانين تحاكم العنف الإلكتروني، والعمل على زيادة الوعي بمخاطره، وتمكين كافة الهويات الجندرية من استخدام التكنولوجيا بأمان وحرية، مع ضمان عدم استخدام قوانين الجرائم الإلكترونية كأداة للقمع وإسكات الأصوات.¹³

في حين تفرض الطبيعة العالمية للإنترنت تحديات من حيث إنفاذ القانون. ويمكن أن يقيم الجناة في بلدان مختلفة، ما يعقد تطبيق القوانين الوطنية. لذلك تساعد القوانين الخاصة بالتحرش عبر الإنترنت في التغلب على هذه التعقيدات وضمان التعاون عبر الحدود لمحاسبة المتحرشين.

مفهوم العنف الرقمي: شموليته وقيوده

في حين يشمل مصطلح "العنف الرقمي" مختلف أنواع العنف القائم على النوع الاجتماعي والذي يُرتكب بمساعدة الأجهزة التقنية والوسائط الرقمية مثل الهواتف المحمولة وتطبيقات الإنترنت والبريد الإلكتروني أو من خلال منصات التواصل الاجتماعي. لكنه يغفل في الكثير من الأحيان البعد الجندري-التقاطعي والهويات المختلفة كما الطبقات الاجتماعية والثقافية للمجتمعات الرقمية.¹⁴

¹² <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/#:~:text=Studies%20across%20the%20world%20show,and%20reach%20of%20digital%20platforms.>
¹³ Finding a difficult balance: Human rights, law enforcement and cyber violence against women | GenderIT.org

مع إدراكنا أن النساء هنّ الأكثر عرضة للعنف الجندري، يجدر بنا التذكير بأن هذا العنف لا يستثني أحداً، فهو يطال مختلف الهويات الجندرية (وتشمل غير الثنائية وغير المتماثلة) ومنها أيضاً لأطفال والرجال في بعض السياقات المحددة.¹⁴

العنف الرقمي في الدول العربية: الواقع والتحديات

يوثق دليل حمل عنوان "رسم خرائط القوانين والخدمات المتعلقة بالعنف ضد النساء والفتيات عبر الإنترنت والعنف المُيسَّر بتكنولوجيا المعلومات والاتصالات في الدول العربية Mapping of laws and services for online and ICT-facilitated violence against women and girls in Arab States."

اللغة الانكليزية والصادر عن هيئة الأمم المتحدة للمرأة - الدول العربية في العام 2022، التشريعات الحالية المتعلقة بالعنف ضد النساء والفتيات عبر الإنترنت في الدول العربية ويحدد الخدمات التي تقدمها الحكومات ومنظمات المجتمع المدني لوقف العنف ضد النساء والفتيات عبر الإنترنت وتيسير تكنولوجيا المعلومات والاتصالات. كما يسلط الضوء على الأطر والممارسات الدولية المتعلقة بالاستجابة للعنف ضد النساء والفتيات على الإنترنت والعنف ضد النساء والفتيات المُيسَّر بتكنولوجيا المعلومات والاتصالات. ويخلص الدليل إلى أنه لا توجد قوانين خاصة بالعنف عبر الإنترنت في الدول العربية، لكنها تعتمد نهج ثلاثي الأبعاد في الفضاء الرقمي ويشمل:

- 1- توسيع قوانين العنف المنزلي لتشمل العنف عبر الإنترنت
- 2- وضع قوانين شمولية ضد كافة أنواع العنف ضد النساء والفتيات (مثال تونس منذ العام 2017)
- 3- قوانين الجرائم الإلكترونية

وبالرغم من إيجابية هذا التطور، يشير الدليل إلى أنه غالبًا ما يُنظر للعنف الرقمي (عبر الإنترنت) على أنه جريمة إلكترونية فقط، ما قد يغفل ليس فقط حاجات النساء والفتيات وحقوقهن، بل كافة الهويات الجندرية-التقاطعية؛ ونضف إلى ذلك أن قوانين الجرائم الإلكترونية قد تنتهك الخصوصية وحرية التعبير.

وقد سنت ثلاث عشرة دولة عربية قوانين لمكافحة الجرائم الإلكترونية، بما في ذلك العنف الإلكتروني ضد النساء والفتيات. وهي تشمل الجزائر والبحرين ومصر والأردن والكويت وليبيا وعمان وقطر والمملكة العربية السعودية ودولة فلسطين والسودان وسوريا والإمارات العربية المتحدة. أما الدول العربية التسع المتبقية فقد طبقت إما قوانين عامة لمكافحة الجرائم الإلكترونية أو لم تتخذ أي تدابير.¹⁵

العنف الرقمي: ظاهرة مُتزايدة في لبنان

يشهد العالم اليوم تصاعدًا مُقلقًا في ظاهرة العنف الرقمي، ولبنان ليس بمنأى عن هذا التهديد المُتزايد الذي يهدد سلامة الأفراد ويُقوّض حقوقهم/ن الأساسية، خصوصًا حرية التعبير والخصوصية. هذا لا يعني أنه علينا أن نمنع استخدام التقنيات الرقمية وأدواتها، لأنه لا يمكن ولا يجب أن نُهمل دور التكنولوجيا وأهميتها كمحرك للتغيير الإيجابي حول العالم. إلا أن عدم الدراية في مجالات استخدامها قد يجعلها أداة للسيطرة وإيذاء الآخرين عبر سوء استخدام السلطة، التمييز، التحيز كما التئمر والتهميش. نحن نرى، كجزء من مسؤوليتنا الاجتماعية، أن فهم الإمكانيات التكنولوجية ومواءمتها مع الأطر القانونية وتوفير حماية واضحة المسار للضحايا هو جزء هام وأساسي من واجبنا الوطني أولاً والإنساني ثانيًا. يهمننا فهم لتكنولوجيا التواصل المعلوماتية. تاريخها، وإمكاناتها كما مواءمة تقدمها السريع مع القوانين.

¹⁵ <https://arabstates.unwomen.org/en/digital-library/publications/2022/03/mapping-of-laws-and-services-for-online-and-ict-facilitated-violence-against-women-and-girls> لمراجعة الدليل كاملاً

العنف الرقمي كأداة للرقابة والحاجة إلى قانون لمكافحة

نسلط الضوء أيضًا على العنف كأداة للرقابة ضد العديد من الأفراد وخصوصًا النساء والفتيات في لبنان، في الفضاء الرقمي. يشمل ذلك العنف الجسدي والجنسي والنفسي، بالإضافة إلى العنف عبر الإنترنت مثل المضايقات والتنمر الإلكتروني، ما يُجبر العديد منهم على فرض رقابة ذاتية على أنفسهم أو الانسحاب من المنصات الرقمية. يؤثر هذا سلبيًا على مشاركتهن في النقاشات العامة، ويحدّ من حريتهن في التعبير، ويَقوِّض فرصهن في التعليم والتوظيف والمشاركة السياسية.

