

دور "الاستخبارات مفتوحة المصدر" (OSINT) في التحقيقات القضائية

The Role of Open-Source Intelligence (OSINT) in Judicial Investigations

د - مناصرة يوسف

خريج جامعة الجزائر

menasra@hotmail.com

ملخص

إن تطور تقنيات وأدوات الاستخبارات مفتوحة المصدر (OSINT) يمثل قفزة نوعية في مجال العدالة الرقمية، حيث باتت الأدلة المستقاة من الفضاء الرقمي عنصراً حاسماً في نزاعات العصر الحديث. يسلط المقال الضوء على دور الاستخبارات مفتوحة المصدر (OSINT) في التحقيقات القضائية، مع التركيز على كيفية استغلال المعلومات الرقمية المتاحة علناً لدعم العدالة. وفي هذا الإطار، يهدف المقال إلى إبراز أهمية OSINT في التحقيقات الشرطية و القضائية وكشف الأنشطة الإجرامية، مع مراعاة الضوابط القانونية والحقوقية لحماية الخصوصية وسلامة الإجراءات. وتوضح النتائج أن OSINT تمكن الجهات القضائية من جمع وتحليل البيانات المتناثرة على الإنترنت، مثل وسائل التواصل الاجتماعي والمواقع الإلكترونية، وربطها للتحقق من الوقائع ورصد تحركات المشتبه فيهم وعلاقاتهم الرقمية. كما تُسهم في تسريع التحقيقات المعقدة التي تشمل كميات كبيرة من البيانات، مع تعزيز قيمة الإثبات الرقمي المقدم للقضاء و مدى مقبوليته. ويؤكد المقال أن إدماج OSINT ضمن المنهجيات القضائية يساهم في بناء ملفات تحقيق أكثر قوة وشفافية، ما يجعلها أداة استراتيجية في دعم العدالة وكشف الحقيقة في عصر الرقمنة.

كلمات مفتاحية: الاستخبارات مفتوحة المصدر، دليل إلكتروني، جريمة سيبرانية، تحقيق رقمي، حجية الدليل.

Abstract:

The development of Open-Source Intelligence (OSINT) technologies and tools represents a qualitative leap in the field of digital justice, as evidence derived from the digital space has become a decisive element in modern-day disputes.

This article highlights the role of OSINT in judicial investigations, focusing on how publicly available digital information can be leveraged to support justice. In this context, the article aims to shed light on the importance of OSINT in police and judicial investigations and in uncovering criminal activities, while taking into account the legal and human rights safeguards necessary to protect privacy and ensure the integrity of procedures.

The findings show that OSINT enables judicial authorities to collect and analyze scattered online data—such as social media platforms and websites—and correlate them to verify facts, monitor suspects' movements, and map their digital connections. It also contributes to accelerating complex investigations that involve large volumes of data, while enhancing the evidentiary value of digital proof presented before courts and its admissibility. The article concludes that integrating OSINT into judicial methodologies helps build stronger and more transparent investigative files, making it a strategic tool for supporting justice and uncovering the truth in the digital age.

Keywords: open-source intelligence, digital evidence, cybercrime, digital investigation, evidentiary value.

مقدمة:

الاستخبارات المستمدة من المصادر المفتوحة، أو ما يُعرف اختصاراً بـ (OSINT (Open Source Intelligence، تعني جمع المعلومات وتحليلها انطلاقاً من مصادر علنية ومشروعة دون اللجوء إلى وسائل قسرية أو غير قانونية، كالتنصت أو القرصنة أو استخدام هويات مزيفة. ورغم أن هذه الأساليب كانت معروفة منذ زمن طويل لدى الأجهزة العسكرية والاستخباراتية، فإنها شهدت خلال العقدتين الأخيرين تطوراً هائلاً بفضل ظهور الويب 2.0 في منتصف سنوات 2000، الذي سمح بتفاعل المستخدمين وإنتاجهم للمحتوى عبر الإنترنت. وقد ساهمت أحداث كالثورات العربية والحرب في فلسطين المحتلة في إبراز أهمية هذه الممارسات، حيث أصبحت وسائل التواصل الاجتماعي وسيلة رئيسية لتداول الصور، ومقاطع الفيديو، والشهادات حول النزاعات والانتهاكات في مناطق يصعب الوصول إليها ميدانياً، مما وفر مصدراً ثرياً للأدلة والوثائق القابلة للتحليل والاستخدام القضائي¹.

كانت عمليات جمع المعلومات في بداياتها يدوية ومحدودة، لكنها تطورت مع إدخال تقنيات الاستخلاص الآلي² scraping، وأصبحت تعتمد على أدوات متقدمة مثل الصور الفضائية، والتعرف على الوجوه، وتحليل الشبكات³ graph theory، والتعلم الآلي⁴ machine learning، مما أتاح دقة أكبر وسرعة في معالجة المعطيات.

وبعد أن كانت الـ OSINT تُعتبر لوقت طويل مجرد وسيلة ثانوية بسبب الشك في موثوقية مصادرها، أصبحت اليوم أداة أساسية في عمل الصحفيين والمنظمات الحقوقية والجهات القضائية، خصوصاً في مجال التحقيق في جرائم الحرب والجرائم ضد الإنسانية⁵، حيث تمكن من تتبع الأدلة الرقمية، وتوثيق الانتهاكات، وإسناد المسؤولية الجنائية بدقة متزايدة. بعبارة أخرى، يمثل الاستخبارات من المصادر المفتوحة تحولاً في منهجية جمع الأدلة والتحقيق الرقمي، يجمع بين المعرفة القانونية، والتقنيات المعلوماتية، وأخلاقيات البحث، بما يخدم العدالة ويدعم توثيق الحقيقة في زمن تتشابك فيه المعلومة مع الأخبار الكاذبة و الـ deepfake⁶.

أيضاً تُعد الاستخبارات مفتوحة المصدر (OSINT) إحدى الأدوات الحديثة التي أحدثت تحولاً ملموساً في مجال الإثبات القضائي، إذ غيرت بصورة عميقة طريقة جمع الأدلة من المصادر العلنية، وحفظها، وإدماجها في الإجراءات القانونية. وفي هذا السياق، تبرز أهمية الموضوع في مجال التحقيقات السيبرانية، حيث تقدم حلولاً مبتكرة لمختلف التحديات التي يطرحها استخدام تقنيات الـ OSINT في الممارسات القضائية المعاصرة.

غير أن هذا النمط الحديث من جمع الأدلة يطرح تحديات قانونية وعملية عديدة، خصوصاً فيما يتعلق بموثوقية البيانات وصحتها، ومشروعية جمعها، وقابليتها للاعتماد القضائي. ومن ثم أصبح من الضروري وضع منهجية دقيقة ومعايير مهنية لتنظيم عملية استخدام هذه الأدلة الرقمية في التحقيقات، مع ضرورة تكوين المتخصصين والمحققين في كيفية جمع وتحليل المعلومات من المصادر المفتوحة بما يضمن سلامة الإجراءات واحترام المعايير القانونية الدولية في الإثبات لاسيما في الجرائم السيبرانية⁷.

فلقد تركت الجرائم السيبرانية أثراً بالغاً على الأنشطة الإجرامية، وأصبحت من بين أكثر القضايا أهمية لأجهزة إنفاذ القانون في جميع أنحاء العالم ومنه يهدف هذا العمل إلى إبراز أهمية استخبارات المصادر المفتوحة OSINT في دعم التحقيقات الجزائية وتعزيز قدرات أجهزة إنفاذ القانون. وبشكل خاص، مع الكم الهائل من البيانات المتاحة عبر الإنترنت حالياً، أصبح لدى أجهزة إنفاذ القانون إمكانية الوصول إلى معلومات جوهرية تتعلق بالجرائم الخطيرة، الأمر الذي جعل من الاستخبارات مفتوحة المصدر أداة فعالة ومؤثرة في تعقب المجرمين والتحقيق في أفعالهم كما أنه من خلال تحليل الممارسات اليومية للضبطية القضائية تبين أن الاستخبارات مفتوحة المصدر توفر طيفاً واسعاً من الأدوات والتقنيات التي تتوافق مع احتياجات التحقيق الجنائي الحديث.

لذا تكمن أهمية دراسة OSINT في أنه:

- يمثل OSINT اليوم أداة إثبات حديثة في مجالات الإثبات الجزائي للجرائم الكلاسيكية و الحديثة.
- يمكن أن تكون المعلومات المستقاة من المصادر المفتوحة عبارة عن قرائن مادية أو رقمية تُدعم بها الملفات القضائية، شريطة أن تُجمع بطريقة شرعية، وأن يتم توثيق مصدرها وسلامتها.

ومن ثم، يمكن صياغة الإشكالية المحورية لهذا البحث على النحو الآتي: ماهي مقبولية الاستخدامات المعاصرة للاستخبارات مفتوحة المصدر، بالنظر إلى تعدد الفاعلين وتنوع مجالات التطبيق، في ظل التعقيد القانوني المرتبط بعمليات جمع وتحليل البيانات العامة داخل فضاء رقمي متغير الحدود؟ وما يثيره من إشكالات قضائية وأخلاقية دقيقة فرعية، هل يُعتبر كل ما هو متاح تقنيًا على الإنترنت "مفتوح المصدر" قانونًا؟، أي هل يجوز استخدام صورة أو منشور من مجموعة مغلقة لمجرد إمكانية الوصول إليه؟

إن هذا الغموض يُحوّل الفضاء الرقمي إلى منطقة رمادية تتقاطع فيها الشفافية مع الحق في الخصوصية، ويثير تساؤلات حول مبدأ التناسب إلى أي مدى يمكن المساس بالحياة الخاصة خدمةً للمصلحة العامة؟ بمعنى أشمل، ديمقراطية الوصول إلى المعلومة وتحليلها ترافقها تحديات كبرى ذات طبيعة منهجية وقانونية، خصوصًا في تقدير القيمة القانونية لهذا النوع من الأدلة على مستوى قضاة المادة الجزائية من حيث المشروعية و الصحة و المقبولية ، مما ينجم عنه صعوبات عملية جمة أمام القضاء الجزائي.

فرغم وفرة المادة الرقمية المتاحة على الشبكة، فإن كثرتها لا تعني بالضرورة تحقيق العدالة، فصحة الأدلة تعتمد على دقة جمعها وحفظها وتحليلها من قبل مختصين مؤهلين، وعلى اعتراف القضاء بمشروعيتها. وهو ما يبرز الحاجة إلى تأهيل مهني وتقني عالٍ في مجال التحقيق الرقمي، لضمان إدماج هذه الأدلة في الإجراءات القضائية بصورة تتفق مع المعايير القانونية.

للإجابة عن هذه الإشكالية الكبرى و الفرعية منها، تم اتباع المنهج الوصفي التحليلي وفقا لخطة ثنائية تتبنى مبحثين، حيث يتناول المبحث الأول ماهية الاستخبارات مفتوحة المصدر يُعطي اللثام عن المفاهيم و المصطلحات في المطلب الأول بينما الثاني منه يشرح استخدامات OSINT و تطبيقاتها المتعددة، يليه المبحث الثاني الذي يفصل في كيفية تحول OSINT من بيانات عامة إلى دليل قضائي و يبين دورها في التحقيقات القضائية لاسيما في مرحلة التحقيق الأولي في مطلب أول و يُسهم المطلب الثاني في مناقشة مقبولية دليل OSINT أمام المحاكم الجزائية في التشريع الجزائري.

