دفاتر السياسة والقانون المجلد: 18 / العدد: 01 (2026) ص ص: 01 - 18

الجرائم الخوارزمية في منصات التواصل الاجتماعي: دراسة قانونية تحليلية لمنصة فيس-بوك في ظل الذكاء الاصطناعي.

lgorithmic Criminality on Social Media Platforms: A Legal and Analytical Examination of Facebook under Artificial Intelligence

أمال بويجياوي*

جامعة البشير الابراهيمي، برج بوعريريج، الجزائر، amel.bouyahiaoui@univ-bba.dz

تاريخ الإرسال:11/03/ 2025* تاريخ القبول2026/01/14* تاريخ النشر: 20 01 /2026

ملخص:

تمثل الجرائم الخوارزمية التي ترتكب عبر منصة فيسبوك مظهرا مستحدث ا للجريمة الرقمية في ظل تطور تقنيات الذكاء الاصطناعي، إذ أضحت الخوارزميات أداة فعّالة في تحليل السلوك الإنساني وتوجيه المحتوى بطرق قد تمس المصالح الفردية والجماعية ، وتكمن الخطورة في إساءة توظيف هذه الأنظمة لتحقيق أغراض غير مشروعة، مثل نشر المعلومات الكاذبة، التأثير الممنهج على الرأي العام، أو انتهاك الخصوصية من خلال معالجة البيانات الشخصية دون موافقة أصحابها. كما ساهم الذكاء الاصطناعي في ظهور ممارسات أكثر تعقيدا، من قبيل التزييف العميق الذي يستعمل لأغراض التضليل والتأثير السياسي ، وتُثير هذه الأفعال إشكالات قانونية جوهرية تتعلق بتحديد الركن المادي والمعنوي للجريمة، فضلا عن صعوبة إسناد المسؤولية الجنائية في ظل الطبيعة الذاتية للتعلم الخوارزمي. ومن ثم، تفرض هذه الجرائم ضرورة تطوير منظومة قانونية متكاملة تواكب التحول الرقمي وتضمن التوفيق بين حرية التعبير وحماية الحقوق الرقمية للأفراد.

الكلمات المفتاحية:

الجرائم الخوارزمية،الذكاءالاصطناعي، منصةفيسبوك،التزييف العميق، المسؤولية الجنائية.

Abstract:Algorithmic crimes committed through the Facebook platform represent a new form of digital criminality shaped by the advancement of artificial intelligence technologies.Algorithms have become powerful tools for analyzing human behavior and directing content in ways that may infringe upon individual and collective interests. The misuse of these systems for unlawful purposes—such as spreading misinformation, manipulating public opinion, or violating privacy through unauthorized data processing—raises significant concerns. Deepfake technologies further exacerbate these risks by enabling deception and political interference. Such practices pose critical legal challenges in identifying criminal elements and attributing responsibility amid the autonomous nature of algorithmic learning. Therefore, a modern legal framework is essential to address these AI-driven threats while ensuring a balance between freedom of expression and digital rights.

Keywords: Algorithmic crimes, Artificial intelligence, Facebook platform, Deepfake, Criminal responsibility

* **أمال بويجياوي**

مقدمة:

شهد العالم خلال العقدين الأخيرين تحولا رقميا عميقا تمثل في بروز منصات التواصل الاجتماعي كأدوات فاعلة في الحياة اليومية للأفراد، ومؤثرة في تشكيل المشهدين الثقافي والسياسي على حد سواء. ومع هذا التحول، تصاعد دور الخوارزميات الذكية، وهي أنظمة قائمة على تقنيات الذكاء الاصطناعي تُستخدم لتنظيم المحتوى وتوجيهه تبعًا لأنماط سلوك المستخدمين، الأمر الذي أحدث انقلابا في أساليب تلقي المعلومات وصناعة الرأي العام..

غير أن هذه الطفرة الرقمية لم تخل من آثار جانبية سلبية، إذ أفرزت نوعا جديدا من الجرائم الرقمية المعقدة، أُطلق عليها اصطلاحًا "الجرائم الخوارزمية". وهي جرائم لا تصدر عن فاعل بشري مباشر، بل تنتج عن سلوك أنظمة الذكاء الاصطناعي التي تتعلم ذاتيا وتتخذ قراراتها بناءً على خوارزميات مستقلة ، ولعل أبرز مثال على ذلك ما كشفته قضية "كامبريدج أناليتيكا"، حين استغلت خوارزميات منصة فيسبوك لتحليل بيانات المستخدمين وتوجيههم سياسيًا دون علمهم، مما أدى إلى انتهاك جسيم لخصوصيتهم وتأثير مباشر على نزاهة العمليات الانتخابية. كما ساهمت خوارزميات المنصة في كثير من الأحيان تضخيم خطاب الكراهية والتحريض على العنف الجماعي، دون وعي أو قصد مباشر من الشركة أو المستخدمين ، وفي هذا السياق، تُطرح إشكالية جوهرية وهي:

ما مدى إسهام الخوارزميات المدعومة بالذكاء الاصطناعي في ارتكاب الجرائم على منصة فيسبوك؟ وما هي الحدود القانونية لمسؤولية الفاعلين التقنيين عنها، في ظل غياب إطار قانوني واضح وملزم؟

تكتسب هذه الدراسة أهميتها من كونها تتناول مسألة قانونية حديثة ومعقدة في آنٍ واحد، تتمثل في تحديد المسؤولية عن محتوى لم يعد من إنتاج الإنسان بالضرورة، بل تولّدت معالمه بفعل أنظمة ذكية تتعلم ذاتيا وتتفاعل استنادًا إلى تحليل سلوك المستخدمين. وتمثل هذه الدراسة محاولة لإعادة النظر في المفاهيم القانونية التقليدية، ولا سيما مفهومي الركن المعنوي والعلاقة السببية، في ضوء التحولات التي أفرزها تطور الذكاء الاصطناعي.

وتهدف الدراسة إلى ما يلي:

تحليل مفهوم الجريمة الخوارزمية في إطار بيئة الذكاء الاصطناعي؛

إبراز دور خوارزميات منصة فيسبوك في إحداث أضرار واقعية على الأفراد والمجتمعات؛

اقتراح آليات تنظيمية مستقبلية تسهم في تقنين عمل الخوارزميات الذكية وضبط مسؤوليتها القانونية.

وقد اعتمدت الدراسة المنهج الوصفي التحليلي من خلال تحليل المفاهيم والنصوص ذات الصلة، إلى جانب المنهج التطبيقي عبر دراسة حالة منصة فيسبوك باعتبارها من أبرز النماذج الواقعية لجرائم الذكاء الاصطناعي.

ولتغطية أبعاد الموضوع، تنقسم هذه الدراسة إلى محوريين رئيسيين:

المحور الأول: ماهية الجريمة الخوارزمية في بيئة الذكاء الاصطناعي

المحورالثاني: مظاهر الجرائم الخوارزمية على فيسبوك وقيام المسؤولية الجنائية

1.المحور الأول: ماهية الجريمة الخوارزمية في بيئة الذكاء الاصطناعي

أفرز التطور السريع في مجالات الذكاء الاصطناعي واقع ا قانونيا جديدا تتداخل فيه الأبعاد التقنية مع المفاهيم التقليدية للجريمة والمسؤولية ، فقد أصبحت الأنظمة الذكية والخوارزميات قادرة على اتخاذ قرارات مستقلة، وتحليل كم هائل من البيانات بطريقة قد تفضي إلى نتائج مؤثرة في الواقع الاجتماعي والقانوني ، ومع هذا التحول، برزت الحاجة إلى دراسة ماهية الذكاء الاصطناعي والخوارزميات من جهة، والجريمة الخوارزمية من جهة أخرى، قصد تحديد طبيعتها وتمييزها عن الجرائم التقليدية، وفهم دوافعها وآليات ارتكابها في بيئة رقمية متغيرة. ومن هذا المنطلق، يتناول هذا المحور بالتحليل الأسس النظرية والفكرية التي يقوم عليها مفهوم الجريمة

الخوارزمية، وذلك من خلال عنصرين رئيسيين:يتناول العنصر الأول مفهوم الذكاء الاصطناعي، أما العنصر الثاني نتناول فيهمفهوم الجريمة الخوارزمية.

1.1. مفهوم الذكاء الاصطناعي

إن فهم المفاهيم والمصطلحات التقنية التي يقوم عليها الذكاء الاصطناعي والخوارزميات خطوة أساسية لبيان طبيعة الجرائم الخوارزمية وتحديد أبعادها القانونية ، فهذه التقنيات أصبحت المحرك الرئيسي لمنصات التواصل الاجتماعي التي باتت تؤثر بعمق في تشكيل السلوك والرأي العام ، ومن أبرز هذه المنصات منصة فيسبوك، التي تُعد من أكثر البيئات الرقمية توظيفا للذكاء الاصطناعي في إدارة المحتوى وتوجيه المستخدمين .

وانطلاقا من ذلك، سنتناول التعريف بالذكاء الاصطناعي والخوارزميات ووظيفتهما في البيئة الرقمية وكذا التعريف بمواقع التواصل الاجتماعي ومنصة فيسبوك، لنتطرق بعدها لدراسة خوارزميات فيسبوك باعتبارها أحد التطبيقات العملية للذكاء الاصطناعي في المجال الرقمي.

1.1. 1. تعريف الذكاء الاصطناعي

يعد تحديد المفاهيم الأساسية خطوة ضرورية لفهم الإطار النظري للدراسة، إذ تسهم التعريفات الدقيقة في توضيح المصطلحات المحورية التي يقوم عليها البحث ، ومن ثم، يتناول هذا العنصر تعريف أبرز المفاهيم ذات الصلة، وهي الذكاء الاصطناعي بوصفه الإطار العام للتقنيات محل الدراسة، والخوارزميات باعتبارها الآلية التشغيلية لهذه الأنظمة، ومواقع التواصل الاجتماعي كبيئة حاضنة لتطبيقاتها، مع التركيز على منصة فيسبوك كنموذج تطبيقي يجسد التفاعل بين هذه المفاهيم في الواقع العملي.

أولا:تعريف الذكاء الاصطناعي والخوارزميات ووظيفتهما في البيئة الرقمية

وفي هذا العنصر سنتناول التعريف بمصطلحي الذكاء الاصطناعي والخوارزميات ووظيفتهما في البيئة الرقمية.

