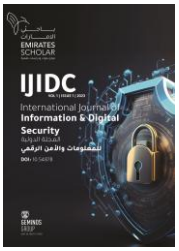

International Journal of Information & Digital Security
Vol 2 Issue 1 (2024)
Pages (40 –58)

Available at www.emiratesscholar.com

تنظيم المنصات الرقمية: دراسة مقارنة

هشام الاسماعيلي
hichamili16@gmail.com
منتدب قضائي وزارة العدل

ARTICLE INFO

Published on 30th of December 2024
Doi: 10.54878/7hc8ny87

KEYWORDS

المنصات الرقمية، السيادة الرقمية، حقوق المستخدم، الاشراف الصارم، توطين البيانات.

HOW TO CITE

تنظيم المنصات الرقمية: دراسة مقارنة. (2024). *International Journal of Information & Digital Security*, *2*(1), 40-58.

ABSTRACT

على مدار العقد الماضي، أصبحت المنصات الرقمية حاضرة وممتدة في الزمان ونتيجة لذلك، أضحت المنصات الرقمية الصينية .والمكان في جميع أنحاء العالم والأميركية إلى حد كبير تعمل على إعادة تنظيم العلاقات بين المواطنين (المستخدمين) والعالم من حولهم عبر تشكيل وتنظيم الحياة الاجتماعية السياسية والاقتصادية... وممارسة الحقوق والحريات في العالم الرقمي. مما يجعل من التنظيم والتأطير القانوني لهذه المنصات والخدمات الرقمية أولوية مركزية بالنسبة للجهات الفاعلة الحكومية بجل دول العالم. ونظرا لتنوع التوجهات التنظيمية المعتمدة حتى الآن، يحاول هذا البحث تحديد الاتجاهات التنظيمية والسمات المشتركة بينها وتصنيفها في عينات محددة، وذلك عبر القيام بدراسة مقارنة ل22 قانونا منظما للمنصات الرقمية، وتجميعهم في أربعة أصناف (النهج الصارم، النهج المستقل، النهج الذي يعزز ويحمي حقوق المستخدم، نهج توطين البيانات) بناءً على أوجه التشابه والاختلاف بينهم، عبر تحديد واستكشاف الميزات أو الخصائص الأساسية التي تتسم بها بعض التوجهات التنظيمية للمنصات الرقمية، بغية تشكيل أرضية ومنطلقاً للنقاش حول الممارسات الفضلى والقوانين الأكثر نجاعة في هذا المجال

مقدمة:

في ظل السياق الرقمي العالمي المتسم باتساع هامش الولوج إلى المحتوى الرقمي ونشره وتأثيره على توجهات وآراء المواطنين، فقد شكل ذلك تحديا للحفاظ على النظام العام والسيادة الرقمية(1). مما ساهم في حدوث فجوة قانونية بين هيمنة المنصات الرقمية على المشهد الإعلامي وقدرات الحكومات على تنظيم المحتوى الرقمي. فالولايات المتحدة، على سبيل المثال، تتبع سياسة السوق الحرة وتقاليدها الديمقراطية المتعلقة بحرية التعبير. حيث كان ترددها في تنظيم المنصات الرقمية سمة مميزة لنمو هذه الأخيرة، حيث تتمتع هذه المنصات بشكل كبير من الحرية مع مسؤولية محدودة فيما يخص تحمل الحد الأدنى من المسؤولية القانونية عما ينشره مستخدموها. وقد أدى هذا إلى خلق توتر مع انتشار تلك المنصات خارج الولايات المتحدة، وخاصة مع السلطات الأوروبية التي تنتهج نموذجاً أكثر يقظة وتنظيماً مشتركاً مع تركيز أكبر على ربط الحرية بالمسؤولية، على النقيض من تركيز الولايات المتحدة على حرية التعبير وحرية السوق الرقمية.

وبالدول التي قد يُنظر فيها إلى أن المنصات الرقمية قد تتحدى هيمنة وإشراف الدولة على الولوج إلى المعلومات وصحتها، كانت المبادرات التنظيمية والتشريعية تميل إلى أن تكون أكثر صرامة؛ حيث تعمل حكومات مثل نيجيريا وسنغافورة على سن قوانين لممارسة قدر أكبر من سيطرة الدولة على الفضاء الرقمي. وبموجب هذه الأنظمة، يمكن على نطاق واسع مطالبة المنصات بمراقبة وتصفية عينة محددة من المحتوى الرقمي بشكل استباقي، وإتاحة بيانات المستخدم للسلطات بشكل عشوائي، وتقليص هامش الحماية المقدم للمستخدم. ويبقى أن نرى ما إذا كان نهج واحد قادراً على التفوق على الآخرين، أو ما إذا كانت الأساليب المتنوعة قادرة على التعايش. فالجهود الرامية إلى إيجاد القواسم المشتركة بين النماذج التنظيمية للمنصات الرقمية لا تزال في مهدها، كما لا توجد مؤسسة دولية رئيسية واحدة يتم من خلالها التفاوض بشأن تنظيم المنصات الرقمية حاليا. فالنهج التنظيمي الواحد الذي قد يناسب الجميع، قد فشل حتى الآن في مراعاة السياقات الوطنية المتعددة.

ومن جانب آجر، وبالإضافة إلى دورها الأساسي في دعم الأعمال التجارية العالمية والاتصالات وانفتاح المجتمعات على بعضها البعض، تمثل المنصات الرقمية في سياق النظام العالمي الحالي أداة للحفاظ على قيم مثل حرية التعبير والولوج إلى المعلومات، وللتنسيق بشأن التحديات العالمية مثل تغير المناخ والتنمية المستدامة. لكن الولايات القضائية الرقمية الجديدة لا تتوفر على إطار قانوني ومؤسساتي يواجه التحديات الرقمية الراهنة المتمثلة في الأخبار الزائفة والمحتوى الرقمي الضار بجميع أصنافه وتجلياته وطبيعته العابرة للحدود.

وبالتالي، فإن القوانين الوطنية الحالية والمقبلة بالعديد من الدول المتعلقة بتنظيم المنصات الرقمية سيكون لها تأثير مباشر على ممارسة المواطنين لحرية التعبير وإمكانية الولوج إلى المحتوى الرقمي. ولهذا، فإن تلك القوانين ستحدد أيضًا بشكل جزئي مدى انفتاح الإنترنت العالمي في المستقبل. فتحقيق التوازن بين الفوائد الكبيرة للإنترنت المنفتح من ناحية والضغط الذي تبذله البلدان لممارسة قوتها عليه من ناحية أخرى، هو التحدي السياسي والقانوني الذي يواجه تنظيم المنصات الرقمية في المستقبل. كما لا ينبغي أن نغفل بأن ترسيخ حوكمة التكنولوجيا، ووضع السياسات المناسبة والمبادرات التشريعية والتنظيمية سوف تتطلب تعاوناً عالمياً وإقليميا.

كما ان نطاق القوانين والسياسات في جميع أنحاء العالم التي تنطبق على المنصات عبر الإنترنت يشكل إطارا ضخما، بما في ذلك، من بين أمور أخرى، قوانين حماية المستهلك، والمنافسة، والإعلام، وتشريعات حماية البيانات. ولأغراض هذه الدراسة، ركز البحث على القوانين التي تتعلق على وجه التحديد بقضايا مسؤولية المنصات الرقمية الوسيطة عن المحتوى الذي ينشئه المستخدم: أي القوانين التي تفرض متطلبات قانونية على كيفية إدارة المنصات الرقمية للمحتوى الرقمي. وتختلف القوانين ومشاريع القوانين التي تم تحديدها للتحليل بشكل كبير من حيث النطاق والنهج والتنفيذ. فبعضها يركز بشكل خاص على السلامة عبر الإنترنت وتنظيم المنصات من خلال قانون منفرد، في حين أن البعض الآخر مجرد بنود في تشريع أوسع نطاقًا. ولكي نتمكن من إجراء تحليل كمي وكيفي ومقارنة النهج التنظيمي عبر مجموعة القوانين موضوع الدراسة، تم اعتماد مؤشرات للتحليل يمكن تطبيقها على كل قانون أو مشروع قانون لتحديد الاتجاهات والاختلافات عبر قوانين تنظيم المنصات الرقمية، وذلك من حيث:

- ما هي أنواع المنصات الرقمية التي يشملها القانون في نطاقه؟
- ما هي طبيعة وفئات المحتوى الرقمي التي ينظمها القانون؟
- ما هي الطريقة التي يتم بها إنفاذ القانون، بما في ذلك من خلال العقوبات ووجود هيئة وطنية تنظيمية مستقلة للإشراف على المنصات الرقمية؟
- ما هي مسؤولية المنصات الرقمية بشأن المحتوى الذي ينشئه المستخدم؟
- ما هي أنواع الالتزامات التي يفرضها القانون على المنصات فيما يتعلق بتعديل المحتوى أو العمليات الأخرى ذات الصلة؟
- ما هو مستوى الحماية التي يوفرها القانون بخصوص حرية التعبير واحترام الخصوصية؟

وعبر اعتماد هذه المؤشرات من أجل تحليل ما مجموعه 22 قانونا، فقد تم تحديد واستخلاص أوجه التشابه والاختلاف بين التوجهات الدولية حول تنظيم المنصات الرقمية؛ والتي تتراوح من التنظيم الصارم الهادف إلى الحفاظ على السيادة الرقمية عبر فرض عقوبات سجنية على مستخدمي وممثلي المنصات دون توفير سبل انتصاف فعالة، إلى توجهات تشريعية تتسم بالإشراف المحدود عبر منح هامش من الاستقلالية للمنصات بشأن تدبير المحتوى الرقمي، مع توفير هيئات وطنية مستقلة لتنظيم المنصات الرقمية. في حين تركز بعض التوجهات على حماية وتعزيز حقوق مستخدمي المنصات الرقمية، وفي الوقت نفسه، تعمل بعض الدول على اتباع نهج توطين البيانات(2).

أولا. التوجهات التنظيمية الدولية للمنصات الرقمية ذات النهج الصارم:

من بين 22 قانونا على الصعيد الدولي الذين تم فحصهم خلال هذا البحث، توجد 09 قوانين تمثل نهج الاشراف الصارم على المنصات الرقمية، وهي كالآتي:

1-مشروع اللائحة التنظيمية لبنغلاديش بشأن وسائل الإعلام الرقمية ووسائل التواصل الاجتماعي والمنصات(2021) :

نشرت لجنة تنظيم الاتصالات في بنغلاديش في 3 فبراير 2022 مشروع اللائحة التنظيمية لوسائل الإعلام الرقمية والاجتماعية والمنصات الرقمية، قصد إدارة المحتوى عبر الإنترنت لحماية المستخدمين والفئات الهشة، بما في ذلك النساء والأطفال؛ ومنع الاحتيال والتهديدات للسلامة العامة والسيادة؛ وتثبيط القرصنة والفحش. ويفرض مشروع اللائحة التنظيمية في بنغلاديش من

الوسطاء، بما في ذلك وسطاء وسائل التواصل الاجتماعي، الالتزام بعدد من المتطلبات، وهي:

- يجب على الوسطاء نشر القواعد واللوائح وسياسة الخصوصية واتفاقية المستخدم بشكل واضح على موقعهم الإلكتروني أو تطبيقهم.
- يجب على الوسطاء ان يبلغوا شروط الخدمة للمستخدمين "بعدم استضافة أو عرض أو تحميل أو تعديل أو نشر أو نقل أو تخزين أو تحديث أو مشاركة أي معلومات تتعلق بما يلي:
- معلومات تنتمي إلى شخص آخر؛
- معلومات غير قانونية أو تشهيرية أو فاحشة أو إباحية أو تتطفل على خصوصية الفرد بما في ذلك الخصوصية الجسدية؛
- مضرة للأطفال؛
- تهدد وحدة البلاد أو سلامتها أو دفاعها أو أمنها أو سيادتها، أو علاقاتها مع الدول الأخرى، أو النظام العام (بما في ذلك الوئام المجتمعي والاجتماعي)، أو ينتهك سرية الحكومة؛
- -تتعارض مع حرب تحرير بنجلاديش وروحها أو شخصياتها الوطنية أو نشيدها أو علمها؛
- مسيئة أو كاذبة أو مهينة أو تهديدية أو تؤذي القيم الدينية؛
- تنتهك حقوق الملكية الفكرية؛
- تنتحل شخصية شخص آخر، أو تكون مضللة، أو تكون زائفة بشكل واضح.
- يجب على وسطاء وسائل التواصل الاجتماعي الذين يقدمون خدمات الرسائل الالكترونية من تمكين تحديد "المنشئ الأول" للمعلومات استجابةً لأمر من المحكمة (3).

وبموجب هذا القانون يمكن فرض عقوبات على شركات المنصات الرقمية؛ قد تصل إلى حوالي 35 مليون دولار أمريكي و/أو السجن لمدة تصل إلى خمس سنوات، إذا لم تتم إزالة المحتوى الرقمي المحظور(4) .

2-قانون المعاملات الإلكترونية والأمن السيبراني في ملاوي (2016):

يجرم قانون المعاملات الإلكترونية والأمن السيبراني بملاواي لسنة 2016 الجرائم الواردة في الباب العاشر، وذلك على النحو التالي:

- الولوج غير المصرح به أو الاعتراض أو التدخل في البيانات؛
- استغلال الأطفال في المواد الإباحية؛
- حظر التحرش عبر الإنترنت؛
- حظر الاتصالات الهجومية؛
- حظر المطاردة السيبرانية؛
- حظر الاختراق والتكسير وإدخال الفيروسات.
- تعطيل نظام الكمبيوتر بشكل غير قانوني.
- حظر البريد العشوائي.
- حظر التجارة غير المشروعة؛
- الشروع في ارتكاب الجرائم أو المساعدة عليها أو التحريض عليها.(5)

وتعاقب المادة 87 من هذا القانون، الاتصالات الإلكترونية "المهينة" التي تنتهك حقوق الخصوصية لأي شخص بغرامات أو بالسجن(6) .

3-قانون مالي رقم 056-2019 بشأن قمع الجرائم الإلكترونية (2019):

يجيز قانون الجرائم الإلكترونية في المواد من 74 إلى 78 تفتيش أجهزة الكمبيوتر ومصادرة البيانات كجزء من التحقيقات الجنائية. وبموجب المادة 75 من هذا القانون يجوز نسخ البيانات وتخزينها على الصعيد الوطني، وتقترح المواد من 83 إلى 86 امكانية اعتراض الاتصالات الالكترونية. وكما يتعين على مقدمي الخدمات الرقمية التعاون مع السلطات، بما في ذلك من خلال التأكد من أن لديهم الوسائل التقنية اللازمة لتسهيل اعتراض الاتصالات(7) .

علاوة على ذلك، يتعين على مقدمي خدمات الاتصالات وضع آليات لرصد أنظمة الأنشطة غير القانونية المحتملة، حيث يعاقب على عدم إبلاغ السلطات بالأنشطة غير القانونية بالسجن لمدة تتراوح بين ستة أشهر وسنتين، وغرامة ما بين (830 دولارًا أمريكيًا إلى 3,318 دولارًا أمريكيًا) أو كليهما (المادة 25)(8) .