المبحث الأول: ماهية الاستخبارات مفتوحة المصدر (OSINT)

تُعَدُّ محاولة وضع تعريف شامل ودقيق لمفهوم الاستخبارات مفتوحة المصدر مسألة معقدة نظرًا لحداثة هذا المجال من جهة، ولطابعه المتطور والمتغير باستمرار من جهة أخرى. فهو يُنظر إليه في بعض السياقات كأداة للشفافية والمساءلة، بينما يُعَدُّه آخرون وسيلةً للمراقبة والسيطرة. و تتنوع مجالات استعمال الـ OSINT، إذ يُستخدم لأغراض أمنية من قبل أجهزة الدولة التي تتعامل أحيانًا مع شركات خاصة كما يُستعمل اقتصاديًا في إطار ما يُعرف بـ "الذكاء الاقتصادي"⁸ وفي المجال الإعلامي، أصبح الصحفيون الاستقصائيون يعتمدون على هذه التقنيات لتوثيق الجرائم والانتهاكات في أماكن يصعب الوصول إليها، كما فعل فريق *Bellingcat* في سوريا⁹، مما يثير إشكالات حول حدود المشروعية وحماية الخصوصية رغم المصلحة العامة.

أما في المجال الأكاديمي، فإن الباحثين الجيوسياسيين يوظفون أدوات الـ OSINT لتحليل التوازنات الدولية باستخدام بيانات الأقمار الصناعية أو النشرات التجارية¹⁰

يتبين من كل ذلك أن الـ OSINT ليس مجرد تقنية، بل منظومة فكرية قانونية أخلاقية متشابكة، تجمع بين المنفعة العامة ومخاطر الانتهاك.

المطلب الأول: مفهوم مصطلح الاستخبارات مفتوحة المصدر OSINT

الاستخبارات مفتوحة المصدر " OSINT " ، تمثل مجالًا معقدًا ومتطورًا يجمع بين التقنيات الحديثة وأساليب التحليل المعلوماتي، وهي تُعنى بجمع المعلومات وتحليلها من مصادر متاحة للعامة عبر الإنترنت أو غيره من الوسائط المفتوحة¹¹.

ورغم أن الترجمات الفرنسية أو العربية تُقابلها غالبًا بمصطلح "المعلومات أو الاستخبارات من مصادر مفتوحة"، إلا أن هذه الترجمة لا تعكس بدقة جوهر المصطلح، إذ تُعفل بعده المعرفي المتعلق بعملية التحليل والاستخلاص الاستراتيجي للمعلومة، وتختزل في مجرد جمع بيانات، بينما يُقصد بـ "intelligence" في اللغة الإنكليزية نظام متكامل من الممارسات التحليلية والتقنية التي تهدف إلى تحويل البيانات الخام إلى معرفة قابلة للاستخدام القانوني أو الاستراتيجي.

كذلك، فإن الإشارة إلى "المصدر المفتوح" لا تعني هنا البرامج الحرة فحسب، بل تمتد لتشمل كل المعلومات المتاحة للعامة بدرجات متفاوتة من النفاذ، سواء كانت منشورة على مواقع إلكترونية، أو في قواعد بيانات، أو على شبكات التواصل الاجتماعي، أو حتى في السجلات الرسمية. وتكمن المهارة في قدرة المحقق أو الباحث على تحديد المعلومة الصحيحة، وتفسيرها في سياقها، وربطها بالأدلة الأخرى.

وعليه يُقصد بمصطلح OSINT، باختصار عملية البحث وجمع وتحليل البيانات والمعلومات المتاحة للعامة. ولا يقتصر الأمر على مجرد استعمال محركات البحث، بل يمثل هذا المجال أداة من أدوات الذكاء الاقتصادي التي تعتمد على منهجيات دقيقة وخبرة فنية متخصصة. ومن خلاله يمكن الحصول على معلومات مفيدة في مجالات التحريات و التقصيات للضبطية القضائية و لم تعد مقتصرة على مجال الاستخبارات و الاستعلامات ، والتحليل الاستراتيجي، إذ أصبح استغلال المعلومات الرقمية المتاحة للعامة جزءاً أساسياً من أدوات التحليل والاستشارة في العديد من المؤسسات الأمنية و القضائية¹².

إن الـ OSINT يمثل اليوم نظاماً جديداً لإنتاج الحقيقة يعتمد على تتبع الآثار الرقمية وربطها لبناء أدلة تُستخدم في كشف الجرائم أو دحض الأخبار المضللة، كما أنّ جمع المعلومات الرقمية لأغراض قضائية له أهمية واضحة في سياق الإثبات، غير أنّ دوره لم يعد يقتصر على ذلك، بل أصبح يُعدّ أداة استراتيجية قيمة سواء للمحامي أو لمكتبه في تقديم دعم استشاري وتحليل استراتيجي لعملائه في الخصومة القضائية¹³. ويقرن مفهوم الاستخبارات المفتوحة بمفاهيم أخرى قريبة منه¹⁴، و التي تعود جذوره إلى فترات ما بعد الحرب الباردة، عندما بدأت أجهزة الاستخبارات الأمريكية في التحول نحو جمع وتحليل المعلومات من المصادر المفتوحة¹⁵. فقد أنشأت وكالة الاستخبارات المركزية الأمريكية عام 2005 المركز الوطني للاستخبارات مفتوحة المصدر OSC امتداداً لخدمة المعلومات الإذاعية الأجنبية FBIS التي نشطت أثناء الحرب الباردة.

وقد تسارعت وتيرة تطور هذا المجال بعد أحداث 11 سبتمبر 2001، حيث أصبح البيان الرقمي هو محور العمل الاستخباراتي، وفق ما عبّر عنه مارك لوفتال¹⁶، ورغم حداثة المصطلح، فإن جمع المعلومات من المصادر المفتوحة ممارسة قديمة استخدمت في المجالات العسكرية والعلمية والاقتصادية. فالجنرال ويلنغتون في عام 1808، مثلاً، وبخ قاداته لأنهم لم يطلعوا على تغييرات في تشكيلات الجيش الفرنسي كانت منشورة في الصحف¹⁷!

إن فلسفة الـ OSINT تقوم على تحويل المعرفة العامة إلى معرفة استراتيجية، أي أن كل معلومة متاحة قد تكون ذات قيمة إذا تم تحليلها وفهم سياقها. الصورة مثلاً ليست مجرد وثيقة بصرية، بل تحمل بيانات مضمّنة (Metadata) تكشف عن تاريخها ومصدرها ومكانها. وبالتالي، فإن كل وثيقة رقمية يمكن أن تتحول إلى "نص" قابل للقراءة والتحليل والاستنتاج.

اليوم، يُقدّر أن نحو 80% من المعلومات التي تستخدمها أجهزة الاستخبارات تأتي من مصادر مفتوحة، وهو ما يعكس التحول الجذري في طريقة جمع الأدلة والمعلومات¹⁸. غير أن هذا التطور يثير تساؤلات قانونية وأخلاقية، خصوصاً بشأن مدى مشروعية استخدام البيانات الشخصية المنشورة على الإنترنت، مثل الصور أو المنشورات التي قد تكشف عن نمط حياة يتعارض مع التصريحات الرسمية أو الضريبية لصاحبها. كما في قضية "جون داروين"، الذي تظاهر بالموت للحصول على التأمين، إلى أن تم اكتشافه من قبل جارة لاحظت صورته على موقع وكالة عقارية بينما¹⁹.

الفرع الأول: فاعلو الاستخبارات مفتوحة المصدر (OSINT)

عندما تتطلب التحقيقات الرقمية درجة عالية من الدقة، يلجأ القضاة عادةً إلى خبراء متخصصين يمتلكون المعرفة التقنية والمنهجية العلمية اللازمة لجمع الأدلة الرقمية وتحليلها بشكل موثوق. بالإضافة إلى هؤلاء الخبراء القضائيين، يمكن للنسابة العامة أو قضاة التحقيق التعاون مع شركاء مختصين في الأمن السيبراني وخبراء المعلوماتية، كما هو الحال مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و الوكالة الوطنية لأمن الأنظمة المعلوماتية (أو ما يُعرف بالوكالة الوطنية للأمن السيبراني)²⁰. وعلى الرغم من أن بعض البيانات قد تكون متاحة للعامة، فإن ذلك لا يعني أنها خاضعة للتداول الحر دون قيود؛ فالحقوق الفردية في الخصوصية وحماية المعطيات الشخصية والملكية الفكرية تظل محمية بموجب القانون. ومن ثم، تثير ممارسة أنشطة OSINT، خصوصًا خارج الإطار القضائي، أسئلة دقيقة حول أصالة المعلومات وشرعية جمعها، ما دفع الفقه الحديث إلى التفكير في صياغة "قانون للاستخبارات مفتوحة المصدر" يوازن بين المصلحة العامة في الوصول إلى المعلومات وحماية الحقوق والحريات الأساسية للأفراد. ويرى الاستخدام العملي لتقنيات OSINT بشكل واضح في التحقيقات المتعلقة بمختلف الجرائم خاصة السيبرانية، حيث توفر هذه المنهجية أدوات دقيقة لدعم الإجراءات القضائية وتحقيق العدالة الرقمية. لكنني على خلاف هذا الرأي و أحبد تضمينها ضمن القواعد العامة في استخلاص الأدلة الإلكترونية تفاديا للتضخم التشريعي.

الفرع الثاني: منهجية ال OSINT وضوابطها القانونية

تتجاوز فعالية جمع المعلومات مفتوحة المصدر مجرد استخدام الأدوات التقنية، إذ تعتمد بشكل رئيسي على المنهجية العلمية في التعامل مع البيانات. فالمهارة الأساسية في OSINT تكمن في القدرة على تحليل المعطيات المتاحة وربطها ببعضها البعض لاستخلاص معرفة جديدة، تمكن الباحث من الوصول إلى نتائج دقيقة وموثوقة يمكن الاعتماد عليها في السياق القضائي أو الأمني²¹.

- أول خطوة في هذه العملية هي تحديد المصادر الموثوقة، حيث يجب اختيار المصادر التي تتمتع بالمصداقية وتخضع لمعايير دقة معلومة ومتاحة للعامة، لتجنب الاعتماد على معلومات مضللة أو غير صحيحة.
- يلي ذلك تصنيف المعلومات وترتيب أولوياتها، أي تقييم أهمية كل معلومة وعلاقتها بالقضية قيد التحقيق، ما يسهل توجيه البحث بشكل فعال ويركز الجهود على العناصر الأكثر صلة.
- وتأتي خطوة توثيق مراحل البحث وإثبات التسلسل الزمني لتوفير دليل ملموس على كيفية الحصول على المعلومات، مما يعزز مصداقية النتائج و يتيح التحقق من سير العملية بشكل متسلسل.
- كما يكتسب ضمان قابلية التتبع والشفافية في الإجراءات أهمية كبيرة، إذ يضمن أن أي طرف ثالث يمكنه مراجعة خطوات البحث والتحقق من صحتها وفق المعايير القانونية المتعارف عليها.
- وأخيرًا، يشمل الضبط القانوني لل OSINT حفظ الأدلة الرقمية بطريقة تتيح التحقق من مشروعيتها لاحقًا، مثل استخدام تقنيات التشفير أو التوثيق الرقمي لضمان عدم التلاعب بالبيانات، وهو ما يجعل هذه الأدلة مقبولة وموثوقة عند عرضها أمام الجهات القضائية.

المطلب الثاني: استخدامات ال OSINT و تطبيقاتها

يمتد استخدام تقنيات ال OSINT إلى مجالات متعددة تشمل أجهزة الاستخبارات والأمن وأقسام الأمن السيبراني والإعلاميين والمحققين الصحفيين والقضاة والمحامين وخبراء الاقتصاد والمال والشركات والباحثين والأكاديميين، كما ظهر جيل جديد من "المحققين المواطنين" الذين يستخدمون الأدوات الرقمية في كشف الحقائق وتوثيق الجرائم والانتهاكات²²، وهو ما أدى إلى تلاقي الممارسات بين المحترفين والهواة في فضاء رقمي مشترك.