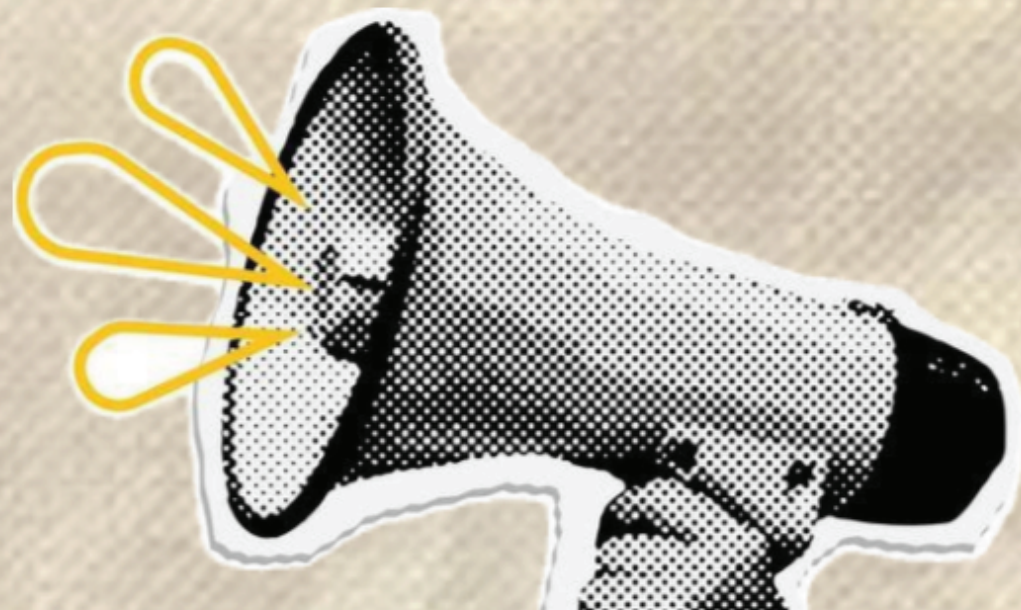
تُشير الدراسات إلى ارتفاع مُقلق في شكاوى "الابتزاز الجنسي" عبر الإنترنت في لبنان (ارتفعت بنسبة 307% في عام 2020)، ما يؤكد الحاجة الملحة إلى وضع إطار لسياسة عامة تُساهم في حماية مُستخدمي/ات الإنترنت، خصوصًا النساء والفتيات، من العنف الرقمي. يتضمّن ذلك توفير آليات وقائية واضحة ورسم مسار تنظيمي فعّال للتعامل مع هذه الجرائم وتحديد أصحاب المصلحة وإشراكهم/ن في إيجاد حلول مُستدامة. يُشدّد هذا البحث على أهمية مُعالجة الرقابة القائمة على النوع الاجتماعي بكافة أشكالها، والتي تُشكّل انتهاكًا لحقوق الإنسان وتُهددًا للمُشاركة الكاملة والفعّالة للنساء في المُجتمع.

سياسات الشركات والتربية الإعلامية والحرية في الفضاء الرقمي – هل من توصيات عملية؟

من هنا، ارتأينا أن تتناول هذه المعالجة البحثية كيفية ربط سياسات الشركات ومواءمتها مع القوانين المحلية؛ وكيفية بثّ ثقافة التربية الإعلامية والمعلوماتية للمواطنين والمواطنات عامة، كما للمستخدمات ومستخدمي الشبكة وكلّ شخص مقيم/ة في لبنان.

تتضمن هذه الورقة تحليلًا لأنواع الجرائم الرقمية التي تُرتكب عبر الإنترنت ووسائل التواصل الاجتماعي، مع الإقرار بصعوبة حصرها جميعًا نظرًا لتطور العالم الرقمي المستمر. كما نقدم توصيات لما نحلم أن يكون مساحة عامة للجميع بعيدًا عن سوء استخدام السلطة والاحتياال والعنف كما التهديدات الرقمية المتزايدة مثل الفيروسات سرقة البيانات، والاحتياال الإلكتروني مع تطور التطبيقات وتلك التي تتعلق بالذكاء الاصطناعي وانتزعت الأشياء وما قد يظهر فيها من ثغرات تقنية. هذه الثغرات تُسهّل على المُخترقين استغلال البيانات الشخصية أو استخدامها لأغراض غير أخلاقية، ما يهدد خصوصية الأفراد ويُعرضهم/ن لخطر الابتزاز أو العنف الرقمي. في هذا السياق نقدم عبر هذا التحليل مجموعة من التوصيات بهدف خلق مساحة عامة آمنة وعادلة للجميع، وذلك بالتأكيد على مبدأ حيادية الشبكة،¹⁷ حماية البيانات الشخصية،¹⁸ الأمن الرقمي، مع مراعاة البُعد الاقتصادي .

كما نتوخى الحريّات بكافة أشكالها وبضرورة توفير بيئة رقمية آمنة وعادلة للجميع. ونحدد أنواعًا كثيرة من الجرائم التي تحصل عبر الإنترنت ووسائل التواصل الاجتماعي، مع الإقرار بصعوبة حصرها كلّها نظرًا لتطور العالم الرقمي المستمر. كما نرى أن العنف الرقمي والذي يشمل انتهاكات للخصوصية وتهديد للأمن الشخصي من جسدي ونفسي، وقد يصل إلى العنف الاقتصادي. كل ذلك يتطلب منا إطارًا قانونيًا لحماية الأفراد والمجتمع بكافة هوياته الجندرية، الطبقات الاجتماعية، والجندرية، العمرية ومن ذوي/ذوات الإعاقة كمقاربة تقاطعية لهذه الهويّات.



¹⁶ <https://globalvoices.org/2021/03/10/online-rape-threats-connect-lebanese-activist-to-thousands-of-other-women-facing-abuse/>
والحكومات، بغض النظر عن المحتوى أو المستخدم أو المنصة أو التطبيق أو الجهاز. لكن علينا أن ننظر إلى ما هو (ISPs) ضمن حيادية الشبكة كافة البيانات الإنترنت بشكل متساوٍ من قبل مزودي خدمة الإنترنت
أبعد من مسألة ما إذا كان ينبغي تنظيم منصات الإنترنت أم لا لبحث في كيفية تنظيمها وما هي الأنماط التي تؤمن فعلاً الأمان للمستخدمين والمستخدمات لا في الظاهر فقط. هذا المفهوم ضروري لدى كتابة القانون خاصة لتفعيل الثقة والعدالة الشفافية وعدم حجب الشبكة مهما كانت الضرورة
نقصد بالبيانات الشخصية تلك التي تتعلق بحياة الإنسان الخاصة، مثل الميول السياسية، المعتقدات الدينية، والمعاملات المالية وغيرها. حماية هذه البيانات هو أمر أساسي وبالع أهمية في ظل تطور التقنيات الحديثة¹⁸
وإنشاء وحدات تخزين المعلومات (أو مستودع البيانات)

الواقع الحالي: لماذا نحن بحاجة لهذا القانون؟

حقوق الإنسان في الفضاء الرقمي - تحديات وفرص

حقوق الإنسان عالمية، مترابطة، وغير قابلة للتجزئة أو التصرف، ويتمتع بها جميع الأشخاص بغض النظر عن المكان الذي يعيش فيه أو الهوية الجندرية أو الخلفية الدينية أو الثقافية أو العرقية.¹⁹ وهذه الحقوق التي يتمتع بها الأشخاص خارج الفضاء السيبراني هي ذات الحقوق التي يجب أن تكون محمية في نطاق شبكة الإنترنت أيضاً.²⁰ كما لكل فرد الحق في التمتع بفضاء رقمي آمن، غير أن تطور شبكات الإنترنت المتسارع، يطرح تحديات تتعلق بالأمن السيبراني. فالهجمات الإلكترونية، واستغلال البيانات الشخصية، والعنف الرقمي تؤكد أنه هنالك حاجة إلى وضع نهج لسياسة رقمية تأخذ في الحسبان الحقوق والحريات الشخصية كما المجتمعية.

توفر البيئة الرقمية فرصاً هائلة لتعزيز حقوق الإنسان والتعلم والتطور، لكنها تُشكل أيضاً مخاطر جديدة إن لم يتم التنبه لها وتنظيم هذا الفضاء بشكل ملائم. فمثلاً، يجب أن تراعي السياسات التي تهدف إلى تعزيز سلامة الأطفال/الطفلات على شبكة الإنترنت، تدابير لضمان تحديد السن، وتجنب الآثار المحتملة على حقوق الإنسان الأخرى مثل انتهاك خصوصية الأفراد وغيرها من السلوكيات الضارة التي قد تشكل تهديداً مستمراً على الخصوصية والحقوق.