4-قانون الاتصالات الرقمية الضارة في نيوزيلندا (2015):

تم تقديم قانون الاتصالات الرقمية الضارة لسنة 2015 لمعالجة بعض الطرق التي يستخدم بها الأشخاص التكنولوجيا لإيذاء الآخرين. والهدف من هذا قانون هو "ردع ومنع وتخفيف الضرر الذي يلحق بالأفراد بسبب الاتصالات الرقمية"، و"تزويد ضحايا الاتصالات الرقمية الضارة بوسيلة سريعة وفعالة للانتصاف". ويجوز لمقدم الشكايات تقديم طلب إلى المحكمة المحلية إذا لم تتمكن لجنة Netsafeمن معالجة الشكاية أو حلها بما يرضي مقدم الشكوى. حيث يمكن رفع دعوى أمام المحكمة المحلية مجانًا، وبدون تمثيل قانوني. وتفرض المحكمة عند الإدانة العقوبات التالية:

- في حالة الشخص الطبيعي؛ بالسجن لمدة لا تتجاوز 6 أشهر أو غرامة لا تتجاوز 5000 دولار.
- وفي حالة المنظمة أو الشركة؛ بغرامة لا تتجاوز 20 ألف دولار أمريكي(9) .

5-مشروع قانون الحماية من الأكاذيب والتلاعب على الإنترنت في نيجيريا (2019):

يسعى مشروع قانون الحماية من الأكاذيب والتلاعب على الإنترنت في نيجيريا المعروف أيضا بقانون وسائل التواصل الاجتماعي، إلى تجريم استخدام وسائل التواصل الاجتماعي في نشر معلومات كاذبة أو ضارة. ويمنح هذا القانون السلطات صلاحيات واسعة لإغلاق الإنترنت وتقييد الوصول إلى منصات التواصل الاجتماعي، من خلال حضر الموارد التي يمكن للمستخدم استخدامها والولوج إليها، كما أنه يقيد المحتوى الذي قد يساهم به المستخدم في الإنترنت(10) . ويحظر القانون على المستخدمين إرسال بيانات "كاذبة" أو التي:

- تؤثر على أمن نيجيريا؛
- تؤثر على الصحة العامة أو السلامة العامة أو المالية العامة؛
- تؤثر على علاقة نيجيريا بالدول الأخرى؛
- تؤثر على نتائج الانتخابات العامة؛
- تسبب العداوة أو الكراهية اتجاه شخص أو مجموعة من الأشخاص.

ويمكن معاقبة عدم الامتثال لحظر المحتوى الرقمي المذكور أعلاه بغرامة قدرها 826 دولارًا أو بالسجن لمدة تتراوح من سنتين إلى ثلاثة سنوات (أو كليهما) للمستخدمين الأفراد؛ وغرامة قدرها 275.550 دولارًا للمؤسسات التجارية(11) .

6-مشروع قانون مكافحة المحتوى الزائف في الفلبين (2019):

ينص مشروع القانون المتعلق بحظر نشر وانتشار المحتوى الزائف على الإنترنت بالفلبيين، على تدابير لمواجهة تأثيراته السلبية على المجتمع، ويفرض عقوبات اتجاه المخالفين لمقتضياته. حيث يمكن لمكتب الجرائم الإلكترونية التابع لوزارة العدل بالفلبين أن يلزم المستخدمين والمنصات الرقمية على إزالة المحتوى الرقمي الذي يتوفر على معلومات زائفة. كما يفرض هذا المشروع غرامة تصل إلى6,200 دولار أمريكي و/أو عقوبة سجنية قد تصل إلى اثني عشر سنة في حق أي شخص يُدان "بإنشاء و/أو نشر محتوى رقمي مع العلم أو الاعتقاد المعقول بأنه يحتوي على معلومات زائفة أو قد تميل إلى تضليل الجمهور(12) .

7-قانون التدخل الأجنبي (التدابير المضادة) في سنغافورة (2021):

يهدف هذا القانون إلى "منع وكشف وتعطيل التدخل الأجنبي في (...) السياسة الداخلية". حيث يتيح لوزير الداخلية إصدار أمر بإزالة المحتوى الرقمي عبر الإنترنت أو تعطيله. فعلى سبيل المثال، يتمتع وزير الداخلية بسلطة الأمر بنشر الرسائل الإلزامية التي صاغتها السلطات، وحظر تنزيل بعض التطبيقات الالكترونية في سنغافورة، والأمر بالكشف عن الاتصالات والمعلومات الخاصة. كما يجرم هذا القانون إجراء اتصالات إلكترونية أو نشر محتويات رقمية تقلل من ثقة المواطنين في الحكومة أو السلطات العامة. كما يمكن فرض عقوبات جنائية شديدة على الأفراد بسبب "التدخل الأجنبي السري من خلال نشاط الاتصالات الإلكترونية" عبر تغريمهم بما يصل إلى 100.000 دولار سنغافوري (حوالي 74.000دولار أمريكي) و/أو السجن لمدة تصل إلى أربعة عشر سنة(13) .

8-قانون كوريا الجنوبية رقم 14080 بشأن تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات (2016):

ينظم هذا القانون استخدام مقدمي الخدمات عبر الإنترنت للبيانات، عبر العديد من الإجراءات؛ كحظر تداول المعلومات غير القانونية، حيث تنص المادة 43 منه على أنه لا يجوز لأي شخص تداول المعلومات التالية من خلال شبكة المعلومات والاتصالات:

- المعلومات ذات المحتوى الفاحش التي يتم توزيعها أو بيعها أو تأجيرها أو عرضها علنًا في شكل تعليمات برمجية أو كلمات أو صوت أو صورة أو فيديو؛
- معلومات ذات محتوى يشوه سمعة أشخاص آخرين من خلال الكشف عن حقيقة أو حقيقة كاذبة بشكل علني ومتعمد للإساءة إلى سمعة شخص ما؛
- المعلومات ذات المحتوى الذي يثير الخوف من خلال التواصل مع أشخاص آخرين بشكل متكرر في شكل رمز أو كلمات أو صوت أو صورة أو فيديو؛
- معلومات ذات محتوى يشوه أو يدمر أو يغير أو يزيف نظام المعلومات والاتصالات أو البيانات أو البرنامج أو ما شابه ذلك أو يتعارض مع تشغيل هذا النظام أو البيانات أو البرنامج أو ما شابه ذلك دون سبب مبرر؛
- المعلومات ذات المحتوى الذي يعتبر غير صحي للأطفال بموجب قانون حماية الأطفال، والتي يتم نشرها لتحقيق الربح دون الوفاء بالواجبات والالتزامات بموجب القوانين ذات الصلة، بما في ذلك واجب التحقق من سن الطرف الآخر؛
- المعلومات ذات المحتوى الذي يقع ضمن أنشطة المضاربة المحظورة بموجب القوانين؛
- المعلومات المتعلقة بمحتوى معاملات البيانات الشخصية التي تنتهك هذا القانون أو القوانين الأخرى المتعلقة بحماية البيانات الشخصية؛
- معلومات ذات محتوى يفشي سرًا مصنفًا بموجب القوانين أو أي سر آخر من أسرار الدولة؛
- معلومات ذات محتوى يشكل نشاطًا محظورًا بموجب قانون الأمن القومي؛
- معلومات أخرى ذات محتوى يحاول أو يساعد أو يحرض على ارتكاب جريمة.

ويعاقب هذا القانون بالسجن مع الشغل لمدة تصل إلى ثلاث سنوات أو بغرامة لا تتجاوز 30 مليون وون كل من يرتكب تشهيرًا بشخص آخر عن طريق الكشف عن حقيقة للعامة من خلال شبكة المعلومات والاتصالات بهدف تشويه سمعته. ويعاقب بالسجن مع الشغل لمدة تصل إلى سبع سنوات أو بغرامة لا تتجاوز 70 مليون وون كل من ينقل أو ينشر برنامجاً خبيثاً مخالفاً لمقتضيات هذا القانون (المادة 70) هذا بالإضافة للمزيد من العقوبات السجنية التي نصت عليها المواد (71 -74-73-72) من قانون تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات(14) .

9-قواعد الاتصالات الإلكترونية والبريدية (المحتوى عبر الإنترنت) في تنزانيا (2020):

أصدرت الحكومة التنزانية لوائح الاتصالات الإلكترونية والبريدية (المحتوى عبر الإنترنت) لسنة 2020 في 17 يوليوز 2020. وهي تعمل على ترسيخ الترخيص وفرض الضرائب على المدونين ومنتديات المناقشة عبر الإنترنت ومذيعي الويب الإذاعي والتلفزيوني. وقد قدمت لوائح المحتوى عبر الإنترنت لعام 2020 أربع فئات محددة من تراخيص المحتوى عبر الإنترنت (الماة4)، وهي كالتالي:

-رخصة تُمنح لمزود خدمة المحتوى عبر الإنترنت الذي يغطي محتواه الأخبار والقضايا الراهنة؛

-ترخيص لتوفير محتوى ترفيهي رئيسي يتم إصداره لمزود خدمة المحتوى عبر الإنترنت الذي يشمل محتواه الموسيقى والأفلام والمسلسلات والمسرحيات والدراما والكوميديا والرياضة وأي محتوى ترفيهي آخر ذي صلة؛

-رخصة لتوفير المحتوى التعليمي والديني السائد تُمنح لمزود خدمة المحتوى عبر الإنترنت الذي يشمل محتواه معلومات دينية ومحتوى يهدف إلى التثقيف؛

- ترخيص البث المتزامن لمرخصي البث الرئيسيين الذين لديهم حقوق التغطية الوطنية.

إذا رفضت السلطات إصدار ترخيص، فيجب عليها إخطار مقدم الطلب خلال أربعة عشر يوماً من تاريخ الرفض مع بيان أسباب الرفض وأي توجيهات أخرى قد تحددها السلطات (المادة 7)، دون الإشارة إلى إمكانية الطعن في قرار رفض إصدار الترخيص.

ويحدد هذا القانون عشر فئات مختلفة من المحتوى الرقمي المحظور، والتي قد يؤدي القيام بها إلى التعرض لعقوبات جنائية مثل الغرامات الباهظة أو السجن. ويتمثل المحتوى الرقمي فيما يلي:

- الإخلال بالأخلاق،

-الاخلال بالخصوصية الشخصية احترام كرامة الإنسان،

-الاخلال بالأمن العام والسلامة الوطنية،

-الأنشطة الإجرامية وأنشطة التجارة غير المشروعة،

- الإخلال بالصحة والسلامة العامة،

-المس بحماية حقوق الملكية الفكرية،

- المس باحترام الدين والمعتقدات الشخصية،

-المعلومات العامة التي قد تسبب الفوضى العامة،

-استخدام اللغات البذيئة والألفاظ الجارحة،

-المحتوى الزائف وغير الصحيح والمضلل، وحظر توفير التكنولوجيا التي تساعد المستخدمين على الولوج إلى المحتوى المحظور.

كما أنه كل من يخالف أحكام هذه اللائحة، تفرض عليه غرامة لا تقل عن خمسة ملايين شلن أو عقوبة سجنية لمدة لا تقل عن اثني عشر شهرًا أو كليهما (المادة 21). (15)

10. مؤشرات تصنيف القوانين ضمن فئة نهج الاشراف الصارم على المنصات الرقمية:

قد تم تصنيف القوانين السالفة الذكر في هذه المجموعة حسب المؤشرات التالية:

← وجود أحكام بالسجن على ممثلي وموظفي المنصات الرقمية لعدم امتثالهم لمتطلبات أو أوامر الإشراف على المحتوى الرقمي؛

← عدم وجود مقتضيات قانونية تفرض وجود آليات تظلم مستقلة عن قرارات السلطات المشرفة، باستثناء قانون الاتصالات الرقمية الضارة في نيوزيلندا.

وتتميز القوانين المشار إليها أعلاه بفرضها عقوبات سجنية محتملة على موظفي المنصات الرقمية نتيجة عدم الامتثال للإجراءات الإشرافية للسلطات العامة على المحتوى الرقمي، فقانون مالي(16) ، على سبيل المثال، يعاقب الموظفين المحليين لدى شركات الخدمات الرقمية غير الممتثلين للقوانين المعمول بها بالسجن لمدة تصل إلى سنتين، في حين يفرض قانون (التدابير المضادة) للتدخل الأجنبي في سنغافورة(17) عقوبات سجنية لمدة قد تصل إلى أربع سنوات.

كما تفرض معظم تلك القوانين على المنصات الرقمية إزالة أو معالجة المحتوى الغير قانوني أو الضار، والذي يمكن أن يصنف في فئة المواد الإباحية أو التحريض على العنف إلى المعلومات المضللة أو الرسائل المناهضة للحكومة. وعلى سبيل المثال، يهدف مشروع مدونة قواعد الممارسات لوسطاء الإنترنت بنيجيريا(18) إلى منع نشر "البيانات الكاذبة". ويحظر قانون كوريا الجنوبية بشأن تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات(19) "المعلومات التي تنتهك حقوق الآخرين"، في حين يحظر القانون التنزاني (20) "السخرية أو الإساءة أو الإضرار بسمعة الدولة أو سياساتها".

فحظر المحتوى "غير القانوني أو الضار" أمر مثير للجدل، خاصة في ظل عدم وجود تعريفات قانونية واضحة، وعدم اتباع نهج يراعي مبادئ الشرعية والضرورة والتناسب التي يؤكد عليها القانون الدولي لحقوق الإنسان، الأمر الذي يمثل تحديا للمستخدمين والمنصات الرقمية في تحديد ما إذا كان المحتوى أو السلوك مخالفا للقانون.

ثانيا. التوجهات التنظيمية الدولية للمنصات الرقمية ذات النهج المستقل:

ومن بين القوانين الـ 22 التي تم فحصها، تجسد 6 أنظمة قانونية النهج الذي يدمج مقدمي الخدمات الرقمية في العملية التنظيمية، ويمنحها هامشا من الحرية لتدبير المحتوى الرقمي الذي تستضيفه، إلى جانب انشاء هيئات تنظيمية مستقلة تتلقى الشكاوى وتسهر على إنفاذ القانون.

1-قانون السلامة على الإنترنت بأستراليا (2021):

يفرض قانون السلامة على الإنترنت بأستراليا على المنصات الرقمية اعتماد وتطوير قواعد جديدة لتنظيم المحتوى غير القانوني، كما يحدد أصناف المحتوى الرقمي الأكثر ضررًا، مثل مقاطع الفيديو التي تعرض الاعتداء الجنسي على الأطفال أو الأعمال الإرهابية، والمحتوى غير الملائم للأطفال، مثل العنف الشديد التأثير والمواد الإباحية. ويهدف هذا القانون إلى تنظيم المحتوى الرقمي عبر:

- مكافحة إساءة استخدام الإنترنت للبالغين الذين تبلغ أعمارهم 18 سنة فما فوق؛
- مكافحة التنمر على الأطفال عبر الإنترنت؛
- العمل على إزالة الصور أو مقاطع الفيديو الحميمة التي تمت مشاركتها عبر الإنترنت دون موافقة الشخص المعني،
- مطالبة مقدمي خدمات الإنترنت العمل على منع وصول المستخدمين إلى المواد التي تظهر سلوكًا عنيفًا وبغيضًا مثل الأعمال الإرهابية؛
- توفير صلاحيات جديدة للسلطات "مفوض السلامة الرقمية" لتنظيم المحتوى غير القانوني بغض النظر عن مكان مركز تجميع البيانات.
- جعل منصات تحميل التطبيقات ومحركات البحث ضمن نطاق المحتوى الخاضع للتنظيم القانوني.