و يُعدّ مجال الـ OSINT تحديًا علميًا وتكوينيًا للمؤسسات الأكاديمية، إذ يتطلب تكوينًا متعدد التخصصات يجمع بين علوم الإعلام، والتحليل الرقمي، والقانون، والأمن المعلوماتي، بما يضمن مؤسسة هذه الممارسات وإدماجها في مناهج التعليم والبحث العلمي. فهو لم يعد مجرد تقنية لجمع البيانات، بل إطارًا معرفيًا ومهنيًا جديدًا يهدف إلى تحويل المعلومات المفتوحة إلى معرفة دقيقة، موثوقة، وقابلة للاستخدام في سياقات قانونية وأمنية مشروعة²³.

الفرع الأول: دور الضبطية و مساعدتي القضاء في توظيف استخبارات المصادر المفتوحة (OSINT)

يكتسب توظيف استخبارات المصادر المفتوحة OSINT أهمية متزايدة لدى أجهزة إنفاذ القانون، إذ تعتمد هذه الجهات على تحليل المحتوى الرقمي العلني لتحديد هوية الجناة ورصد أنشطتهم، مع التأكيد على أن فعالية هذه التحقيقات تقوم على الجمع بين التحري الرقمي والعمل الميداني. وقد برز هذا الدور بوضوح في قضية "Johnny Hallyday" سنة 2019، حيث تمكنت النيابة المالية الفرنسية من إثبات إقامته الفعلية داخل فرنسا بالاستناد إلى منشوراته العلنية على منصة "إنستغرام"، ما سمح بإخضاع النزاع حول تركته للقانون الفرنسي²⁴. وفي ساهمت العديد من الصور و الفيديوهات المنشورة على اليوتوب في التعرف و القبض على مجرمين خطيرين منها قضية هشام الوهراني قائد عصاة بفوكة بولاية تيبازة، وتم القبض عليه بعد أيام من ظهوره مع عصابته في مقطع فيديو في 16 أكتوبر 2025 وهم يعذبون مواطنًا بالضرب وأسلحة بيضاء²⁵.

ويمتد دور OSINT ليشمل مهنة المحاماة، إذ يمكن المحامي المتمكن من تقنيات البحث في المصادر المفتوحة من تعزيز الملفات القضائية أو ما قبل القضائية من خلال جمع أدلة مرتبطة بجرائم المساس بالأنظمة المعلوماتية أو التزيف أو المنافسة غير المشروعة أو التشهير. كما يُسهم هذا النوع من التحليل في فهم معمق للملفات عبر الحصول السريع على البيانات القانونية للشركات، وفهم تنظيمها الداخلي، ووضع آليات يقظة قانونية دقيقة. ويُعدّ تقديم الأدلة المستخلصة من OSINT أمام القضاء أحد مظاهر توسيع دور المحامي في دعم مرافعاته وتعزيز حججه²⁶.

كما يضطلع المحضر القضائي بدور محوري في توظيف OSINT، إذ تُعدّ المعايير الإلكترونية التي ينجزها ذات حجية قانونية معتبرة في المواد المدنية إلى أن يثبت العكس، مما يجعلها وسيلة إثبات قوية عند توثيق المعلومات المستقاة من المصادر المفتوحة. ويؤدي الجمع بين نتائج تحليل OSINT وحجية محاضر المعاينة إلى منح الملف قوة إثبات إضافية، وفق طبيعة القضية وخصوصياتها²⁷. أما الخبراء والمحققون الخاصون، فقد أصبح لجوء الأطراف إليهم مفيدًا بصورة خاصة عندما يكونون متمرسين في البحث عبر المصادر المفتوحة. فالتقارير التي يعدونها قد تُقبل كأدلة أمام المحاكم، وهو ما أقرته الاجتهادات القضائية التي اعتبرت أن نتائج تحقيقات المحقق الخاص تُعامل وفق الضوابط ذاتها المطبقة على غيرها من وسائل الإثبات. ومع ذلك تبقى سلطة القاضي التقديرية هي الفيصل في تقدير قيمة هذا التقرير ووزنه في السيرورة القضائية²⁸.

الفرع الثاني: استخدامات OSINT في الوقاية و مكافحة الجرائم

تلعب استخبارات المصادر المفتوحة دورًا متقدمًا في الوقاية من الجرائم التقليدية مثل السرقة، والاحتيال، والعنف، من خلال تحليل المنشورات العلنية، وتتبع التحركات والأنماط الاجتماعية التي قد تكشف بوادر السلوك الإجرامي. كما تتيح مراقبة الأسواق الرقمية والإعلانات المشبوهة تحديد الأنشطة التي ترتبط بسرقات المركبات أو الاتجار غير المشروع. وفي الجرائم الحديثة كالجرائم السيبرانية، والتطرف الرقمي، والاتجار بالبشر عبر الشبكة، تمكن OSINT من تتبع الهويات الرقمية، ورصد البنية الشبكية للجماعات الإجرامية، وتحليل البيانات الضخمة للكشف عن الروابط الخفية بين الفاعلين. وتؤكد الأبحاث أن اعتماد OSINT يعزز القدرة على كشف الجريمة في مراحلها المبكرة وتحسين فعالية الاستجابة الأمنية²⁹.

يمكن استخدام نتائج الرصد في مجالات متعددة، أهمها:

1. الكشف المبكر عن التهديدات السيبرانية، عبر رصد عمليات بيع أدوات الاختراق أو تبادل بيانات الدخول المسروقة.
 2. تتبع الجرائم المالية وغسل الأموال من خلال مراقبة حركات العملات المشفرة في الأسواق المظلمة.
 3. مكافحة الإرهاب الرقمي، حيث تُستخدم المنتديات المظلمة لتجنيد العناصر أو تمويل العمليات.
 4. تحليل أنماط الجريمة المنظمة وتفكيك شبكاتها عبر جمع بيانات مترابطة من مصادر مفتوحة ومغلقة.
- هذه التطبيقات تعكس أن OSINT والرصد التقني للشبكة المظلمة أصبحا من ركائز العمل الأمني الحديث، سواء في مرحلة جمع المعلومات أو في مرحلة التحليل الاستراتيجي.
- تشير استخبارات المصادر المفتوحة إلى العملية المنهجية لجمع وتحليل البيانات المتاحة للعامة من مصادر متعددة تشمل منصات التواصل الاجتماعي، والسجلات العامة، ووسائل الإعلام، وأنظمة المراقبة، وحتى شبكات الإنترنت المظلم ³⁰ Dark Web و يكمن الهدف الأساسي منها هو استخلاص معلومات استخباراتية من المعلومات المتاحة عبر الإنترنت، أهمها الويب المفتوح، والويب العميق والويب المظلم وتوفّر كل طبقة من هذه الطبقات قدرًا مهمًا من البيانات التي يمكن أن تساعد المحققين و تكون قابلة للاستخدام العملي ³¹ بفضل تطوير العديد من الأدوات والتقنيات لاستخدامها في التحقيقات المفتوحة المصدر ³².

المبحث الثاني : OSINT : من بيانات عامة إلى دليل قضائي

يُعد تحريك الدعوى العمومية في مواجهة الجرائم رهينًا بقدرة السلطات المختصة على الكشف المبكر عن الأفعال الإجرامية وتوصيفها بدقة، وهو ما يجعل استخبارات المصادر المفتوحة أداة مركزية في دعم العمل القضائي. إذ تمكن هذه التقنية من رصد المؤشرات الأولى للجريمة من خلال البيانات المتاحة علنًا على الإنترنت خاصة إذا كانت الجريمة سيبرانية، سواء تعلق الأمر بعمليات احتيال رقمي، أو تشهير، أو اعتداءات على الأنظمة المعلوماتية، أو ترويج محتوى غير مشروع. وتتيح OSINT للنسابة العامة وأجهزة الضبطية القضائية إمكانية تتبع البصمة الرقمية للمشتبه فيهم، واستقاء قرائن أولية تساهم في توجيه التحقيق، عبر تحليل المنشورات في شبكات التواصل الاجتماعي، ومراقبة التحركات الرقمية، وتجميع البيانات المشتتة التي يمكن أن تكشف الطبيعة التقنية للجريمة وأساليب مرتكبيها. كما تسمح هذه المقاربة بتعزيز فعالية آليات التبليغ والمتابعة، لاسيما عندما تكون الجريمة عابرة للحدود أو تستند إلى هويات رقمية وهمية.

وفي مرحلة التحقيق، تتكامل تقنيات OSINT مع أدوات التحليل الجنائي الرقمي، لتوسيع دائرة الأدلة التي يمكن اعتمادها في الدعوى العمومية. فإلى جانب البيانات المستخلصة من الأجهزة الإلكترونية والأنظمة المعلوماتية كالبريد الإلكتروني، سجلات المكالمات، معاملات الدفع الإلكتروني، وتحديد المواقع الجغرافية تُعد المعلومات العلنية على الويب مفتاحًا مهمًا لفهم سياق الجريمة وربط عناصرها ببعضها. وتساعد OSINT في تمييز الأدلة المتاحة للعامة عن الأدلة المخزنة في أنظمة خاصة، وفي استخلاص بيانات وصفية تُستخدم لتحديد هوية المستخدمين أو موقع الخوادم أو زمن ارتكاب الفعل، دون المساس بسرية المحتوى. وهكذا، تصبح الأدلة الرقمية بكل أصنافها سواء كانت علنية أو تقنية متخصصة مرتكزًا أساسيًا لإثبات المسؤولية الجزائية، وهو ما يجعل الاعتماد على OSINT خطوة حتمية في مواجهة الجرائم التقليدية ذات البعد الرقمي، والجرائم المستحدثة التي يفرزها الفضاء السيبراني.

وتُنجز هذه العمليات داخل مختبرات التحليل الجنائي المتخصصة، التي توفر بيئة تقنية متطورة تساعد الخبراء على ضمان سلامة الأدلة، والحفاظ على تسلسلها الزمني، وصون مصداقيتها أمام القضاء. وبالتالي، فإن التحقيق في الجرائم السيبرانية يتطلب تعاونًا وثيقًا بين أجهزة إنفاذ القانون وخبراء الأدلة الرقمية، في إطار منهجي يجمع بين الدقة التقنية والضمانات القانونية، لضمان فعالية العدالة في الفضاء الرقمي ³³. لكن في المقابل، أدى استخدام تقنيات تشفير البيانات إلى خلق عقبات حقيقية أمام سلطات التحقيق، إذ لم يعد بالإمكان الوصول بسهولة إلى المعلومات المخزنة على الهواتف الذكية أو الحواسيب، مما يجعل جمع الأدلة الرقمية أكثر تعقيدًا. ورغم أن التشفير يضمن الحق في الخصوصية وأمن المعلومات، فإنه قد يتحول إلى حاجز أمام العدالة عندما يعطل كشف الحقيقة ³⁴.