1.تعريف الذكاء الاصطناعي ووظيفته في البيئة الرقمية (Artificial Intelligence)

يقصد بالذكاء الاصطناعي "تلك النظم أو البرمجيات المصممة لمحاكاة قدرات الإنسان الذهنية، من خلال تنفيذ مهام معقدة كالتعلم، واتخاذ القرار، والتعرف على الأنماط، ومعالجة اللغة الطبيعية" .وقد عرفته منظمة التعاون الاقتصادي والتنمية(OECD)(OECD, 2024) بأنه: "نظام قائم علىالتكنولوجيا يُمكنه تحليل البيانات وتفسيرها والتعلم منها، ثم استخدام ما)تعلمه لأداء مهام معيّنة بشكل مستقل(OECD, 2019)

ويعد الذكاء الاصطناعي كمفهوم اخر بأنه" تلك القدرة التي تمتلكها الأنظمة الحاسوبية أو الآلات الذكية على تقليد الذكاء البشري، وذلك من خلال أدائها لمهام معقّدة كالتعلم، والتحليل، واتخاذ القرارات، وحل المشكلات، بالاعتماد على خوارزميات متطورة ومعالجة كميات هائلة من البيانات"(ج،د،ع، 2020، صفحة 6).

وقد أكدت الاستراتيجية العربية للذكاء الاصطناعي على ضرورة إخضاع هذه النظم لإطار قانوني وتنظيمي صارم، يكفل استخدامها بطريقة آمنة ومنصفة، لا سيما في الجوانب المتعلقة بصون الخصوصية والحدّ من التحيز والتمييز الخوارزمي.

وفي إطار المنصات الرقمية، يوظَّف الذكاء الاصطناعي في تنظيم المحتوى الذي يعرض على المستخدم، واستباق تفضيلاته، إلى جانب إدارة التبليغات وحذف المحتوى غير المرغوب فيه بآلية آلية(زغلول، 2023، صفحة 62).

2. تعريف الخوارزميات(Algorithms) ووظيفتها في البيئة الرقمية

يقصد بالخوارزمية: "مجموعة مرتّبة من الخطوات أو التعليمات المنطقية، المصمّمة لحل مشكلة معينة أو تنفيذ مهمة محددة بشكل آلي ودقيق".وإذا رجعنا إلى السياق الرقمي، نجد بأن الخوارزميات تشكل الأساس البرمجي الذي تعتمد عليه نظم الذكاء الاصطناعي لتحليل البيانات، تصنيف المعلومات، وتوجيه المحتوى، كما هو الحال في خوارزميات التوصية على منصات التواصل الاجتماعي.

كما أن الخوارزمية في مجال الذكاء الاصطناعي تمثل أداة حسابية تعتمد على تحليل كميات ضخمة من البيانات لاستخلاص قرارات بشكل آلي، لاسيما عبر تقنيات التعلم الآلي ، غير أن تعقيد بنيتها وكثرة المتغيرات التي تقوم عليها جعلت الباحثين يصفونها بـ "الصندوق الأسود"، إذ يصعب تفسير آلية عملهابدقة ، ويزداد هذا الغموض مع

الحماية القانونية المقررة لها في إطار أسرار المهنة والملكية الفكرية، فضلا عن إمكانية تكوّنها من عدة خوارزميات فرعية تزيد من صعوبة الكشف عن منطقها الداخلي(زغلول، صفحة 62).

ثانيا: تعريف **مواقع التواصل الاجتماعيوالفيس-بوك:**

إضافة الى تعريف مصطلحي الذكاء الاصطناعي والخورزميات سنعرف في هذا العنصر كل من مصطلحي مواقع التواصل الاجتماعي ومنصة فيس-بوك.

1.تعريف مواقع التواصل الاجتماعي

قبل الخوض في تعريف مصطلح الفيس -بوك علينا أولا تعريف مواقع التواصل بصفة عامة، حيث عرفها الباحث مرسي مشري": أنها تلك الشبكة الاجتماعية الرقمية التي لها هويات اجتماعية، ينشئها أفراد أو منظمات لديهم روابط نتيجة التفاعل الاجتماعي، تنشأ من أجل توسيع وتفعيل العلاقات المهنية أو علاقات الصداقة "

وعرفها الأستاذ زاهر راضي :" مواقع التواصل الاجتماعي هي منظومة من الشبكات الإلكترونيةالتي يسمح للمشترك فيها بإنشاء موقع خاص به ، و من ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الاهتمامات نفسها"(الزهراء و سالم عطية، 2020، صفحة 371).

2. تعريف منصةالفيس-بوك

التعريف الإجرائي للفيس-بوك: "هو عبارة عن موقع الكتروني للتواصل الاجتماعي، ومن خلاله يتم التواصل مع الأصدقاء والتعرف عليهم، تبادل الصور والنصوص والفيديوهات والربط، وهو منبر افتراضي كذلك للشباب للتعبير عن أفكارهم وأرا ءهم ومعتقداتهم(الزهراء و سالم عطية، صفحة 372).

موقع الفيسبوك يقدم خدماته مجانا للمستخدمين، ويجني أرباحه من الإعلانات، بما في ذلك إعلانات شعار الموقع، كما أنه يمكن مستخدميه من إنشاء ملفات شخصية تتضمن بعض الصور والاهتمامات الشخصية، ويتيح لهم تبادل الرسائل والمحادثات العامة أو الخاصة وكذا الانضمام إلى والطريقة التي يتجه بها شعور المستخدم.

.1.1.2خورزميات الفيس-بوك كأحد تطبيقات الذكاء الاصطناعي

أضحى الذكاء الاصطناعي يشكل المحرك الخفي للعالم الافتراضي، حيث تعتمد أغلب المنصات الرقمية على تقنياته في إدارة المحتوى وتحليل سلوك المستخدمين. ويعد الفيس-بوك من أبرز النماذج التي تجسّد هذا التفاعل بين الذكاء الاصطناعي والخوارزميات، إذ تو ظف المنصة أنظمة ذكية متطورة لتحليل البيانات الضخمة، وتخصيص التجربة الرقمية لك ل مستخدم على نحو دقيق. كما تلعب ملفات تعريف الارتباط (Cookies)دورا محوريا في جمع المعلومات وتغذية الخوارزميات بالمعطيات اللازمة لتطوير أنماط التنبؤ والتوصية، مما يثير تساؤلات قانونية وأخلاقية حول حدود استخدام هذه التقنيات وتأثيرها على الخصوصية في ظل الذكاء الاصطناعي.

أولا: دور الذكاء الاصطناعي في العالم الافتراضي

أصبح لأنظمة الذكاء الاصطناعي دور مفصلي في العالم الافتراضي عن طريق تحليل البيانات بهدف اكتشاف الاتجاهات، حيث تمتلك برامج الذكاء الاصطناعي القدرة على تحديد ما إن كانت العلامة التجارية تعرض مدح أو ذم أو بشكل محايد من خلال الجمع لبيانات وسائل التواصل الاجتماعي وتحليل تلك البيانات، وتقوم منصات الاستماع الاجتماعي المدعومة بالذكاء الاصطناعي بتحليل الاتجاهات والطريقة التي يتجه بها شعور المستخدم.كما أطلقت منصة فيسبوك " في العام 2013 نتيجة رغبتها في السيطرة على شبكات التواصل للعشرين سنة القادمة، مركز أبحاث متطور للذكاء الاصطناعي " Research Al Facebook" ، أو ما عرف اختصا ار بـ) FAIR)، له فروع في نيويورك وباريس بقيادة رائد الذكاء الاصطناعي "يان لوكا" ، وذلك بهدف تطوير الموقع لتتناسب أكثر مع المستخدم، ويتضمن ذلك أن تكون الإعلانات موجهة ، بالإضافة إلى إحداث تحسينات في برامج الدردشة الآلية مع مجموعة الأصدقاء (الزبيدي و شاهين، 2024، صفحة 26).

- وتعتبر شركة "مايكروسوفت" الشريك الحصري للفيس-بوك في تقديم خدمة إعلانات الشعار، ويقوم الفيس بوك بطرح الإعلانات التي تتضمنها قائمة الإعلانات الخاصة بشركة "مايكروسوفت" فقط(الجزيرة، 2015).

ثانيا: الفيس-بوك وعلاقته بملفات تعريف الارتباط في ظل الذكاء الاصطناعي

الفيس بوك كغيره من المواقع الإلكترونية يستخدم ملفات تعريف الارتباط(دهشان، 2020، صفحة 122)لغرض تحقيق أهداف معينة مثل التأكد من هوية المستخدم، ومحاولة الحفاظ على أمان الحساب، ولا يستطيع الحصول على تلك الملفات إلا بموافقة المستخدم، حيث لا يجوز لصاحبها مشاركتها مع أي موقع أو كيان آخر، لأن ذلك يعد انتهاك لخصوصية المستخدم ويشكل جريمة جنائية.

كما يستخدم موقع الفيس -بوك خوارزميات برمجية تُبنى عن طريق الذكاء الاصطناعي، حيث يمكنها القيام بعمليات يستحيل على العقل البشرى تصديقها لو ذُكرت أمامه من عشر سنوات ماضية، حيث علىسبيل المثال: يستطيع الفيس بوك تحديد اهتمامات المستخدم من خلال (تفاعلاته على صور أو منشورات معينه، ومتابعته لمنتجات محددة) وكل ذلك من أجل استخدامها في عرض إعلاناتله تتوافق معاهتماماته، وأيضاً عرض محتوى يتوافق على اهتماماته لجعله يتواجد في الموقع أطول فترة ممكنة في يومه.

وللوهلة الأولى قد يعتقد البعض أن ما يقوم به الفيس بوك تجاه المستخدم يعد انتهاك للخصوصية، ولكن المتمعن في الأمر يجد أن الفيس بوك – مثل باقي مواقع الشبكة العنكبوتية – يعرض سياسة استخداملأى مشترك جديد يرغب في التسجيل به، ويجب على المستخدم قبول الشروط الموجودة في تلك السياسة من أجل إكمال تسجيله واستخدام الموقع، ومن ضمن شروط سياسة الاستخدام ينصّ على موافقة المستخدم على قيام الفيس بوك بالحصول على بياناته واستغلالها في أغراض تجارية، وبالتالي تكون تلك الموافقة التي أعطاها المستخدم للفيس بوك هي المخرج القانوني والذى يجعل ما يقوم به الفيس بوك من انتهاكات بشأن خصوصية المستخدم غير مجرم(Meta, 2023).