¹⁹ <https://www.ohchr.org/ar/what-are-human-rights>

²⁰ <https://www.ohchr.org/en/topic/digital-space-and-human-rights>

موازنة حماية الحقوق وحرية التعبير

بينما تسعى الدول إلى حماية الحقوق المرتبطة بالسلامة على الإنترنت من خلال إزالة المحتوى الضار، قد يتعارض ذلك مع حرية التعبير. لذلك على صانعي/ات السياسات في لبنان أن يأخذوا في عين الاعتبار تأثير السياسات الرقمية على حقوق الإنسان لضمان أن يكون الإنسان محور التحول الرقمي وموجه نحو الحقوق.

للتكنولوجيا تأثير إيجابي في التواصل والتعليم والصحة والتجارة، كما في الحركة العالمية، لكنها تطرح أيضاً تحديات مثل قضايا الخصوصية والاعتماد المفرط عليها والفجوة الرقمية. لذلك، يجب الاستفادة من إمكانيات التكنولوجيا بشكل مسؤول والعمل على معالجة تحدياتها لضمان مستقبل أفضل للجميع في لبنان.

وتُشكل الموروثات الثقافية التنميطية للأدوار الجندرية والقوانين والسياسات التمييزية وكراهية النساء والتمييز الجندري، عوامل تُساهم في تهميش أصوات النساء والفتيات وقمع حريتهن في التعبير، خصوصاً في الفضاء الرقمي. يتفاقم هذا الوضع في لبنان، حيث تُشير الإحصاءات إلى أن النساء والفتيات يُشكلن الغالبية العظمى من النجاة/ ضحايا من العنف الإلكتروني،²¹ ما يؤثر على مشاركتهن الكاملة في الحياة العامة. لذلك، بات من الملح وضع قوانين مناهضة لهذا العنف وتؤسس لنهج قائم على النوع الاجتماعي لحماية جميع مستخدمي/ات الإنترنت، خصوصاً النساء، في ظلّ تزايد الجرائم الإلكترونية وتحدياتها.

وتشمل هذا الأنشطة العنيفة سرقة بيانات رسائل تهديد، قضايا خصوصية، تنمر تتعرض له النساء في عالم السياسة والاقتصاد قد يدفع بهن للثني عن المشاركة السياسية.²² نحن نرى في هذه الورقة البحثية أن هذه السلوكيات العنيفة والتحديات، لا تساهم فقط في تقويض مصداقية الشبكات لا بل وتقلل من الاعتماد على التكنولوجيا كداعم أساسي لتمكين النساء في عالم الريادة والعمل عن بعد، كما المشاركة في عالم السياسة. هذا الواقع يؤدي إلى عملية اقضاء كبيرة تشكل خطراً كبيراً في المجتمع.

على الصعيد العالمي تعددت أنماط الجرائم الرقمية حيث تمّ الكشف عن أكثر من 30 ألف حادثة جريمة إلكترونية في كلّ أنحاء العالم بين تشرين الثاني 2022 وتشرين الأول 2023 دأبت منظمة "فيمايل" على توثيق عدد الجرائم الإلكترونية التي ارتكبت ضد النساء والفتيات فبلغت 1,123 في العام 2018، و1,270 حالة في عام 2019، و315 حالة في الربع الأول من العام 2020، أي بزيادة قدرها 184 بالمئة. هذه الأرقام لم تزل تُسجل ارتفاعاً حيث ارتفعت نسبة الشكاوى لقضايا جرائم إلكترونية عبر خدمة "بلغ" التابعة لقوى الأمن الداخلي في العام 2022 وبلغت نسبة الشكاوى المقدمة من النساء 70%، وفي العام 2023 بلغت 67%.²³ وفي وقت لا يوجد دراسات وتقارير علمية محلية شاملة وذات بعد جندري لهذا النوع من الجرائم، يمكننا التزجيج أن يكون سبب ارتفاع نسبة الشكاوى المقدمة من النساء في لبنان ناتجة عن زيادة وعيهنّ بحقوقهنّ، زيادة عدد مستخدمي/ات الشبكة، لتوفر خدمات الإبلاغ عن الجرائم الإلكترونية من قبل منظمات محلية والحملات للتعريف عنها، بالإضافة إلى زيادة تعرضهنّ للعنف الإلكتروني.

الأسباب الموجبة:

على الرغم من أهمية حماية الخصوصية في العصر الرقمي، لا توفر التشريعات اللبنانية الحالية تعريفاً واضحاً أو آليات حماية شاملة لهذا المفهوم عبر أي تعريف معاصر، ما يترك المسألة للتفسير القضائي. تنص المادة 14 من الدستور اللبناني (23 أيار 1926) على أن "للمنزل حرمة ولا يسوغ لأحد الدخول إليه إلا في الأحوال، والطرق المبينة في القانون". أما مصطلح الحرية، فقد ورد في المادتين الثامنة والثالثة عشرة، حيث تشير المادة 8 إلى أن "الحرية الشخصية مصونة وفي حمى القانون"،²⁴ بينما تشمل المادة 13 حرية التعبير، ابداء الرأي والتجمع. كما تعهدت مقدمة الدستور اللبناني بانتماء لبنان إلى منظمة الأمم المتحدة واتباع مبادئها والإعلان العالمي لحقوق الإنسان (الصادر في العام 1948) والعهد الدولي الخاص بالحقوق المدنية والسياسية.²⁵ فيكرس الإعلان العالمي لحقوق الإنسان هذا الحق في الخصوصية ضمن المادة 12، التي تمنع التدخل التعسفي في الحياة الخاصة للأفراد وتضمن الحماية القانونية ضد التدخلات.

21 <https://www.statista.com/topics/9384/gendered-abuse-online/#topicOverview>

22 للمزيد يمكن قراءة الخبر عبر الرابط الإلكتروني التالي: <https://www.skeyesmedia.org/ar/News/News/08-03-2023/10537>

23 <https://tinyurl.com/ecys3w74>

24 <http://77.42.251.205/LawArticles.aspx?LawTreeSectionID=263836&lawId=244058&language=ar>

25 <https://tinyurl.com/Universal-Declaration>

26 <https://www.ohchr.org/ar/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

على صعيد الاتحاد الأوروبي وفيما يتعلق بحماية البيانات الشخصية (GDPR) على سبيل المثال تتضمن اللائحة العامة قانون شامل لحماية البيانات (الصادر في العام 2016 ودخل حيز التطبيق منذ 25 أيار 2018) الأفراد، ويقدم لهم/ن القدرة على التحكم أكثر في بياناتهم/ن الشخصية وتصحيحها أو حذفها. كما يقدم حق نقل البيانات والاعتراض على معالجتها وتوحيد قوانين حماية البيانات في كافة الدول الأعضاء في الاتحاد.

كما يلزم القانون المنظمات بالشفافية والحصول على الموافقة على أي استخدام للمعلومات، مع تعيين مسؤول/ة حماية البيانات والإبلاغ عن الانتهاكات كما تطبيق غرامات مالية كبيرة لدى حدوثها.