ويمنح القانون **لجنةeSafety** صلاحيات موسعة لحماية جميع الأستراليين عبر معظم المنصات ومنتديات الإنترنت، وذلك بإلزام مزودي خدمة الإنترنت بمنع الولوج إلى المحتويات الرقمية التي تظهر سلوكيات عنيفة مقيتة مثل الأعمال الإرهابية مثلا. كما يتطلب القانون من المنصات الرقمية اعتماد قواعد ومدونات داخلية جديدة والتي تكتسي طابعا إلزاميا. ويمكن لهذه القواعد والمدونات، أن تلزم مقدمي الخدمات عبر الإنترنت والمنصات باكتشاف وإزالة المحتوى غير القانوني مثل الاعتداء الجنسي على الأطفال أو أعمال الإرهاب. وتكون هذه القواعد قابلة للتنفيذ من خلال العقوبات المدنية والأوامر القضائية للتأكد من امتثال مقدمي الخدمات عبر الإنترنت. ويفرض هذا القانون عقوبات مدنية لمقدمي الخدمات عبر الإنترنت الذين لا يحترمون الالتزامات المفروضة عليهم، كإبلاغ السلطات عن المحتوى غير القانوني(21) .

2-مشروع قانون مكافحة الأضرار عبر الانترنت بكندا (2024):

بتاريخ 26 فبراير 2024، قدمت حكومة كندا مشروع قانون جديد يتعلق بمكافحة الأضرار عبر الإنترنت، وهو إطار تنظيمي للمنصات الرقمية للحفاظ على سلامة المواطنين عبر الانترنت، ولجعل

المنصات مسؤولة عن المحتوى الذي تستضيفه. ويستهدف هذا المشروع سبعة أنواع من المحتوى الضار على وجه التحديد:

- المحتوى الذي يشكل اعتداء جنسيًا على الأطفال أو الذي يعيد إيذاء أحد الناجين؛
- المحتوى الحميمي الذي يتم نشره دون موافقة؛
- المحتوى المستخدم للتنمر على الأطفال؛
- المحتوى الذي يحث الطفل على إيذاء نفسه؛
- المحتوى الذي يحرض على الكراهية؛
- المحتوى الذي يحرض على العنف؛
- المحتوى الذي يحرض على التطرف العنيف أو الإرهاب.

وبموجب مشروع القانون، ستخضع خدمات وسائل التواصل الاجتماعي لثلاثة التزامات:

- واجب التصرف بمسؤولية؛
- واجب حماية الأطفال؛
- واجب جعل محتوى معين غير قابل للولوج، وتحديدًا (1) المحتوى الذي يشكل اعتداء جنسيًا على الطفل أو يعيد إيذاء أحد الناجين و(2) والصور الحميمة المنشورة دون موافقة.

وتنطبق هذه الالتزامات على خدمات الوسائط الاجتماعية بما في ذلك قنوات البث المباشر عبر الأنترنت والخدمات الرقمية التي يتم تحميلها بواسطة المستخدم. وذلك عبر حثها على تقليل مخاطر التعرض للمحتوى الضار؛ وتوفير وسائل وآليات واضحة ويمكن الولوج إليها للإبلاغ عن المحتوى الضار وحظر المستخدمين؛ ووضع تدابير حماية خاصة للأطفال؛ واتخاذ إجراءات للتصدي للاستغلال الجنسي للأطفال والنشر غير التوافقي للمحتوى الحميمي.

ومن شأن هذا القانون إنشاء **لجنة السلامة الرقمية** و**أمين مظالم السلامة الرقمية**. وستقوم اللجنة بالإشراف على الإطار التنظيمي الجديد وإنفاذه، وسيعمل أمين المظالم كمدافع عن المستخدمين والضحايا المحتملين عبر المنصات الرقمية(22) .

3-قانون الاتحاد الأوروبي للخدمات الرقمية (2022):

يهم قانون الخدمات الرقمية تنظيم وسطاء الانترنت والمنصات عبر الإنترنت مثل الأسواق والشبكات الاجتماعية ومنصات مشاركة المحتوى ومتاجر التطبيقات ومنصات السفر والإقامة عبر الإنترنت بجميع دول الاتحاد الأوروبي. ويتمثل هدفه الرئيسي في منع الأنشطة غير القانونية والضارة عبر الإنترنت وانتشار المعلومات المضللة. كما ينص على مقتضيات جديدة بشأن حقوق المستخدمين للأنترنت، وواجبات الشركات والمنصات الرقمية.

حقوق مستخدمي الأنترنت:

نص هذا القانون على مجموعة من المقتضيات التي تعزز حقوق مستخدمي الانترنت وخاصة المنصات الرقمية، وذلك من خلال:

- إعلام المستخدمين على قرار إزالة المحتوى بواسطة المنصات، مع امكانيتهم الاعتراض على ذلك القرار؛
- إمكانية ولوج المستخدمين إلى آليات حل النزاعات المرتبطة بالخدمات الرقمية في بلدهم الأصلي؛
- توفير مزيد من الأمان ومعرفة أفضل للبائعين الحقيقيين للمنتجات التي يشتريها المستخدمون؛
- التزامات أقوى لمنصات الإنترنت الكبيرة جدًا لتقييم وتخفيف المخاطر على مستوى التنظيم العام لخدمتهم فيما يتعلق بحقوق المستخدمين؛
- توفير آليات الاستجابة السريعة للأزمات، مع تدابير إضافية لإدارة المخاطر لأزمات الصحة العامة والأمن العام؛
- توفير إجراءات حماية جديدة للقاصرين؛
- حظر إعلانات منصات الإنترنت التي تستهدف القاصرين أو التي تستخدم بيانات شخصية حساسة؛
- حظر الممارسات غير العادلة، عبر فتح المجال أمام شركات الانترنت لتقديم المزيد من الخيارات للمستهلكين لاختيار الخدمات المبتكرة؛
- تقديم خدمات أفضل وأسعار أقل للمستهلكين(23) .

قواعد جديدة تخص شركات الإنترنت:

فرض قانون الخدمات الرقمية العديد من الواجبات والامتيازات لشركات الانترنت، وهي كالتالي:

- إزالة العوائق التي تمنع الشركات من اتخاذ تدابير طوعية لحماية مستخدميها من المحتوى أو السلع أو الخدمات غير القانونية؛
- استخدام الشركات لآليات جديدة بسيطة وفعالة للإبلاغ عن المحتوى والسلع غير القانونية التي تنتهك حقوقها، بما في ذلك حقوق الملكية الفكرية، أو تتنافس بشكل غير عادل؛
- قد تصبح الشركات أيضًا "مُبلغين موثوقين" عن محتوى أو سلع غير قانونية، مع إجراءات ذات أولوية خاصة وتعاون وثيق مع المنصات الرقمية؛
- يجعل قانون الخدمات الرقمية العمليات الداخلية للمنصات عبر الإنترنت أكثر شفافية، ويسمح باتخاذ قرارات تجارية أكثر استنارة(24) .

قواعد جديدة للمنصات عبر الإنترنت:

فرض قانون الخدمات الرقمية العديد من الواجبات والامتيازات للمنصات الرقمية، وهي كالتالي:

- اعتماد تدابير لمواجهة السلع أو الخدمات أو المحتوى غير القانوني عبر الإنترنت، مثل توفير آلية للمستخدمين للإبلاغ عن هذا المحتوى، مع ضرورة تعاون المنصات مع "المُخبرين الموثوقين"؛
- فرض التزامات جديدة بشأن إمكانية تتبع المستخدمين من رجال الأعمال في الأسواق عبر الإنترنت، للمساعدة للتعرف على بائعي السلع غير القانونية؛
- ضمانات فعالة للمستخدمين، بما في ذلك إمكانية اعتراضهم على قرارات الإشراف على محتوى المنصات؛
- اعتماد تدابير لتعزيز شفافية خدمات المنصات عبر الإنترنت، بما في ذلك استخدام بعض الخوارزميات ذات الصلة؛
- التزامات المنصات الضخمة (التي تستضيف حوالي أكثر من 10% من سكان الاتحاد الأوروبي) بمنع إساءة استخدام أنظمتها، من خلال اتخاذ إجراءات

قائمة على تقييم المخاطر، ومن خلال عمليات تدقيق مستقلة لأنظمة إدارة المخاطر الخاصة بها؛

- سيتمكن الباحثون المعتمدون من طرف السلطات من الولوج إلى بيانات المنصات الرئيسية، من أجل التدقيق في شفافيتها وطرق عملها؛
- يتعين على جميع الوسطاء عبر الإنترنت الذين يقدمون خدماتهم في الاتحاد الأوروبي، سواء تم تأسيسهم في الاتحاد أو خارجه، الالتزام بقواعد قانون الخدمات الرقمية؛
- تعزيز وتوضيح شروط الإعفاءات من المسؤولية، فالمنصات والوسطاء ليسوا مسؤولين عن السلوك غير القانوني للمستخدمين ما لم يكونوا على علم بالمحتوى غير القانوني ويتهاونون في إزالته؛
- توفير مزيد من اليقين القانوني بشأن التفاعل مع السلطات؛ حيث سيتعين على المنصات التعاون مع السلطات التي تصدر أوامر قانونية تتضمن الحد الأدنى من المعايير المشتركة؛
- إنشاء هيكل إشرافي يتناسب مع تعقيد الفضاء الإلكتروني، حيث سيكون للدول الأعضاء بالاتحاد الأوروبي الدور الأساسي في تنفيذ قانون الخدمات الرقمية، بدعم من **مجلس أوروبي جديد للخدمات الرقمية**؛ وبالنسبة للمنصات الرقمية الضخمة، ستتولى المفوضية الأوروبية السهر على تنفيذ واحترام قانون الخدمات الرقمية (25).

إطار إنفاذ قانون الخدمات الرقمية:

يتضمن إنفاذ قانون الخدمات الرقمية مجموعة كاملة من إجراءات التحقيق والعقوبات التي يمكن أن تتخذها السلطات الوطنية والمفوضية الأوروبية. وبموجب هذا القانون، تتمتع المفوضية بصلاحيات التحقيق وفرض العقوبات.

صلاحيات التحقيق:

- إرسال طلب للحصول على معلومات للتحقق من امتثال المنصات للقانون؛
- طلب الولوج إلى بيانات وخوارزميات المنصات الرقمية الضخمة، على سبيل المثال لتقييم كيفية ترويج الخوارزميات الخاصة بالمنصة للمحتوى غير القانوني؛
- إجراء مقابلات مع أي شخص قد يكون لديه معلومات حول موضوع التحقيق (لا يمكن إجراء المقابلات إلا بموافقة الشخص ولا يمكن إجباره)؛
- إجراء عمليات التفتيش في مقر المنصات الرقمية الضخمة بعد التشاور مع **"المنسق الوطني لتنفيذ قانون الخدمات الرقمية"** في الدولة العضو بالاتحاد الأوروبي، والذي قد يحتاج بدوره لتقديم طلب تصريح صادر من المحكمة المختصة.

صلاحيات فرض العقوبات:

تطبق غرامات على المنصات الرقمية قد تصل إلى 6% من حجم أرباحها السنوية في جميع أنحاء العالم، وذلك في حالة:

- خرق الالتزامات المترتبة عن قانون الخدمات الرقمية؛
- عدم الالتزام بالتدابير المؤقتة؛
- الإخلال بالتعهدات.

كما تطبق عقوبات دورية تصل إلى 5٪ من متوسط حجم الربح اليومي في جميع أنحاء العالم عن كل يوم تأخير في الامتثال للتدابير الاستباقية أو التدابير المؤقتة أو الالتزامات (بعد عدم الامتثال لقرار المفوضية الاوروبية بشأن اتخاذ التدابير اللازمة بشأن المحتوى غير القانوني). وكإجراء أخير، إذا استمر الانتهاك وتسبب في ضرر جسيم للمستخدمين كتهديد لحياة الأشخاص أو سلامتهم، يمكن المفوضية الاوروبية أن تطلب التعليق المؤقت للخدمة الرقمية(26) .

كما أنه بموجب قانون الخدمات الرقمية تم بتاريخ 17 فبراير 2024 انشاء **المجلس الأوروبي للخدمات الرقمية**، والذي هو عبارة عن هيئة استشارية مستقلة، ويتألف من منسقي الخدمات الرقمية في الدول الأعضاء بالاتحاد الأوروبي وترأسه المفوضية الأوروبية، ويعمل على تحقيق الأهداف التالية:

- ← المساهمة في التطبيق المتسق لقانون الخدمات الرقمية والتعاون الفعال بين منسقي الخدمات الرقمية والمفوضية الأوروبية فيما يتعلق بالمسائل التي يغطيها قانون الخدمات الرقمية؛
- ← التنسيق والمساهمة في تقديم الإرشادات والتحليلات التي تضعها المفوضية الأوروبية ومنسقو الخدمات الرقمية والسلطات المختصة، بشأن القضايا الناشئة في السوق الالكترونية الداخلية والتي لها علاقة بقانون الخدمات الرقمية؛
- ← مساعدة منسقي الخدمات الرقمية والمفوضية الأوروبية في الإشراف على المنصات الرقمية ومحركات البحث الإلكترونية الضخمة(27) .

4-مشروع قانون تنظيم السلامة على الإنترنت ووسائل الإعلام بأيرلندا (2022):

يعمل مشروع قانون تنظيم السلامة على الإنترنت ووسائل الإعلام في أيرلندا لسنة 2022 على سد الفجوة القانونية وإنشاء إطار تنظيمي قوي للتعامل مع انتشار المحتوى الضار عبر الإنترنت، من خلال تمكين **"اللجنة الإعلام (أو مفوض السلامة عبر الانترنت)** من مراقبة مقدمي الخدمات الرقمية ومدى التزامهم بقوانين السلامة عبر الإنترنت. ويعمل على تصنيف المحتوى الضار ضمن أكثر من 42 جريمة جنائية موجودة في القانون الأيرلندي. فعلى سبيل المثال، يتضمن المحتوى الضار عبر الإنترنت، ذلك المحتوى الذي يقوم شخص ما من خلاله بتوزيع أو نشر رسالة تهديد أو رسالة مسيئة بشكل جسيم لشخص ما، أو إرسال رسالة تهديد أو مسيئة بشكل جسيم إلى شخص آخر. ويتضمن القانون أيضًا فئات محددة من المحتوى الضار عبر الإنترنت، وهي كالآتي:

-مواد رقمية خطيرة تتعلق بالتنمر عبر الإنترنت؛

-المواد التي من المحتمل أن تشجع أو تروج لاضطرابات الأكل أو إيذاء النفس أو الانتحار؛

- المواد التي تتيح المعرفة بوسائل إيذاء النفس أو الانتحار.