في إطار تقنيات الذكاء الاصطناعي، تتمح البيانات المستخرجة من ملفات تعريف الارتباط (Cookies) مع خوارزميات التعلم الآلي من أجل بناء نماذج تنبؤيه دقيقة لسلوك المستخدمين ، وتهدف هذه النماذج إلى استباق اهتمامات الأفراد، سواء فيما يتعلق بنوعية المحتوى المعروض أو الإعلانات الموجّهة إليهم ، ويسهم هذا التكامل في أداء عدد من الوظائف المحورية، من أبرزها:

1.ترتيب المنشورات في صفحة "آخر الأخبار" وفقا لأنماط السلوك السابقة؛

2.عرض إعلانات مصممة خصيصا بما يتوافق مع تفضيلات المستخدم وسلوكياته الرقمية؛

3.تعزيز أو تقليص ظهور محتوى معين، بناءً على خوارزميات تحليل التفاعل والتأثير.

ويعد هذا التداخل بين الذكاء الاصطناعي وملفات تعريف الارتباط الأساس التقني لما يُعرف بـ "الاستهداف السلوكي (BehavioralTargeting) "، وهو نهج أثار انتقادات قانونية وأخلاقية واسعة، لا سيما عقب فضيحة Cambridge Analytica، التي كشفت عن إساءة استخدام بيانات ملايين المستخدمين لأغراض التأثير على الميول السياسية والانتخابية.

ورغم تأكيدات شركة "ميتا" (فيسبوك سابق ا) على أن جمع البيانات يتم بموافقة المستخدم، إلا أن الغموض المحيط بسياسات الخصوصية، وغياب الشفافية في آليات تشغيل الذكاء الاصطناعي، دفع العديد من الجهات التنظيمية، خاصة في أوروبا، إلى التشكيك في مشروعية هذه الممارسات(Meta, 2023).

1.2.مفهوم الجرائم الخوارزمية

إن الخوارزميات قد تستخدم ليس فقط لتحسين الخدمات، بل أيضًا لاستغلال تحيّزات المستخدمين، وتوجيه سلوكهم بطرق غير مشروعة، مما قد يؤدي إلى أفعال تحمل صفات جنائية أو ضارة اجتماعيا، وهو ما يبرر تصنيف بعض مخرجات الخوارزميات ضمن الأفعال الجرمية، ومن أمثلة هذه الجرائم جريمة التمييز العنصري أو العرقي الناتج عن خوارزميات تصنيف المستخدمين، التلاعب بالخوارزميات لتوجيه الرأي العام أو نشر أخبار مضللة، استغلال خوارزميات التسويق لاستهداف فئات هشة نفسيا أو اقتصاديًا، اتخاذ قرارات آلية تؤدي إلى ضرر مادي أو معنوي دون رقابة بشرية كافية.

وفي هذا المضمار سنتطرق الى تعريف الجريمة الخوارزمية وخصائصها في عنصرأول، وفي عنصر ثان سنشيرإلى الفرق بين الجريمة الخوارزمية والجريمة التقليدية ودوافع ارتكابها.

1.2.1. تعريف الجريمة الخوارزمية وخصائصها

تعد الجريمة الخوارزمية من المفاهيم المستحدثة في البيئة الرقمية، إذ نشأت مع تطور أنظمة الذكاء الاصطناعي واعتمادها المتزايد على الخوارزميات في اتخاذ القرارات وتنفيذ الأفعال ، ويهدف هذا العنصر إلى تحديد مفهوم الجريمة الخوارزمية وبيان خصائصها المميزة، بما يسمح بفهم طبيعتها القانونية والتقنية، وكيفية تمييزها عن غيرها من الجرائم الإلكترونية التقليدية.

أولا: تعريف الجريمة الخوارزمية

الجريمة الخوارزمية:(Algorithmic Crime) هي صورة جديدة وأكثر تطورًا من الجرائم المعلوماتية، ترتبط بالذكاء الاصطناعي والخوارزميات، تقوم على استغلال الخوارزميات الذكية في ارتكاب أفعال غير مشروعة، مثل:

1.التلاعب بالمحتوى في وسائل التواصل (التضليل – الأخبار الزائفة)؛

2.برمجيات التنبؤ التي تستغل البيانات الشخصية بطريقة غير مشروعة؛

3.توجيه الإعلانات أو القرارات بشكل منحاز أو مضلل بفعل خوارزميات الذكاء الاصطناعي.

الجريمة خوارزمية تدخل ضمن الإطار الأوسع للجرائم المعلوماتية، لكنها متميزة عنها من حيث الآلية (الاعتماد على الخوارزميات والذكاء الاصطناعي بدلا من مجرد استخدام الأجهزة والشبكات).

الجريمة الخوارزمية ليست جريمة تقليدية يرتكبها إنسان مباشر، وإنما هي جريمة ترتبط بعمل الخوارزميات (algorithms)المستخدمة في الذكاء الاصطناعي ومنصات التواصل .والخوارزمية كما أشرنا من قبل هي مجموعة أوامر مبرمجة لتنفَّذ تلقائيًا، لكنها أحيانًا قد تؤدي – عن قصد أو دون قصد إلى نتائج ضارة أو غير قانونية.

والمقصود بالجريمة الخوارزمية هي: "أي فعل أو قرار صادر عن نظام خوارزمي (معزز بالذكاء الاصطناعي أو تحليل تنبؤي) يسبب ضررًا أو تمييزًا غير مبرر بحق فرد أو فئة، مما يؤدي إلى انتهاك حقوق محمية قانونيًا، دون وجود رقابة بشرية كافية أو دليل واضح على قصد إجرامي مباشر"(السباعي، 2024).

ثانيا: خصائص الجريمة الخوارزمية

من بين خصائص الجريمة الخوارزمية نذكر مايلي:

1.ارتباطها بالذكاء الاصطناعي وطبيعتها المتخفية:

فهي تعتمد على الخوارزميات الذكية القادرة على التعلم واتخاذ قرارات مستقلة ، ويمكن كذلك أن تظل الجريمة الخوارزمية غير مرئية لفترة طويلة، إذ تمارس عبر قرارات آلية دقيقة (مثل التمييز الخفي في التوظيف أو القروض) يصعب على الضحية إدراكها فورا.

2.الطبيعة التكنولوجية المعقدة والغامضة

الجرائم الخوارزمية تعتمد على تقنيات متقدمة مثل التعلم الآلي والذكاء الاصطناعي، مما يجعلها صعبة الكشف بسبب قدرتها على التكيف مع أنظمة الأمن ، مثال: استخدام خوارزميات التعلم العميقلإنشاء محتوى مزيفبهدف التشهير أو الاحتيال المالي (الرزاق، 2024، صفحة 432). غالبًا ما توصف الخوارزميات بـ"الصندوق الأسود"، مما يجعل فهم منطقها الداخلي أو التحقق من أسباب النتيجة أمرا بالغ الصعوبة، وهذا يصعب الأمر من اثبات الركن المادي والمعنوي للجريمة.

3.العالمية والطابع غير المباشر

الجريمة المعلوماتية بصفة عامة وبما فيها الجريمة الخوارزمية من الجرائم العالمية العابرة للحدود الوطنية، إذ ترتكب في بلد معين عبر خوارزمية تعمل على خادم موجود في دولة أخرى، وضحايا ها قد تكون في أماكن مختلفة، ما يطرح إشكالية الاختصاص القانوني والقضائي(خليفي، 2016، صفحة 255)

كما أن الجريمة الخوارزمية لا تنشأ بفعل بشري مباشر كما هو الحال في الجرائم التقليدية، بل تنشأ نتيجة لعمل الخوارزمية بعد برمجتها أو تشغيلها، والمسؤولية هنا تصبح موزعة بين المبرمج، الشركة المالكة، أو المستخدم.

4.الإضرار بالحقوق المعنوية والفكرية أكثر من المادية المباشرة

مثل الحق في الخصوصية، حرية الرأي، الحق في المعلومة الصحيحة.

5.الاستقلالية وقابلية التطور الذاتي

تتسم الخوارزميات، ولاسيما في مجالي التعلم الآلي والتعلم العميق، بقدرتها على الاستقلالية وقابلية التطور الذاتي، إذ يمكن أن تولد أنماطا سلوكية جديدة لم تبرمج مسبقا، مما يصعب من إمكانية التنبؤ بمخرجاتها (زغلول ط.، الصفحات 43-44). وقد تمتد آثار هذه المخرجات لتشمل عددا واسعا من الأفراد في فترة زمنية قصيرة، خاصة عبر منصات التواصل الاجتماعي أو في النظم المالية والجنائية. كما أن قدرة الخوارزميات على التحسن المستمر بمرور الوقت يزيد من خطورة الجرائم المرتبطة بها ويجعل توقعها أكثر تعقيدًا(Biggio, 2017, p. 3)

1.2.2.الفرق بين الجريمة الخوارزمية والجريمة التقليدية ودوافع ارتكابها

أدى تطور الذكاء الاصطناعي واعتماد الخوارزميات في مجالات متعددة إلى بروز أنماط جديدة من السلوك الإجرامي تختلف في طبيعتها وآليات ارتكابها عن الجرائم التقليدية ، ومن هنا تبرز أهمية التمييز بين الجريمة الخوارزمية التي ترتكب باستخدام الأنظمة الذكية والخوارزميات الذاتية التعلم،والجريمة التقليدية التي تعتمد على الفعل البشري المباشر. ويسعى هذا العنصر إلى تحليل دوافع ارتكاب الجرائم الخوارزمية، سواء كانت بدوافع مالية أو سياسية أو بدافع التحكم في المعلومات، بما يعكس التحول في بنية الجريمة في ظل الثورة الرقمية.