بالعودة الى لبنان، من الجدير بالذكر أنه عند صياغة الدستور اللبناني في عام 1926، لم يكن من المتوقع أن يتجاوز مفهوم الحرية والحياة الشخصية حدود الحقوق المعروفة آنذاك لتشمل ما أصبح مألوفًا اليوم في عصر المعلوماتية والتطور الرقمي. يمكن تلخيص أربعة عناصر رئيسية للخصوصية كما يلي:

خصوصية الجسدية

حماية الأفراد من أي انتهاك جسدي؛

خصوصية الاتصالات والمراسلات

حق الأفراد في الحفاظ على سرية اتصالاتهم/ن، بما في ذلك البريد الإلكتروني والمكالمات الهاتفية؛

الخصوصية المكانية

حماية حرمة المسكن والقواعد المنظمة للتفتيش في الأماكن الخاصة والعامة؛

الخصوصية المعلوماتية

تنظيم إدارة البيانات الشخصية على الأجهزة الإلكترونية والإنترنت، ما يتيح للأفراد التحكم في معلوماتهم/ن الشخصية مثل البيانات الصحية والمالية والاجتماعية، وتحديد كيفية وصول الآخرين إلى هذه المعلومات، سواء كانت محفوظة على البريد الإلكتروني أو منصات التواصل الاجتماعي. يعتبر هذا أمرًا حساسًا، نظرًا لاحتمالية مشاركة المستخدمين/ات لمعلوماتهم/ن دون مراعاة جوانب الخصوصية والرقابة.²⁷

صدر قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي في لبنان (يسمى أيضًا قانون 2018/81) في 10 تشرين الأول من العام 2018²⁸، كقانون فريد في التشريع اللبناني هدفه معالجة الأمور القانونية-الإلكترونية من الناحية المدنية والتجارية والجزائية. في شباط 2024، أصدرت مؤسسة سمير قصير بالتعاون مع منظمة "نواة" للمبادرات القانونية تقريرًا حمل عنوان "نحو قانون حديث لحماية البيانات ذات الطابع الشخصي في لبنان"، يُشدد على ضرورة إقرار تعديلات جوهرية فيما يتعلق بحماية الخصوصية والبيانات ذات الطابع الشخصي. ويصف التقرير هذا القانون بالقديم حيث أحكامه غير فعالة لحماية البيانات في الوقت الحالي، وهو غير شمولي ولا يراعي مبدأ "الاستقلالية الذاتية للفرد" بشكل كامل، ولا يشترط موافقة صاحب/ة البيانات على معالجة بياناته/ا. وذكر التقرير أن نسبة الالتزام به محدودة جدًا ويتم خرقه من من قبل قوى وشخصيات سياسية خلال أوقات مختلفة مثال الحملات الانتخابية.

يُعدّ التحليل المُفصّل لأطر حماية البيانات هو أمر بالغ الأهمية في سياق العنف الرقمي، لا سيما العنف القائم على النوع الاجتماعي. تُساهم حماية البيانات في حماية الضحايا بمنع مشاركة معلوماتهم/ن الحساسة التي قد تُستخدم لإيذائهم/ن، خصوصًا النساء والفتيات الأكثر عرضة للعنف عبر الإنترنت كما المهمشين/ات والمستضعفين/ات. كما توفر هذه الأطر مسارًا لمحاسبة الجناة خاصة في قضايا العنف الجندري مثل التحرش والمضايقة. وتُساهم هذه الآليات في بناء الثقة وتشجيع الإبلاغ: الضحايا وكاشفي/ات الفساد على الإبلاغ والسعي للحصول على الدعم.



²⁷ <http://77.42.251.205/ViewResearchPage.aspx?id=57&language=ar>؛ هانيا محمد علي فقيه. حماية الحق في الخصوصية المعلوماتية دراسة تحليلية لواقع الحماية وتحديات العصر. الرابط الإلكتروني

²⁸ <http://legiliban.ul.edu.lb/Law.aspx?lawId=278573&language=ar>

²⁹ https://www.skeyesmedia.org/documents/bo_filemanager/Data-Protection-Report_AR.pdf

مُكافحة العنف الرقمي :

تعميم منظور النوع الاجتماعي والتقاطعية

في هذا السياق، نرى -وبعد مراجعة التقارير والقوانين- أن تحديث القانون ومراجعته انطلاقًا من مفهوم سياسات تعميم منظور النوع الاجتماعي Gender Mainstreaming والتقاطعية Intersectionality مسؤولية وطنية، تُساهم بمعالجة العنف عبر الإنترنت بفعالية، بما في ذلك العنف القائم على النوع الاجتماعي.

إن فهم العنف الرقمي وجذوره ضروري لمعالجة أسبابه، كما فهم التطور التكنولوجي والمعلوماتي أيضًا والربط بين المفهومين ضروري للغاية لدى المشرع/ة. فالعنف الإلكتروني له علاقة متجذرة بالموثوثات الثقافية القائمة منذ زمن طويل خارج إطار العالم الرقمي، لتنتقل إليه وتساهم في تعزيز التمييز وسوء استخدام السلطة كفائض للقوة ما يسمح بتمديد واقع الهيمنة عبر الإنترنت. قد تكون أحد الأسباب الرئيسية للعنف الإلكتروني هو الانتقال غير المنظم للمعايير الاجتماعية التي تبرر السلوك العدواني من العالم الواقعي إلى الفضاء الرقمي.

قد يُعزّز نقص الوعي بالسلامة الرقمية انتشار هذه السلوكيات، حيث قد تتردد النجاة/ الضحايا في الحديث عن التجارب المؤذية أو لا يعرفون/ن كيفية طلب المساعدة. كما نواجه نقصًا في التشريعات وضعفًا في مواكبة التطور التكنولوجي السريع، بالإضافة إلى نقص الخبرات في هذا المجال.

من هنا تبرز أهمية العمل على الدراية الإعلامية والمعلوماتية كإطار أساسي لوضع سياسات ومشاريع في هذه الحالة. فمن خلال تعزيز مهارات التفكير النقدي، وتشجيع المواطنة الرقمية المسؤولة، وإنشاء مساحات شاملة لخلق بيئة رقمية تقاطعية بمقاربة حمائية وأكثر أمانًا واحترامًا للجميع، حيث يتم دمج آليات ومسارات عملية للدراية الإعلامية والمعلوماتية والبرامج الوطنية في القطاعين العام والخاص. وبناءً على ذلك، من الضروري وضع قوانين تحمي من العنف الرقمي. على أن يكون إطارًا قانونيًا، تقاطعيًا شموليًا يركز على قضايا حقوق الإنسان والحريات، ومنها:

قوانين مكافحة التنمر الرقمي: تشمل المضايقات والتنمر عبر المنصات الرقمية لتصل لكل أنواع العنف الرقمي وحماية كاشفي/ات هذه الجرائم ان كانت المصلحة العامة هي الهدف الأساس. كما حماية الضحية/الناجية من الانتقام أو الثأر في حال تقدمت بالشكوى

قوانين حماية البيانات والخصوصية: بما في ذلك التصدي لمن ينتهك الخصوصية مثل مشاركة الصور أو البيانات الشخصية بدون إذن قوانين خطاب الكراهية والتحريض: أي كل ما ينتج عنه عنف رقمي مثل المحتوى الذي يحرض على العنف أو الكراهية ضد الأفراد بناءً على خصائصهم/ن الشخصية مثل العرق، النوع الاجتماعي أو التوجه الجنسي أو غير ذلك من الخصائص. هذا الخطاب ينتشر بسرعة في البيئة الرقمية



في لبنان لا يمكن اعتبار أي فعل جريمة أو فرض عقوبة عليه إلا إذا كان هناك نص قانوني يحدد ذلك بشكل واضح. لذلك لا يمكن فرض عقوبة على أفعال غير محددة بوضوح قانونيًا، من هنا الحاجة إلى نص قانوني يحدد أركانه والعقوبات المترتبة عليه. قانون العقوبات اللبناني الحالي، الذي وُضع في الأربعينيات، لا يتضمن نصوصًا تتعلق بجرائم انتهاك الخصوصية المعلوماتية، ما يُعقد مسألة معاقبة مرتكبي/ات هذه الجرائم في ظل التطور التكنولوجي. في حين يتيح التشهير في الفضاء الرقمي نشر معلومات مسيئة أو كاذبة عبر الإنترنت بهدف الإضرار بسمعة شخص ما أو التشهير به/ا. هذا النوع من الجرائم يتسم بسرعة الانتشار وسهولة الوصول إلى جمهور واسع، ما يزيد من حدة الضرر الذي يمكن أن يلحق بالفرد، مما يستوجب وضع قوانين متطورة تتماشى مع هذه التحديات الحديثة.