ويمنح هذا القانون صلاحيات موسعة **"للجنة الإعلام"** للمراقبة والإنفاذ وفرض العقوبات لضمان الامتثال لمقتضيات قانون السلامة عبر الإنترنت. وكجزء من هذه الصلاحيات، يجوز لها طلب توفير المعلومات التي تعتبر ذات صلة بتقييم امتثال الخدمة عبر الإنترنت، وتعيين مسؤولين معتمدين لإجراء تحقيقات في حالات عدم الامتثال الجهة المسؤولة، والسعي، إذا كان ذلك ملائما، إلى فرض عقوبات مالية وإدارية(28).

5-قانون الاتصالات الرقمية الضارة في نيوزيلندا (2015):

يتناول قانون الاتصالات الرقمية الضارة في نيوزيلندا لسنة 2015 بعض الطرق التي يستخدم بها الأشخاص التكنولوجيا لإيذاء الآخرين. ويهدف إلى منع وتقليل تأثير التنمر عبر الإنترنت والمضايقة والإباحية الانتقامية وغيرها من أشكال الإساءة والترهيب. وينص القانون على:

-تدابير جديدة لمساعدة الأشخاص المتأثرين بالاتصالات الرقمية الضارة من خلال توفير إمكانية ولوج المستخدمين إلى**" وكالة تلقي الشكاوى"** ووسائل الانصاف القضائية. وقد أنشئ القانون وكالة لتلقي الشكاوى المتعلقة بالاتصالات الرقمية الضارة وإبلاغ الأشخاص بالخيارات المتاحة لهم للتظلم. وتهدف هذه الوكالة إلى تقليل الضرر الذي يلحق بالأشخاص المستهدفين عبر الإنترنت عن طريق التحسيس والوساطة والتفاوض للمساعدة في التوصل إلى حل لكلا الطرفين المعنيين. ولا يمكن لـهذه الوكالة معاقبة الأشخاص على أفعالهم عبر الإنترنت، أو إجبارهم على اتخاذ إجراء معين.

-جرائم جنائية جديدة لمعاقبة الجناة على الانترنت. فبموجب هذا القانون، قد يكون من غير القانوني إرسال رسائل ونشر مواد عبر الإنترنت تسبب عمدًا اضطرابًا عاطفيًا خطيرًا لشخص ما، حيث يمكن للشرطة التحقيق في تلك الحالة. ويتعين على الشرطة ووكالة تلقي الشكاوى التأكد من عدم إزالة أو إزالة أي محتوى عبر الإنترنت مطلوب كدليل قبل القبض على المتهم(29).

- تعريف مصطلح "الاتصالات الرقمية" الذي يعني النطاق الكامل للاتصالات الإلكترونية والرقمية. ويمكن أن يشمل ذلك إرسال رسائل نصية أو رسائل بريد إلكتروني، أو نشر تعليقات عبر الإنترنت على Facebook أو منصة X أو مواقع التواصل الاجتماعي الأخرى أو في منتدى أو مدونة عبر الإنترنت، أو نشر صور فوتوغرافية أو مقاطع فيديو حميمة عبر الإنترنت.

-العوامل التي سيأخذها القاضي في الاعتبار عند تحديد ما إذا كان أي شخص عاقل قد تسبب في ضرر عاطفي خطير عبر الاتصالات الرقمية:

- ما مدى تطرف اللغة (إذا كانت تتضمن لغة)
- السن والخصائص النفسية؛
- ما إذا كان المنشور مجهول الهوية؛
- تكرار الحادث؛
- عدد الاشخاص الذين شاهدوا المحتوى الرقمي؛
- ما إذا كان الخبر صحيحا أو كاذبا؛
- السياق الذي ظهر فيه الاتصال الرقمي؛

كما انه إذا تمت إدانة الشخص، فيمكن أن يحكم عليه بالسجن لمدة تصل إلى سنتين أو غرامة تصل إلى 50 ألف دولار. أما إذا كانت شركة، فيمكن تغريمها بما يصل إلى 200.000 دولار(30).

6-قانون السلامة على الإنترنت بالمملكة المتحدة(2023):

يعد قانون السلامة على الإنترنت ببريطانيا لسنة 2023 عبارة عن مجموعة من القواعد التي تحمي الأطفال والبالغين عبر الإنترنت. من خلال فرض العديد من الالتزامات على شركات التواصل الاجتماعي وخدمات البحث الالكتروني، لتحميلها المسؤولية عن سلامة مستخدميها على منصاتها، من أجل تقليل مخاطر استخدام خدماتها في أنشطة غير قانونية، وإزالة المحتوى غير القانوني عند ظهوره. وبموجب هذا القانون تم إحداث **لجنة"Ofcom"** التي تعتبر الجهة التنظيمية المستقلة للسلامة على الإنترنت. وتتوفر على صلاحيات واسعة لتقييم وإنفاذ امتثال مقدمي الخدمات الرقمية للإطار القانوني المعني بالسلامة على الانترنت.

<u>نطاق تطبيق القانون:</u>

ينطبق القانون على خدمات البحث والخدمات التي تسمح للمستخدمين بنشر المحتوى عبر الإنترنت أو التفاعل مع بعضهم البعض. ويتضمن ذلك مجموعة من مواقع الويب والتطبيقات الالكترونية والخدمات الرقمية المتعددة، بما في ذلك خدمات الوسائط الاجتماعية ومواقع "التخزين السحابي cloud storage" لملفات المستخدمين ومنصات مشاركة الفيديو والمنتديات عبر الإنترنت وخدمات المواعدة وخدمات المراسلة الفورية عبر الإنترنت.

كما ينطبق هذا القانون على الخدمات الرقمية حتى لو كانت الشركات التي تقدم هذه الخدمات خارج التراب الوطني للمملكة المتحدة، بشرط أن يكون لديها روابط بهذه الدولة. ويتضمن ذلك ما إذا كانت الخدمة تضم عددًا كبيرًا من مستخدمي المملكة المتحدة، أو إذا كانت تشكل سوقًا مستهدفة، مع استشعار وجود خطر بحدوث ضرر كبير لهؤلاء المستخدمين.

<u>الجرائم الجديدة التي أدخلها القانون:</u>

أضاف هذا القانون مجموعة من الجرائم ذات الصلة بالمنصات الرقمية، وهي كالآتي:

- التشجيع أو المساعدة على إيذاء النفس بشكل خطير؛
- الوميض السيبراني cyberflashing (تتضمن هذه الممارسة عادةً قيام الجناة بإرسال صور جنسية غير مرغوب فيها إلى أشخاص عبر وسائل التواصل الاجتماعي أو تطبيقات المواعدة، ولكن يمكن أيضًا أن تتم عبر خدمات مشاركة البيانات مثل Bluetooth وAirdrop. وفي بعض الحالات، يمكن أن تظهر الصورة على الجهاز الالكتروني للشخص، حتى لو تم رفض التوصل، مما يعني أن الضحايا يضطرون إلى رؤية الصورة؛
- إرسال معلومات كاذبة بقصد إحداث ضرر غير بسيط؛
- التهديد بواسطة الاتصالات الرقمية؛
- إساءة استخدام الصور الحميمة(31) ؛
- تصيد الصرع على الانترنت online epilepsy trolling (تصيد الصرع هو استخدام الصور المتحركة مثل صور GIF والوسائط الأخرى التي تثير نوبات الصرع لدى الأشخاص المصابين بالصرع الحساس للضوء. ويتم إجراء هذا الفعل لإذلال الأفراد المصابين بهذه الحالة وإحداث الأذى لهم وإحباطهم)(32) .

<u>أنواع المحتوى الرقمي التي ينظمها القانون:</u>

- المحتوى غير القانوني: وهو عبارة عن أنواع المحتوى والأنشطة غير القانونية التي تحتاج المنصات إلى حماية المستخدمين منها والمنصوص عليها في القانون، وهي كالتالي:
  - الاعتداء الجنسي على الأطفال؛
  - السلوك المسيطر أو القسري؛
  - العنف الجنسي الشديد؛
  - المواد الإباحية المتطرفة؛
  - الاحتيال؛
  - جرائم النظام العام العنصرية أو الدينية؛
  - التحريض على العنف؛
  - الهجرة غير الشرعية وتهريب البشر؛
  - الترويج أو تسهيل الانتحار؛

- إساءة استخدام الصور الحميمة؛
- بيع المخدرات أو الأسلحة غير المشروعة؛
- الاستغلال الجنسي؛
- الإرهاب.

- المحتوى المضر بالأطفال: يحدد القانون فئات المحتوى الضار الذي ينبغي على المنصات الرقمية العمل على حماية الأطفال من التعرض إليه، وهي كالتالي:
  - المواد الإباحية؛
  - المحتوى الذي يشجع أو يروج أو يقدم تعليمات بشأن الأذى الذاتي واضطرابات الأكل أو انتحار؛
  - التنمر؛
  - المحتوى المسيء للأخلاق أو الذي يحض على الكراهية؛
  - المحتوى الذي يصور أو يشجع على العنف أو التعرض إلى الإصابة الجسدية الخطيرة؛
  - المحتوى الذي يشجع الأعمال المثيرة والتحديات الخطيرة؛
  - المحتوى الذي يشجع على ابتلاع أو استنشاق أو استعمال المواد الضارة.

آلية السهر على تطبيق القانون:

أصبحت **لجنة "Ofcom"** بموجب قانون السلامة على الأنترنت هي الجهة المنظمة والمشرفة على تعزيز السلامة عبر الإنترنت من خلال مراقبة مدى حماية المنصات الرقمية لمستخدميها من المحتوى الرقمي غير القانوني والضار. كما يمكن لهذه اللجنة اتخاذ إجراءات ضد الشركات التي لا تلتزم بمقتضيات القانون المشار إليه، حيث يمكنها تغريم الشركات بما يصل إلى 18 مليون جنيه إسترليني أو 10% من إيراداتها السنوية العالمية. كما يمكنها بعض موافقة القضاء من تحريك مسطرة المتابعة الجنائية ضد كبار مديرين شركات الانترنت والمنصات الذين لا يستجيبون لطلبات المعلومات المقدمة من لجنة "Ofcom"، أو في حالة عدم امتثالهم للمقتضيات والطلبات المتعلقة بسلامة الأطفال أو الاعتداء الجنسي على الأطفال واستغلالهم(33).

7. معايير تصنيف القوانين في فئة الاشراف المستقل على المنصات الرقمية:

تم تصنيف القوانين السالفة الذكر في هذه المجموعة حسب المؤشرات التالية:

- وجود هيئة تنظيمية وطنية مستقلة تسهر على تنفيذ القانون ؛

- إنفاذ القانون من قبل الجهات التنظيمية بما يتماشى مع ضمانات حرية التعبير؛

- تركز العقوبات الناجمة عن خرق القانون بشكل كبير على الغرامات وتجعل العقوبة السجنية استثناءا؛

-إدماج أصحاب المصلحة المتعددين في العملية التنظيمية (الشركات والمنصات الرقمية والمستخدمين).

وقد اتسمت القوانين التنظيمية التي اتبعت النهج المتسم بالاستقلالية، باحترام المسافة الفاصلة بين المصالح الحكومية والخاصة، واعتماد جهة تنظيمية مستقلة تسهر على تنفيذ القانون في إطار احترام حرية التعبير. فعلى سبيل المثال، فوفقا للمادة 233 من القانون الاسترالي للسلامة على الانترنت؛ تكون صلاحيات **"المفوض الأسترالي للسلامة الإلكترونية"** محدودة إذا كان تطبيقها "ينتهك أي مبدأ دستوري يتعلق بالحرية الضمنية للاتصال السياسي "(34). كما تتيح المادة ZU139 من مشروع قانون تنظيم السلامة على الإنترنت ووسائل الإعلام في أيرلندا للمنصات الرقمية تقديم مذكرات للجهة التنظيمية إذا كانت بعض المقتضيات القانونية والعقوبات، من وجهة نظرها، تنتهك بشكل مفرط حرية التعبير لمستخدميها(35).

كما أن الإطار التنظيمي بموجب هذا النهج ليس مطلقا، بل محدود من حيث السلطات ونطاق التطبيق. فعلى الرغم من أن الغرامات التي تفرضها هذه الأنظمة على المنصات الرقمية تعد ضخمة - يمكن لقانون الخدمات الرقمية للاتحاد الاوروبي وحده فرض غرامة على المنصة الرقمية قد تصل إلى 6% من إيراداتها السنوية العالمية (المادة 74)- إلا أنها تضع ضمانات لمواجهة أي آثار سلبية على ممارسة الحقوق الأساسية المنصوص عليها في الميثاق الأوروبي لحقوق الإنسان، ولا سيما حرية التعبير والمعلومات والحق في عدم التمييز (المادة 48) ؛ ويجب على منسقي الخدمات الرقمية والمفوضية الأوروبية استخدام البيانات التي يتم الولوج إليها فقط لغرض مراقبة وتقييم الامتثال للقانون، ويجب أن يأخذوا في الاعتبار حقوق ومصالح المنصات الرقمية ومحركات البحث ومتلقي الخدمات الرقمية، بما في ذلك حماية البيانات الشخصية، وحماية المعلومات السرية، وخاصة الأسرار التجارية، (المادة 40)(36) .

وما يمكن استنتاجه، هو أن القوانين التي تتبع نهج التنظيم والاشراف المستقل، تميل إلى تحقيق التوازن بين إشراف سلطات الدولة على المنصات الرقمية ومكافحة المحتوى الضار من جهة، والالتزام بحماية الحقوق والحريات من جهة أخرى.

ثالثا. التوجهات التنظيمية الدولية للمنصات الرقمية الرامية لتعزيز حقوق المستخدم:

ومن بين القوانين المقارنة الـ 22 التي تم تحليلها، تجسد أربع أنظمة قانونية نهج التنظيم الذي يعزز ويحمي حقوق مستخدمي المنصات الرقمية.

1-قانون منصات الاتصالات في النمسا (2020):

كجزء من حزمة تنظيمية لمكافحة خطاب الكراهية على الإنترنت، أدخلت النمسا التزامات جديدة على المنصات الرقمية بواسطة قانون منصات الاتصالات الذي دخل حيز التنفيذ في 1 يناير 2021. وتنطبق مقتضيات هذا القانون على المنصات الوطنية والأجنبية على حد سواء، ويمكن في حالة عدم الامتثال للقانون إنزال عقوبات ليس فقط على المنصة نفسها ولكن أيضًا على مديريها الإداريين.

أ. منصات الاتصالات التي يتم يشملها القانون:

ينطبق قانون منصات الاتصالات بالنمسا على مقدمي خدمات الاتصالات الهادفة للربح الوطنية والأجنبية، الذين يستضيفون أكثر من 100.000 مستخدم من النمسا أو تحقق إيرادات في النمسا تزيد عن 500.000 يورو سنويا.