وتشير القاعدة العامة في القانون الجنائي إلى أن كل مراحل الدعوى من اكتشاف الجريمة إلى صدور الحكم تدور حول مسألة الإثبات وبما أن الأدلة الرقمية أصبحت أساسية في كشف الحقيقة، فقد انتقل الاهتمام من البحث عن الاعترافات التقليدية إلى الاعتماد على التحليل التقني للأجهزة والبيانات. رغم ذلك، فإن جمع الأدلة الرقمية يمس بالضرورة الحياة الخاصة للأفراد، خصوصاً لأن البيانات المخزنة على الأجهزة الشخصية تكشف تفاصيل دقيقة عن حياة الأشخاص. ومن ثم، تقوم القواعد الإجرائية الجزائية الوطنية المتعلقة باستخلاص الأدلة الإلكترونية على مبدأ أساسي يتمثل في تحقيق التوازن بين فعالية تطبيق القانون وحماية حقوق الإنسان، خاصة الحق في الخصوصية³⁵ و حماية المعطيات الشخصية. فلولا وجود نصوص قانونية تُجيز إجراءات المساس بالمعطيات الإلكترونية (الإعتراض، الإلتقاط الإلكتروني، المراقبة الإلكترونية.. الخ)، لاعتُبرت تلك الأفعال جرائم قائمة بذاتها. ويستند هذا الإطار الحمائي إلى التزامات الجزائر الدولية، لاسيما الإعلان العالمي لحقوق الإنسان³⁶، والعهد الدولي للحقوق المدنية والسياسية³⁷، والميثاق الإفريقي لحقوق الإنسان والشعوب³⁸، وإلى ما تقره تشريعات معظم الدول. ولتحقيق هذا التوازن، يجب توفر ثلاثة شروط رئيسية مبدأ التناسب والإشراف القضائي واحترام حسن سير العدالة³⁹. وهذا يعني أنه لا يمكن السماح بجمع كل أنواع البيانات لأي نوع من الجرائم، ويجب أن يكون ذلك تحت إشراف قضائي أو سلطة مستقلة.

وتتصل هذه المسائل أيضاً بمبدأ مشروعية الدليل، الذي يقتضي أن تكون وسائل جمع الأدلة نزيهة وغير مشروعة. ومع أن الاجتهاد القضائي سمح في بعض الحالات باستخدام التحليل المشروع أو الاستراتيجيات التقنية مثل إنشاء حسابات وهمية أو مواقع إلكترونية مزيفة لاكتشاف المجرمين في جرائم التمييز و خطاب الكراهية⁴⁰ و الجرائم الخطيرة جدا مثل الجرائم الجنسية المرتكبة ضد الأطفال⁴¹، فإنه يرفض و يحظر الأساليب التي تمس الحقوق الأساسية للأفراد أو تُعد استفزازاً لارتكاب الجريمة.

ومع تطور الواب 3.0، و ثورة الذكاء الاصطناعي وتقنيات التحليل المفتوح للمصادر التي باتت تمثل أدوات جديدة في جمع الأدلة. فالمحققون باتوا يعتمدون على البيانات المتاحة عبر الإنترنت كالمنشورات، صور، مواقع تواصل اجتماعي وهي موارد يمكن أن تقدم أدلة مهمة ومفتوحة المصدر. ومع ذلك، فإن الاعتماد المفرط أو الآلي على هذه المعلومات يثير تساؤلات قانونية حول موثوقيتها، مشروعيتها، واحترامها للخصوصية.

ولا تُستخدم تقنيات OSINT فقط لتحديد هوية الفاعلين الإجراميين، بل ساهمت أحياناً في توقيفهم ومتابعتهم قضائياً⁴². لكن وفرة المحتوى المجرّم المتداول على الإنترنت لا تعني بالضرورة تحقيق العدالة، إذ تبقى قابلية قبول هذه الأدلة مرهونة بدقة العمل الذي يقوم به محللو OSINT وبكفاءة السلطات المختصة. فهذه الأخيرة تحتاج إلى الإلمام الكافي بكيفية إدماج الأدلة الرقمية ضمن الإجراءات القانونية وفقاً للمعايير المعتمدة.

بناءً على هذا الطرح، نستعرض كيفية إجراء التحقيقات في المصادر المفتوحة و مراحلها و ضوابطها و الإشكالات التي يُمكن أن تثيرها عملياً و أمام المحاكم الجزائية في مطلب أول، بينما المطلب الثاني يُعرج على مقبولة دليل OSINT أمام المحاكم الجزائية في التشريع الجزائري التي لا يمكن لها تخرج عن المألوف في القواعد الإجرائية للإثبات.

المطلب الأول: التحقيق في المصادر المفتوحة

إن الأدلة الرقمية متغيرة بطبيعتها ومتأثرة بالتطور التقني المستمر، وهو ما يجعلها متطيرة وسريعة الزوال. لذلك، فإن جمعها يجب أن يتم بسرعة وباحترافية عالية مع احترام الإجراءات القانونية والضمانات القضائية. و لا تزال هناك تحديات قائمة في جمع الأدلة المستقاة من المصادر المفتوحة إلى غاية وصولها أمام المحاكم. ومع ذلك، بدأت تظهر عدة أدوات⁴³ ومبادرات تهدف إلى تسهيل دمج المعلومات المستخلصة من المصادر المفتوحة في الإطار القضائي وتعزيز قيمتها القانونية.

وتؤسس الفقرة الأخيرة من المادة 20 من قانون الإجراءات الجزائية الجديد⁴⁴ إطاراً قانونياً يسمح لضباط وأعوان الشرطة القضائية باستخدام الأجهزة التقنية والإلكترونية لمعينة الجرائم وإثباتها، وفق كفاءات تُحدّد بنص تنظيمي، وهو ما يفتح الباب لتوظيف منهجيات الاستخبارات مفتوحة المصدر OSINT في العمل القضائي. فهذه المادة، بصياغتها الواسعة، تُقرّ مبدأ مشروعية اعتماد الوسائل التقنية الحديثة دون حصرها في أدوات معينة، مما يشمل أدوات الرصد الرقمي، وتحليل المحتوى المنشور للامة، وتتبع الآثار الرقمية الظاهرة، شريطة احترام الضوابط التنظيمية لاحقاً. كما تُجسّد المادة انتقال المشرّع نحو الاعتراف بالدليل الرقمي في شكله الحديث، بما فيه الدليل المستخرج من المصادر المفتوحة، وتُرتّب ضمناً التزام الضبطية بمهنية تقنية تحترم المشروعية، والضرورة، والتناسب، وحماية الحياة الخاصة، باعتبار أن أي استعمال للأدوات الإلكترونية يجب أن يتم وفق إجراءات مضبوطة لا تسمح بالتعسف أو المساس غير المبرر بالحقوق الأساسية. وبذلك تشكل الفقرة أساساً لتقنين عمل OSINT في التحقيقات الجزائية، لكنها في الوقت نفسه تجعل مشروعيتها مرتبطة بالكفاءات التنظيمية اللاحقة التي ينبغي أن تُحدّد شروط الجمع، والتوثيق، وحفظ البيانات المفتوحة، لضمان قبولها القضائي واحترامها لضمانات المحاكمة العادلة. يقصد بـ التحقيق في المصادر المفتوحة جمع المعلومات والبيانات المتاحة للامة عبر الإنترنت أو السجلات العلنية أو وسائل الإعلام أو قواعد البيانات القانونية، بغرض توثيق الوقائع قبل الانتقال إلى التحقيق الميداني المباشر.

الفرع الأول: مراحل جمع وتحليل المعلومات في OSINT

وهذا النوع من التحقيق يتطلب أسلوب تنفيذ محدد Modus operandi يشمل مراحل أساسية. وتُعدّ إجراءات التحقيق OSINT أكثر من مجرد بحث رقمي أو استعمال عبر محركات البحث، إذ تقوم على هيكلية علمية لمراحل جمع وتحليل المعلومات، يمكن تلخيصها في ثلاث خطوات مترابطة⁴⁵: -فضلاً عن ما أوردناه أعلاه في منهجية OSINT و ضوابطها القانونية-

1. **مرحلة الرصد والمراقبة:** تتمثل في جمع أولي ومنهجي للمعلومات ذات الصلة بالموضوع محل التحقيق خلال فترة زمنية محددة، بغية تكوين قاعدة بيانات أولية.

2. **مرحلة التحليل والتصفية:** يتم في هذه المرحلة فرز المعلومات حسب الأهمية والمصادقية، مع تحديد الثغرات المعلوماتية التي تستوجب التحقق الميداني لاحقاً. في هذه المرحلة، يعتمد المحققون على أدوات بحث متقدمة، مثل المعاملات البوليانية (Boolean Operators)⁴⁶، وتقنيات تحليل الشبكات، وتطبيقات رسم الروابط⁴⁷.

3. **مرحلة التحقق الميداني:** بعد جمع وتحليل المعلومات، يتم الانتقال إلى الميدان للتحقق من صدقية ما تم جمعه عبر المصادر المفتوحة. وتشمل هذه المرحلة مراجعة الوثائق الأصلية، واستجواب الشهود، والتنسيق مع المؤسسات المعنية كالأرشفات الوطنية أو مكاتب التوثيق حيث أن الهدف النهائي هو إعداد تقرير موثق زمنياً يروي "قصة" الموضوع أو الكائن محل التحقيق بدقة واستناداً إلى أدلة يمكن التحقق منها.

ويتيح هذا النوع من التحريات للمحققين استخدام برامج مفتوحة المصدر لجمع وتحليل البيانات من مصادر متعددة، بما في ذلك منصات شبكات التواصل الاجتماعي والمدونات والمنشورات ومنصات المشاركة بالصور والفيديو، مع التركيز على المعلومات المتاحة للجمهور، مثل الرسائل العامة، تحديثات الحالة، المحادثات، التفاعلات الاجتماعية، البيانات الوصفية، والمحتوى المرئي أو السمعي. تبدأ هذه العملية بتحديد المعلومات المفيدة وفق هدف محدد، مثل عناوين البريد الإلكتروني وأسماء المستخدمين وعناوين بروتوكول الإنترنت وأسماء النطاقات والحسابات الاجتماعية، ثم التحقق من صحتها لضمان موثوقيتها ودقتها وقابليتها للتحقق في أي وقت. بعد ذلك تُحلل المعلومات لتحديد الاتجاهات والسلوكيات والأحداث ذات الصلة، ويتم فرزها وتجميعها لإنتاج بيانات شاملة يمكن استخدامها عملياً أو تقديمها أمام القضاء عند الحاجة، مع الالتزام التام بحقوق الإنسان والمبادئ التوجيهية المتعلقة بالخصوصية والشرعية والتناسب والمساءلة والضرورة، إذ لا تمنح هذه التحريات صلاحية للمحققين بإجراء أي تحقيقات سرية خارج الإطار القانوني والقضائي⁴⁸.

الفرع الثاني: الإشكاليات القانونية للتحقيق في المصادر المفتوحة

يمثل الـ OSINT، منهجية تقوم على جمع واستغلال المعلومات المتاحة للجمهور بحرية، سواء عبر الصحف، أو المواقع الإلكترونية، أو شبكات التواصل الاجتماعي. ورغم أن اللجوء إلى المصادر المفتوحة لا يُعد في ذاته ممارسة غير قانونية، باعتبار أن طبيعتها قائمة على العلنية، إلا أن كل مرحلة من مراحل هذا العمل قد تُرتب على صاحبها مسؤولية قانونية إذا لم تُحترم الضوابط التشريعية المقررة. فليس كل ما هو متاح مباحاً، ولا يمكن استخدام نتائج الأبحاث بصورة مشروعة إلا إذا روعيت القواعد القانونية في كامل مسار العملية، أي أثناء البحث، والجمع، ثم الاستغلال لاحقاً. ولا OSINT موقع متزايد الأهمية في العمل القانوني، ولا سيما في المجال القضائي⁴⁹.

تقتضي مرحلة البحث احترام شرط أساسي يتمثل في الاعتماد على مصادر "مفتوحة" حصراً، أي تلك التي تُقدم بياناتها إلى الجمهور دون قيد. غير أن صفة "المفتوح" لا تعني بالضرورة سهولة الوصول، إذ تعتمد منهجية الـ OSINT على مبدأ الارتكاز الذي يقوم على استخدام معلومة للوصول إلى معلومة أخرى. ويُستبعد بذلك كل شكل من أشكال التحايل أو القرصنة، مثل انتحال الهوية الإلكترونية بغرض الوصول إلى بيانات معينة. كما يجب أن يكون الوصول مشروعاً وغير مخالف لأحكام تجريم الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات⁵⁰، إذ قد ينقلب عمل الباحث إلى فعل مجرم إذا استُخلص أن الولوج إلى البيانات تم دون ترخيص، حتى وإن كان سبب التمكن منها يعود لخلل تقني في حماية الموقع. وقد أظهرت أحكام قضائية أن مجرد العلم بعدم الأهمية بالولوج يكفي لترتيب المسؤولية، ولو كان الدخول الأول ناتجاً عن إنعدام أو ضعف في تأمين النظام⁵¹.