أولا: الفرق بين الجريمة الخوارزمية والجريمة التقليدية

يتجلى الفرق بين هاتين الجريمتين من خلال:

1.من حيث الفاعل المجرم

عنصر الفاعل في الجرائم التقليدية أو المعلوماتية يسند مباشرة إلى الإنسان الذي يتخذ القرار ويستعمل الوسيلة، وتنقسم فئات مرتكبي الجرائم المعلوماتية إلى أربعة أصناف رئيسية: موظفو مراكز الحاسوب الذين يشكّلون الغالبية بحكم خبرتهم التقنية، والموظفون الساخطون الذين يستغلون معرفتهم بالأنظمة للإضرار بمؤسساتهم، والهواة أو "الهاكرز" الذين يمارسون الاختراق بدافع التسلية أو التحدي، وأخيرا أفراد الجريمة المنظمة الذين يوظفون التقنيات في أنشطة إجرامية واسعة لتحقيق مكاسب غير مشروعة (سياب، 2009، الصفحات 223-224)، بينما في الجريمة الخوارزمية يكون التنفيذ المباشر صادرا عن نظام ذكي (خوارزمية/روبوت) قادر على التعلم والتطور الذاتي، فتظهر أنماط سلوكية غير متوقعة، ويغدو تحديد من ينسب إليه الفعل وتجسيد المسؤولية الجنائية بين المبرمج أو المشغل أو المزود أكثر تعقيداً من النموذج التقليدي للمساءلة.

2.من حيث وسيلة ارتكاب الجريمة

تنفذ الجرائم التقليدية عادة عبر وسائل مادية واضحة، وهي تتسم بوجود ملموس يمكن الرجوع إليه لإثبات وقوع الجريمة و تحمل الفاعل المسؤولية ، في المقابل ترتكز الجرائم الخوارزمية على منظومات تقنية قائمة على برمجيات وخوارزميات ذكية تعمل بمعالجة ذاتية للبيانات، لتنفيذ أعمال مثل توليد محتوى مزيف أو شن هجمات إلكترونية ضد أنظمة معلوماتية، دون تدخل بشري لحظي أو مباشر ، هذه الطبيعة التقنيّة المعقدة والتشعبية للأدلة تجعل من الصعب إثبات مسؤولية الفاعل أو تتبع المصدر التقني للجريمة، مما يطرح تحديات قانونية جوهرية في مجال الشفافية والمساءلة".

3.من حيث الزمان والمكان

تقتصر الجرائم التقليدية على مكان وزمان معين ، مما يسهل نطاق التحقيقات وتحديد الاختصاص القضائي، وفي المقابل تمتد الجرائم الخوارزمية إلى ما وراء القيود الجغرافية والزمانية، إذ يمكن أن تنفذ عمليات إلكترونية متعددة ومتزامنة خلال ثوانٍ، عبر شبكات الإنترنت أو من خلال دول متعددة في آن واحد، دون وجود 'مساحة

جريمة'، وهذه الطبيعة العابرة للحدود تفوق قدرة القانون الجنائي التقليدي على تحديد مكان وقوع الجريمة وربطها بزمن محدد، مما يفرض تحديات كبيرة فيما يخص إثبات وقوع الفعل وتحديد نطاق اختصاص السلطات القضائية المختصة.

4.من حيث التسبب في الضرر

تختلف الجرائم التقليدية عن الجرائم الخوارزمية من الناحية النوعية والكيفية ، ففي الجرائم التقليدية، يكون الضرر عادة ماديا أو جسديا مباشرا، ويمكن إدراكه وقياسه واقعي ا. أما في الجرائم الخوارزمية، فإن الضرر غالبا ما يكون غير مادي، وقد لا يظهر أثره فور وقوعه، بل يكشف في فترات لاحقة، مما يجعل من الصعب حصره وتحديده بدقة، وبالتي يصعب وضع التكييف القانوني الملائم وتحديد الجزاء المناسب.

5. من حيث الاثبات

يصعب في كثير من الأحيان العثور على أثر مادي للجريمة الخوارزمية، والسبب في ذلك يعود إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان (الرزاق، الصفحات 431-432)، فهي تتطلب الاعتماد على مسارات إلكترونية متقدمة تشمل تتبع الكود البرمجي، وتفريغ وتحليل السجلات الرقمية، ووثائق الأنشطة التي ينفذها الذكاء الاصطناعي ، هذه الأدلة الرقمية غالبا ما تكون هشة أو قابلة للتلاعب، وتتطلب أدوات تقنية متقدمة وخبرات متخصصة لجمعها وتحليلها، وهو ما يشكّل تحدي ا قانونيا وإجرائيا حقيقيا في إثبات مثل هذه الجرائم، وهذا على عكس الجرائم التقليدية الأخرى التي يميل اثباتها في كثير من الأحيان الى السهولة.

ثانيا: دوافع ارتكاب الجريمة الخوارزمية

دوافع ارتكاب الجريمة الخوارزمية عديدة ومتنوعة، نذكر أهممها:

1.الدوافع الإجرامية، النفسية والاجتماعية

من بين أخطر دوافع ارتكاب الجريمة الخوارزمية ما يمكن تسميته بـ : الدوافع الإجرامية المحضة، حيث أن فعل المجرم يتمثل في السعي إلى ابتكار أنماط جديدة من الجريمة صعب اكتشافها عبر الوسائل التقليدية لمكافحة الجريمة المعلوماتية ، وفي هذا الإطار يلجأ الجناة إلى استغلال ثغرات أنظمة التعلم الآلي (MachineLearning Vulnerabilities)بهدف تضليل الخوارزميات أو توجيه سلوكها بشكل منحرف عن المسار المتوقع، مما يؤدي إلى نتائج إجرامية بالغة الخطورة قد تمس النظام العام والأمن القانوني للمجتمع(صغير، 2023). إن هذا النوع من الدوافع يُظهر أن الخطر الحقيقي لا يكمن فقط في الأبعاد الاقتصادية أو السياسية للجريمة الخوارزمية، بل أيضًا في الإبداع الإجرامي الذي يجعل من التكنولوجيا الحديثة بيئة خصبة لابتكار جرائم غير مسبوقة، وهو ما يفرض على المشرّع ضرورة تطوير قواعد خاصة للتجريم والعقاب تتلاءم مع الطبيعة المستحدثة لهذه الأفعال.

كما تعد الرغبة في الشهرة وإبراز التفوق التقني من بين الدوافع الدافعة على ارتكاب جرائم خوارزمية، حيث يرغب المبرمجون أو القائمون على الاختراق في إثبات مهاراتهم التقنية بمنصات يسهل اختراقها أو أنظمة الذكاء الاصطناعي، سعيا إلى الشهرة والاعتراف ضمن المجتمع التقني. وفي بعض الحالات الأخرى يسيطر عليهم دافع الانتقام، إذ يستغلون خوارزميات معينة لاستهداف أشخاص أو مؤسسات بعينها، على نحو يمكنهم من توجيه ضرر مدروس ضدهم، مستغلين الطبيعة الحديثة لهذه الأنظمة لتعويض نقاط الضعف القانونية التقليدية.

2.التحدي الذهني

تتسم الأجهزة التابعة للنظام المعلوماتي وكذلك الأنظمة الأمنية بالتعقيد وصعوبة اختراقها، وتحاط بهالة من القدرات التي تبين صعوبة أو استحالة التجسس عليها، وهذه الأمور تكون بمثابة استفزاز لمهارات وإمكانيات بعض الأشخاص المصابين بخلل في التفكير، وتثير فيهم رغبة التحدي، حينئذ بفهم خاطئ منه يسلك طريق الإجرام فيرتكب الجريمة

3.الدوافع الماليةوالربح السريع

من أبرز العوامل المؤدية إلى ارتكاب الجرائم الخوارزميةالدوافع المالية والربح السريع، حيث يسعى الجناة إلى تحقيق أرباح غير مشروعة وسريعةمن خلال التلاعب بالأسواق المالية عبر خوارزميات التداول الآلي، التي تمكّنهم من استغلال الفوارق الزمنية الدقيقة في حركة الأسعار بما يحقق مكاسب آنية يصعب كشفها بالوسائل

التقليدية. كما يستغل المجرمون تقنيات الذكاء الاصطناعي في ابتكار صور جديدة من الاحتيال، مثل إنشاء هويات رقمية مزيفة أو استخدام تقنيات التزييف العميق (Deepfake)(الشاوي، 2024، صفحة 81)لتزوير المستندات والصوت والصورة في المعاملات البنكية، وهو ما يشكّل خطراً جسيماً على نزاهة الأنظمة المالية ويزيد من صعوبة الإثبات الجنائي في ظل البيئة الرقمية المعقدة.

4.الدوافع الاستخباراتية والاستراتيجية

من أخطر الدوافع الكامنة وراء ارتكاب الجريمة الخوارزمية، إذ تستغل الجهات الفاعلة الخوارزميات وإمكانات الذكاء الاصطناعي لشن عمليات تجسس إلكتروني واسعة النطاق وجمع معلومات حساسة، الأمر الذي يذلك يؤثر مباشرة على الأمن القومي ويقوّض مبدأ السيادة المعلوماتية. كما تُستخدم الخوارزميات كأداة رئيسية في الحروب السيبرانية(Cyber Warfare)، وذلك من خلال مهاجمة البنى التحتية الحيوية، وتعطيل شبكات الاتصالات، وتنفيذ هجمات رقمية منسقة تحدث أضرارا بالغة للأنظمة الحكومية والاقتصادية، ما يؤدي إلى اضطرابات اجتماعية وسياسية كبيرة(بوخاري و شاوش، 2023، الصفحات 41-42).

5.الدوافع السياسية والأيديولوجية

تعتبرالدوافع السياسية والأيديولوجية أداة فعّالة لارتكاب الجرائم الخوارزمية، حيث يوظّف الفاعلون وسائل الذكاء الاصطناعي والخوارزميات للتلاعب بالرأي العام عبر ضخ محتوى سياسي مضلل أو توجيهالمحتوى السياسي لصالح أيديولوجيات معينة ، على سبيل المثال، تسهم المنصات الاجتماعية التي تعتمد على خوارزميات التوصية في تعزيز ما يعرف بـ "فقاعات التصفية (filterbubbles) "و"الغرف الصدى " (echochambers)، ما يؤدي إلى ربط الأفراد بأفكار متطرفة أو دون وجهة نظر متنوعة، في حين يسهل نشرأخبار مزيفة أو دعاية متحيّزة بفعالية عبر الخوارزميات بهدف خدمة أجندات سياسية محددة أو جماعات متطرفة(Pariser, 2011, p. 9) .