المنصات التي تم استثناؤها من قانون منصات الاتصالات: الأسواق عبر الإنترنت، والموسوعات الإلكترونية غير الربحية (مثل ويكيبيديا)، ومنصات التعلم، ومنصات شركات الصحف والتلفزيون التي تستضيف عروضا صحفية، والتطبيقات المستخدمة للتواصل الفردي.

ويخضع محتوى الفيديو الموجود على منصات مشاركة الفيديو لقواعد قانون خدمات الوسائط السمعية والبصرية، بينما ينطبق قانون منصات الاتصالات على باقي أنواع المحتوى الرقمي. ويتعين على السلطة التنظيمية الاحتفاظ بقائمة (تصريحية) للمنصات التي تحكمها القواعد الجديدة، وكما يجب تجميع هذه القائمة بمبادرة من السلطة

التنظيمية لأنه لا يوجد التزام على المنصة بإخطار الهيئة التنظيمية عند بدء خدماتها أو إنهائها(37) .

ب. الالتزامات المترتبة على منصات الاتصالات:

يفرض القانون مجموعة من الالتزامات على المنصات الرقمية، والتي يمكن اجمالها فيما يلي:

- تعيين وإخطار السلطة التنظيمية عن ممثل أو مفوض المنصة المسؤول عن الامتثال لقانون منصات الاتصالات، والذي ينبغي أن يتحدث باللغة الألمانية؛
- القيام بإعداد "إجراء فعال وشفاف" للإبلاغ عن المحتوى غير القانوني وحذفه في غضون 24 ساعة إذا كانت عدم شرعية المحتوى الرقمي واضحة لشخص عادي، أو في غضون 7 أيام إذا كان الفحص التفصيلي ضروريًا؛
- ينبغي توفير آلية لتقديم الشكاوى للمستخدمين المتأثرين بالحذف أو الحظر لتجنب "الحظر الزائد"؛
- يشتمل المحتوى غير القانوني، على سبيل المثال، على التشهير، أو المضايقة، أو المواد الإباحية التي تتضمن قاصرين، أو المحتوى العنصري، أو التمييزي، أو الاشتراكي القومي، أو الصور غير المصرح بها، أو المطاردة عن طريق وسائل الاتصالات؛
- الإبلاغ عن عدد ونتائج الإشعارات سنويًا (أو نصف سنويًا إذا تجاوز عدد المستخدمين المليون)؛
- القيام بتخزين المنشورات المحذوفة لمدة عشرة أسابيع على الأقل، احتمالا لأي ملاحقة قضائية؛
- دفع مساهمة تمويلية في موازنة الهيئة التنظيمية المشرفة على إنفاذ قانون منصات الاتصالات(38) .

ج. العقوبات التي يمكن فرضها في حالة عدم الامتثال للقانون:

في حالة عدم الامتثال للالتزامات التي يفرضها القانون على المنصات الرقمية، يمكن فرض غرامات قد تصل إلى 10 ملايين يورو على المنصة (اعتمادًا على عدة عوامل، مثل الإيرادات وعدد المستخدمين وسوء السلوك السابق وخطورة الانتهاك وطول مدته). علاوة على ذلك، من الممكن فرض غرامة تصل إلى مليون يورو على أعضاء مجلس الإدارة إذا فشلوا، بناءً على طلب من الهيئة التنظيمية، في تعيين ممثل أو مفوض المنصة المسؤول عن الامتثال لقانون منصات الاتصالات(39) .

د. الجرائم التي يشملها القانون:

يحدد قانون منصات الاتصالات عدد من الجرائم التي يمكن اقترافها بالمنصات الرقمية، من بينها:

- الإكراه؛
- التهديد؛
- المطاردة عبر الانترنت؛
- التصوير المسيء وغير المصرح به؛
- الابتزاز؛
- التمثيل الإباحي للقاصرين؛
- التحريض على الكراهية(40) .

ه. حقوق مستخدمي المنصات الرقمية:

تلتزم المنصات الرقمية بموجب القانون باعتماد إجراءات فعالة وشفافة لمعالجة الشكايات المقدمة من المستخدمين. حيث ينبغي أن توفر المنصات للمستخدمين الآليات والخيارات الضرورية التي يمكن الولوج إليها بسهولة وبشكل مستمر من أجل تقديم تقارير وشكايات، وكما يحق لهم الحصول على معلومات حول كيفية متابعة المنصة لتقريرهم وشكايتهم، إضافة إلى ضرورة إعلامهم بمآل الشكاية. وينبغي توفير هذه المعلومات للمستخدمين من كلا الجانبين؛ المستخدم المُبلغ وموفر أو مقدم المحتوى الرقمي. كما ينص القانون على أن إجراءات البث في الشكاية تكون في غضون أسبوعين من طرف المنصات الرقمية، وهو ما يعتبر سريعًا بما فيه الكفاية. كما يمكن تقديم طعن ضد قرار مزود المنصة إلى **مكتب الشكايات** (Beschwerdestelle)، التابع لهيئة الإذاعة النمساوية، والتي ويتم تعيين أعضائها من قبل رئيس النمسا، بناء على توصية من الحكومة، وبالاتفاق مع لجنة من البرلمان. وتعتبر هذه الهيئة مستقلة تماماً عن الحكومة، وهي هيئة إدارية تخضع قراراتها عادة للمراجعة القضائية.

ومن جهة أخرى فمكتب الشكاوى، يفتقر إلى السلطة لفرض قرار إلزامي اتجاه المنصات الرقمية، حيث يكتفي بتقديم مقترحات تعد عبارة عن حل ودي بين المستخدم وموفر المنصة. الشيء الذي يمكن اعتباره مؤشرا إيجابيا يتمظهر في عدم تهديد المنصات الرقمية بغرامة فورية، ولكن بدلاً من ذلك يتم إعطاؤهم المشورة (الحل الودي أو الرأي) أو المبادئ التوجيهية (الإخطار)، وهذا يقلل من التقييد الصارم للمنصات ويساعد على تطوير المعايير والممارسات الفضلى في هذا المجال. وهكذا يعتبر تحديد واجبات ومسؤوليات المنصات لاحترام حقوق المستخدمين بواسطة قانون منصات الاتصالات النمساوي مثالًا تشريعيًا تقدميًا(41) .

2-مشروع القانون رقم 2630 بشأن الحرية والمسؤولية والشفافية على الإنترنت ("قانون الأخبار الزائفة") بالبرازيل (2020):

يهدف مشروع قانون الأخبار الزائفة بالبرازيل إلى توفير إطار قانوني أكثر أمانًا للتعامل مع المعلومات المضللة المنتشرة في المنصات الرقمية، ويعمل على توضيح كيف تتفاعل السياسة العامة للدولة مع المنصات الرقمية في سياق هيمنتها المتنامية وآثارها الضارة.

ويتناول الفصل الأول أهداف القانون وتعريفاته. ويهدف القانون في مادته الأولى إلى وضع "معايير وإرشادات وآليات الشفافية لمقدمي شبكات التواصل الاجتماعي ومحركات البحث وخدمات الرسائل الفورية". ويوضح القانون أنه يشمل جميع مقدمي الخدمات الرقمية الذين يقدمون هذه الخدمات للمواطنين البرازيليين ولديهم أكثر من 10 ملايين مستخدم من البرازيل.

ويتناول الفصل الثاني الالتزامات العامة المتعلقة بمساءلة مقدمي الخدمات الرقمية. حيث يُطلب من منصات التواصل الاجتماعي وخدمات المراسلة ومحركات البحث إنتاج تقارير "الشفافية" نصف سنوية مفصلة للغاية، والإبلاغ عن إجراءات وقرارات الإشراف الخاصة بها. ويجب أن تتضمن هذه التقارير عدد التدابير المطبقة، مع التمييز إذا تم اتخاذ القرار للامتثال لشروط الخدمة الخاصة بهم، أو لقرارات المحكمة، أو لقانون الأخبار الكاذبة نفسه. ويجب عليهم أن يوضحوا أنواع الأنظمة الآلية التي يتم استخدامها للإشراف على المحتوى وعدد القرارات التي اتخذتها هذه الأنظمة.

بالإضافة إلى ذلك، يمكن للسلطات أن تطلب من خدمات المراسلة الرقمية تسجيل تفاعلات المستخدمين والكشف عنها

لمدة تصل إلى 60 يومًا كجزء من التحقيقات والملاحقة القضائية؛ كوقت وتاريخ الرسالة، وما إذا تم إرسال الرسالة أو تم استلامها. ويحظر القانون صراحة أي ربط لهذه التسجيلات بمحتوى الرسالة، مما يجعل هذا القانون متوافقًا مع معايير التشفير بواسطة الخدمات الرقمية.

ويحدد الفصل الثالث مجموعة من المعايير الهادفة إلى تعزيز شفافية المحتوى والإعلانات الرقمية. ففي حالة الحملات الانتخابية مثلا، يجب على مقدمي الخدمة الرقمية أيضًا الإعلان عن المبلغ الذي أنفقه المرشحون والأحزاب، وفترة تداول المحتوى، ومعايير التصنيف العامة للجمهور المستهدف بالإعلان الانتخابي.

وينشئ الفصل الرابع نظاما خاصا لحسابات الإدارات والهيئات الحكومية وأصحاب المناصب العامة. وينص على أن هذه الحسابات لا يمكنها تقييد الولوج إلى رسائلها ومنشوراتها. وبالتالي فهذا القانون، لا يتيح للسياسيين امكانية منع الصحفيين أو المنظمات غير الحكومية، على سبيل المثال، من رؤية منشوراتهم على وسائل التواصل الاجتماعي. وفي الفصل الخامس، يشجع مشروع القانون الحكومات الفيدرالية وحكومات الولايات والبلديات على تعزيز الثقافة الإعلامية في جميع مستويات التعليم.

ويفرض الفصل السادس من مشروع القانون عقوبات على المنصات الرقمية تتراوح بين التحذيرات والغرامات (تصل إلى 10٪ من حجم الارباح السنوية المحققة في البرازيل) إلى وقف العمليات، مع الأخذ في الاعتبار خطورة المخالفة والعود والقوة الاقتصادية لمقدم الخدمة الرقمية. كما أن أي غرامات ناجمة عن هذه العقوبات يتم تحويلها إلى وزارة التربية والتعليم لتمويل برامج التربية الإعلامية.

ويحدد الفصل السابع وظائف جديدة للجنة التوجيهية للإنترنت البرازيلية، وهي الهيئة التي تشرف على خدمات الإنترنت بالبرازيل. وقد أسند لها مشروع القانون المسؤولية عن تقديم مبادئ توجيهية لإنشاء مدونة قواعد سلوك لمنصات التواصل الاجتماعي ومحركات البحث وخدمات الرسائل الالكترونية، مع إجراء دراسات وتقارير وتوصيات لدعم التشغيل المسؤول لمقدمي الخدمات الرقمية.

ويحث الفصل الثامن مقدمي الخدمات الرقمية على إنشاء "مؤسسة ذاتية التنظيم" تتولى التعامل مع بلاغات وشكايات المستخدمين بشأن الحسابات والمحتويات الرقمية المخالفة للقانون، واتخاذ الإجراءات الواجب تنفيذها من قبل أعضائها.

ويسلط الفصل التاسع الضوء على الظروف التي يصبح فيها نشر الأخبار الزائفة بمثابة عقوبة جنائية، أي عندما يؤدي النشر الجماعي للرسائل الالكترونية التي تحتوي على معلومات كاذبة إلى الإضرار بنزاهة العملية الانتخابية أو التسبب في ضرر جسدي.

وأخيرا، ينص الفصل العاشر على إنشاء ممثل وطني لأي منصة رقمية عن طريق شخص اعتباري مسجل بطريقة قانونية في البرازيل، مع تحديد هويته وطريقة الاتصال به على الموقع الإلكتروني للمنصة.

ويعد هذا القانون دليلاً مهمًا على أن البرازيل تدرك مخاطر نظام الاتصالات المعاصرة، حيث يهدف إلى معالجة هذه المخاطر من خلال وضع معايير أعلى للشفافية في الإشراف على المحتوى الرقمي يراعي مصلحة المستخدمين، مما يجعله نموذجًا لتنظيم المنصات الرقمية(42) .

3-قواعد تكنولوجيا المعلومات في الهند (المبادئ التوجيهية للوسيط ومدونة أخلاقيات الوسائط الرقمية) (2021):

تعتبر قواعد تكنولوجيا المعلومات أطارا قانونيا تقدميا، لأنه يركز بشكل خاص على حماية المرأة من انتشار الجرائم الجنسية على وسائل التواصل الاجتماعي. ويؤكد على حاجة وسطاء وسائل التواصل الاجتماعي ومقدمي المحتوى عبر الإنترنت، سواء لأغراض الترفيه أو المعلومات، إلى الالتزام الصارم بالدستور والقوانين الوطنية بالهند، وذلك عبر العديد من المقتضيات، وهي كالتالي:

أ. التزامات وواجبات وسطاء الأنترنت بموجب قواعد تكنولوجيا المعلومات:

- العناية الواجبة: تتضمن قواعد تكنولوجيا المعلومات بعض التزامات العناية الواجبة للوسيط، والتي تشمل واجب نشر القواعد واللوائح الخاصة به، وسياسات الخصوصية واتفاقيات المستخدم للولوج للخدمات الرقمية، إما على موقعه على الويب و/أو التطبيق الالكتروني. كما يجب أن توضح المواد المنشورة مسؤولية المستخدم بعدم "استضافة أو عرض أو تحميل أو تعديل أو نشر أو نقل أو تخزين أو تحديث أو مشاركة" أي شكل من أشكال المعلومات التي:
  - تنتمي إلى شخص آخر؛
  - تشهيرية، أو فاحشة، أو إباحية، أو متعدية على خصوصية الفرد، أو غير متوافقة مع قوانين البلاد؛
  - تشكل خطرا على القاصرين؛
  - تؤدي إلى انتهاك أي حق من حقوق الملكية الفكرية؛
  - خادعة أو مضللة فيما يتعلق بأصل الرسالة؛
  - تنتحل شخصية شخص آخر؛
  - تعيق سلامة الوطن أو الدفاع عنه أو أمنه أو سيادته أو العلاقات الودية مع الدول الأجنبية أو النظام العام أو تؤدي إلى التحريض على أي جريمة معترف بها؛
  - تحتوي على أي فيروس برمجي أو أي برنامج مصمم لإتلاف أو مقاطعة وظيفة أي مورد كمبيوتر؛
  - زائفة وغير صحيحة بشكل واضح، مهما كان شكلها، أو بهدف تضليل أو مضايقة شخص ما.
- الاخطارات المقدمة للمستخدم: يجب على الوسيط إخطار المستخدم بأن عدم الامتثال لما ذكر أعلاه قد يؤدي إلى إنهاء حقوق الولوج أو الاستخدام الخاصة. كما أن القواعد واللوائح وسياسات الخصوصية قد تخضع لتعديلات دورية، والتي يجب إخطار المستخدمين بها في الوقت المناسب.
- إجراءات الإنفاذ التي يتعين اتخاذها: من أجل معالجة الشكاوى التي يثيرها المستخدمون أو الضحايا، يجب على الوسطاء تعيين مسؤول التظلمات، ويجب نشر تفاصيله للعامة، والذي يستقبل تلك الشكاوى ويبث فيها في غضون شهر واحد.