وتكتسي الأبحاث ذات الطابع الخاص والحساس خصوصية إضافية، خاصة عندما يتعلق الأمر بملفات جنائية أو جهات قد يشكل جمع المعلومات بشأنها خطراً على الباحث أو تدخلاً غير مشروع في تحقيقات جارية. ويُعد احترام قواعد الأمن العملياني⁵² OPSEC ضرورة عملية وقانونية في آن واحد، لتفادي تنبيه الأشخاص أو الكيانات المستهدفة بالأبحاث، أو تعريض الأدلة لخطر الإتلاف قبل تثبيتها⁵³. أما في مرحلة الجمع، فلا بد من توخي الحذر عند استخدام تقنيات مثل الـ scraping، أي الاستخراج الآلي للمعطيات، إذ يمنع القانون استخراج جزء جوهري من قاعدة بيانات أو نسخ موقع بالكامل دون إذن من منتج القاعدة، لما في ذلك من مساس بحقوقه. كما يثير التعامل مع البيانات المسربة⁵⁴ leaks إشكالات جديدة، لأن تنزيلها أو الاحتفاظ بها قد يُعد بمثابة إخفاء مواد متحصلة من جريمة. وفي المقابل، تتيح البيانات الحكومية المفتوحة هامشاً واسعاً للاستخدام المشروع، شريطة احترام قواعد حماية المعطيات الشخصية كلما احتوت الملفات على بيانات مُعرّفة بالأشخاص⁵⁵.

وعند الانتقال إلى مرحلة الاستغلال، لا يعني مجرد جمع المعلومة أنه يمكن نشرها أو إعادة استخدامها بحرية، إذ قد يؤدي ذلك إلى المساس بحقوق المؤلف عبر استعمال محتوى محمي دون إذن⁵⁶، أو إلى انتهاك الحياة الخاصة من خلال إعادة نشر بيانات شخصية، حتى لو كانت متاحة علناً⁵⁷. ويُوازن القضاء بين الحق في الخصوصية وحق الجمهور في الإخبار وفق معايير دقيقة تتعلق بالمصلحة العامة والغاية من النشر وطريقة الحصول على المعلومات. كما يشكل نشر المعلومات⁵⁸ doxxing والمطاردة الإلكترونية e-stalking⁵⁹ ممارسة مجرّمة تمس بخصوصيات الأشخاص.

وفي السياق القضائي، يثبت الـ OSINT أهميته في مراحل ما قبل الخصومة، من خلال جمع عناصر الإثبات اللازمة للدعوى المدنية⁶⁰ أو الجزائية، كما يساعد في التحقيقات الجنائية على تحديد هوية الجناة بالاعتماد على الآثار الرقمية العلنية. وتُقبل معطيات OSINT أمام القضاء شريطة تثبيتها بطريقة تضمن قابليتها للتحقق، كتوثيق خطوات البحث، أو التقاط الشاشات، أو اللجوء إلى المحضر القضائي، أو أرشفة الصفحات عبر أدوات موثوقة. وقد اعترفت الاجتهادات الحديثة بالقيمة الثبوتية للأرشفات الرقمية مثل Wayback Machine⁶¹. ويُسهّم المحامون المكونون في OSINT، إضافة إلى المحققين الخاصين، في تعزيز الملفات القضائية عبر تقارير قابلة للتقديم أمام القضاء، مع

احتفاظ القاضي بسلطته التقديرية في تقدير قيمتها. كما تستفيد قوات الأمن من هذه المنهجية في التحقيقات الجنائية، وتظهر العديد من القضايا الحديثة كيف سمح تحليل الآثار الرقمية للمنشورات العامة بإثبات وقائع أو تحديد أماكن أو زمن وجود أشخاص، بما يعزز التكامل بين العمل الرقمي والميداني⁶².

و عليه، يمكن القول إن ممارسة الـ OSINT في التحقيقات القضائية تطرح مجموعة من الإشكالات القانونية الدقيقة، أبرزها:

- **مسألة الشرعية واحترام خصوصية الأفراد:** فجمع البيانات من المصادر المفتوحة يجب أن يتم دائماً ضمن إطار يحترم القوانين الوطنية والدولية المتعلقة بحماية المعطيات الشخصية، ولا سيما عند تحليل المحتوى المنشور على منصات التواصل الاجتماعي، وذلك لتفادي أي انتهاك لحق الخصوصية أو المسؤولية القانونية للباحث. كما أن أي استخدام للمعلومات يجب أن يلتزم بمبادئ الأمن العملياتي لضمان حماية هوية الباحث والحفاظ على سلامة سير التحقيقات الجارية.

- **سلامة الدليل الرقمي:** لا يُعتدّ بالمعلومة إلا إذا أمكن إثبات مصدرها وتمايمتها، ولهذا الغرض تُستخدم تقنيات التحقق بالتجزئة Hashing لتأكيد أن البيانات لم يتم تعديلها بعد جمعها .

- **قابلية القبول القضائي:** تُعد المعلومات المستخلصة من المصادر المفتوحة قرائن مادية يمكن أن تساند الدليل الرئيسي أمام القضاء، شريطة أن تكون موثقة ومؤرخة وفق المعايير المعترف بها دولياً⁶³.

المطلب الثاني: مقبولة دليل OSINT أمام المحاكم الجزائرية في التشريع الجزائري

تُعد الأدلة المستخرجة من تقنيات الاستخبارات مفتوحة المصدر OSINT من أبرز المستجدات في منظومة الإثبات الحديثة، لاسيما في ظل التحول الرقمي واتساع استخدام المنصات المفتوحة لنشر المعلومات. وعلى الرغم من غياب نص صريح في التشريع الجزائري يحدد الطبيعة القانونية لهذه الأدلة، إلا أنّ المبادئ العامة في قانون الإجراءات الجزائية، والقواعد الدستورية المتعلقة بحماية الحياة الخاصة و المعطيات الشخصية، تمنح القاضي الجزائري إطاراً لتقدير مدى قبولها. وتثير هذه الأدلة سؤالاً جوهرياً يتعلق بشروط مشروعيتها من جهة، وقيمتها الإثباتية من جهة ثانية، مما يبرر تقسيم هذا المطلب إلى فرعين أساسيين:

الفرع الأول: شروط مشروعية جمع أدلة OSINT

يخضع أي دليل رقمي، بما في ذلك الأدلة المستخلصة من المصادر المفتوحة، لشرط جوهري يتمثل في احترام الضوابط الدستورية والإجرائية التي تضمن حماية الحياة الخاصة والمعطيات الشخصية. فالقاضي الجزائري لا يعتد بأي معلومة رقمية جُمعت بصورة تنطوي على اختراق للأنظمة المعلوماتية أو تجسس غير مشروع بمعنى غياب الإذن القضائي كما في تقنيات الاعتراض الإلكتروني و التسرب الإلكتروني و المراقبة الإلكترونية، حتى ولو كانت منتشرة على الفضاء الرقمي. وعليه، فإن معالجة البيانات المفتوحة يجب أن تتم دون خرق لسرية الاتصالات، أو التحايل للوصول إلى بيانات غير موجهة للعامة، وإلا وقع الدليل في دائرة البطلان.

إضافة إلى ذلك، يشترط القاضي توافر سلامة سلسلة الحيازة الرقمية أو تسلسل العهدة (Chain of custody) رغم عدم النص عليها بصريح النص لكن معمول بها كمعيارية في توثيق الأدلة بالمخبر العلمي شاطوناف و المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني⁶⁴، بما يتيح التحقق من عدم التلاعب بالمعلومات منذ لحظة جمعها إلى غاية تقديمها للعدالة. كما يشترط أن تكون المعلومة متاحة للجمهور بصفة مشروعة، وأن يتم جمعها ضمن إطار قانوني واضح، سواء من طرف ضباط الشرطة القضائية، أو بموجب إذن قضائي، أو ضمن مهام النيابة العامة. ويُشترط أيضاً أن تُوثق عمليات البحث، وأن تُدوّن المنهجية التقنية المتبعة خطوة بخطوة، لأن غياب التوثيق يُفقد الدليل مصداقيته العلمية والقضائية و هو النهج الذي تبنته اتفاقية بودابست والإتفاقية الأومية⁶⁵ في صحة الأدلة الإلكترونية.

وتواجه إجراءات جمع الأدلة الرقمية لاسيما في المصادر المفتوحة، رغم هذا التنظيم، تحديات عميقة مرتبطة بمدى انسجامها مع المبادئ الدستورية والحقوق الأساسية؛ فالتوسع في أساليب جمع هذا النوع من الأدلة يرافقه بالضرورة مخاطر تمسّ بضمانات الأفراد، مما يفرض إعادة

توازن بين فعالية التحقيقات وحماية الحقوق. ويبدو هذا التوجه جلياً في الاجتهاد القضائي الصادر عن محكمة العدل الأوروبية بشأن الاحتفاظ بالبيانات والولوج إليها، حيث شيدت المحكمة - في ظل غياب إطار تشريعي أوروبي واضح - نظاماً قضائياً متدرجاً يهدف إلى تعزيز حماية الحياة الخاصة. وقد نقلت محكمة النقض الفرنسية هذا الاجتهاد في عدة أحكام أكدت عدم توافق بعض قواعد الإجراءات الفرنسية مع القانون الأوروبي، ومع ذلك لم يشهد التشريع الفرنسي أي إصلاح منذ سنة 2022، مما جعل صحة التحقيقات تستند إلى النظام الصارم للجزاءات الإجرائية⁶⁶. ويظهر هذا الوضع الحاجة الملحة إلى إعادة بناء نظام جمع الأدلة الرقمية على أساس إطار تشريعي صريح، لا على اجتهادات قضائية متفرقة، من خلال التركيز على تعزيز الضمانات المحيطة بتقنيات جمع الدليل الرقمي، وتصنيف جديد للأدلة الإلكترونية⁶⁷، بما في ذلك تحديد الضوابط الزمنية للتدخل والرقابة القضائية.

أما على صعيد التعامل العملي، فإن التطور المستمر للتكنولوجيا يزيد من تعقيد مهمة التحقيق؛ إذ يواجه المحققون كميات هائلة من البيانات المخزنة محلياً أو عبر الخوادم السحابية ضمن آجال زمنية مضيقّة، مما يجعل الذكاء الاصطناعي أداة واعدة لتحليل البيانات رغم ما يثيره من تساؤلات حول موقعه في نظام الإثبات. وبالموازاة، تنتج وسائل التواصل الاجتماعي وغيرها كميات ضخمة من المعلومات المتاحة للعامة، ما يجعلها مصدراً مهماً للتحري عند اللجوء إلى تقنيات OSINT، غير أن استخدام هذه التقنيات بطريقة واسعة أو آلية يظل محفوفاً بإشكاليات قانونية معقدة.

الفرع الثاني: القيمة الإثباتية لأدلة OSINT أمام القاضي الجزائري

تتوقف القوة الثبوتية لأدلة OSINT على مدى صدقيتها، وارتباطها بالواقعة الإجرامية، وقدرتها على الإقناع. فالقاضي الجزائري لا يمنح هذه الأدلة قيمة مطلقة، بل يقدرها وفق مبدأ الاقتناع الشخصي المبني على أدلة مشروعة ومتناسقة. وتزداد قوة OSINT عندما تكون المعلومات واضحة المصدر، مثبتة زمنياً، قابلة للتحقق تقنياً، وخالية من أي مؤشرات على التلاعب أو التحريف الرقمي⁶⁸.