تُعدّ جرائم الذم والقدح عبر الإنترنت من التحديات القانونية الحديثة في لبنان، حيث تُعدّ شبكة الإنترنت وسيلة علنية تُمكن من نشر الإساءات والتشهير على نطاق واسع يمكن أن يصل إلى ملايين الناس عبر مواقع التواصل الاجتماعي والبريد الإلكتروني. يطرح هذا الأمر تساؤلات حول إمكانية تطبيق أحكام قانون العقوبات اللبناني، خصوصًا المادتين 582 و584، المتعلقة بجرائم الذم والقدح على الأفعال المرتكبة عبر الإنترنت. وتثير هذه المسألة الحاجة إلى النظر في مدى اعتبار الإنترنت وسيلة نشر وفقًا للمادة 209 من قانون العقوبات، إضافة إلى ضرورة تنظيم الاختصاص القضائي للنظر في دعاوى القدح والذم المرتكبة عبر الإنترنت.

نحو بيئة رقمية آمنة في لبنان : دروس من قانون الخدمات الرقمية

بعد طول انتظار صدر قانون الخدمات الرقمية Digital Service Act في تشرين الأول 2022 ودخل حيز التنفيذ في 25 آب 2023 في كافة بلدان الإتحاد الأوروبي (19 دولة رسميًا). والقانون عبارة عن مجموعة من الأسس التنظيمية وهدفها حماية المستخدم/ة من المحتوى الضار مثل العنف وإجبار المنصات الكبرى على معالجة هذه المشكلات بفعالية أكبر. أهمية هذه القانون أنه يضع معيارًا عالميًا محتملاً لحوكمة المنصات يستطيع من خلاله المشرع/ة اللبناني العمل على نموذج تحكيمي مماثل، كما يُحمل المنصات لدى تطبيقه كاملًا مسؤولية المخاطر المجتمعية الناجمة عن استخدام خدماتها وضرورة أن تكون أكثر شفافية حول كيفية عمل أنظمتها الخوارزمية وحماية مجتمعه الرقمي. رغم التحديات من المتوقع أن يوفر القانون بيئة أكثر أمانًا ويسهل الإبلاغ عن العنف وحماية الضحايا كما تعزيز الثقة عبر الشفافية والمساءلة.

لذلك نرى أن تطوير قوانين الإنترنت وإنفاذها أمر حيوي لعدة أسباب:

- توفير الحماية القانونية للأفراد من كافة الهويات في مجتمع الشبكات وضمان حقوقهم/ن في الخصوصية والسلامة
- توفير الأطر القانونية الوقائية والردعية
- تفعيل آليات التنظيم الذاتي للمساءلة عبر عدة دوائر وسلطات تنفيذية وطنية شاملة، وتساعد على محاسبة الجناة وتوفير سبل العدالة للضحايا/ النجاة
- تقديم الحماية القانونية والدعم النفسي للضحايا/ النجاة، بما في ذلك الموارد القانونية، المعونة القضائية وتدابير الحماية



ما هي النقاط الاساسية المقترحة في البحث الحالي وما هو الإطار التشريعي المقترح :

تعريف العنف الرقمي وما هي الأفعال المجرمة:

تتعدد التعريفات المتعلقة بالعنف الرقمي، فيما يلي نظرة عامة على بعض هذه التعريفات وأهم المصطلحات

يُعدّ العنف الرقمي ظاهرة عالمية ومتنامية. تشمل مجموعة من السلوكيات الضارة التي تُرتكب عبر وسائل رقمية، ولكل بلد سياقه الخاص وأشكاله المختلفة من هذه الظاهرة، منها المراقبة الإلكترونية، اختراق الحسابات الشخصية، ونشر صور خاصة دون موافقة، وكلها تهدف إلى التحكم بالضحية/ الناجية أو إيذاؤها.

وللأسف، نفتقر للأبحاث الشاملة حول هذه الظاهرة في لبنان وفي العديد من البلدان، ما يحول دون فهم تجارب النجاة/ ضحايا العنف الرقمي. ومع ذلك، من خلال التعريف بأنواعه الأكثر شيوعاً، نسعى إلى تقديم معرفة وحلول عملية وقانونية لمعالجة هذه السلوكيات، والتي تشمل انتهاك الخصوصية، والإساءة، والاستغلال الجنسي، وجرائم التحريض وبث الكراهية، بالإضافة إلى التهديد بالعنف الجسدي.

يُخلّف هذا النوع من العنف آثاراً سلبية عميقة على ضحاياه، قد تصل إلى الاكتئاب، ضعف أو فقدان الثقة بالنفس، القلق، والعزلة الاجتماعية. كما يساهم في خلق بيئة رقمية غير آمنة وسامة، بعيدة عن الحرية. هذا الواقع يتطلب استجابات متعددة المستويات للتصدي له، من خلال الوقاية والتوعية، وصولاً إلى التدخل القانوني لحماية النجاة/ الضحايا، ورسم مسار رادع، وبناء مجتمع رقمي أكثر أماناً للجميع.

ولعل من الضروري فهم علاقات القوة وتحليل ديناميكياتها من ناحية جندرية لفهم معمق أكثر فعالية للعنف الرقمي، أيّ بتحويل كل عمل وكل حملة في الفضاء الرقمي إلى جزء من دراسة بناء القوة المبنية على النوع الاجتماعي في الفضاء الرقمي. هنا تكمن أهمية التعريف الذي يقدمه صندوق الأمم المتحدة للسكان في ورقة نصائح بشأن الإبلاغ عن العنف الرقمي: دليل مرجعي عملي للصحفيين/ات ووسائل الصادر عام 2021 التالي: "أي عمل من أعمال العنف يرتكبه فرد أو أكثر ويعود إلى عدم المساواة في النوع الاجتماعي والمعايير الجنسانية ويُرتكب ويُساعد ويتفاقم ويُضخم جزئياً أو كلياً باستخدام تكنولوجيات المعلومات والاتصالات أو وسائل الإعلام الرقمية، ضدّ شخص على أساس نوعه الاجتماعي".

ويشمل العنف الرقمي التنمر الإلكتروني، التحرش، نشر معلومات خاطئة، مضلة وضارة. هذه السلوكيات تتطلب استجابة شاملة منها التربية المعلوماتية، الإشراف على المحتوى، وإجراءات الإبلاغ. يجب على المدارس والمؤسسات التعليمية تعزيز ثقافة المعرفة والاحترام، فيما يلعب صانعو/ات السياسات دوراً في سن تشريعات لمعالجة هذه القضايا وضمان محاسبة الجناة، وعلى شركات التكنولوجيا أن تتحمل مسؤولية توفير بيئة آمنة عبر الإنترنت ومسار للإبلاغ عن أيّ عنف قد يحدث. هذه الجهود التشاركية من كافة الأطراف هي ضرورة لعالم رقمي أكثر أماناً وشمولية. هذا قد يساهم في التخفيف من أضرار التنمر الإلكتروني وتعزيز احترام المستخدمين/ات حول العالم رقمياً.



من هم/ن النجاة/ ضحايا العنف الرقمي وأنواعه الأكثر انتشارًا؟

في الحقيقة يمكن أن تقع كل من النساء والرجال ضحايا للعنف الرقمي. لكن تشير أغلب الأرقام إلى أن النساء والفتيات معرضات بشدة لهذا النوع من العنف.³⁰ ليس فقط. أنهن أكثر عرضة للاستهداف بالعنف الرقمي، بل يمكن أن يعانين من آثار ونتائج ممكن تؤدي إلى أذى ومعاناة جسدية، نفسية واقتصادية.