ب. تدابير امتثال إضافية لوسطاء وسائل التواصل الاجتماعي:

- العناية الواجبة: من السمات المميزة لهذه القواعد أنها تخلق تمييزًا بين وسطاء وسائل التواصل الاجتماعي الأقل حجما ووسطاء وسائل التواصل الاجتماعي المهمين. حيث يعتمد ترسيم الحدود على عدد

المستخدمين، وبمجرد تحديده من خلال إخطار الحكومة، فإنه سيكون بمثابة العتبة بين الاثنين. حيث توفر القواعد تدابير امتثال إضافية لوسطاء وسائل التواصل الاجتماعي المهمين نظرًا للحجم الكبير من المستخدمين والمحتوى الذي يقومون بمعالجته. وباستثناء معايير حجم المستخدم، يمكن للحكومة أن تفرض نفس الأحكام على أي وسيط آخر أيضًا من خلال إشعار يوجه له. ويجب مراعاة العناية الواجبة التالية من قبل الوسطاء عبر:

- تعيين كبير مسؤولي الامتثال، ليتولى مسؤولية ضمان الامتثال والإشراف على وظائف الوسطاء؛
- تعيين جهة اتصال تعمل كحلقة وصل مع وكالات إنفاذ القانون؛
- تعيين مسؤول التظلمات المقيم؛
- نشر تقرير الامتثال بشكل دوري لمدة ستة أشهر، والذي يحتوي على تفاصيل ومحتويات الشكاوى التي تم التعامل معها والمحتويات الرقمية التي تمت إزالتها أو مقاطعتها من قبل الوسطاء في متابعة أنشطة المراقبة الخاصة بهم.

- المنشئ الأول: تنص القواعد على مسؤولية إضافية على وسطاء وسائل التواصل الاجتماعي المهمين المشاركين في تقديم خدمات المراسلة لمساعدة وكالات إنفاذ القانون على تحديد وتتبع المنشئ الأول لأي معلومات مثيرة للجدل أو إشكالية. ولا يمكن تنفيذ ذلك إلا بأمر من محكمة مختصة أو السلطة المختصة. كما لا يمكن ممارسة هذه السلطة إلا من أجل مكافحة أي جريمة تهدد سلامة الدولة أو أمنها، أو تحرض على ارتكاب الاغتصاب أو الاعتداء الجنسي على الأطفال أو غيرها من الجرائم الخطيرة. ومع ذلك، لا يجوز اللجوء إلى ذلك عند توفر وسائل أقل تدخلاً، ويجب استخدامه كملاذ أخير.
- تدابير خاصة للجرائم الجنسية: تفرض القواعد على الوسطاء نشر بعض المعايير التكنولوجية لتحديد أي مادة قد تصور أو تحاكي الجرائم الجنسية مثلا، ويجب أن يتم ذلك في غياب أي تحيز أو تمييز، مع إيلاء أقصى قدر من الاهتمام للخصوصية وحرية التعبير.

إخطار المستخدم بشأن إزالة المحتوى: في حالة قيام وسيط الخدمات الرقمية بإزالة أو تقييد الوصول إلى أي معلومات أو بيانات، يجب عليه التأكد من أن المستخدم على علم بذلك، بما في ذلك أسباب هذا الإجراء، بعد تزويده بإخطار خلال مدة معقولة. كما يجب أن يشرف على عملية حذف المحتوى الرقمي مسؤول التظلمات المقيم(43) .

4-مشروع قانون بولندا بشأن حماية حرية التعبير على مواقع التواصل الاجتماعي (2021):

يهدف مشروع قانون حماية حرية التعبير على مواقع التواصل الاجتماعي ببولاندا إلى حماية حق المستخدمين في الولوج إلى المعلومات وحرية التعبير على منصات التواصل الاجتماعي. حيث ينص على أنه من غير القانوني لمنصات التواصل الاجتماعي التي تضم أكثر من مليون مستخدم مسجل في بولندا إزالة المحتوى الذي لا يحظره القانون البولندي بشكل صريح.

- ويتضمن القانون ثلاث ركائز أساسية، وهي:
  - تسهيل الإبلاغ عن المحتوى "غير القانوني"؛
  - إنشاء آليات التظلم والشكاوى ومجلس حرية التعبير؛
  - تقارير الشفافية.
- ويحدد القانون أربع فئات من المحتوى "غير القانوني" الذي يمكن للمستخدمين الإبلاغ عنه لمنصات التواصل الاجتماعي، وهي:
  - المحتوى الذي ينتهك الحقوق الشخصية؛
  - المعلومات المضللة؛
  - المحتوى الإجرامي؛
  - المحتوى المسيء للآداب العامة، على سبيل المثال، من خلال الإشادة بالعنف.
- وتماشيًا مع هدفه المعلن المتمثل في حماية المستخدمين البولنديين من "رقابة" منصات التواصل الاجتماعي، يفرض القانون على شركات التكنولوجيا والمنصات الرقمية توفير العديد من آليات التظلم والتعويض عن الضرر، والتي يمكن إجمالها فيما يلي:
  - يتعين على منصات التواصل الاجتماعي إنشاء آلية شكوى مباشرة أو آلية "تظلم داخلية" للمستخدمين للطعن في المحتوى أو الحساب الذي تم حظره أو تقييده. كما يجب أن تتيح آليات الشكاوى أيضًا للمستخدمين إمكانية الإبلاغ عن المحتوى غير القانوني.
  - ينبغي على المنصات تقييم الشكايات وتقارير المحتوى المقدمة من المستخدمين والرد عليها خلال 48 ساعة. ويؤدي عدم امتثالها بذلك إلى فرض عقوبات مالية عليها.
  - يمكن للمستخدمين غير الراضين عن تعامل المنصة مع شكاواهم (سواء تظلم المستخدم أو تقرير المحتوى) من رفع قضيتهم إلى "مجلس حرية التعبير".
  - يعتبر "مجلس حرية التعبير" بمثابة محكمة الاستئناف النهائية للمستخدمين الذين تمت إزالة المحتوى أو الحساب الخاص بهم بواسطة المنصة الرقمية، وكذلك للمستخدمين الذين تم رفض تقرير المحتوى الخاص بهم. وسيقوم المجلس، المؤلف من خمسة أعضاء، بتقييم ما إذا كان المحتوى مسموحًا به أو محظورًا بموجب القانون، بما في ذلك ما إذا كان ينتهك الآداب العامة أو يشكل معلومات مضللة. وتكون عملية تقديم المستخدمين للشكوى إلى المجلس عبر الإنترنت في الغالب.
  - تمنح المنصات 24 ساعة للامتثال لأي حكم صادر عن مجلس حرية التعبير لاستعادة المحتوى أو الحساب الرقمي.
  - إذا تم بالفعل تقييم المحتوى على أنه قانوني من قبل المجلس، فلن يتمكن مزود خدمة الإنترنت من تقييد الولوج إليه إذا تم إعادة تحميله بواسطة مستخدم آخر.
  - يتداول المجلس في جلسات مغلقة ولا يأخذ أدلة أخرى غير تلك المقدمة من المستخدم والمنصات. وهذا يعني أنه لن يستمع المجلس إلى أي آراء خبراء أو أطراف ثالثة في حكمه بشأن إزالة المحتوى الرقمي.
  - يتعين على المنصات تعيين واحد إلى ثلاثة ممثلين مقرهم في بولندا يكونون مسؤولين عن التعامل مع شكاوى المستخدمين والاتصال بالسلطات البولندية، بما في ذلك مجلس حرية التعبير. ويجب نشر المعلومات المتعلقة بهؤلاء الممثلين وتفاصيل

الاتصال ذات الصلة على موقع المنصة الإلكترونية.

- يتطلب القانون من المنصات نشر سياسات الإشراف الخاصة بها وقواعدها للتعامل مع الشكاوى عبر الإنترنت. ويتعين على المنصات أيضًا تقديم تقارير شفافية سنوية حول جهودها لفي مجال مكافحة المحتوى غير القانوني والمعلومات المضللة. ويُطلب من المنصات التي تتلقى أكثر من 100 شكاية خلال السنة نشر تقارير الشفافية كل 6 أشهر لتفصيل كيفية تعاملها مع الشكاوى. ويتم نشر التقارير على مواقع المنصة وكذلك إرسالها إلى مكتب الاتصالات الإلكترونية (44).

5.مؤشرات تصنيف القوانين في فنة تعزيز حقوق مستخدمي الانترنت:

تم تصنيف القوانين المشار إليها في هذه المجموعة حسب المؤشرات التالية:

- ← التركيز على تمكين مستخدمي المنصات الرقمية من العديد من الصلاحيات والحقوق عبر تعزيز شفافية تدبير المحتوى الرقمي من قبل المنصات وتوفير سبل الانتصاف الفعالة؛
- ← التنصيص على إزالة المحتوى غير القانوني بعد إخطار المستخدم، بدلاً من متطلبات المراقبة الاستباقية للمحتوى الرقمي؛
- ← جل العقوبات عبارة عن غرامات، مع مسؤولية محدودة لموظفي المنصات الرقمية.
- ← فرض توفير مخاطب رسمي أو من يمثل المنصات الرقمية على الصعيد الوطني.

وبناء عليه، فقد تم تقييم تلك التشريعات بناء على بأربع مؤشرات، وهي: آليات التظلم والطعن للسماح للمستخدمين بالاعتراض على عمليات إزالة المنصة، وتقارير الشفافية، وإجراءات الشكاوى، وشروط الخدمة الرقمية. كما يضع نهج تعزيز حقوق المستخدم عبء تنظيم وتجويد المحتوى الرقمي على المنصة، عبر تشجيع التنظيم الذاتي. وهكذا، فإن التركيز على العمليات والآليات التي تسمح للمستخدمين والمجتمعات والمنصات بممارسة هامش من حرية اتخاذ القرار وموازنة الحقوق والمسؤوليات هو النهج الأكثر ملائمة مع الإطار التنظيمي للمنصات الرقمية القائم على تعزيز وحماية حقوق الإنسان.

رابعا. نهج توطين البيانات كتوجه لتنظيم الإشراف على المنصات الرقمية:

تميزت ثلاثة أنظمة من ضمن القوانين موضوع الدراسة، بالإشارة بوضوح إلى توطين البيانات كجزء من نهجها في الإشراف على المحتوى الرقمي.

1.قواعد إزالة وحظر المحتوى غير القانوني عبر الإنترنت بباكستان (2021):

أصدرت وزارة تكنولوجيا المعلومات والاتصالات الباكستانية قواعد إزالة وحظر المحتوى غير القانوني عبر الإنترنت لسنة 2021، وبموجب المادة 37 من هذا القانون أصبحت هيئة الاتصالات الباكستانية تتوفر على صلاحية إزالة أو حظر أو إصدار توجيهات لإزالة أو منع الولوج إلى المعلومات إذا رأت ذلك ضروريًا فيما يتعلق، من بين أمور أخرى، التحريض على أي جريمة بموجب قانون(45) .

وينص القانون على شرط التسجيل لدى هيئة الاتصالات الباكستانية وإنشاء مكتب مسجل بشكل دائم في باكستان من قبل شركات المنصات الرقمية، قبل أن يتم منح هذه الشركات الإذن بإنشاء المحتوى في باكستان، الأمر الذي يعد بمثابة تحرك نحو "توطين البيانات". كما تلزم المادة 9 من هذا القانون مقدمي خدمات الانترنت وشركات التواصل الاجتماعي بإنشاء خوادم قاعدة بيانات في باكستان لتسجيل وتخزين البيانات والمحتوى عبر الإنترنت(46) . إضافة إلى إلزامهم باعتماد آليات مناسبة للإشراف على المحتوى بما في ذلك نظام الإشراف على المحتوى القائم على الذكاء الاصطناعي، وضرورة توفر مشرفي المحتوى على دراية جيدة بالقوانين الوطنية ذات الصلة (47).

2.القانون الاتحادي الروسي رقم 242 FZبشأن تعديل بعض القوانين التشريعية المتعلقة بتحديث إجراءات معالجة البيانات الشخصية في شبكات المعلومات والاتصالات (قانون توطين البيانات):

يفرض قانون توطين البيانات الروسي لسنة 2015، معالجة البيانات الشخصية للمواطنين الروس باستخدام خوادم الكترونية تتواجد في الأراضي الروسية. كما يلزم مشغلي البيانات الروس والأجانب الذين يقومون بجمع البيانات الشخصية للمواطنين الروس، بما في ذلك عبر الإنترنت، بتسجيل وتخزين وترتيب وتحديث، واستخراج تلك البيانات باستخدام قواعد البيانات الروسية. ويتطلب القانون أيضًا من مشغلي البيانات إخطار **(هيئة حماية البيانات الروسية)** بموقع الخوادم حيث ستتم معالجة البيانات الشخصية الروسية قبل بدء معالجة تلك البيانات. ويقدم القانون تعريفا واسعا لمعالجة البيانات باعتبارها أي إجراء أو مجموعة من الإجراءات يتم تنفيذها على البيانات الشخصية، كالتسجيل والتنظيم والتراكم والتخزين والتحيين والتحرير والاستخراج (48) .

وينطبق هذا القانون على جميع مشغلي البيانات والأطراف الثالثة التي تعمل بموجب ترخيص مشغلي البيانات. ومشغل البيانات هو هيئة حكومية أو بلدية، أو كيان قانوني، أو شخص طبيعي:

-ينظم أو ينفذ، بمفرده أو بالاشتراك مع أشخاص آخرين، معالجة البيانات الشخصية؛

-يحدد أغراض معالجة البيانات الشخصية، ومحتوى البيانات الشخصية، واستخدام البيانات الشخصية.

كما يشمل قانون البيانات الشخصية للمواطنين الروس، والتي تتضمن على نطاق واسع أي معلومات تشير بشكل مباشر أو غير مباشر إلى مواطن روسي محدد أو يمكن تحديد هويته.

لا ينطبق هذا القانون على الحالات التالية:

- ← بيانات مطلوبة لتحقيق الأغراض المنصوص عليها في اتفاقية دولية أو القانون الدولي للوفاء بالتزام مشغل البيانات بموجب القانون الروسي.
- ← من أجل إنفاذ القانون والإجراءات القضائية.
- ← من قبل السلطات الحكومية الروسية المعنية بتقديم الخدمات العامة.
- ← للصحافة أو وسائل الإعلام أو غيرها من الأنشطة العلمية أو الأدبية أو الإبداعية إذا لم تنتهك حقوق الخصوصية للأفراد (49).