إن اختلاف الدوافع المؤدية إلى ارتكاب الجرائم الخوارزمية لا يغير من عدم مشروعيتها، غير أنه يلعب دورا مهما في توجيه التكييف القانوني لهذه الجرائم وفي تقدير العقوبة المستحقة عنها، إذ قد يؤدي إلى التشديد في حالة الدوافع السياسية أو الإرهابية التي تمس بالأمن القومي، أو يعتبر ظرفا كاشف ا لطبيعة الجريمة في باقي الحالات.بالغ الصعوبة، يتطلّب خبرة تقنية متخصصة وأدوات تحليل متقدمة، وهي إمكانات لا تتوافر عادة لدى الأفراد المتضررين من مخرجات هذه الأنظمة.

2. المحورالثاني : مظاهر الجرائم الخوارزمية على الفيس-بوك وقيام المسؤولية الجزائية في ظل الذكاء الاصطناعي

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى إعادة تشكيل البيئة الرقمية، بحيث لم يعد الفضاء الافتراضي مجرد وسيلة للتواصل الاجتماعي أو تبادل المعلومات، بل تحول إلى مجال تتخلله أنماط إجرامية مستحدثة تستند إلى الخوارزميات كأساس في التنفيذ والتأثير. وتعد منصة فيسبوك نموذجا بارزا لهذا التحول، إذ أظهرت التجارب الحديثة أن الاعتماد على الخوارزميات في إدارة البيانات والمحتويات قد أفرز مظاهر خطيرة للجريمة تمس الأفراد والمجتمعات على حد سواء. وفي ظل هذه التحولات، برزت الحاجة إلى مناقشة مدى قدرة القواعد الجنائية التقليدية على استيعاب هذه الأفعال وتحديد المسؤولية الجزائية عنها، الأمر الذي يستدعي تناول المظاهر العملية لهذه الجرائم من جهة، وإشكالية قيام المسؤولية الجزائية في ظل الذكاء الاصطناعي من جهة ثانية.

2.1. مظاهر الجرائم الخوارزمية في فضاء الفيس-بوك

تعد منصة فيس -بوك من أبرز البيئات الرقمية التي تحتضن مظاهر الجرائم الخوارزمية، بحكم اعتمادها الواسع على الخوارزميات في إدارة المحتوى، وتوجيه الإعلانات، ومعالجة البيانات ، وقد أدى هذا الاعتماد إلى بروز أنماط إجرامية جديدة تتجاوز الأطر التقليدية للجرائم المعلوماتية، من قبيل خرق الأمان،

والتلاعب بالمحتوى المرئي، فضلًا عن استغلال البيانات في تغذية الصراعات السياسية والاجتماعية. وبالنظر إلى خطورة هذه المظاهر يمكن التوقف عند أربع صور لهذه الجرائم ضمن العنصرين التاليين:

2.1.1.جريمتي خرق الأمان وإفشاء البيانات والتلاعب عبر الفيديوهات المزيفة

يُعتبر خرق الأمان وإفشاء البيانات من أبرز الجرائم الخوارزمية التي تهدد مستخدمي فيس -بوك، إذ تستغل الخوارزميات في الوصول غير المشروع إلى المعطيات الشخصية والتصرف فيها بطرق غير مشروعة. كما برز إلى جانب ذلك التلاعب عبر الفيديوهات المزيفة (Deepfakes)الذي يوظف تقنيات الذكاء الاصطناعي لتوليد محتوى مرئي مضلل يصعب كشفه، بما يحمله من مخاطر على الخصوصية والأمن المعلوماتي وسلامة النقاش العام.

أولا: جرائم خرق الأمان وإفشاء البيانات

تعد جرائم خرقات الأمان وإفشاء البيانات من أخطر الجرائم الخوارزمية التي شهدتها منصة فيس -بوك، حيث كشفت واقعة عام 2018 عن هشاشة البنية الأمنية للمنصة، بعد اكتشاف خلل في خاصية "View As"التي تمكن المستخدم من معاينة حسابه كما يظهر للآخرين ، هذا الخلل البرمجي استغل من قِبل جهات مجهولة للوصول غير المشروع إلى بيانات شخصية تخص ما يقارب 29 مليون حساب، شملت معلومات حساسة مثل الموقع الجغرافي، تاريخ الميلاد، البريد الإلكتروني، وأماكن العمل، وهو ما يشكل انتهاكا صارخا لحق الأفراد في الخصوصية الرقمية ، ولم يتوقف الأمر عند حدود الضرر الفردي، بل ترتب عنه مساءلة قانونية واسعة لشركة "ميتا"، إذ فرض الاتحاد الأوروبي عليها غرامة مالية قدرت بـ 251 مليون يورو، استنادا إلى أحكام اللائحة العامة لحماية البيانات الأوروبية (GDPR)التي تلزم مزودي الخدمات الرقمية باتخاذ التدابير التقنية والتنظيمية اللازمة لضمان أمن البيانات ، هذه الواقعة تعكس كيف يمكن لخلل خوارزمي بسيط أن يتحول إلى جريمة كبرى تمس الملايين، وتؤكد على ضرورة تشديد الرقابة القانونية على شركات التكنولوجيا العملاقة لضمان التوازن بين الابتكار التكنولوجي وحماية الحقوق الأساسية للمستخدمين(رويترز، 2024)

ثانيا:جرائم التلاعب عبر الفيديوهات المزيفة(Deepfakes)

إن تقنية "التزييف العميق" من أخطر تطبيقات الذكاء الاصطناعي التي توظَّف عبر منصات مثل فيس -بوك، حيث تنشئ الخوارزميات مقاطع مرئية مزيفة يصعب تمييزها عن الحقيقة، وتستخدم للتشهير أو نشر التضليل، وهي في وتيرة متسارعة تحوى التطور(شحاته، 2023، صفحة 174)، ومن أبرز الأمثلة:

1.فيديومزيف للرئيس الفرنسي ماكرون في نوادي الثمانينات

في عام 2024، كشف فريق التحقق من رويترز أن فيديو يظهر الرئيس "إيمانويل ماكرون" وهو يرقص في نادٍ وهو في الحقيقة خدعة: تم تركيب وجهه اصطناعيا على لقطات قديمة لراقصين في كاليفورنيا (Reuters, 2024).

2.إعلانات مزيفة لفيديوهات رئيس الوزراء البريطاني ريشي سوناك

بحسب تقارير، ظهرت أكثر من 100 إعلان مزيف على فيس-بوك تقنع الجمهور بأن رئيس الوزراء البريطاني يتحدث عن قضايا وهمية في مشاريع؛ الإعلان استهدفت ما يصل إلى 400,000 شخص، ما أطلق تحذيرات بوجود خطر انتخابي حقيقي بسبب تقنيات الذكاء الاصطناعي(Guardian, 2024).

3. فيديو الرئيس الأميركي جو بايدن

في نوفمبر 2020، جرى تداول نسخة معدلة من فيديو للرئيس الأميركي "جو بايدن" وهو يضع ملصق "I Voted"على طفلته خلال الانتخابات النصفية، حيث عدّل ليظهر سلوكه بشكل مريب، مما أثار نقاش واسعا حول سياسة فيس-بوك في التعامل مع الفيديوهات المزيفة(Wired, 2020)

2.1.2.جريمتي تضخيم خطاب الكراهية ضد الأقليات واستغلال البيانات السياسية

تشكل الخوارزميات في فيس -بوك أداة قوية لتضخيم خطاب الكراهية ضد الأقليات، حيث تسهم آليات التوصية في نشر المحتويات العنيفة والتحريضية على نطاق واسع، مما يعمّق الانقسامات الاجتماعية ويهدد السلم الأهلي ، وإلى جانب ذلكأفرزت الممارسات المرتبطة باستغلال البيانات السياسية خطورة مضاعفة، إذ يتم توظيف

المعطيات الشخصية للمستخدمين في حملات انتخابية موجّهة تهدف إلى التأثير في قناعاتهم واختياراتهم السياسية، بما يطرح تحديات جدّية أمام حماية الحقوق والحريات الديمقراطية.

أولا: تضخيم خطاب الكراهية ضد الأقليات

تعد مسؤولية فيس -بوك عن تضخيم خطاب الكراهية والتحريض ضد الأقليات من أبرز مظاهر الجرائم الخوارزمية، إذ كشفت تقارير أممية أن خوارزميات المنصة أسهمت في تسريع وتوسيع نطاق نشر المحتوى العدائي ضد أقلية "الروهينغا" المسلمة في ميانمار، وذلك عبر آلية التوصيات التي تعتمدها فيس -بوك في ترتيب وعرض المنشورات، هذا السلوك لم يكن مجرد تقصير في المراقبة، بل تدخلا خوارزميا فاعلا مكّن خطاب الكراهية من الوصول إلى جمهور أوسع، بما أفضى إلى نتائج خطيرة تمثلت في التحريض المباشر على العنف والتمييز، وارتكاب انتهاكات جسيمة لحقوق الإنسان ، وقد ترتب عن ذلك رفع دعاوى جماعية ضد شركة "ميتا" أمام القضاء في عدة دول، بدعوى تواطؤها في تسهيل نشر هذا الخطاب وعدم اتخاذ التدابير اللازمة للحد من مخاطره، الأمر الذي يثير مسؤوليتها المدنية والجنائية على حد سواء، استنادا إلى مبادئ القانون الدولي لحقوق الإنسان والقواعد الوطنية المنظمة لمكافحة خطاب الكراهية والتحريض على العنف.

وللإشارة فإن فيس -بوك زعم لاحقا اتخاذه إجراءات للحد من هذه الانتهاكات، إلا أن المنصة بقيت أداة أساسية استخدمت لنشر الشائعات والدعاية المحرضة، وهو ما ساعد بشكل كبير على تأجيج التوترات الاجتماعية وارتكاب أعمال عنف واسعة النطاق ضد هذه الأقلية(UNHRC, 2018).

ثانيا: استغلال البيانات السياسية -فضيحة كامبريدج أناليتيكا-

تقصد بـجريمة استغلال البيانات السياسية تلك الأفعال غير المشروعة التي تقوم على جمع أو معالجة أو استخدام البيانات الشخصية للمواطنين لأغراض سياسية دون رضاهم الواعي ، أو بمخالفة القوانين المنظمة لحماية الخصوصية، وتتمثل خطورتها في أن البيانات، ولا سيما المرتبطة بالاتجاهات الفكرية والميول الحزبية والسلوك الانتخابي، يمكن أن تستعمل للتأثير على الخيارات الديمقراطية للأفراد عبر استهدافهم برسائل موجهة، أو تضليلهم من خلال محتوى مخصص يبنى على خوارزميات دقيقة.