وفي القضايا المرتبطة بالإرهاب، الجرائم السيبرانية، والتحريض عبر الإنترنت، يُمكن لأدلة OSINT أن تشكل عنصراً حاسماً، لأنها غالباً ما ترصد السلوك الإجرامي في الفضاء الرقمي بشكل علني. ومع ذلك، فإن القاضي يشترط دوماً أن تُقدّم هذه الأدلة ضمن تقرير تقني محكم، وأن تُدعم بقرائن أخرى عند الاقتضاء، لأن الاعتماد الحصري على البيانات المفتوحة قد يطرح إشكالات تتعلق بالتحقق من الهوية الرقمية أو المساءلة القانونية.

وفي القانون الجزائري، يركز نظام الإثبات الجزائي على مبادئ أساسية عديدة من أهمها المشروعية المبني على مبدأ حسن النية و مبدأ التناسب الذي يساير مبدأ الحفاظ على الحريات الفردية و الجماعية. و يثار التساؤل حول حجية و قوة الدليل ذي الطبيعة الالكترونية في المواد الجزائية⁶⁹. فلكي يكون للدليل الإلكتروني حجية فيجب أن تكون المعطيات الرقمية متاحة بمعنى قابلة للاستغلال و تكون مفهومة و واضحة Inteligible و منه يجب أن يخضع الدليل الإلكتروني لأربعة معايير تقنية : معيار الرسمية Authenticité، السلامة Integrité، متقفاة (تاركة للأثر) traçabilité و أخيرا معيار الديمومة⁷⁰.

وبناءً على ذلك، تُعدّ OSINT أدلة مكتملة وذات أهمية متزايدة، بشرط أن تستوفي الشروط السالفة كي تصبح قابلة للاستعمال القضائي، وتندرج ضمن الأدلة الرقمية التي يعترف بها القاضي الجزائري في إطار سلطته التقديرية.

و تعكس المادة 349 من قانون الإجراءات الجزائية الجديد مبدأ حرية الإثبات الذي يفتح الباب أمام القاضي لقبول مختلف أنواع الأدلة، بما فيها الأدلة المستمدة من المصادر المفتوحة على الإنترنت. فالأدلة الإلكترونية الناتجة عن OSINT مثل الأرشيفات الرقمية، منشورات وسائل التواصل الاجتماعي، بيانات المواقع، الصور، التسجيلات، تُعد طرقاً مشروعة للإثبات ما دامت جُمعت بطريقة قانونية ولا يخالف استخدامها نصاً خاصاً. ويمثل هذا اتساقاً مع الاتجاه العالمي الذي يعترف بالقيمة الثبوتية لمخرجات OSINT في الجرائم السيبرانية، الاقتصادية، الإرهابية، أو جرائم القذف و التشهير، خاصة عندما تكون هذه البيانات قابلة للتحقق، مؤرخة، ويمكن تأكيد صدقيتها عبر

التحليل المتقاطع ، غير أن المادة تشترط لضمان حجية الأدلة الإلكترونية منها OSINT أن تُعرض ضمن إجراءات الخصومة وأن تُناقش حضورياً أمام القاضي، وهو ما يفرض على جهة الادعاء تقديم هذه الأدلة في شكل تقارير تقنية واضحة تبين مصدرها، طريقة جمعها، وأدوات حفظها مثل لقطات الشاشة المثبتة بمحضر، أرشيفات، سجلات التتبع المفتوحة. فالقاضي الجزائي رغم تمتعه بحرية الاقتناع، لا يمكنه بناء حكمه إلا على الأدلة التي خضعت للمناقشة الوجيهة، مما يعني أن أي معلومة OSINT لا تُعرض وتُناقش لا يمكن أن تكون أساساً للحكم. وبذلك توازن المادة بين مرونة قبول الأدلة الرقمية المفتوحة وضمانات المحاكمة العادلة عبر احترام مبدأ الوجيهة والتحقق القضائي⁷¹.

خاتمة:

تُعد استخبارات المصادر المفتوحة مورداً بالغ الأهمية في دعم التحقيقات القضائية الحديثة، إذ أصبحت أداة لا غنى عنها في كشف الجرائم السيبرانية وفهم أنماط النشاط الإجرامي عبر الفضاء الرقمي. فمع تزايد اعتماد المجرمين على تقنيات متطورة لاستغلال الثغرات الرقمية، تبرز OSINT كوسيلة فعالة تمكّن جهات التحقيق من تتبع المؤشرات الرقمية، وتحليل المعلومات المتاحة علناً، والوصول إلى معطيات يمكن أن تعزز الأدلة التقليدية وتثري مسار التحري القضائي.

وتكمن قوة OSINT في قدرتها على توفير معطيات آنية حول التهديدات والأنشطة الإجرامية، من خلال رصد المصادر العامة مثل الوسائط الإعلامية ومنصات التواصل الاجتماعي، مما يساعد سلطات التحقيق على كشف حملات البرمجيات الخبيثة أو محاولات الاختيال الإلكتروني في مراحلها الأولى. كما تساهم في تقييم حجم التهديد وتحديد نقاط الضعف الرقمية، الأمر الذي يسمح بتوجيه مجريات التحري وتحديد أولويات العمل القضائي بشكل أكثر دقة وفعالية.

وإلى جانب ذلك، تدعم OSINT التعاون بين جهات التحقيق والأجهزة الأمنية والهيئات المختصة، بما يعزز تبادل المعلومات ويرفع من فعالية الجهود المشتركة لمكافحة الجريمة السيبرانية. ومن خلال دمج أدوات OSINT ضمن المنظومات القضائية، يصبح بالإمكان تعزيز قدرات الرصد، وتحليل المخاطر، والاستجابة الاستباقية للوقائع الإجرامية، وهو ما يجعلها ركيزة مهمة في تطوير مناهج التحقيق في عصر يغلب عليه الطابع الرقمي.

بذلك أصبحت الاستخبارات مفتوحة المصدر نقطة التقاء بين المعلومة الرقمية والدليل المادي، إذ يتيح إدماجها ضمن أساليب التحري الميداني بناء ملفات إثبات أكثر صلابة وشفافية، شريطة أن تُستخدم في إطار احترام الشرعية الإجرائية وضمانات حماية الحياة الخاصة. وبهذا، تبرز OSINT كأداة استراتيجية في خدمة العدالة، تدعم التحقيقات التقليدية وتمنحها بعداً جديداً يستجيب لتعقيدات البيئة الرقمية.

كما تكشف الدراسة عن الوجه المزدوج لاستخبارات المصادر المفتوحة، فهي من جهة وسيلة قوية لكشف الحقيقة وتعزيز الشفافية في التحقيقات القضائية، لكنها من جهة أخرى قد تُستغل كأداة للتأثير أو التوجيه خارج نطاق الإجراءات السليمة لأن فعاليتها في إنتاج الحقيقة الرقمية لا تعني بالضرورة فعاليتها في ضمان العدالة القضائية.

وفيما يأتي النتائج المتوصل إليها:

1. تحوّل OSINT من تقنية استخباراتية إلى ممارسة مجتمعية ومؤسسية واسعة يعكس تطوراً عميقاً في طرق إنتاج المعرفة وتوثيق الوقائع، خاصة في مجال الجرائم.
2. اعتماد الجهات القضائية على OSINT أصبح واقعاً، حيث بات المحققون والقضاة والمحامون يوظفون المعلومات الرقمية المتاحة للعامة لتوثيق الجرائم الكلاسيكية و السيبرانية و حتى الدولية وجمع الأدلة القابلة للاستخدام القضائي.

3. التحوّل الرقمي الضخم وزيادة تدفق المعلومات جعلاً من OSINT أداة أساسية لفهم وتحليل الأوضاع السياسية والاجتماعية والاقتصادية المعقدة.
4. انفتاح استخدام OSINT على فاعلين متعدّدين مثل الصحفيين، المنظمات غير الحكومية، الباحثين، والشركات، مما عزّز دوره في كشف الحقائق ومتابعة النزاعات وانتهاكات حقوق الإنسان.
5. القضاء لم يعد بمنأى عن الثورة الرقمية، إذ أصبح جزءاً من منظومة تعتمد على الأدلة الرقمية ومصادر المعلومات المفتوحة لتحسين فعالية التحقيقات وتعزيز دقة الإثبات.
6. إن النظام القانوني الجزائي يجب أن يتطور نحو بناء منظومة متكاملة ومنهجية للأدلة الرقمية في الإجراءات الجنائية، عبر تعاون مشترك بين القضاة، والمحققين، والخبراء في الأدلة الرقمية، وخبراء الأمن السيبراني، حتى تكون العدالة الجنائية عادلة وفعّالة في آن واحد.

أما الإقتراحات الموصى به فهي:

1. وضع إطار قانوني صريح لتنظيم أدوات جمع الأدلة الالكترونية منها OSINT بما يواكب التطور التكنولوجي المستمر، بدل الاعتماد على تطبيقات قضائية متفرقة.
2. إدماج أنظمة الذكاء الاصطناعي في التحقيقات الرقمية وفق ضوابط قانونية تُحدد شروط استخدامها، طبيعة رقابتها، وضمانات عدم المساس بالحقوق الأساسية.
3. تقنين استعمال OSINT في التحقيقات القضائية عبر تحديد شروط جمع البيانات المفتوحة، وضوابط التمييز بين ما هو متاح للعامة وما هو محمي بالخصوصية.
4. إعداد دليل وطني منهجي لجمع الأدلة الرقمية يحدد الخطوات الفنية، ويحافظ على سلسلة الحيازة الرقمية. Chain of custody.
5. تطوير آليات مراقبة قضائية مسبقة عند جمع البيانات الرقمية واسعة النطاق أو الآلية، لتفادي أي خرق للحقوق الأساسية.
6. إعادة هيكلة النصوص الإجرائية المتعلقة بالأدلة الإلكترونية في شكل قانون موحد أو فصل مستقل داخل قانون الإجراءات الجزائية، يوفّر رؤية متكاملة وشاملة.
7. إرساء آلية مراجعة دورية للتشريع الرقمي و الأدلة الالكترونية لضمان ملاءمته مع التغيرات المستمرة في التكنولوجيا، خاصة ما يتعلق بالذكاء الاصطناعي.

قائمة المراجع:

- ¹ Schaurer, Florian, et Jan Störger. 2011. « The evolution of OSINT ». Journal of US Intelligence Studies, 2011.
- ² Scraping هو عملية آلية لجمع البيانات من صفحات الويب عبر استخراج محتواها النصي أو الصوري أو البنيوي باستخدام برمجيات متخصصة، بهدف إعادة تحليلها أو معالجتها في سياقات بحثية أو استخباراتية. ويُعد المرجع العلمي الأساسي لهذا المفهوم كتاب:
- Web Scraping with Python by Ryan Mitchell , O'Reilly books, USA, 2018.
- ³ نظرية الرسوم البيانية Graph Theory هي فرع من الرياضيات وعلوم الحاسوب يدرس البنى الشبكية المكوّنة من عُقد (Nodes) وروابط (Edges)، ويُستفاد منها في تتبع العلاقات بين الأشخاص والكيانات وتحديد شبكات التواصل في التحقيقات الرقمية، خصوصاً عند تحليل البيانات المفتوحة، OSINT. أنظر:
- Douglas B. West, Introduction to Graph Theory, 2nd Edition, Prentice Hall, 2001.
- ⁴ التعلّم الآلي (Machine Learning) هو أحد فروع الذكاء الاصطناعي يقوم على تطوير خوارزميات تمكن الحاسوب من التعلم تلقائياً من البيانات واكتشاف الأنماط واتخاذ القرارات دون برمجة صريحة، ويُستخدم في التحقيقات الرقمية لتحليل البيانات الضخمة، والتعرّف على السلوكيات المشبوهة، وتصنيف المحتوى الجنائي. أنظر: Tom M. Mitchell, Machine Learning, McGraw-Hill, 1997.