3.القانون رقم 5651 بشأن تنظيم البث في شبكة الإنترنت ومكافحة الجرائم التي ترتكب خلال البث عبر الإنترنت بتركيا (2007):

ينظم القانون التركي المتعلق بتنظيم البث في شبكة الإنترنت ومكافحة الجرائم التي ترتكب خلال البث عبر الإنترنت (2007) المحتوى المحظور، مثل صور إساءة معاملة الأطفال والفحش على الإنترنت، كما يتيح حظر المواقع الإلكترونية. وبموجب هذا القانون:

- ← يُطلب من مزودي خدمة الإنترنت الاندماج في "رابطة جمعية مزودي الانترنت". ويحصل مقدمو خدمات التابعون للجمعية على "شهادة أو ترخيص" للعمل بشكل قانوني بتركيا، في حين لا يتمكن أولئك الذين ليسوا أعضاء بالرابطة من تقديم خدمات الانترنت داخل البلاد.
- ← يمكن إصدار أوامر الحظر من قبل المحاكم أو المدعون العامون أو هيئة تقنيات الاتصالات. ويمكن إزالة مواقع الويب في تركيا التي تحتوي على محتوى محظور، في حين يمكن حظر مواقع الويب الموجودة في الخارج وتصفيتها من خلال مزودي خدمة الإنترنت.
- ← يمكن تنفيذ أوامر الحظر إذا ادعى أي فرد أو كيان قانوني انتهاك الخصوصية، أو إذا كان المحتوى يعتبر "تمييزيًا أو مهينًا لأفراد معينين في المجتمع". ويتعين على مزودي خدمات الإنترنت أيضًا حظر الولوج إلى عناوين URL محددة خلال 4 ساعات من تلقي الطلب.
- ← تتعرض المواقع الإلكترونية المنشئة في الخارج للحجب في حالة الاشتباه في احتوائها على ثماني فئات من المحتوى المحظور، بما في ذلك: صور إساءة معاملة الأطفال، المحتوى الذي يشجع تعاطي المخدرات، توفير المواد الخطرة على الصحة، الفحش، مواقع الدعارة، مواقع القمار، التشجيع على الانتحار(50) .
- ← يجب على مزودي شبكات التواصل الاجتماعي التي تتوفر على مليون مستخدم من تركيا، بغض النظر عن أصلهم، اتخاذ التدابير اللازمة لتخزين بيانات المستخدمين الأتراك في تركيا (51).

4.معايير تصنيف القوانين في فئة تنظيم المنصات الرقمية عبر توطين البيانات:

- ⇐ تم تصنيف القوانين المشار إليها في هذه المجموعة حسب المؤشرات التالية:
- ← وجود مقتضيات قانونية تفرض على المنصات الرقمية توطين البيانات على المستوى الوطني؛
- ← قلة أو عدم وجود ضمانات كافية لحماية حرية التعبير وحماية المعطيات الشخصية والحق في الخصوصية؛
- ← غياب هيئة تنظيمية مستقلة تسهر على تتبع إنفاذ القانون المعني بتنظيم المنصات الرقمية.

ويعد مفهوم توطين البيانات مصطلحا شاملا يغطي مجموعة متنوعة من القيود والمتطلبات الوطنية المتعلقة بتدفق البيانات عبر الحدود ومعالجتها وتخزينها. وتحظر النسخة الأكثر صرامة، والتي يشار إليها أحيانًا باسم "التوطين الصارم"، جميع عمليات نقل البيانات الشخصية عبر الحدود. ويتجسد أحد الأمثلة على ذلك إلى حد ما في اللائحة العامة لحماية البيانات للاتحاد الأوروبي والتي تحظر تدفق البيانات إلى بلدان معينة (مع مراعاة الاستثناءات بما في ذلك البلدان القليلة نسبيًا التي توفر قوانينها حماية كافية للبيانات المنقولة). وفي الصين مثلا، لا يجوز نقل أنواع معينة من البيانات خارج البلاد دون موافقة الحكومة. وفي بعض الحالات قد يُسمح بمشاركة البيانات عبر الحدود في بعض البلدان ولكن مع استثناءات لأنواع معينة من المعلومات الحساسة، مثل البيانات الصحية والمالية والمتعلقة بالأمن الوطني التي لا يمكن تصديرها، فعلى سبيل المثال، يشترط المغرب على الشركات التي تشارك في أنشطة ذات "أهمية حيوية" وتستخدم بيانات حساسة، توطين بنيتها التحتية الرقمية على الأراضي المغربية (52).

ورغم العدد الضئيل نسبيًا من البلدان التي تشير إلى توطين البيانات في قوانينها الخاصة بتعديل المحتوى الرقمي، إلا أنه ما يلاحظ حاليا هو قيام العديد من البلدان الأخرى بفرض توطين البيانات في الإصلاحات التشريعية التي تستهدف الاقتصاد الرقمي؛ كالبرازيل والصين واليابان. وتتجلى عملية التوطين في أشكال عديدة، بدءاً من السماح بنقل البيانات خارج البلاد طالما يتم الاحتفاظ بنسخة منها وطنيا (النسخ المتطابق) إلى الحظر القانوني أو الفعلي على تصدير البيانات. وتشمل الأسباب المنطقية للتوطين: الخوف من الاعتماد على الدول الأجنبية؛ والاستعمار الجديد (سيطرة الشركات الدولية الكبرى على الولوج إلى التكنولوجيا)؛ والقلق من أن تحاول دول أخرى من الولوج إلى البيانات المخزنة داخل حدودها (بما في ذلك المراقبة من قبل أجهزة الاستخبارات الأجنبية)؛ وفقدان السيطرة على البيانات؛ وحماية الشركات الوطنية من المنافسة الأجنبية؛ وتعزيز تطوير القدرة التقنية الوطنية والحوسبة السحابية؛ وأمن البيانات (لأنه من الصعب حماية البيانات خارج البلاد)؛ وحماية البيانات (قد لا تحمي القوانين الأجنبية البيانات بشكل كافٍ)؛ وإعاقة التحقيقات الجنائية التي تجريها أجهزة إنفاذ القانون(53) .

خلاصات واقتراحات:

حاول هذا البحث تسليط الضوء على أهم التحديات التي يفرضها التنظيم القانوني العالمي للمنصات الرقمية، والمتمثلة أساسا في الفجوة بين الواقع والسياقات الوطنية والتقدم التكنولوجي المتسارع عبر شبكة شبه عالمية للأنترنت من جهة، والتنظيمات الوطنية المتباينة في التعامل مع حوكمة المنصات الرقمية من جهة أخرى.

حيث تتسم الإطارات القانونية المنظمة للمنصات الرقمية عبر العالم بالتباين والاختلاف، نتيجة لخصوصية السياقات الوطنية التي تحكمها اعتبارات سياسية واقتصادية واجتماعية وثقافية وأمنية، الشيء الذي يصعب معه محاولة التوصل إلى إطار دولي موحد بشأن حوكمة المنصات الرقمية. واستجابة لهذه الحقائق، يقدم البحث بعض المقترحات؛ كخطوات محتملة لصناع السياسات، والهيئات التي تسعى إلى تحقيق التوازن بين السيادة الرقمية الوطنية وتعزيز وحماية الحقوق والحريات عبر المنصات الرقمية، والاستثمار في التعاون الدولي والحفاظ على شبكة أنترنت عالمية ومنفتحة، وهي كالتالي:

- ⇐ **إنشاء معجم مشترك حول تنظيم المنصات الرقمية وتعزيز التعاون من خلال شبكات الهيئات التنظيمية:**

على الرغم من التباين بين التوجهات الوطنية المعنية بتنظيم المنصات الرقمية، إلا أن هناك انسجام كبير في اللغة التي تستخدمها الحكومات عند التعامل مع تنظيم المنصات، وفي أغلب الأحيان فيما يتصل بقضايا الأمن، وتخفيف الأضرار وحماية المستخدمين. ويتعين على الحكومات أن تمكن هيئاتها التنظيمية المعنية من السعي إلى التوصل إلى إجماع دولي بشأن:

- تحديد القيم التي تؤطر التنظيم القانوني للمنصات بشكل واضح، ومحاولة تحقيق الإجماع حول التوجهات الأنسب لتنظيم المنصات الرقمية الناشئة في جميع أنحاء العالم؛

- تعزيز الشبكات الدولية الرسمية والغير الرسمية للهيئات التنظيمية، من أجل تعزيز تبادل المعلومات والخبرات الفنية؛
- ضمان تعاون الهيئات التنظيمية في تصميم وتنفيذ التنظيمات ضمن حدود التشريعات الوطنية؛
- الاستثمار في التكنولوجيا التي تعمل على بناء وتعزيز التوافق المؤسسي بين الهيئات التنظيمية وشبكاتها.

⇐ **صياغة تشريعات تنظيم المنصات الرقمية على أساس نهج احترام وتعزيز حقوق الإنسان:**

ينبغي أن يتم اعتماد التشريعات التنظيمية للمنصات الرقمية وسياسات تعديل المحتوى الخاصة بمقدمي الخدمات الرقمية ضمن إطار القانون الدولي لحقوق الإنسان، وخاصة تلك المعترف بها دوليا، كالعهد الدولي الخاص بالحقوق المدنية والسياسية وغيره من الصكوك الدولية والإقليمية، وهذا يعني أنه:

- يتعين على الدول أن تسن قوانين واضحة وشفافة بما فيه الكفاية لإدارة المحتوى عبر الإنترنت، وأن ينطبق الأمر نفسه على سياسات تعديل المحتوى الخاصة بالمنصات الرقمية. كما ينبغي للقوانين والسياسات أن توازن بعناية بين حقوق المستخدمين في البحث عن المعلومات والأفكار من جميع الأنواع وتلقيها ونقلها وبين الحقوق أو المصالح المتنافسة الأخرى عبر الإنترنت، مثل حرية التعبير وعدم التمييز والخصوصية...؛
- يتطلب تحقيق هذا التوازن اتباع نهج غير ثنائي في إدارة المحتوى أو تعديله. فالقيود المفروضة على أنواع مختلفة

⇐ **تعزيز التعاون الثنائي والمتعدد الأطراف في مجال البرمجيات والقطاع الرقمي:**

لا يزال التعاون العالمي في مجال تنظيم البرمجيات والقطاع الرقمي محدودا. فإلى جانب الجهود التنظيمية الرامية إلى التأطير القانوني للمنصات الرقمية حاليا، فمن الأهمية بمكان أن تأخذ الحكومات على محمل الجد متطلبات مواكبة تكنولوجيا الذكاء الاصطناعي الحديثة والمستجدة باستمرار. وينبغي أن تتضمن هذه الجهود ما يلي:

- اعتماد إطار معياري للتعاون العابر للحدود بشأن العمليات المشتركة وقواعد الممارسة الجيدة بشأن تنظيم المنصات الرقمية وتكنولوجيا الذكاء الاصطناعي ذات الصلة؛
- التمويل المشترك للاستثمار التكنولوجي السيادي، حيث يمكن تحديد المتطلبات المجتمعية المتبادلة وتلبيتها من خلال مشروع موحد؛
- تمويل مشترك لصناديق التكنولوجيا المستقلة لدعم تطوير التقنيات والمعايير الأفضل لتنظيم المنصات الرقمية؛
- تعزيز الشبكات الرسمية وغير الرسمية للتعاون الرقمي بين الحكومات لدعم تطوير البرمجة التكنولوجية المتعددة الأطراف والتعاون بشأنها.

من المحتوى عبر الإنترنت يجب أن تتجاوز الثنائية المتمثلة في "الحذف/الترك" لتشمل تدابير أخرى، مثل وضع علاما تميز أنواع معينة من المحتوى الرقمي، ك"التصنيف الرقمي" للمعلومات عبر الانترنت. مع التأكيد على أن آليات التظلم والإنصاف تشكل ضمانة أساسية ضد قرارات تعديل المحتوى الخاطئة؛

- تقديم الدعم لمواصلة تطوير تشريعات تنظيمية تركز على الأهداف والنتائج والعمليات التي تقدمها المنصات الرقمية، بدلاً من التركيز بشكل كبير على أجزاء فردية من المحتوى أو سلوك المستخدم.
- ينبغي أن تتم عملية صياغة القوانين بطريقة تشاركية تسمح بتقديم مدخلات متنوعة، وتستند إلى التحليل التجريبي، ومصحوبة بتقييمات الأثر؛
- إنشاء آليات مستقلة للإشراف على المنصات الرقمية وفقاً للمصلحة العامة وبما يتوافق مع الالتزامات الدولية؛
- ضمان صياغة القوانين بدقة كافية لتمكين الفرد من تنظيم سلوكه وفقًا للقانون؛
- ينبغي عند صياغة القانون اتباع نهج يضع معايير محددة وواضحة ويترك للقاضي سلطة تقديرية لتحديد مدى استيفاء تلك المعايير.
- تحديد ما هو محظور بشكل واضح ودقيق، وكذلك من يمكن تحميله المسؤولية عن عدم الامتثال لتطبيق الحظر؛
- ضمان أن يتطلب القانون الشفافية وسبل الانتصاف الفعالة، لتجنب منح سلطة تقديرية لا محدودة لتقييد حرية التعبير للمكلفين بتنفيذ وتطبيق القانون.

⇐ **إنشاء مجلس وطني لتدبير المنصات الرقمية:**

تعد المجالس الوطنية لتدبير المنصات الرقمية عبارة عن هيئات متعددة الأطراف (المجتمع المدني، الخبراء...) تعقد بانتظام لمعالجة تعديل المحتوى والتحديات المرتبطة بحرية التعبير والخصوصية في الفضاء الرقمي. ويمكن لهذه المجالس أن تقوم بمجموعة واسعة من الوظائف، بما في ذلك:

- توفير منتدى منتظم لمناقشة المعايير ومشاركة أفضل الممارسات بشأن معايير تعديل المحتوى الرقمي؛
- إنشاء مدونات لقواعد السلوك بشأن مكافحة خطاب الكراهية عبر الإنترنت؛
- تطوير المعايير ومشاركة الممارسات الفضلى فيما يتعلق بالشفافية والمساءلة، وخاصة بما يتعلق باستخدام الذكاء الاصطناعي والخوارزميات للكشف عن الخطاب والمحتوى الغير قانوني بالمنصات الرقمية؛
- مناقشة قضايا الاختصاص القضائي العابر للحدود الوطنية المرتبط بالدعاوي المرفوعة ضد المنصات الرقمية العالمية.