فيما تشكل المعرفة أهمية أساسية للأشخاص المنخرطين في التغيير الاجتماعي من الضروري تعلم تحليل ديناميكيات القوة من أجل تحديد أين ينبغي التحرك لتحقيق أكبر قدر من التأثير. من هنا وضع خطة عمل فعالة وتعريف بعض مظاهر السلوكيات العنيفة من اعتداء على الأفراد أو المجموعات أو المؤسسات مسار بحثي لا بد منه.

30



من أنواع العنف الرقمي الأكثر انتشارًا نذكر التالي

المطاردة الرقمية Cyberstalking : متابعة أنشطة شخص معين على الانترنت بشكلٍ يسبب القلق والخوف، المضايقة، التتبع، التهديد والسيطرة. مثال: استخدام تطبيقات تتبع الهاتف عبر نظام تحديد المواقع العالمي GPS.

الابتزاز الجنسي عبر الإنترنت Sextortion : هو شكل من أشكال الإكراه والفساد من أجل ابتزاز خدمات جنسية من الضحية/ الناجية، وهو استغلال جنسي مبني على سوء استخدام السلطة. يحصل عندما يهدد شخص ما بتوزيع مواد خاصة وحساسة باستخدام وسيط إلكتروني وقد يحصل مع الجميع خاصة النساء والأطفال/ الطفلات

العنف الرقمي القائم على الصورة Image-Based Violence : ظاهرة عنف رقمي منتشرة ودائمة التطور وتشمل أشكالاً مختلفة من التوزيع بغرض الأذية أو سوء استخدام كما وسيلة الحصول على مواد مصورة لأشخاص آخرين بمساعدة تقنيات الرقمية. مثال نشر صور عارية دون إذن، أو ما يسمى بالإيحاء الانتقامية أو تلقي صوراً جنسية غير مرغوب فيها

التنمر الرقمي Cyberbullying

يعكس مصطلح التنمر سلوك عدواني هدفه التهميش والأذى. من هنا يُعتمد إهانة، أو تهديد أو إحراج أو مضايقة مستخدم/ات الشبكة وهو سلوك عدواني متكرر يستهدف الأفراد بهدف إيذائهم نفسيًا واجتماعيًا. يتضمن هذا السلوك السلبي أفعال مثل نشر الشائعات، التهديد، الإهانة، الإحراج، والانتحال. يتم ارتكاب هذه الأفعال عبر مختلف المنصات الرقمية، من مواقع التواصل الاجتماعي كما منصات مشاركة الصور والفيديوهات. أخطار التنمر الرقمي لا تقتصر على الضحية/ الناجية فقط، بل تمتد لتشمل المجتمع ككل

التحرش الرقمي Cyber-harassment : هو شكل من أشكال العنف السيبراني ويشمل أي سلوك مستمر ومتكرر وممتد من خارج العالم الرقمي كفائض القوة تجاه الضحايا/ النجاة عبر التهديد بالعنف، أو نشر الأكاذيب التشهيرية التي قد تسبب في إحراج الضحية/ الناجية، كما انتحال شخصية الضحايا/ النجاة. وقد ينتهك المتحرشون خصوصية الضحايا/ النجاة عن طريق نشر معلوماتهم/ن الحساسة، مثل الصور العارية أو أرقام الهوية أو قد يستخدم المتحرشون التكنولوجيا لقطع الاتصال بالإنترنت. غالبًا ما يستهدف التحرش الإلكتروني النساء والفتيات ويطلق عليه "العنف الإلكتروني ضد النساء والفتيات أو العنف السيبراني ضد النساء والفتيات كما يحدث ضد صغار السن من الفتيان) الذي يتضمن

● رسائل بريد إلكتروني أو رسائل أخرى غير مرغوب فيها ذات طابع جنسي صريح؛

● الإيحاءات المسيئة في وسائل التواصل الاجتماعي وغيرها من المنصات؛

● التهديد بالعنف الجسدي أو الجنسي؛

● خطاب الكراهية بمعنى اللغة التي تشوه أو تهين أو تهدد أو تستهدف فردًا ما على أساس هويته (الجنسانية) و/أو سمات أخرى (مثل التوجه الجنسي أو الإعاقة)



التشهير الإلكتروني والابتزاز عبر الإنترنت: وقد يتحول هذا النوع من العنف إلى الابتزاز الجنسي (الابتزاز من خلال التهديد بنشر معلومات خاصة أو بيانات رقمية أو صور أو مقاطع فيديو قد يكون لها طابع جنسي)؛ والإساءة القائمة على الصور (مشاركة الصور الحميمة دون تراض)؛ والتشهير (استخدام التكنولوجيا لنشر المعلومات الشخصية الخاصة ونشر الشائعات أو المعلومات الكاذبة عنهم/ن)؛ والتنمر السيبراني. وقد يتحول إلى عنف قائم على النوع الاجتماعي. وقد يقوم به أفراد أو عصابات رقمية Digital Mobbing.

القرصنة الإلكترونية Online Hacking : هي عملية اختراق غير قانونية لأجهزة الحاسوب والشبكات بهدف الوصول لمعلومات حساسة أو التلاعب بها أو تدميرها عبر شبكة الإنترنت ويقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة برامج مساعدة الدخول إلى حاسوب آخر والتعرف على محتويات عن طريق استغلال نقاط الضعف في أنظمة الحماية للوصول غير المصرح به إلى حسابات وبيانات شخصية أو خاصة. وتشمل عمليات القرصنة مجموعة واسعة من الأنشطة، مثل سرقة الهويات، والابتزاز، والتجسس، ونشر البرامج الضارة.

الاستغلال الجنسي للأطفال/الطفلات عبر الإنترنت Online Sexual Exploitation & Sexual Abuse of Children : يشير هذا المصطلح إلى قوة التكنولوجيا وتأثيرها على مجموعة واسعة من الأفعال الجرمية والتي تستهدف الأطفال/الطفلات جنسيًا عبر استخدام تكنولوجيا المعلومات والاتصالات. لتسهيل ارتكابها بالكامل. هذه الأفعال تشمل، على سبيل المثال لا الحصر، إنتاج المواد الإباحية المتعلقة بالأطفال والطفلات، توزيعها، حيازتها، الإغواء، والابتزاز الجنسي للأطفال/الطفلات كما إفسادهم/ن والاتصال المباشر بالأطفال/الطفلات لأغراض جنسية. هذه الأفعال الجرمية غالبًا ما تتم عبر الإنترنت أو عبر الأجهزة المحمولة، تستغل ثقة الأطفال/الطفلات وضعفهم/ن، وتترك آثارًا نفسية واجتماعية عميقة وطويلة الأمد على الضحايا/ النجاة.

ويُقصد بمصطلح "المواد الإباحية المتعلقة بالأطفال/الطفلات" أي مادة تصور بصريًا طفل/ة منخرط/ة في سلوك جنسي حقيقي أو يحاكي سلوكًا جنسيًا صريحًا أو أي تصوير للأعضاء الجنسية للطفل/ة لأغراض جنسية في المقام الأول وبالتالي تعزيز الأثر الضار الطويل الأمد للإساءة إلى الأطفال/الطفلات من ممارسة أنشطة جنسية مع الأطفال/الطفلات، سواء بالإكراه أو عن طريق استغلال علاقة الثقة، أو من خلال استهداف الأطفال/الطفلات الضعفاء بما في ذلك ما قد يحدث داخل الأسرة أو في المدرسة أو أي مكان آخر حين تساهم التكنولوجيا في توسيع نطاق هذه الجرائم وتسهيل ارتكابها عبر الحدود الجغرافية.

كما يُعتبر خطاب الكراهية عبر المنصات Online Hate Speech نوع من العنف الرقمي. يتضمن خطاب الكراهية استخدام المنصات الرقمية لنشر أو التحريض على العنف أو التمييز أو الكره ضد أفراد أو مجموعات بناءً على صفات مثل العرق، الدين، النوع الاجتماعي والتوجه الجنسي. يمكن أن يؤدي هذا النوع من الإساءة إلى الأذى نفسيًا وجسديًا، والإقصاء كما العنف الجسدي.