وتبرز هذه الجريمة باعتبارها شكلا جديد ا من الجرائم الخوارزمية أو الجرائم المعلوماتية ذات البعد السياسي، إذ تستغل التطور التقني في الذكاء الاصطناعي وتحليل البيانات الضخمة (Big Data)من أجل التأثير على الإرادة الشعبية، مما يمسّ مباشرة مبادئ الشفافية، والعدالة الانتخابية، وحرية الاختيار التي يقوم عليها النظام الديمقراطي. ومن أبرز استغلال البيانات السياسية -فضيحة كامبريدج أناليتيكا-

1.خلفية الفضيحة

برزت فضيحة "كامبريدج أناليتيكا**(Cambridge Analytica)** "سنة 2018 باعتبارها إحدى أبرز القضايا التي كشفت عن مخاطر الاستغلال غير المشروع للبيانات السياسية ،فقد تمكّنت الشركة، عبر تطبيق بحثي مرتبط بفيس-بوك، من جمع بيانات شخصية لأكثر من خمسين مليون مستخدم دون الحصول على موافقة صريحة منهم، وهو ما يشكل انتهاكا واضحا لمبدأ الرضا المستنير الذي تعدّه تشريعات حماية البيانات شرطا أساسيا لمعالجة المعلومات الشخصية (Al Jazeera, 2018).- .

2.الأسلوب المتبع في الاستغلال

اعتمدت الشركة على ما يعرف بتقنية الاستهداف النفسي **(PsychographicProfiling)**، حيث جمعت بيانات دقيقة عن اهتمامات المستخدمين وسلوكهم على الإنترنت، بما في ذلك الإعجابات والتفضيلات، لتبنى عليها نماذج تحليلية تهدف إلى التأثير في الخيارات السياسية ، وبذلك تحوّل استخدام الخوارزميات من أداة تسويقية مشروعة إلى وسيلة للتأثير غير المشروع على الإرادة الانتخابية للناخبين(Guardian, 2018).

3. الخلفية القانونية للفضيحة

من منظور قانوني، مثّلت هذه الفضيحة انتهاكا للحق في حماية البيانات الشخصية والحق في الخصوصية، كما تمثل خرقا لالتزامات المنصات الرقمية مثل فيس -بوك تجاه مستخدميها ، ففي إطار اللائحة الأوروبية لحماية البيانات العامة GDPR، يعتبر أي جمع أو معالجة للبيانات دون أساس قانوني أو موافقة صريحة من المعنيين،

عملاغير مشروع يعرّض الفاعل للمساءلة ، وبذلك فإن تصرّف "كامبريدج أناليتيكا" يدخل في نطاق المعالجة غير المشروعة للبيانات ذات الطبيعة السياسية، وهو ما يكتسي خطورة إضافية باعتباره يمس بحقوق أساسية كحرية الرأي والتعبير والحق في المشاركة السياسيةِ.(DW, 2018)

4.النتائج المترتبة

لقدأثارت الفضيحة ردود فعل واسعة، حيث فرضت السلطات البريطانية والأمريكية غرامات على فيس -بوك بلغت ملايين الدولارات، كما اضطرت الشركة الأم إلى إعلان إفلاس "كامبريدج أناليتيكا"، وعلى صعيد آخر قادت هذه الواقعة إلى إطلاق حملات جماهيرية مثل DeleteFacebook، وأعادت النقاش حول ضرورة وضع إطار قانوني صارم يوازن بين حرية الابتكار التكنولوجي وحماية الحقوق الأساسية للمستخدمين(Vox, 2018) تعد هذه الفضيحة كمثال صارخ على جريمة استغلال البيانات السياسية، حيث تم استغلال الثغرات القانونية والتقنية للتأثير في الديمقراطية من خلال التلاعب غير المشروع بالناخبين، وهي تكشف في الوقت ذاته عن قصور المنظومات القانونية التقليدية في مواجهة الجرائم الخوارزمية الحديثة، مما يفرض تطوير تشريعات أكثر صرامة لضمان نزاهة العملية الديمقراطية وحماية المعطيات ذات الطابع السياسي.

2.2.قيام المسؤولية الجزائية للجرائم الخوارزمية على منصة فيس-بوك في ظل الذكاء الاصطناعي

تثير الجرائم الخوارزمية المرتكبة عبر فيس -بوك إشكاليات قانونية عميقة، لاسيما فيما يتعلق بإسناد المسؤولية الجزائية، فإذا كان الركن المادي للجريمة يتحقق من خلال الأفعال التي تنتجها الخوارزميات أو تستغل عبرها، فإن إثبات الركن المعنوي وتحديد الفاعل الحقيقي يظلان من أعقد المسائل ، ومن ثمّ فإن قيام هذه المسؤولية يقتضي الوقوف أولا على الأركان المكونة لها، ثم بيان إشكالات تحديد المسؤول عنها عمليا.

2.2.1.أركان المسؤولية الجزائية في الجرائم الخوارزمية

تعد أركان المسؤولية الجزائية الأساس الذي يقوم عليه إسناد الجريمة إلى فاعلها، فهي التي تمكّن من التمييز بين الفعل المشروع وغير المشروع. وفي سياق الجرائم الخوارزمية على فيس -بوك، يكتسي هذا الموضوع خصوصية بالغة، نظرا لتعقيد الطبيعة التقنية للخوارزميات وصعوبة ضبط علاقتها بالركن الشرعي والمادي والمعنوي، ومن ثمّ فإن الوقوف على هذه الأركان يعد خطوة ضرورية لفهم كيفية قيام المسؤولية الجزائية في هذا المجال المستحدث.

أولا: الركن الشرعي

يقصد بالركن الشرعي مبدأ "لا جريمة ولا عقوبة ولا تدابير أمر بغير قانون " (الأمر، 1966)"، أي ضرورة وجود نص قانوني يجرم الفعل ويحدد له عقوبة مقررة سلف ا، ويكتسي هذا الركن أهمية خاصة في الجرائم الخوارزمية، إذ تُعد ظاهرة حديثة نسبياولم تحظبعد بتنظيم قانوني تفصيلي في معظم التشريعات.

وبالنسبة لما يتعلق بمنصة فيس -بوك، فإن خرق الأمان وإفشاء البيانات أو التلاعب بالمحتوى عبر الفيديوهات المزيفة، وكذلك استغلال البيانات السياسية أو تضخيم خطاب الكراهية، كلها أفعال قد لا تذكر صراحة في القوانين العقابية، وإنما يمكن إسنادها إلى نصوص عامة كجرائم انتهاك الخصوصية، أو نشر الأخبار الكاذبة، أو التحريض على التمييز والكراهية.

إن هذا الوضع يثير إشكالية مدى كفاية النصوص التقليدية لمواجهة خطورة الجرائم الخوارزمية، إذ إن غياب تنظيم صريح قد يفتح المجال لإفلات مرتكبيها من العقاب، أو يضع القضاء أمام صعوبات في التكييف. وهو ما يفرض ضرورة تطوير نصوص قانونية حديثة تراعي خصوصية الذكاءالاصطناعي والخوارزميات، بما يحقق الأمن القانوني ويضمن احترام مبدأ الشرعية الجنائية.

ثانيا: الركن المادي

يصد بالركن المادي النشاط الخارجي المجرَّم قانون ا، إذ لا يعاقب على مجرد النوايا أو الميول الداخلية ما لم تتجسد في سلوك ملموس. ويعد هذا الركن إحدى الدعائم الأساسية التي تقوم عليها الجريمة ومن ثَمّ المسؤولية الجزائية المترتبة عنها(بامو، 2011/2010، صفحة 46) ، وإذا ما طُبِّق هذا المفهوم على الجرائم الخوارزمية

في فيس-بوك، أمكن القول إن السلوك الإجرامي قد يتحقق من خلال أفعال إيجابية غير مشروعة، مثل استغلال الخوارزميات في اختراق خصوصية المستخدمين أو نشر فيديوهات مزيفة مضللة، كما قد يتحقق عن طريق الامتناع، كإحجام المنصة عن التدخل لوقف خطاب الكراهية أو منع استغلال البيانات السياسية رغم علمها بخطورته، ويتحدد الركن المادي للجريمة ضمن عناصر ثلاث هي:

1.السلوك الاجرامي

يقصد بالسلوك الجرمي ذلك الفعل أو الامتناع الذي يجرّمه القانون ويُشكّل الركن المادي للجريمة. وفي إطار الجرائم الخوارزمية، يكتسي هذا السلوك خصوصية مرتبطة بآليات الذكاء الاصطناعي وقدرته على إنتاج أفعال تتجاوز التدخل البشري المباشر. فقد يتجسد السلوك الإجرامي في صورة أفعال إيجابية، مثل اختراق أنظمة الحماية عبر خوارزميات متطورة، أو نشر فيديوهات مزيفة (Deepfakes)تضلل الرأي العام على منصات التواصل. كما قد يظهر في شكل أفعال سلبية أو امتناعا، مثل تجاهل المنصة التزاماتها في مراقبة المحتوى المحرض على العنف أو في حماية بيانات المستخدمين من الاستغلال السياسي.

إن خطورة السلوك الجرمي في الجرائم الخوارزمية تكمن في أنه غالبًا ما يتم بصورة غير مرئية وسريعة تتجاوز قدرة الأفراد العاديين وحتى السلطات على رصده، مما يجعل إثباته وإسناده إلى فاعل محدد من أعقد الإشكالات القانونية المعاصرة.

2.النتيجة

النتيجة في الركن المادي للجريمة هي عبارة عن الأثر غير المشروع الذي يترتب على السلوك الإجرامي ويضر بالقيم أو المصالح التي يحميها القانون. وفي الجرائم الخوارزمية على فيسبوك، قد تتخذ هذه النتيجة صورا متعددة، مثل المساس بحق الأفراد في الخصوصية نتيجة تسريب بياناتهم، أو الإضرار بسمعة الأشخاص من خلال نشر فيديوهات مزيفة، أو تهديد السلم الاجتماعي عبر تضخيم خطاب الكراهية والتحريض على العنف، فضلًا عن التأثير غير المشروع في إرادة الناخبين عن طريق استغلال بياناتهم السياسية.