الملحق رقم1 : القوانين ومشاريع القوانين موضوع الدراسة

القوانين المعتمدة والسارية المفعول

الدولة	القانون	تاريخ الاعتماد
مالاوي	قانون المعاملات الإلكترونية والأمن السيبراني في ملاوي (2016)	2017
مالي	قانون مالي رقم 056-2019 بشأن قمع الجرائم الإلكترونية	2020
نيوزيلاندا	قانون الاتصالات الرقمية الضارة في نيوزيلندا	2015
سنغافورة	قانون التدخل الأجنبي (التدابير المضادة) في	2021
كوريا الجنوبية	قانون كوريا الجنوبية رقم 14080 بشأن تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات	2016

تنزانيا	قواعد الاتصالات الإلكترونية والبريدية (المحتوى عبر الإنترنت)	2020
أستراليا	قانون السلامة على الإنترنت	2021
الاتحاد الأوروبي	قانون الخدمات الرقمية	2022
نيوزيلندا	قانون الاتصالات الرقمية الضارة	2015
المملكة المتحدة	قانون السلامة على الإنترنت	2023
النمسا	قانون منصات الاتصالات	2020
الهند	قواعد تكنولوجيا المعلومات في الهند (المبادئ التوجيهية للوسيط ومدونة أخلاقيات الوسائط الرقمية)	2021
باكستان	قواعد إزالة وحظر المحتوى غير القانوني عبر الإنترنت	2021
روسيا	القانون الاتحادي الروسي رقم FZ242 بشأن تعديل بعض القوانين التشريعية المتعلقة بتحديث إجراءات معالجة البيانات الشخصية في شبكات المعلومات والاتصالات (قانون توطين البيانات)	2015
تركيا	القانون رقم 5651 بشأن تنظيم البث في شبكة الإنترنت ومكافحة الجرائم التي ترتكب خلال البث عبر الإنترنت	2007

مشاريع القوانين

الدولة	مشروع القانون	تاريخ الاقتراح
بنغلاديش	مشروع اللائحة التنظيمية لبنغلاديش بشأن وسائل الإعلام الرقمية ووسائل التواصل الاجتماعي والمنصات	2021
نيجيريا	مشروع قانون الحماية من الأكاذيب والتلاعب على الإنترنت	2019
الفلبين	مشروع قانون مكافحة المحتوى الزائف	2019
كندا	مشروع قانون مكافحة الأضرار عبر الانترنت	2024
ايرلندا	مشروع قانون تنظيم السلامة على الإنترنت ووسائل الإعلام	2022
البرازيل	مشروع القانون رقم 2630 بشأن الحرية والمسؤولية والشفافية على الإنترنت ("قانون الأخبار الزائفة")	2020
بولندا	مشروع قانون حماية حرية التعبير على مواقع التواصل الاجتماعي	2021

المراجع:

1-يمكن تعريف السيادة الرقمية على أنها توجه استراتيجي يهدف إلى إعادة تأكيد سلطة الجهات الفاعلة في الدولة على الفضاء الإلكتروني، بما في ذلك سلطتها في مجال تطوير التكنولوجيا الرقمية. وعلى هذا النحو، تتطلب السيادة الرقمية الاعتراف بحقوق الدول فيما يخص تطوير واستخدام الآليات والسياسات اللازمة لتنظيم الأنشطة السيبرانية داخل حدودها الترابية.
Folashadé Soulé, 'Digital Sovereignty in Africa: Moving beyond Local Data Ownership', Center for International Governance Innovation, Policy Brief No. 185 — June 2024, page 1. تاريخ التصفح: 2024/07/01
https://www.cigionline.org/static/documents/PB_no.185.pdf

2- David Medine, 'Data Localization: A "Tax" on the Poor', CGD Working Paper 674. Washington, DC: Center for Global Development, page 3. تاريخ التصفح
2024/06/03https://www.cgdev.org/publication/data-localization-tax-poor

3- Internet Society, 'Internet Impact Brief: Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021', 4 March 2022. تاريخ التصفح 2024/06/04
https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-bangladesh-regulation-for-digital-social-media-and-ott-platforms-2021/#:~:text=Bangladesh's%20draft%20Regulation%20requires%20intermediaries,on%20their%20website%20or%20app.

4- Shahzeb Mahmood, 'BANGLADESH: LEGAL AND POLICY IMPLICATIONS OF THE PROPOSED OTT, DIGITAL AND SOCIAL MEDIA REGULATIONS', Techglobal Institute, 2024/06/04 تاريخ التصفح
https://techglobalinstitute.com/research/bangladesh-ott-and-social-media-regulations/

5- Council of Europe, 'Octopus Cybercrime Community: Malawi',2024/06/06 تاريخ التصفح
https://www.coe.int/en/web/octopus/-/malawi

6-Freedom House, 'Freedom on the Net 2022: Malawi' تاريخ التصفح
2024/06/06https://freedomhouse.org/country/malawi/freedom-net/2022

7- Council of Europe, 'Octopus Cybercrime Community: Mali',2024/06/06 تاريخ التصفح

https://www.coe.int/en/web/octopus//mali#:~:text=The%20new%20Law%20n%C2%B0,territory%E2%80%9D%20(article%202).

8- Simone Toussi, 'New Mali Cybercrime Law Potentially Problematic to Digital Rights', The Collaboration on International ICT Policy for East and Southern Africa, February 21, 2020. تاريخ التصفح 2024/06/07
https://cipesa.org/2020/02/new-mali-cybercrime-law-potentially-problematic-to-digital-rights/

9- Netsafe, 'WHAT IS THE HDCA?', 1st September 2021, 2024/06/06 تاريخ التصفح
https://netsafe.org.nz/what-is-the-hdca/

10- Verengai Mabika, 'Internet Impact Brief: Nigeria's Protection from Internet Falsehood and Manipulation Bill 2019', 21 February 2022, page 6. 2024/06/07 تاريخ التصفح
https://www.internetsociety.org/wp-content/uploads/2022/02/IIB-Nigeria-Social-Media-Bill.pdf

11- Tech against Terrorism, 'THE ONLINE REGULATION SERIES 2021: NIGERIA', Nov 30, 2021.2024/06/07 تاريخ التصفح

https://techagainstterrorism.org/news/2021/11/30/the-online-regulation-series-2021-nigeria

12- Asia Centre and Council of Asian Liberals and Democrats, 'Defending Freedom of Expression: Fake news laws in east and Southeast Asia', 2020, pages 28-29. 2024/06/08 تاريخ التصفح
https://asiacentre.org/wp-content/uploads/Defending_Freedom_of_Expression_Fake_News_Laws_in_East_and_Southeast_Asia.pdf

13- Human Rights Watch, 'Singapore: Withdraw Foreign Interference (Countermeasures) Bill', October 13, 2021. 2024/06/08 تاريخ التصفح
https://www.hrw.org/news/2021/10/13/singapore-withdraw-foreign-interference-countermeasures-bill

14- The Korean Law Information Center, 'ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION', 23. September 2016 .2024/06/09 تاريخ التصفح
https://law.go.kr/LSW/lsInfoP.do?lsiSeq=181842&viewCls=engLsInfoR&urlMode=engLsInfoR#EJ44:7

15- THE ELECTRONIC AND POSTAL COMMUNICATIONS (ONLINE CONTENT) REGULATIONS, 2020, SUBSIDIARY LEGISLATION to the Gazette of the United Republic of Tanzania No.29 Vol. 101 dated 17 th July, 2020 Printed by the Government Printer, Dodoma by Order of Government, Supplement No. 29, 17 th 7, 2020. تاريخ التصفح 2024/08/01
https://www.tcra.go.tz/uploads/documents/sw-1619088125-The%20Electronic%20and%20Postal%20Communications%20(Online%20Content)%20Regulations,%202020.pdf

16- Conseil de l'Europe, « Octopus Cybercrime Community : Mali -Statut concernant la Convention de Budapest», تاريخ التصفح 2024/06/09https://www.coe.int/fr/web/octopus/-/mali

17- Singapore Statutes Online, « Foreign Interference (Countermeasures) Act 2021". تاريخ التصفح
2024/06/10https://sso.agc.gov.sg/Act/FICA2021/Uncommenced/20221013155608?DocDate=20211125

18-Amnesty International, 'Nigeria: NITDA Code of Practice must comply with International Human Rights Law',
June 24, 2022 Index Number: AFR 44/5818/2022. تاريخ التصفح
2024/06/10https://www.amnesty.org/en/documents/afr44/5818/2022/en/

19-DLA Piper, 'DATA PROTECTION LAWS OF THE WORLD: South Korea', 31 May 2024, Page 4. تاريخ التصفح 2024/06/11
https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=KR

20- Article 19, 'Tanzania: Online Content Regulations 2020 extremely problematic in the context of COVID-19 pandemic', JANUARY 19, 2021,2024/06/14 تاريخ التصفح
https://www.article19.org/resources/tanzania-online-content-regulations-problematic-covid-19-pandemic/

21-Esafety Commissioner, 'Learn about the Online Safety Act', 18/03/2024. تاريخ التصفح
2024/06/16https://www.esafety.gov.au/newsroom/whats-on/online-safety-act#:~:text=What%20is%20the%20Online%20Safet

y,harmful%20behaviour%20and%20toxic%20content.

22- Government of Canada, 'Proposed Bill to address Online Harms', 2024-04-20. تاريخ التصفح 2024/06/20https://www.canada.ca/en/canadian-heritage/services/online-harms.html

23- European Commission, 'A Europe fit for the digital age: new online rules for users'. تاريخ التصفح 2024/06/22https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-users_en

24- European Commission, 'Europe fit for the Digital Age: New online rules for businesses'. تاريخ التصفح 2024/06/22https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-businesses_en

25- European Commission, 'Europe fit for the Digital Age: new online rules for platforms', تاريخ التصفح 2024/06/22https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-platforms_en

26-The European Commission, 'The enforcement framework under the Digital Services Act', تاريخ التصفح 2024/06/23 https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement#ecl-inpage-lo5rgw1q

27-The European Commission, 'European Board for Digital Services', 16 July 2024. تاريخ التصفح 2024/06/24 https://digital-strategy.ec.europa.eu/en/policies/dsa-board

28-Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Act 2022', 5 April 2023, تاريخ التصفح 2024/06/24

https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/

29-New Zealand Police, 'Harmful Digital Communications'.2024/06/25 تاريخ التصفح https://www.police.govt.nz/advice-services/cybercrime-and-internet/harmful-digital-communicationshdc#:~:text=The%20Harmful%20Digital%20Communications%20Act,forms%20of%20abuse%20and%20intimidation.

30-Community Law, 'Criminal offences under the Harmful Digital Communications Act'. تاريخ التصفح 2024/06/25 https://communitylaw.org.nz/community-law-manual/chapter-34-bullying-harassment-and-sexual-harm/cyberbullying-protections-against-online-digital-harassment/criminal-offences-under-the-harmful-digital-communications-act/

31-Government activity, 'Cyberflashing to become a criminal offence', 13 March 2022. تاريخ التصفح 2024/06/26https://www.gov.uk/government/news/cyberflashing-to-become-a-criminal-offence

32-Niamh Ancell, 'the dark side of internet trolling: cyber flashing and epilepsy trolling explained', 08 February 2024. 2024/06/27 تاريخ التصفح https://cybernews.com/editorial/cyber-flashing-epilepsy-trolling-explained/

33-Department for Science, Innovation & Technology, 'Online Safety Act: explainer', 8 May 2024. 2024/06/28 تاريخ التصفح https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#:~:text=The%20Online%20Safety%20Act%202023,users'%20safety%20on%20their%20platforms.

34-Commonwealth of Australia Explanatory Memoranda, 'ONLINE SAFETY BILL 2021', تاريخ التصفح 2024/06/28http://classic.austlii.edu.au/au/legis/cth/bill_em/osb2021164/memo_0.html

35-Electronic Irish Statute Book, 'Online Safety and Media Regulation Act 2022', تاريخ التصفح 2024/06/29https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/print#part12

36-EUR-Lex, 'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)',2024/06/29 تاريخ التصفح https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

37-Reich-Rohrwig Hainz, 'Communication platforms face new obligations and high fines in

Austria', Lexology, March 22 2021, تاريخ التصفح 2024/06/29
https://www.lexology.com/library/detail.aspx?g=fcf46df4-4694-4f10-b11b-67564a824470

38-Reich-Rohrwig Hainz, Supra.

39-Ibid.

40- Sharon Schmidt, 'AUSTRIA: AUSTRIA'S DRAFT COMMUNICATION PLATFORM ACT – A SUMMARY', November 26, 2020.2024/06/29 تاريخ التصفح
https://oblin.at/newsletter/austria-austrias-draft-communication-platform-act-a-summary/

41-Organization for Security and Co-operation in Europe, 'Legal review of the draft Federal Act on Measures to Protect Users on Communications Platforms (Kommunikationsplattformen-Gesetz – KoPI-G) by the Republic of Austria', 15 October 2020, pages- 18-19.

42-Tomaz, Tales. 2023. "Brazilian Fake News Bill: Strong Content Moderation Accountability but Limited Hold on Platform Market Power." Javnost - The Public 30 (2): 254–257. 2024/06/30 تاريخ التصفح
https://doi.org/10.1080/13183222.2023.2201801

43-Vijay Pal Dalmia, 'A Brief Into The Information Technology (Guidelines For Intermediaries And Digital Media Ethics Code) Rules, 2021', Mondaq, 29 December 2022.2024/07/05 تاريخ التصفح
https://www.mondaq.com/india/social-media/1266276/a-brief-into-the-information-technology-guidelines-for-intermediaries-and-digital-media-ethics-code-rules-2021

44-Tech against Terrorism, 'THE ONLINE REGULATION SERIES | POLAND', November 16, 2021. تاريخ التصفح
2024/07/07https://techagainstterrorism.org/news/2021/11/16/the-online-regulation-series-poland

45-One Trust Data Guidance, 'Pakistan - Data Protection Overview', July 2024. تاريخ التصفح

15
2024/07/https://www.dataguidance.com/notes/pakistan-data-protection-overview

46-Digital Rights Foundation, 'Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2020: Legal Analysis', November 30, 2020, page 15. 2024/07/17 تاريخ التصفح
https://digitalrightsfoundation.pk/wp-content/uploads/2020/12/Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules-2020_-Legal-Analysis.pdf

47-The Gazette of Pakistan, Extra, 13 October 2021, page 1762. تاريخ التصفح
2024/07/20https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF

48-John Tomaszewski & Jason Priebe, 'Fortress Russia – The Russian Data Localization Law', Syfarth, May 4, 2015.2024/07/23 تاريخ التصفح

https://www.globalprivacywatch.com/2015/05/fortress-russia-the-russian-data-localization-law/

49-Ksenia Andreeva, Anastasia Kiseleva and Alena Neskoromyuk, Morgan Lewis, 'Data Localization Laws: Russian Federation, Practical Law Country Q&A', 22-Jul-2021. Pages 1-5. تاريخ التصفح
2024/07/23
https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf

50-Tech against terrorism, 'The online Regulation Series, Turkey', October 2020. تاريخ التصفح
2024/07/27
https://techagainstterrorism.org/news/2020/10/23/the-online-regulation-series-turkey#:~:text=The%20Regulation%20of%20Publications%20on,enables%20the%20blocking%20of%20websites

51-Ayşegül Zengin, 'Social Media Law', August 5, 2020.2024/07/27 تاريخ التصفح
https://aysegulzengin.av.tr/social-media-law/

52-David Medine, 'Data Localization: A "Tax" on the Poor', Supra, pages 3-4.

53-David Medine, 'Data Localization—a Hidden Tax on the Poor', Blog Post, March 27, 2023. تاريخ التصفح
2024/08/05https://www.cgdev.org/blog/data-localization-hidden-tax-poor