ويجب التنبيه إلى التزييف العميق Deepfakes ومخاطره، وهو عبارة عن ملفات فيديو (أفلام) أو ملفات صوتية مزيفة تنشر في الفضاء الرقمي. هذه الملفات تم التلاعب بها باستخدام الذكاء الاصطناعي خصوصًا وأنها سهلة الانتاج حيث تسمح الخوارزميات في البرامج أو التطبيقات إمكانية إنتاج صور متحركة، أفلام تسجيلات صوتية مزيفة يصعب التحقق منها بسهولة. ويمكن استخدام هذا المحتوى لنشر العنف رقميًا. فيما يشير مصطلح "Doxxing" وهو اختصار لعبارة "إسقاط الوثائق"، إلى نشر المعلومات الشخصية والخاصة علنًا ودون موافقة مسبقة وهي تشمل عنوان السكن أو أرقام الهواتف أو عناوين البريد الإلكتروني أو التفاصيل المالية. هذا الفعل قد يكون وسيلة للتخويف أو لتشجيع الآخرين على مضايقة الضحية/ الناجية.



الآليات :

حماية الضحايا/ النجاة من توفير دعم قانوني ونفسي، آلية آمنة وسرية للإبلاغ عن جرائم العنف الرقمي وكيفية حماية الفئات المهمشة كما تحديد دور الجهات المختصة من مؤسسات أمنية، وزارة العدل، القضاء وزارة الاتصالات ومنها هيئة تنظيم الاتصالات كما وزارة التربية والتعليم وأي وزارة أو ادارة معنية أخرى.

من الأطراف المعنية، أي من الحكومة إلى مؤسسات A Multi Stakeholder Governance Approach تتطلب مكافحة جرائم العنف الرقمي تضافر جهود حوكمة أصحاب المصلحة الدولة، القضاء إلى التقنيين/ات كما المجتمع المدني والأهلي من المؤسسات التربوية وصولاً إلى الفرد. حيث يشكل تطبيق مقترحات، لبناء نظام حماية قوي للناجيات/ضحايا جرائم العنف الرقمي وتعزيز ثقافة الأمن السيبراني والتربية المعلوماتية للجميع من كافة الأطياف والطبقات الاجتماعية وكل مقيم/ة في لبنان. ويمكن لأصحاب المصلحة العمل على وضع مسار وآلية عمل شاملة ولا مركزية لحماية النجاة/ ضحايا العنف الرقمي في لبنان، مع التركيز على توفير الدعم اللازم لهم/ن وتمكينهم/ن من الإبلاغ عن الجرائم بسهولة وسرية بعيداً عن اللوم والحفاظ على الخصوصية وتقديم كل حاجات التمكين النفسي والمجتمعي من خلال ما يلي:

1- آلية شاملة لحماية النجاة/ ضحايا الجرائم الإلكترونية في لبنان

وضع قوانين وسياسات لتحديد الجرم في قضايا العنف الرقمي ودرجاته.

أسس إبلاغ سهلة، واضحة وتضمن سرية البيانات عبر بناء نظام حمائي شامل ضد العنف الرقمي يشمل سياسات حكومية واضحة في كل الإدارات وتدريب مدربين/ات على كيفية تلقي الشكاوى والتعامل معها. دعم المبادرات الخاصة في الشركات وفي المؤسسات التربوية على وجه الخصوص.

بناء تحالفات من قضاة وقاضيات كما لجنة من المحامين/ات لتقديم المعونة القضائية والاستشارة خصوصاً لمن لا يملك القدرة المادية لذلك. كما وزارات العدل، الاتصالات، الشؤون الاجتماعية والشركات.

وضع سياسات واضحة لحماية البيانات الشخصية في الفضاء الرقمي، تكون مسؤولة عن تنظيم جمع وتخزين واستخدام هذه البيانات.

تطوير آليات فعّالة للإبلاغ عن جرائم العنف الرقمي، مع ضمان سرية بيانات الضحايا/ النجاة وتوفير الدعم اللازم لهم/ن وحماية كاشفي/ات الفساد في هذه القضايا.

توفير خطوط ساخنة ومتخصصة تعمل على مدار الساعة وتقدم الدعم الأولي للضحايا/ النجاة.

توفير خدمات دعم نفسي وقانوني مجانية ومتخصصة لضحايا/ النجاة من الجرائم الإلكترونية، سواء كانوا أطفالاً/ طفلات أو بالغين/ات. يمكن تحقيق ذلك من خلال إنشاء مراكز دعم متخصصة في كافة المناطق اللبنانية. كما توفير منصات إلكترونية آمنة وسرية لتقديم البلاغات، ما يتيح للضحايا/ النجاة الإبلاغ عن الجرائم دون الحاجة إلى التوجه شخصياً إلى مراكز الشرطة.

تطوير قوانين ملزمة للمتابعة النفسية مع تحديد الكلفة وضمان حصول كافة الفئات المجتمعية المستهدفة عليها. بالإضافة إلى تحديد الجهة المخولة العمل على تفعيلها، تطبيقها ومراجعتها.

تنظيم برامج توعية واسعة النطاق حول الجرائم الإلكترونية وكيفية الوقاية منها، مع التركيز على الفئات المستضعفة مثل النساء، الأطفال/ الطفلات وكبار/كبيرات السن.

تطوير وتطبيق برامج حماية كاشفي/ات الفساد أو مطلقي/ات الصفارة أو الشهود/ الشاهدات، وحماية هوية الضحايا/النجاة الذين/ اللواتي يكشفن ما حصل وقد يقدمن الشكاوى أو البلاغ، وقد يتعرضون/ن للانتقام.



آلية شاملة لتعزيز قدرات المؤسسات الحكومية، الأمنية والقضائية

- تدريب عناصر الأجهزة الأمنية والقضائية على التعامل مع الجرائم الإلكترونية، بما في ذلك جمع الأدلة الرقمية وتحليلها كما برنامج للتعامل مع كاشفي/ات العنف وضمان حمايتهم/ن.
- التعاون الاقليمي والمحلي من أجل تعزيز التعاون لمكافحة العنف الرقمي العابرة للحدود، وتبادل البيانات المتخصصة بناء على أسس الشفافية وحماية البيانات الشخصية.
- دعم المنظمات غير الحكومية التي تعمل في مجال مكافحة العنف الرقمي، وتعزيز دورها في التوعية وتقديم الدعم للضحايا/ النجاة.
- بناء شراكات مع منظمات المجتمع المدني والمؤسسات الدولية لتبادل الخبرات والمعرفة في مجال النوع الاجتماعي والجرائم الإلكترونية.

حماية الفئات الضعيفة/المهمشة

- توفير حماية خاصة للأطفال/ات من خلال تفعيل القوانين التي تجرم استغلال الأطفال/الطفلات جنسياً عبر الإنترنت، وتوفير برامج توعية للأطفال/الطفلات وأولياء الأمور
- حماية النساء والفتيات من العنف الإلكتروني، مثل التحرش والابتزاز، من خلال توفير الدعم القانوني والنفسي لهن
- توفير خدمات دعم مخصصة لذوي وذوات الإعاقات الذين قد يكونون أكثر عرضة لوقوع ضحية العنف الرقمي

التعديلات التشريعية

- تحديث القوانين اللبنانية وتفعيل تطبيقها وفق التطورات التكنولوجية لتشمل العنف الرقمي ومواءمتها مع التطورات المستجدة

التوعية والوعي المجتمعي

- دور المؤسسات التربوية من خلال برامج التربية الإعلامية والمعلوماتية
- دور وسائل الإعلام من خلال تطبيق أدبيات وسلوكيات مهنية وأخلاقية خلال التغطية بعيداً عن التسريبات ودون مشاركة الأسماء أو معلومات خلال التحقيق؛ كما العمل على محتوى متخصص يشجع على التفكير النقدي والجانبى دون إثارة مشاعر الخوف أو الغضب، اي مضمون يساعد على تجنب مخاطر العنف ويقدم مسار وآليات في حال حدوثه
- تعزيز الشراكة مع منظمات المجتمع المدني للوصول إلى الفئات الضعيفة وتقديم الدعم اللازم لها

البعد الاقتصادي

- تخصيص ميزانية واضحة، شفافة وملزمة لتنفيذ أي من المقترحات
- العمل مع المنصات الكبرى على تخصيص دعم من مردود الإعلانات عبر صفحاتها لتمويل مشاريع ضمن المسؤولية المجتمعية لهذه الشركات Corporate Social Responsibility Fund.