وتزداد خطورة النتيجة في هذا السياق بسبب اتساع نطاقها وسرعة انتشارها، إذ يمكن أن تطال ملايين المستخدمين في وقت وجيز، ومن ثمّ، فإن تحديد ها بدقة يعد شرطًا أساسيا لقيام المسؤولية الجزائية عن الجرائم الخوارزمية.

3.العلاقة السببية

العلاقة السببية حلقة الوصل بين السلوك الإجرامي والنتيجة غير المشروعة، إذ لا يكفي لقيام الجريمة مجرد تحقق السلوك، بل يجب أن يُثبت أن هذا السلوك هو الذي أدى إلى وقوع النتيجة المعاقب عليها قانونًا. وفي مجال الجرائم الخوارزمية على فيس -بوك، تبرز إشكالية معقدة في تحديد هذه العلاقة، نظرا للطابع التقني للخوارزميات واعتمادها على آليات التعلم الذاتي التي قد تُنتج نتائج غير متوقعة حتى بالنسبة لمبرمجيها.

فقد يستغل مثلا خرق أمني في خوارزمية المنصة لجمع بيانات المستخدمين، فتترتب عنه نتيجة متمثلة في إفشاء تلك البيانات على نطاق واسع؛ أو تُستخدم خوارزميات التوصية في نشر محتويات تحريضية، فينشأ عنها تضخيم خطاب الكراهية أو التحريض على العنف. في هذه الحالات يُعد إثبات السببية أمرًا ضروريًا لإسناد الجريمة إلى الفاعل البشري أو المعنوي، سواء كان المبرمج، أو المستخدم، أو الشركة المالكة.

غير أن التعقيد التقني للخوارزميات يطرح تحديًا كبيرًا أمام القضاء، يتمثل في صعوبة إثبات أن النتيجة كانت نتاجًا مباشرًا للسلوك الإجرامي وليس مجرد أثر عرضي لعمل النظام الذكي. ولهذا برزت الحاجة إلى تطوير مقاربات قانونية حديثة تأخذ بعين الاعتبار خصوصية العلاقة السببية في الجرائم الخوارزمية.

ثالثا: الركن المعنوي

يعد الركن المعنوي أساسا لا غنى عنه لقيام المسؤولية الجزائية، فهو الذي يكشف عن الإرادة الإجرامية الكامنة وراء السلوك (الوهاب و لبيض، صفحة 690). وبخلاف الجرائم التقليدية التي تتجسد فيها نية الفاعل بشكل

مباشر، فإن الجرائم الخوارزمية تثير إشكالات خاصة، نظرًا لاعتمادها على أنظمة الذكاء الاصطناعي التي تعمل بشكل شبه مستقل عن تدخل بشري مباشر. فقد تتخذ

1.صورة القصد الجنائي

عندما يقوم المستخدم أو المبرمج بتوظيف خوارزميات فيس -بوك عمدًا لتحقيق نتيجة غير مشروعة، كالتلاعب بالبيانات السياسية أو نشر فيديوهات مزيفة للإضرار بسمعة شخص معين. كما يمكن أن تأخذ شكل

2.الخطأ غير العمدي

إذا تم تشغيل أو برمجة الخوارزميات بإهمال أو تقصير، مما أدى إلى تسريب بيانات المستخدمين أو تضخيم محتوى يحض على الكراهية.

وبذلك، فإن الركن المعنوي في هذه الجرائم يتراوح بين القصد المباشر والقصد الاحتمالي والخطأ غير العمدي، وفقًا لطبيعة السلوك ودرجة سيطرة الفاعل البشري على النظام الخوارزمي، الأمر الذي يفرض على القضاء تحديات خاصة في التكييف وإثبات النية أو الإهمال في بيئة تقنية معقدة.

2.2.2.إشكالات تحديد المسؤول الجزائي عن الجرائم الخوارزمية وعقوبته

يثير تحديد المسؤولية الجنائية عن الجرائم الخوارزمية إشكالات متعددة نظرًا لتوزع الأدوار بين عدة أطراف، إضافة إلى الطبيعة الذاتية للتقنيات المستعملة. ويمكن إبراز أهمها فيما يلي:

أولا: مسؤولية المبرمج

يتحمل المبرمج قسطًا من المسؤولية متى ثبت أنه صمّم الخوارزمية على نحو يسمح بسلوك ضار، أو أغفل وضع الضمانات اللازمة للحد من مخاطرها. ويُنظر إلى المبرمج هنا باعتباره الفاعل الأصلي أو المساهم في الجريمة، تبعا لمدى قصده أو تقصيره(Allen & Widdison, 1996, p. 9).

ثانيا: مسؤولية المستخدم

يعتبر المستخدم الطرف الأكثر ارتباطا بتقنيات الذكاء الاصطناعي، بحكم العلاقة المباشرة التي تجمعه بها، والتي تمكّنه من التحكم في توجيهها واستغلال خصائصها ومزاياها.

والمستخدم: في الأصل هو: "من يستعمل الخوارزمية أو النظام في نشاط عملي (فرد، موظف، جهة تستفيد من الخدمة مباشرة". مثلًا: صحفي يستخدم أداة توليد محتوى بالذكاء الاصطناعي.

ويعد المستخدم مسؤولا إذا استعمل الخوارزمية عمدا في أعمال إجرامية، كالتلاعب بالبيانات أو نشر محتويات مضللة. فالمستخدم هو صاحب القرار المباشر في توجيه الأداة نحو غرض غير مشروع،مما يؤديإلى صدور سلوك مُجرم ومعاقب عليه قانونا. ويُمكن أن يتخذ سلوك المستخدم المجرم صورتين أساسيتين:

الصورة الأولى:قد تنشأ الجريمة عن فعل صادر حصريا من المستخدم، بحيث يكون وجود الفعل الجرمي متوقفا على سلوكه وحده، وهنا يتحمل المسؤولية الجنائية الكاملة وتوقع عليه العقوبة منفردا.

الصورة الثانية:أن تقع الجريمة نتيجة سلوك مشترك بين المالك الحقيقي أي المزود للخدمة أو المستخدم وبين طرف خارجي آخر، وفي هذه الحالة تُصبح المسؤولية جنائية مشتركة، وتتوزع العقوبة تبعًا لدور كل مساهم في الفعل(مريم، و لبيض، صفحة 690).

ثالثا: مسؤولية الشركة المالكة أو المزودة للخدمة

المالك هو: "من يملك الحق القانوني على النظام أو الخوارزمية (شخص طبيعي أو شركة)، سواء استعملها بنفسه أو فوّض غيره لاستعمالها. مثلًا: شركة إعلامية تملك الترخيص أو المنصة، لكنها تعطي صلاحيات لموظفيها لاستخدامها.

والشركة باعتبارها شخصا معنويا يتمتع بالشخصية القانونية، يمكن مساءلة الشركة التي تملك أو توفر الخوارزمية متى ثبت أنها سيطرت على التقنية واستفادت منها، مع علمها أو تقصيرها في مراقبة أنشطتها. ويطرح ذلك في إطار المسؤولية الجنائية للأشخاص المعنويين . وكما أشرنا سابقا فقد تنشأ بين المالك الحقيقي أي المزود للخدمة أو المستخدم وبين طرف خارجي آخر، وفي هذه الحالة تُصبح المسؤولية جنائية مشتركة، وتتوزع العقوبة تبعًا لدور كل مساهم في الفعل. وقد يكون السلوك الاجرامي منفردا ناتجا عن الشركة المالكة

بدون تدخل المستخدم أو طرف اخر وهنا تتحمل المسؤولية الجزائية للوحدها وفي نفس الوقت توقع عليها العقوبة منفردة.

وللإشارة فقد يجتمع الوصفان في شخص واحد إذا كان من يملك النظام هو ذاته من يقوم باستعماله " المالك والمستخدم"، بينما قد ينفصلان في حال ملكية شركة للتقنية وتمكين موظفيها أو عملائها من استعمالها. وتترتب على هذا التمييز آثار مهمة على مستوى المسؤولية الجنائية، حيث يُسأل المالك عن التقصير في الرقابة أو الإشراف، بينما يُسأل المستخدم عن الأفعال غير المشروعة التي باشرها مباشرة باستخدام الأداة.

رابعا: مسؤولية "مستقلة" للخوارزمية أو الروبوت

يشكل هذا الطرح إشكالًا فقهيا وقانونيا، فهناك من ينادي بإمكانية الاعتراف بالخوارزمية ككيان مسؤول جنائيًا، نظرًا لقدرتها على التعلم واتخاذ قرارات مستقلة، بينما يرى الاتجاه الغالب أن ذلك غير ممكن لغياب الإرادة والتمييز بالمعنى القانوني. وبالتالي يبقى هذا المجال محل جدل لم يُحسم بعد تشريعيا (Parliament, 2017) .

إن تعدد الفاعلين المحتملين يجعل من الصعب إسناد المسؤولية الجنائية في الجرائم الخوارزمية على نحو قاطع، وهو ما يفرض على التشريعات إيجاد حلول مرنة تجمع بين تحميل الأفراد مسؤولياتهم الخاصة، وضبط مسؤولية الأشخاص المعنويين، دون الانسياق وراء فكرة الاعتراف بالشخصية الجنائية للخوارزمية ذاتها.

الخاتمة:

وفي خاتمة بحثنا هذا يتبيّن لنا أن الجرائم الخوارزمية على منصات التواصل الاجتماعي، ولا سيّما على منصة فيس-بوك، تمثل تحديا قانونيا معقدا وغير مسبوق، نتيجة لتغلغل تقنيات الذكاء الاصطناعي في البنية التشغيلية لهذه المنصات. فلم تعد الجريمة نتاج إرادة بشرية خالصة، بل أصبح للخوارزميات دور فعّال ومباشر في توليد أفعال قد تترتب عنها أضرار اجتماعية أو سياسية أو اقتصادية واسعة النطاق .