⁵ تُبرز الحرب في أوكرانيا، وقبلها الحرب في سوريا، الدور الكبير الذي أصبحت تلعبه شبكات التواصل الاجتماعي في توثيق النزاعات المسلحة من خلال ما ينشره الأفراد من صور وفيديوهات وشهادات مباشرة من ميادين القتال. فقد أصبحت هذه الوسائل الرقمية بديلاً عملياً عن الحضور الميداني للصحفيين، نظراً لصعوبة الوصول إلى مناطق الصراع، مما جعل المواطن العادي يتحول إلى فاعل في إنتاج المعلومة ونقلها.

Perrot, Sophie., et al. « L'Open Source Intelligence dans la guerre d'Ukraine ». *Politique étrangère*, 2022/3 Automne, 2022. p.63-74. CAIRN.INFO, shs.cairn.info/revue-politique-etrangere-2022-3-page-63?lang=fr.

Cardoso Teixeira, Gisela. (2025). L'intégration de l'OSINT dans le fact-checking en contexte de guerre. 10.13140/RG.2.2.15265.31841.

⁶ Ghernaouti, Solange. « 9. Criminalistique informatique et investigation numérique ». *Cybercriminalité : Comprendre. Prévenir. Réagir*, Dunod, 2023. p.198-222. CAIRN.INFO, shs.cairn.info/cybercriminalite-comprendre-prevenir-reagir--9782100858699-page-198?lang=fr.

⁷ Letoqueux, Hervé. et al. « La contribution de l'Osint aux enquêtes portant sur des crimes internationaux ». *Hérodote*, 2022/3 N° 186, 2022. p.57-68. CAIRN.INFO, shs.cairn.info/revue-herodote-2022-3-page-57?lang=fr.

⁸ من قبل شركات مثل *Eurasia Group* و *Oxford Analytica* و *Maplecroft*.

⁹ بيلينغكات هي مجموعة دولية مستقلة من الباحثين والمحققين والصحفيين المواطنين، تستخدم التحقيقات مفتوحة المصدر ووسائل التواصل الاجتماعي لسبر أغوار مواضيع متنوعة، بدءاً من تجار المخدرات المكسيكيين والجرائم ضد الإنسانية، وصولاً إلى رصد استخدام الأسلحة الكيميائية والصراعات حول العالم. بفريق عمل ومساهمين منتشرين في 20 دولة حول العالم، تعمل في مجال فريد يجمع بين أحدث التقنيات، وأبحاث الطب الشرعي، والصحافة، والتحقيقات، والشفافية، والمساءلة. أنظر الموقع الرسمي : <https://www.bellingcat.com>

¹⁰ هناك عدة شركات مثل شركة *Stratfor* تعمل في مجال الاستخبارات الخاصة والتحليلات الاستراتيجية، و *Jane's Information Group* المتخصصة في الاستخبارات العسكرية و *Control Risks* و *The Risk Advisory Group* في تحليل المخاطر الأمنية والسياسية. كما تقدم شركات مثل *Palantir Technologies* و *Booz Allen Hamilton* تحليلات البيانات الضخمة والخدمات الاستشارية الاستخباراتية للحكومات والمؤسسات الخاصة. جميع هذه الشركات تجمع المعلومات من مصادر مفتوحة وخاصة لتحويلها إلى تحليلات استراتيجية تدعم اتخاذ القرار.

¹¹ Le Deuff, Olivier. « L'Open Source Intelligence (OSINT) : origine, définitions et portée, entre convergence professionnelle et accessibilité à l'information ». *I2D - Information, données & documents*, 2021/1 n° 1, 2021. p.14-20. CAIRN.INFO, shs.cairn.info/revue-i2d-information-donnees-et-documents-2021-1-page-14?lang=fr.

¹² . A. Dorange Directrice juridique & associée, OSINT et recherche de preuves numériques : c'est (aussi) utile pour les avocats *Ogma Intelligence Article réalisé pour la Rédaction du Village de la Justice* .[25/10/2025]

¹³ . A. Dorange. *Idem*.

¹⁴ مفاهيم قريبة من OSINT :

- HUMINT، أي الاستخبارات البشرية، وتعتمد على جمع المعلومات عبر العلاقات أو المصادر البشرية.
- SIGINT، وتعني باعتراض الاتصالات والإشارات الإلكترونية.
- GEOINT، وتعتمد على المعلومات الجغرافية وصور الأقمار الصناعية.
- MASINT، وهي الاستخبارات العلمية والتقنية المستخلصة من أجهزة القياس والكشف المتقدمة.
- CYBERINT، التي تركز على الجوانب الأمنية وحماية المعلومات أثناء عمليات البحث والتحليل.

<https://drane-versailles.region-academique-idf.fr/spip.php?rubrique201>.

¹⁵ في عام 1992، وضع نص قانون إعادة تنظيم الاستخبارات (Intelligence Reorganization Act) أهدافاً واضحة. وتشترط القانون، بشكل خاص، استخدام "معلومات موضوعية وخالية من التحيز"، بما يخدم المصلحة المباشرة للأمة.

¹⁶ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th Edition, Los Angeles, California : CQ Press, 2017

¹⁷ Emeline joug, « L'OSINT », DU EMI - Inspé de Lyon, l'Université Lyon, Publié le 4 juillet 2025. <https://inspe.univ-lyon1.fr/duemi/2025/07/04/losint/> [02/11/2025].

¹⁸ YouTube، ماذا تعرف عن استخبارات المصادر المفتوحة؟، <https://www.youtube.com/watch?v=Bpx6MLYbyB4>.

¹⁹ <https://www.theguardian.com/uk/2009/nov/11/canoe-man-john-darwin-panama>.

²⁰ المادة 05 من المرسوم الرئاسي رقم 05-20 المؤرخ في 24 جمادى الأولى 1441 هـ الموافق 20 جانفي 2020 تنص على وضع منظومة وطنية لأمن الأنظمة المعلوماتية . الجريدة الرسمية عدد 04 المؤرخة في 26 جانفي 2020.

²¹ Sampson, F. (2016). Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings: Using open source intelligence (OSINT) in criminal proceedings. *The Police Journal: Theory, Practice and Principles*, 90(1), 55-69. <https://doi.org/10.1177/0032258X16671031>.

²² Global Investigative Journalism Network (GIJN) — "Citizen Investigations Guide" <https://gijn.org/resource/citizen-investigation-guide/>

²³ Le Deuff, Olivier. *Ibid*.

²⁴ Claudia Weber, Avocat et Jean-Baptiste Olivo, Juriste Stagiaire, Quel est le cadre légal de l'OSINT 1re Parution: 19 mars 2024 4.11 /5 .Village de la justice . <https://www.village-justice.com/articles/quel-est-cadre-legal-osint,49186.html>

²⁵ ندوة صحفية لوكيل الجمهورية لدى محكمة القليعة بخصوص قضية المدعو " هشام الوهراني " بتاريخ 2025/10/21.

²⁶ Claudia Weber, *Ibid.*

²⁷ *Idem*

²⁸ *Idem*

²⁹ Rogers, M, *Open Source Intelligence and Cybercrime Investigations*. Springer.2019

³⁰ أثبتت التجارب الدولية أن رصد الشبكة المظلمة أصبح ضرورة عملية في مكافحة الجرائم المنظمة والجرائم السيبرانية. ففي القضايا الكبرى مثل Silk Road و AlphaBay و Hansa Market، أظهرت التحريات أن تتبع المعاملات الرقمية عبر هذه الأسواق غير القانونية أدى إلى تفكيك شبكات عالمية لتجارة المخدرات والأسلحة وغسل الأموال. وقد ساهم استخدام تقنيات الرصد في تحديد هويات المتورطين، رغم اعتمادهم على أسماء مستعارة وتقنيات تشفير معقدة، وذلك بفضل دمج المعطيات المستخلصة من الشبكة المظلمة مع البيانات المتاحة في الإنترنت السطحي ومصادر OSINT الأخرى.

³¹ Horan, Cecelia & Saiedian, Hossein. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*. 1. 580-596. 10.3390/jcp1040029.

³² من أبرز هذه الأدوات خلال الأشهر الأخيرة:

- Google Dorks، Maltego، Spiderfoot، إضافة إلى محركات البحث التقليدية مثل Google.
 - Google Dorks: تستخدم استعلامات بحث متقدمة لجمع البيانات ذات الصلة بكفاءة عالية.
 - Maltego: أداة متخصصة في التحقيقات الجنائية الرقمية، تمتاز بقدرتها على تحليل العلاقات المعقدة بين مصادر البيانات المفتوحة.
 - Spiderfoot: أداة أخرى مميزة تُستخدم في عمليات البحث عن أسماء النطاقات DNS lookups، واستخراج عناوين البريد الإلكتروني، وتحليل ملفات التعريف على وسائل التواصل الاجتماعي، وجمع البيانات من محركات البحث.
- تسهل هذه الأدوات مجتمعة في تعزيز فعالية التحقيقات مفتوحة المصدر وتوسيع نطاقها في مجالات متعددة.

³³ BENNANI Hniya & EL MAYSOUR Mohammed Amine, *L'Open Source Intelligence à l'ère numérique : un spectre éthico-politique entre pouvoir, preuves et limites judiciaires*, *Revue Droit et Société*, Vol. 6, n°17, Avril-Juin 2025.

³⁴ *Idem.*

³⁵ المادة 15 من إتفاقية بودابست.

³⁶ الإعلان العالمي لحقوق الإنسان، 1948.

³⁷ العهد الدولي الخاص بالحقوق المدنية والسياسية، 1966.

³⁸ الميثاق الإفريقي لحقوق الإنسان والشعوب، 1981.

³⁹ د- مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، الطريق إلى تحول أدلة الإثبات في المادة الجزائية، دراسة مقارنة، دار الخلدونية، 2018، ص 349-351.

⁴⁰ المادة 26 من القانون رقم 20-05 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهم، مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، ج.ر. عدد 25 صادر في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020.

⁴¹ المواد 120-124 من قانون الإجراءات الجزائية الجديد حول التسرب.

⁴² فعلى سبيل المثال، أدت مقاطع الفيديو التي وثقت الإعدامات خارج القانون التي نفذها العسكري الليبي محمود الورفلي إلى إصدار المحكمة الجنائية الدولية أول مذكرة توقيف بحقه. ومؤخرًا، مكّنت الصور والفيديوهات التي نشرها مثيرو الشغب في مبنى الكابيتول بالولايات المتحدة من تحديد هوياتهم وتوقيفهم من قبل مكتب التحقيقات الفدرالي FBI. وحتى الجرائم الإرهابية التي وثقها جنود الاحتلال الإسرائيلي الصيبيانيين واستعرضوها على الأنترنت ومواقع التواصل الاجتماعي ساهمت في إدانة الكيان بالمحكمة الجنائية الدولية من خلال المصادر المفتوحة. -فيديوهات منشورة على اليوتوب-.

⁴³ تشمل أدوات ووسائل التحقيق الجزائي في مجال OSINT استخدام محركات البحث المتقدمة وتقنيات Google Dorking، وأرشيفات الإنترنت مثل Wayback Machine، وأدوات تحديد المواقع والتحليل الجغرافي، إضافة إلى أدوات تتبع وتحليل الحسابات على شبكات التواصل الاجتماعي، ووسائل البحث العكسي عن الصور والفيديوهات مثل TinEye و InVid، وأدوات تحليل البنية التقنية للمواقع والأنظمة كخدمات WHOIS و DNS وتتبع عناوين الـ IP، ومنصات فحص الخوادم مثل Shodan و Censys، وأدوات تحليل البيانات الضخمة وربطها مثل Maltego و Hunchly، إلى جانب أدوات التحقق من صحة الصور والفيديوهات والبيانات الوصفية.