مسؤولية الشركات وخوارزميات البيانات

منذ وقت ليس ببعيد كثيراً اعتبر مستخدمو/ات وسائل التواصل الاجتماعي أن هذه المنصات هي مكان يساعد على تمكين المواطنين/ات كما لنشر الأفكار والتواصل بحرية دون قيود لكن مع الوقت بدأت شكوك كثيرة حول دور هذه المنصات من خلال المعلومات والبيانات شخصية التي تجمعها والخوارزميات. والجدير ذكره أن هذه الخوارزميات هي مجموعة متسلسلة من القواعد والحسابات التي تستخدمها منصات التواصل الاجتماعي لتحديد أولويات المحتوى الذي يراه المستخدمون/ات في صفحاتهم/ن. تعتمد هذه القواعد على سلوك المستخدم/ة، أهمية المحتوى، وشعبية المنشورات في السياق المحلي للمحتوى وهي تختلف من منصة إلى أخرى. هذه الخوارزميات لها إحدًا تأثير كبير من خلال دراسة تفاعل مستخدمي/ات المنصات مع البيانات الخاصة. لذلك، اليوم أكثر من أي وقت مضى، على منصات تكنولوجيا التواصل الاجتماعي الكبرى، أن تخضع خوارزمياتها لرقابة تنظيمية صارمة لضمان حماية حقوق المستخدمين والمستخدمين عالميًا من أيّ عنف رقمي أو تحريض على الكراهية ينشأ من جراء خوارزميات وسائل التواصل الاجتماعي التي يمكن أن تصبح ضارة وفق حسب البيانات التي تجمعها شركات التكنولوجيا الكبرى. هذا النموذج قد يحقق أرباح مادية للشركات لكن عواقبه قد تكون وخيمة على المدى الطويل على حقوق الإنسان. من هنا الدعوة إلى شفافية الخوارزميات المستخدمة في البحث عن المعلومات ومعالجتها وتقديمها وهيكلها وإجراءاتها الأساسية.

الذكاء الاصطناعي وانترنت الاشياء

يمكن للذكاء الاصطناعي أن يساعد في أتمتة العمليات وتحسين الكفاءة لأجهزة إنترنت الأشياء Internet of Things فتتمكن من التعلم من بيئتها واتخاذ القرارات بناءً على هذا التعلم، دون تدخل بشري. ومع توسع استخدام هذه التقنيات، يتعرض الناس لأشكال جديدة من الجرائم السيبرانية، بما في ذلك العنف القائم على النوع الاجتماعي. وتظهر حالات كثيرة العنف المنزلي عبر استخدام شبكة إنترنت الأشياء كوسيلة لارتكابها. لا تزال الأطر القانونية والمعارية للجرائم الإلكترونية محايدة تجاه أشكال محددة من الجرائم التي ترتكب عبر الإنترنت أو الأشكال التي تيسرها التكنولوجيا والتي تؤثر على الجميع ومنهن النساء³².

التثقيف على المعلوماتية

المحتوى الرقمي يكبر والبيانات الضخمة تتسع بسرعة وتدفق بمعدل غير معروف ولا يمكن التنبؤ به حاليًا، ولكن من المقلق تخيله. هذا التطور لا بد من أن يترافق مع استراتيجيات أساسية مبنية على الدراية الإعلامية والمعلوماتية ليس فقط لفهم المحتوى الذي يتم استهلاكه، بل أيضًا لما يتم إنتاجه مع مراعاة التنوع، الحرية، الديمقراطية، المساواة والعدالة الجندرية كما السياقات المحلية. وترتكز المهارات على التالي :

- تدريبات على تحليل المحتوى الرقمي لكشف ومسح أي عنف في المحتوى؛
- تقييم المحتوى العنفي الذي يمكن أن يتحول لفعل؛
- ابتكار محتوى يقدم بديل عن العنف ويُحدث الفرق في تقديم المعلومة المفيدة
- تطوير أدوات وموارد تعليمية ذات المصادر المفتوحة OER لمساعدة مختلف الجهات على إدماج منظور النوع الاجتماعي في أنشطتها، وتعزيز مشاركتها في مكافحة العنف الرقمي
- تشجيع البحوث والدراسات حول ظاهرة العنف الرقمي في لبنان، وذلك لفهم هذه الظاهرة بشكل أفضل وتطوير استراتيجيات فعالة لمعالجتها

32 مراجعة اتفاقية اسطنبول، ولا سيما التوصية العامة الأولى للاتفاقية، كأساس لأطر "النوع الاجتماعي" للعنف الرقمي
33 Human Rights Watch | سوء استخدام تدابير الجرائم الإلكترونية يُلغى المحادثات الأمية

اضطراب المعلومات وتأثيره على خلق خطابٍ معادٍ

هنالك أهداف أساسية وراء مبدأ حياد الشبكة وهو أن إدارة المحتوى الرقمي يجب أن يأخذ بعين الاعتبار عند تطوير المنصات الرقمية الإبداع وحرية التعبير وتبادل الأفكار خصوصًا في ظل اضطراب المعلومات أو ما يحدد عبر المعلومات المضللة، الخاطئة والضارة؛ كلها تعتمد (عن قصد أو غير قصد) على معلومات غير مؤكدة فعليًا وممكن أن تُساهم في نشر مفاهيم غير صحيحة وقد تؤدي إلى خطاب الكراهية نشهد تأثيره خلال الأزمات وفي ديناميكية النزاعات وحالات العنف والعمل في قضايا إنسانية.

لا يمكن أن ننسى الفرص التي تنتج عن التطور السريع لتكنولوجيا المعلومات الرقمية. لكن تشير دراسات التواصل عبر الإنترنت إلى تفاعل خطاب الكراهية واضطراب المعلومات مع اللغة والصور المجردة من الإنسانية والمدعومة بخوارزميات الانتشار السريع. لذلك هنالك ضرورة للعمل على البيانات الضخمة وحقوق الانسان والثقة.

أخيرًا، يشدد هذا البحث على أهمية التعامل مع ظاهرة العنف الرقمي بشكلٍ جادٍ وفعال، من خلال تضافر جهود جميع الأطراف المعنية. ويؤكد على ضرورة سنّ قانون شامل لمكافحة هذه الظاهرة، يُراعي الخصوصية الجندرية والتقاطعية، ويوفر الحماية اللازمة للضحايا/ الناجيات.

وقدم توصيات عملية لضمان إدماج مبادئ العدالة والمساواة المبنية على النوع الاجتماعي بشكلٍ فعال على أن تُعالج الجرائم الإلكترونية بطريقة تحمي الحقوق الأساسية، مع ضمان شفافية المفاوضات ومشاركة منظمات حقوق الإنسان ومنظمات³³ حقوق النساء والفتيات. كما يشدد على مراعاة حقوق جميع الفئات، بما في ذلك الأشخاص ذوو وذوات الإعاقة والأشخاص ذوو وذوات الدخل المحدود والفئات الاجتماعية المختلفة، في جميع الأنشطة المتعلقة بمكافحة العنف الرقمي. واستند في ذلك إلى دراسة نماذج لمشاريع قائمة، وإلى الموارد والمراجع الدولية .