وبناءً على ما سبق، يمكن اقتراح جملة من التوصيات، أهمها:

1. قصور التشريعاتفي ملاحقة الجريمة الخوارزمية، باعتبار أن أغلب القوانين صيغت في إطار الجرائم التقليدية أو المعلوماتية ولم تستوعب خصوصية الذكاء الاصطناعي.
2. تداخل أركان الجريمة الخوارزمية بين الركن المادي والمعنوي والشرعي، مع بروز صعوبة في تحديد المسؤولية بدقة بين المستخدم، المطور، والمنصة.
3. اتساع نطاق الضرر للجرائم الخوارزمية، بسبب قدرتها على تجاوز الحدود المكانية والزمانية، فضلًا عن سرعة الانتشار وتأثيرها العابر للدول.
4. غياب آليات رقابية فعّالة داخل المنصات، مما يسمح باستمرار الممارسات الضارة مثل نشر الأخبار الزائفة أو التلاعب السياسي عبر البيانات.

وبناء على ما سلف ذكره فإننا نقترح ما يلي:

1 - ضرورةإدراج نصوص على المستوى الدولي والداخلي خاصة بالجرائم الخوارزمية، بما يضمن تحديد المسؤولية الجنائية بدقة.

2 - على المنصات الرقمية الكبرى، وعلى رأسها فيسبوك، القيام بتعزيز الشفافية في آليات عمل خوارزمياتها، وتمكين الهيئات الرقابية من التدقيق فيها.

3 - إنشاء هيئات دولية متخصصة لمراقبة الجرائم الخوارزمية العابرة للحدود، بما يضمن التعاون القضائي الدولي في ملاحقتها.

4 - تخصيص قضاة مؤهلين ومتخصصين للنظر في قضايا الجرائم الإلكترونية والخوارزمية، بما يعزّز دقّة الأحكام وجودة العدالة

5 - اعتماد أنظمة فعّالة لحماية المعلومات، مع مراجعتها وتحديثها بشكل دوري لضمان مواكبتها للتطور التقني المتسارع.

6 - تشجيع الأبحاث الأكاديمية متعددة التخصصات (قانونية، تقنية، اجتماعية) لفهم طبيعة هذه الجرائم وصياغة حلول عملية لها.

7 - . تطوير وعي المستخدمين من خلال برامج توعية رقمية تبرز مخاطر الذكاء الاصطناعي وتحد من الاستعمال السلبي للخوارزميات.

8 - تكثيف الجهود التوعوية الموجّهة للمواطنين، ولا سيّما فئة الشباب، حول مخاطر استخدام المواقع المشبوهة، وذلك عبر تفعيل دور مؤسسات المجتمع المدني والهيئات التربوية والإعلامية في نشر الثقافة الرقمية السليمة، والحدّ من السلوكيات والممارسات غير الأخلاقية عبر الإنترنت.

قائمة المراجع:

أولا– المرجع باللغة العربية

1 -الدوريات والملتقيات

-أسامة شحاتة سالي(2023) الذكاء الاصطناعي والتقنيات والأدوات الرقمية المتخصصة في الكشف عن الأخبار الزائفة مجلة الدراسات الإعلانية والاتصالية، مجلد 3، عدد 2،ص ص 173-185.

-بوخاريأحمدوشعبان شاوشجم ال(2023) الذكاء الاصطناعي، الخوارزميات وحروب الجيل الخامس: قراءة في الاستراتيجيات الجديدة .مجلة مصداقية، مجلد 5، عدد 2، ص ص 37-48.

-خليفي محمد (2016) إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، عدد 1، ص ص 253-260.

-دهشان يحي إبراهيم(2020)المسؤولية الجنائية عن جرائم الذكاء الاصطناعي .مجلة الشريعة والقانون، عدد 82،.ص ص 100-144.

-زبيديمحمد عباس وشاهين نور قيس(2024) أزمة النص الجنائي في مواجهة جرائم الذكاء الاصطناعي: دراسة تحليلية،مجلة جامعة الزيتونة الأردنية للدراسات القانونية، إصدار خاص، ص ص 19-38.

شاوينغم محمد علي(2024)التكييف القانوني لسلوك التزييف العميق .مجلة جامعة تكريت للحقوق، مجلد 9، عدد 2، جزء 2، صرص 77-105.

سعداوي فاطمة الزهراء وعطية الحاج سالم (2023)، مواقع التواصل الاجتماعي وتشكيل القيم الإفتراضية لدى الشباب الجزائري: الفيسبوك نموذجا: دراسة تحليلية لعينة من شباب مدينة ورقلة المستخدم للفيسبوك." مجلة الباحث في العلوم الإنسانية والاجتماعية، مجلّد 15، العدد 2 (حزيران 2023)، ص ص 87-94.

-سياب حكيم (د.ت)السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، مجلد 1، عدد 1، ص ص 212-240.

-طارق أحمد زغلول، خوارزميات الذكاء الاصطناعي والعدالة الجنائية التنبئية دراسة وصفية تحليلية تأصيلية مقارنة، مجلة الدراسات القانونية والاقتصادية، لمجلد 9، العدد 2، يونيو 2023، كلية عين شمس، مصر، ص ص 31-306.

عبد الوهاب مريم ولبيض هنذ(2023)المسؤولية الجنائية عن جرائم الذكاء الاصطناعي .مجلة القانون والعلوم البينية، مجلد 2، عدد 2، ص ص 680-694.

عباس الزبيدي محمد (2024) نور قيس شاهين، أزمة النص الجنائي في مواجهة جرائم الذكاء الاصطناعي، دراسة تحليلية، مجلة جامعة الزيتونة الأردنية للدراســــــــات القانونية، اصدار خاص، ص ص 19-38.

-مصباح عبد المحسن عبد الرزاق رنا، تأثير الذكاء الاصطناعي على الجريمة الالكترونية، المجلة العلمية لجامعة الملك فيصل، العلوم الإنسانية والإدارية، مجلد 22، عدد 1، ص ص430-437.

2 -مذكرات الماجستير

-لقمان، باسمو(2010)المسؤولية الجنائية للشخص المعنوي عن جريمة تلويث البيئة .مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح – الجزائر.

3 -**القوانين**

-الأمر (66-156)المؤرخ في 18 صفر1386الموافق8 يونيو سنة 1966 المتمموالمعدل لقانون العقوبات ج .ر عدد مؤرخة في بتاريخ 11 يونيو 1966.

4 -المواقع الالكترونية

-بن صغير، فؤاد(2023) العدالة الخوارزمية في القانون المغربي،موقع مغرب القانون**https://maroclaw.com**، أطلع عليه بتاريخ 10/227 /2025

-منظمة التعاون الاقتصادي والتن مية(2024)، نبذة عن المنظمة ، موقع منظمة التعاون الاقتصادي والتنمية . https://www.oecd.org، أطلع عليه بتاريخ 9/20/ 2025.

-جامعة الدول العربية(2020) الاستراتيجية العربية للذكاء الاصطناعي: نحو رؤية عربية مشتركة .الأمانة الفنية لمجلس الوزراء العرب للاتصالات والمعلومات.https://www.arabunion.org/،أطلع عليه بتاريخ 8/28/ 2025.

-وكالة "رويترز (2024) الاتحاد الأوروبي يفرض على ميتا غرامة قدرها 251 مليون يورو بسبب خرق بيانات فيسبوك 17 .ديسمبر https://www.reuters.com، أطلع عليه بتاريخ 9/19/ 2025

-سباعي، عدنان (2024) المسؤولية الجنائية والمدنية عن التحيز الخوارزمي: نحو تجريم الانحياز الخفي للذكاء الاصطناعي وتأصيله في التشريع المغربي ، مجلة القانون والأعمال الدولية، جامعة حسن الأول. متاح عبر : https://www.droitetentreprise.com،أطلع عليه بتاريخ 10/25/ 2025.

-عربية، شبكة الجزيرة(2015) موسوعة الجزيرة/https://www.aljazeera.net،أطلع عليه بتاريخ 10/25/ 2025

جزيرة (2018) .كامبريدج أناليتيكاوفيسبوك: الفضيحة حتى الآن https://bit.ly/4dS1M4s. ، أطلع عليه بتاريخ 2025/10/25.

-مجلس حقوق الإنسان التابع للأمم المتحدة. (دون تاريخ) .تقارير ودراسات حول الذكاء الاصطناعي وحقوق الإنسانhttps://bit.ly/3T8sYwq ، أطلع عليه بتاريخ19/9/2025.

Meta PlatformsInc(2023)،سياسة الخصوصية: كيفية استخدام ملفات تعريف الارتباط والتقنيات المشابهة، متاح عبر: https://www.facebook.com/privacy/policies/cookies،أطلع عليه بتاريخ 9/20/ 2025.

ثانيا-المراجع باللغة الاجنبية

Books

Pariser, E. (2011). The filter bubble: What the internet is hiding from you. New York: Penguin Press

Research Articles / Papers

- Allen, T., &Widdison, R. (1996). Can computers make contracts? Harvard Journal of Law & Technology, 9.

-Biggio, B., &Roli, F. (2017). Wild patterns: Ten years after the rise of adversarial machine learning. arXiv preprint. arXiv:1712.03141

-European Parliament. (2017). Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

-Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Web sites

-Al Jazeera. (2018, March 28). Cambridge Analytica and Facebook: The scandal so far. https://www.aljazeera.com/news/2018/3/28/cambridge-analytica-and-facebook-the-scandal-so-far

-DW. (2018). Facebook's Cambridge Analytica data scandal: What you need to know. https://www.dw.com/en/facebooks-cambridge-analytica-data-scandal-what-you-need-to-know/a-43071390

-Reuters. (2024, March 21). Fact check: Macron dancing clip is altered 80s nightclub footage. https://www.reuters.com/fact-check/macron-dancing-clip-is-altered-80s-nightclub-footage-2024-03-21/?utm_source=chatgpt.com
-The Guardian. (2018, March 26). The Cambridge Analytica files: The story so far. https://www.aljazeera.net/tech/2018/3/22
-The Guardian. (2024, January 12). Deepfake video adverts of Rishi Sunak on Facebook spark alarm about AI risk to election. https://www.theguardian.com/technology/2024/jan/12/deepfake-video-adverts-sunak-facebook-alarm-ai-risk-election?utm_source=chatgpt.com
-Vox. (2018, December 21). Delete Facebook: All the scandals that led to people deleting Facebook--
-Wired. (2020, November 30). A doctored Biden video is a test case for Facebook's deepfake policies. https://www.wired.com/story/a-doctored-biden-video-is-a-test-case-for-facebooks-deepfake-policies/?utm_source=chatgpt.com