⁴⁴ المادة 20 فقرة أخيرة من ق.إ.ج الجديد ((يمكن ضبط و أعوان الشرطة القضائية أن يستعملوا المعايير و إثبات الجرائم أجهزة تقنية أو إلكترونية وفقاً للكميات المحددة عن طريق التنظيم)). قانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، ج.ر. عدد 54 ص 7. الصادرة بتاريخ 13 غشت 2025م.

<https://syntheticdrugs.unodc.org/syntheticdrugs/ar/cybercrime/detectandrespond/investigation/OSINT.html>.

⁴⁶ العمليات البولنباتية Boolean Operators هي تقنيات بحث منطقية تُستخدم لتحسين دقة النتائج عند البحث في قواعد البيانات أو محرركات البحث، وتعتمد على منطق جورج بول في الربط بين الكلمات المفتاحية. وتُعد من أهم الأدوات العلمية المعتمدة في منهجيات OSINT لأنها تسمح بتصفية المعلومات، توسيع نطاق البحث، أو تضيقه بطريقة ممنهجة. وتعتمد أساساً على ثلاثة معاملات رئيسية: AND, OR, NOT.

⁴⁷ مثل برنامج IBM i2 Analyst's Notebook (ANB) هو أحد أقوى الأدوات المستخدمة عالمياً في تحليل الروابط، خاصة في مجالات الاستخبارات، مكافحة الجريمة المنظمة، مكافحة الإرهاب، الجرائم المالية، والجرائم السيبرانية. يقوم على تحويل البيانات الخام إلى خرائط مرئية للعلاقات والارتباطات بين الأشخاص، الكيانات، الأحداث، الاتصالات، الحسابات البنكية، المواقع... إلخ.

⁴⁸ تحريات الاستخبارات المفتوحة المصدر - Synthetic Drug Strategy

⁴⁹ Claudia Weber, Avocat et Jean-Baptiste Olivo, Juriste Stagiaire, Quel est le cadre légal de l'OSINT 1re Parution: 19 mars 2024 4.11 /5 .

⁵⁰ المواد 394 مكر - 394 مكرر8 من قانون العقوبات الجزائري.

⁵¹ د- مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، 2018، ص 139-151.

⁵² OPSEC هو منهج أمني يهدف إلى حماية المعلومات الحساسة عبر تحديد ما يمكن أن يكشف عن هوية المحقق أو منهجيته، ثم تقليل المخاطر الناتجة عن كشفها.

وتُستخدم في OSINT لضمان بقاء الباحث غير مكشوف أثناء جمع المعلومات ومنع استغلال نشاطه الرقمي من قبل المجرمين أو الأطراف المستهدفة.

<https://niccs.cisa.gov/training/catalog/tonex/fundamentals-operations-security-opsec>.

⁵³ Claudia Weber, Ibid.

⁵⁴ يشير مصطلح Leaks إلى تسريب معلومات أو وثائق حساسة من مصدر داخلي أو خارجي إلى العلن، غالباً دون إذن، ويستعمل في سياق الأمن الرقمي للكشف عن بيانات مخزنة في قواعد بيانات أو خوادم غير مؤمنة. ويُعد تحليل هذه التسريبات جزءاً من منهجيات OSINT لاكتشاف الثغرات أو التحقق من صحة المعلومات المسربة.

Michael Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 10th Edition.

⁵⁵ Claudia Weber, Avocat et Jean-Baptiste Olivo, Juriste Stagiaire, Quel est le cadre légal de l'OSINT 1re Parution: 19 mars 2024 4.11 /5 .

⁵⁶ أنظر المواد: 151-152-153-154-155-156-157-158 من الأمر 05/03 المؤرخ في 19 جمادي الأولى عام 19/24 الموافق لـ 19 يوليو سنة 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة .

⁵⁷ قانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية عدد 34 مؤرخة في 10 يونيو 2018، الصفحة 11.

⁵⁸ يشير Doxxing إلى عملية جمع ونشر معلومات شخصية أو حساسة عن فرد معين دون موافقته، اعتماداً على مصادر مفتوحة مثل السجلات العامة ووسائل التواصل الاجتماعي، بهدف الإيذاء أو الابتزاز أو التشهير. ويُعد هذا السلوك تهديداً خطيراً للخصوصية ويُعامل كاعتداء رقمي في الدراسات الأمنية.

لمزيد من الشرح حول جرائم المعطيات الشخصية، أنظر كتابنا، المعطيات الشخصية و الجريمة، الفصل الثاني، دار الخلدونية، 2025. أيضاً أنظر:

Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 2015.

⁵⁹ يشير l'e-stalking إلى الملاحقة الإلكترونية المتكررة لشخص عبر الإنترنت باستخدام الرسائل، التتبع، أو مراقبة نشاطه الرقمي بطريقة تسبب له الخوف أو الاضطراب. ويُعد شكلاً من أشكال التحرش السيبراني ذي خطورة عالية بسبب طبيعته المستمرة والخفية.

Delbreil, Alexia., et al. « Chapitre 42. Le stalking : comment mieux protéger les victimes ? ». *Violences aux personnes Comprendre pour prévenir*, Dunod, 2014. p.502-516. CAIRN.INFO.

⁶⁰ يُعد الحكم الصادر عن محكمة باريس بتاريخ 6 يوليو 2023 (رقم 10326/21) من أبرز الاجتهادات القضائية الحديثة التي استعانت بالأرشيف الرقمي كوسيلة إثبات، حيث استندت المحكمة إلى بيانات مستخرجة من أداة Wayback Machine لتحليل نشاط الموقع الإلكتروني محل النزاع وتحديد ما إذا كانت محتوياته متاحة في تاريخ معين. ورغم أن المحكمة خلصت إلى أن الأرشيف لا يثبت واقعة "submission" المدعى بها، فإن اعتمادها عليه يُعتبر اعترافاً صريحاً بالقيمة الثبوتية للأرشيفات الرقمية المفتوحة المصدر، بوصفها جزءاً من وسائل OSINT التي يمكن للقاضي الاستناد إليها عند تقييم الوقائع التقنية. أنظر أيضاً:

Tribunal judiciaire de Paris, 6 juillet 2023, 21/10326

Tribunal judiciaire de Paris, 4 août 2022, 22/54655

Tribunal de grande instance de Paris, 28 septembre 2021, 17/14337

⁶¹ تُعد Wayback Machine أداة أرشفة رقمية تابعة لـ Internet Archive تسمح باسترجاع النسخ السابقة للمواقع الإلكترونية كما كانت في تواريخ مختلفة، مما يجعلها وسيلة مهمة للتحقيقات الرقمية والـ OSINT عبر تتبع تغير المحتوى واكتشاف الحذف أو التلاعب. وتوفر قاعدة ضخمة من اللقطات snapshots التي تُستخدم كمرجع تاريخي موثوق للمحتوى المنشور على الويب <https://bellingscat.gitbook.io/toolkit/more/all-tools/internet-archive>.

استخدم: <https://web.archive.org/>

أنظر قرار محكمة النقض الفرنسية، الغرفة الاجتماعية (2022) المقاطع التي تظهر استعمال وسائل OSINT في هذه الوثائق القضائية هي كل ما يتعلق بجمع معلومات مفتوحة المصدر من الإنترنت، كالأرشيفات الرقمية وصفحات الويب والصور والكتالوجات المنشورة للعامّة. وبالاعتماد على الوجه الثاني للنقض، فالعناصر التي تُعدّ OSINT في صلب القرار هي «saisies de page Internet»: أي حجز أو استخراج صفحات من موقع إلكتروني للشركة—وهو استخدام مباشر لمصادر رقمية مفتوحة «présence... sur son site Internet». تحليل محتوى الموقع الإلكتروني للشركة كدليل على ممارسات تجارية مضللة «mentions figurant sur son site Internet». الاعتماد على العبارات المنشورة على الموقع («savoir-faire Made in France», etc.) كأدلة مفتوحة المصدر والفهارس المنشورة للعامّة. «catalogues» publiés تُعتبر أيضاً OSINT لأنها مواد متاحة للجمهور. هذه الفقرات الأربع تمثل بوضوح عناصر استخبارات مفتوحة المصدر OSINT استخدمتها المحكمة، لأن القاضي استند إلى معطيات منشورة ومتاحة للعامّة (مواقع، صفحات، فهارس) دون الحاجة لوسائل تحقيق سرية.

Cour de cassation, chambre sociale, 30 mars 2022, n°20-12.263

⁶² Revue Hérodote, "La contribution de l'OSINT aux enquêtes portant sur des crimes internationaux" cairn.info.

⁶³ نظرًا لغياب معايير دولية موحدة تنظم إدارة الأدلة الرقمية، ظهرت عدة مبادرات رائدة مثل مبادرة Bellingcat بالتعاون مع شبكة العمل القانوني العالمي (GLAN) التي أنشأت وحدة *Justice and Accountability* لإثبات فعالية المعلومات المستخلصة من المصادر المفتوحة في الإجراءات القضائية. ومبادرة الرابطة الدولية للمحامين (IBA) عبر تطبيق ⁶³ eyeWitness to Atrocities المخصص لمساعدة المحققين على جمع الأدلة الرقمية وحمايتها في سياق المتابعات الجنائية، كما قدمت الباحثة الكندية Ritu Gill تطبيقًا مبتكرًا باسم Forensic OSINT، يتيح للمختصين توثيق وتحليل المحتوى الإلكتروني وضمان تكامل البيانات من خلال خاصية التجزئة، التي تمنح المعلومة الرقمية قوة قانونية أكبر عند تقديمها كدليل أمام القضاء.

⁶⁴ المعهد الوطني للأدلة الجنائية وعلم الإجرام/ دو معتمد في مجال الأدلة الجنائية من خلال اعتماد 72 طريقة تحليلية وفق المعيارين الدوليين إيزو 17020 و إيزو 17025 من قبل هيئة الاعتماد الجزائرية .

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

⁶⁵ المادة 35 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية اعتمدها الجمعية العامة في 2024/12/24 وبتاريخ 25 أكتوبر 2025 بالعاصمة هانوي، فيتنام تم فتح باب التوقيع على أول اتفاقية عالمية لمنع الجريمة السيبرانية والتصدي لها لمواجهة التهديد المتصاعد لتلك الجرائم، إذ تسهل إساءة استخدام تكنولوجيا المعلومات والاتصالات ارتكاب جرائم مثل الإرهاب، والاتجار بالبشر، والجرائم المالية، وتخريب المخدرات على نطاق غير مسبوق. ووقعت الاتفاقية 65 دولة.

⁶⁶ CASTETS-RENARD, Céline. Quelles nouveautés en matière de preuve numérique ? Justice et Cassation, 2017, p. 23

⁶⁷ د- مناصرة يوسف، الدليل الإلكتروني، المرجع السابق، ص 41 و مابعدا.

⁶⁸ Matthieu Audibert. La preuve numérique au coeur des enquêtes judiciaires, quels enjeux et quelles perspectives en procédure pénale ?. Les notes du Centre de Recherche de la Gendarmerie Nationale, 2025, avril 2025 (114).

⁶⁹ Eoghan Casey, Handbook of Digital Forensics and Investigation. Academic Press. 2009. P.567. Voir <https://books.google.co.uk/books>.

⁷⁰ Raphael d'Assgnies directeur de CELOG, Alexandre Drevet, Les cahiers technique de celog, opcit, p. 10.

⁷¹ QUÉMÉNER, Myriam. Le numérique, nouveau vecteur de l'administration de la preuve en matière pénale. Dalloz IP/IT, 2024, p. 61.